ARTICLE:

THE CREATION OF QUALIFIED SIGNATURES WITH TRUSTED PLATFORM MODULES[1]

WRITTEN BY:
FREDERIC STUMPF, MARKUS SACHER, CLAUDIA ECKERT AND **ALEXANDER ROßNAGEL**

Increasing numbers of personal computers are now shipped with an integrated smart card, called the trusted platform module (TPM). This module is designed to carry specific data related to the platform and to provide the software running on the computer with this information. Since this technology is very similar to a generic smart card, it could also be used in e-commerce to attempt to link the use of a particular computer to a particular transaction effected over the internet. The potential of the TPM is discussed in this article, and consideration is given as to whether a TPM could be used to carry information related to the purported user. The authors also examine whether the TPM can be used as a secure signature creation device that conforms to the EU Electronic Signature Directive as well as to the German Electronic Signature Law.

Introduction

A qualified electronic signature that confirms to article 5(1) of the EU Electronic Signature Directive[2] (EU Directive) and § 2(3) of the Signature Act 2001 (SigG) is an advanced signature as specified by article 2(2) of the EU Directive and § 2(2) of SigG, which is based on a qualified certificate and which is created by a secure signature creation device. These signatures may be considered to be a component for e-commerce transactions in the future, since they are capable of linking a particular computer to a particular transaction effected over the internet. Digital signatures are not widely used, and it is asserted that the failure to use digital signatures thereby deprives the market for electronic commerce of an important source of potential growth.[3] Users generally do not use smart cards for the purpose of using an advanced signature. A promising approach to overcome this shortcoming is to use an additional hardware module called the Trusted Platform Module (TPM) to create an advanced signature. The TPM is already available in more than 60 million personal computers.[4] This technology is supported by many hardware vendors and is therefore widespread.[5] One of the properties required of this chip is to perform the necessary cryptographic functions to create an advanced signature. However, the ability to perform the required mathematical operations is not enough to use this device to create an advanced signature. This is due to the requirements for a compliant device for the creation of an advanced signature, as set out in article 5(1) and Annex I – III of the EU Directive and the Signature Act 2001.

This article considers whether the TPM can be used to create qualified electronic signatures, and if so, whether such signatures could be used in e-commerce. The potential risks and defences relating to the threats in e-commerce are set out before demonstrating how the trusted platform module works. Thereafter, the article considers whether the TPM fulfills the technological requirements of article 5(1) of the EU Directive and § 2(3) SigG, together with the criteria provided for in Annex III of the EU Directive and § 17 Abs. 1 SigG, as well as § 15 Signature Decree 2001 (SigVO).

Perceived problem

In contrast to the physical world, where goods may be directly exchanged for currency, when selling goods or services at a distance, such as over the internet,

[1] *A shorter version of this article first appeared in German in Datenschutz und Datensicherheit, No. 05-2007, ed. J. Bizer, D. Fox, H. Reimer.*

[2] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12.*

[3] *European Commision Press Release, ' Electronic signatures: legally recognised but cross-border take-up too slow' , (IP/06/325, 17.03.2006).*

[4] *Reiner, Datenschutz und Datensicherheit (DuD), 2006, p. 666.*

[5] *Atmel, Infineon, National Semiconductor, STMicroeletronic.*

It is argued that by identifying both parties to a transaction based on qualified signatures, trust in transaction processes can be improved.

payment is not made at the same time the goods or services are provided, in the same way as buying and selling through a catalogue by mail order. The seller needs to be assured that they will be paid, and the buyer wants to be reassured that they will receive the goods or services in exchange for authorizing payment. In the on-line environment, an e-mail address and the use of a password is usually necessary to identify the parties to the transaction. Both items of information can be obtained very easily through the use of malicious software, such as a Trojan horse, keylogger, or by social engineering (phishing). Furthermore, these forms of attack cannot be prevented by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) cryptographic protocols, since the attacks are made at the end of the communication channel, where confidential data is available in plaintext. This is one reason why many customers perceive there is a high danger that their data may be misused. As a result of these attacks, it can be difficult to prove that an agreement was concluded,[6] which might make it difficult for a vendor to enforce a contract.[7]

In general, vendors identify their customers based on e-mail addresses. An e-mail address can be generated by using false or fictional names. This means vendors that fail to use any other form of verification are at a high risk of being subject to attempts at fraud. It is argued that by identifying both parties to a transaction based on qualified signatures, trust in transaction processes can be improved. Qualified signatures require the use of a smart card. However, smart cards are not widely used for this purpose. The trusted platform module specified by the trusted computing group provides similar functionalities to a smart card. The difference is, that this technology is already widespread and can be used now. It is therefore necessary to determine whether the TPM could be used as secure signature creation device.

Technical background

The Trusted Computing Group (TCG) is a non-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices. The core of the specifications provided by the TCG is the Trusted Platform Module (TPM),[8] which is basically a smart card soldered on the mainboard of a personal computer. Similar to a smart card, the TPM offers the following functionalities: the generation of asymmetric and symmetric keys with the hardware based physical random number generator; signature creation, hash value creation and asymmetric encryption; the provision of hardware protected storage; the provision of a trusted counter for the validation of certificates and platform integrity measurement and integrity reporting.

Before shipping a personal computer containing a TPM, the TPM is disabled. Before the TPM can be used, it must be initiated by executing the *Take_Ownership* command. This command must be carried out by a user, who also has to enter a password, named the *owner-password*. This owner-password is used to generate the storage-root-key (SRK), which protects other keys by encrypting them. The SRK is stored in the non-volatile storage of the TPM and it is only possible to obtain access to this key by entering the correct password. Obtaining access to the TPM-generated keys is therefore only possible if the SRK has not been altered and the user enters the correct password. To enter this password, it is necessary to obtain access to the functions provided by the trusted platform module. If the password has been lost, the user cannot obtain access to the keys stored in the module. However, by using the physical-presence[9] command of the TPM, a new password can be created. Since this process

[6] *Alexander Roßnagel and Andreas Pfitzmann, Neue Juristische Wochenschrift (NJW) 2003, 1209 (22.04.2003).*

[7] *Oberlandesgericht Köln, Neue Juristische Wochenschrift (NJW) 2006, 1676f.*

[8] *Trusted Computing Group, Trusted Platform Module (TPM) Specifications, Technical Report, (2006), https://www.trustedcomputinggroup.org/.*

[9] *On the IBM Thinkpad this proof is made by pressing the FN-button during the bootstrap procedure.*

deletes the previous SRK, it is not possible to obtain access to data that has been encrypted with the previous SRK.

Since the creation and storing of keys are critical operations, it is important that these functions are reliably enforced and compatible to the specification. The specification therefore requires that all TPM products be certified by the international common criteria standard.[10] The current TPM specification 1.2 demands a certification according to evaluation assurance level 4 (EAL 4).

The TPM chip has the functionality to create its own signature keys with the help of the physical random number generator. The private portion of the generated key is then encrypted with the SRK, which is stored in the non-volatile storage of the TPM. The generated keys can be 2048 bit long and are based on the P1363 standard,[11] which uses RSA as the signature scheme. The TPM possesses its own RSA engine, which is used for signature creation and asymmetric key operations. This engine can create signatures based on the PKCS#1 standard.[12] Additionally, the TPM uses SHA-1 as defined in FIPS-180-1[13] for secure hashing. It should be noted that recently discovered weaknesses[14] in the used SHA-1 hash function, specified as the used hash-function by the TCG, could possibly facilitate attacks. An adversary might therefore exploit this vulnerability to forge a correct signature.

The TPM specification requires that all TPM products be certified according to FIPS 140-2, which defines the security requirements for cryptographic modules. A TPM that conforms to the specification is therefore *tamper-evident*, but not *tamper-resistant*.[15] It has no countermeasures against the unauthorized extractions of secret keys. However, many TPM vendors offer higher protection mechanisms for stored keys. This is because the TPM is, in essence, a smart card, and the vendors extend their own smart card cores to fit the TPM specification. This is, for example, the case with the Infineon SLE 66 C product family[16] and the ST Microelectronics ST19W family.[17] The underlying smart card core possesses extensive preventive measures against unauthorized extractions of keys, such as light sensors or active shields to detect an attack. These products meet the EAL5+ certification, as well as the *tamper-resistance* without difficulty.

Testing SigG conformity

In order to create a qualified electronic signature, the signature must pass the requirements specified in article 5(1) of the EU Directive and § 2 No. 3 SigG. According to these provisions, the signature must be created with a secure signature creation device. The detailed requirements are defined in annex III of the EU Directive and for Germany in § 17(1) SigG and § 15(1) and (5) SigVO. According to the provisions of annex 1(I)(1) of SigVO, the secure signature creation device must fulfill the assurance level EAL 4 and be tested against an attacker with a high attack potential (strength of function high). As already shown, this requirement is not covered by the TPM specification, but can be fulfilled by the TPM products.

According to the provisions of annex III(1)(b) of the EU Directive and to § 17 (1) SigG, the signature creation device must reliably detect a potential forgery or a modification of the signature. Annex III of the EU Directive provides as follows:

> Requirements for secure signature-creation devices
> 1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
>
> > (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
> > (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
> > (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

A forgery or a modification of a signature is recognizable if the verification mechanism of a digital signature cannot be bypassed or deactivated.[18] Forging a

[10] *The Common Criteria for Information Technology Security Evaluation (CC), version 2.3, http://www.commoncriteriaportal.org/.*

[11] *IEEE P1363: Standard Specifications For Public-Key Cryptography, available on-line at http://grouper.ieee.org/groups/1363/.*

[12] *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 RFC 3447, available on-line at http://tools.ietf.org/html/rfc3447, 2003.*

[13] *Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic. Modules, available on-line at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, 2002.*

[14] *Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, ‘Finding collisions in the full SHA-1,’ In Advances in Cryptology – CRYPTO 2005, Springer, Volume 3621, 2005, 17–36.*

[15] *Oliver Kömmerling and Markus Kuhn, ‘Design Principles for Tamper-Resistant Smartcard Processors’, Proceedings of the USENIX Workshop on Smartcard Technology, Chicago, 10-11 Mai, 1999.*

[16] *Infineon Technologies AG, Product Brief Security & Chip Card ICs SLE 66C42P, 2002.*

[17] *STMicroelectronics, Product Brief, ST19WL34 Smartcard MCU with MAP, 2004, available on-line at http://www.st.com/stonline/products/literature/bd/10928/st19wp18-tpm-c.pdf.*

[18] *Bundesrats-Drucksache. 966/96, 36f.*

signature is not detectable if an unauthorized person can obtain access to the signature key. This situation could occur in the following cases:

- The same signature pair is generated multiple times.[19]
- The private key used for signature creation can be obtained through the public key.[20]
- The private key can be guessed.[21]
- The private key is copied during generation and transferred to another unauthorized person.[22]
- The private key is accessible or useable in a stolen or found signature creation device.[23]

The TPM uses a physical random number generator for key generation, which causes the distribution of all keys to have an equal probability. In combination with keys consisting of 2048 bit, every key is unique with sufficient probability. The key length used by the TPM is appropriate for signature keys until 2011[24] with respect to the implemented hash function, which is, despite the SHA-1 weakness, applicable until 2009. The key length means it is almost impossible to guess the private key, and the RSA algorithm provides assurance that the private key cannot be computed based on the public key. The requirement that the keys must not be revealed according to § 15(1)(2) SigVO (*tamper-resistance*) is not fulfilled by the TPM specification. However, it is suggested that the TPM products meet that requirement. The TPM also protects the signature key against the use by others through the owner-password, therefore fulfilling requirement (c) of the EU Directive. The method of generating a secure owner-password is discussed in the following section.

The TPM specification meets the basic requirements of annex III of the EU Directive, but does not meet all formal requirements of the Signature Act 2001. The available products fulfill all requirements of the German signature law from the technical perspective. Therefore, these products can be validated according to annex 1 of the SigVO[25] and approved as secure signature creation devices.

Qualified Electronic Signature

As already described in the preceding section, the TPM provides the functions to create an advanced signature. Since the TPM was originally designed to carry platform-specific data and information about the user, it must be determined whether it can also be used for this purpose.

Identification

The basic difference between the smart card with the ability to create an advanced signature and the TPM, is that a smart card is directly bound to a certain user, while the TPM is shipped without personal certificates. In order to use the TPM to carry information relating to the user, it is therefore necessary that a certification service provider (CSP) identifies the owner of a TPM and certifies the corresponding public signature key. The applicant for a qualified certificate must therefore, according to the provisions of annex II(d) of the EU Directive and § 5 (1)(1) SigG, be clearly identified by the CSP, for example, by validating their identification card, if such a form of identification is acceptable. The user can physically visit the CSP for this purpose, or a third party may, in accordance with the provisions of § 4(5) SigG, validate the identity of the user. The German PostIdent method run by the German Post AG may be a useful method to use for this purpose. This method is still used by many on-line credit institutes to identify their customers according to the provisions of § 154 Tax Law. The identification can therefore be accomplished in the post office or at the applicant's home. After the identification process is complete, the applicant receives a unique code, which is used to assign the signature key to a person. This code must be transferred over secure channels to the applicant. This can be achieved by certified mail or physically handed over to the applicant in person.

Issuing Qualified Certificates

In Germany, there are additional requirements to be fulfilled when issuing a qualified signature, although similar problems exist under the terms of the EU Directive which are described in article 2(10) of the EU Directive. According to §§ 5(6) and § 15(7)(2) SigG, the certification service provider must ensure that the applicant that wishes to obtain a signature is in possession of a secure signature creation device - in this case, the TPM. Qualitatively, both requirements of §§ 5(6) and § 15(7)(2) SigG are identical. For this purpose, a protocol is introduced, illustrated in Figure 1, that fulfils the requirement of proving the possession of a

[19] *See also annex III(1)(a) EU Directive.*

[20] *See also annex III(1)(b) EU Directive.*

[21] *See also annex III(1)(b) EU Directive.*

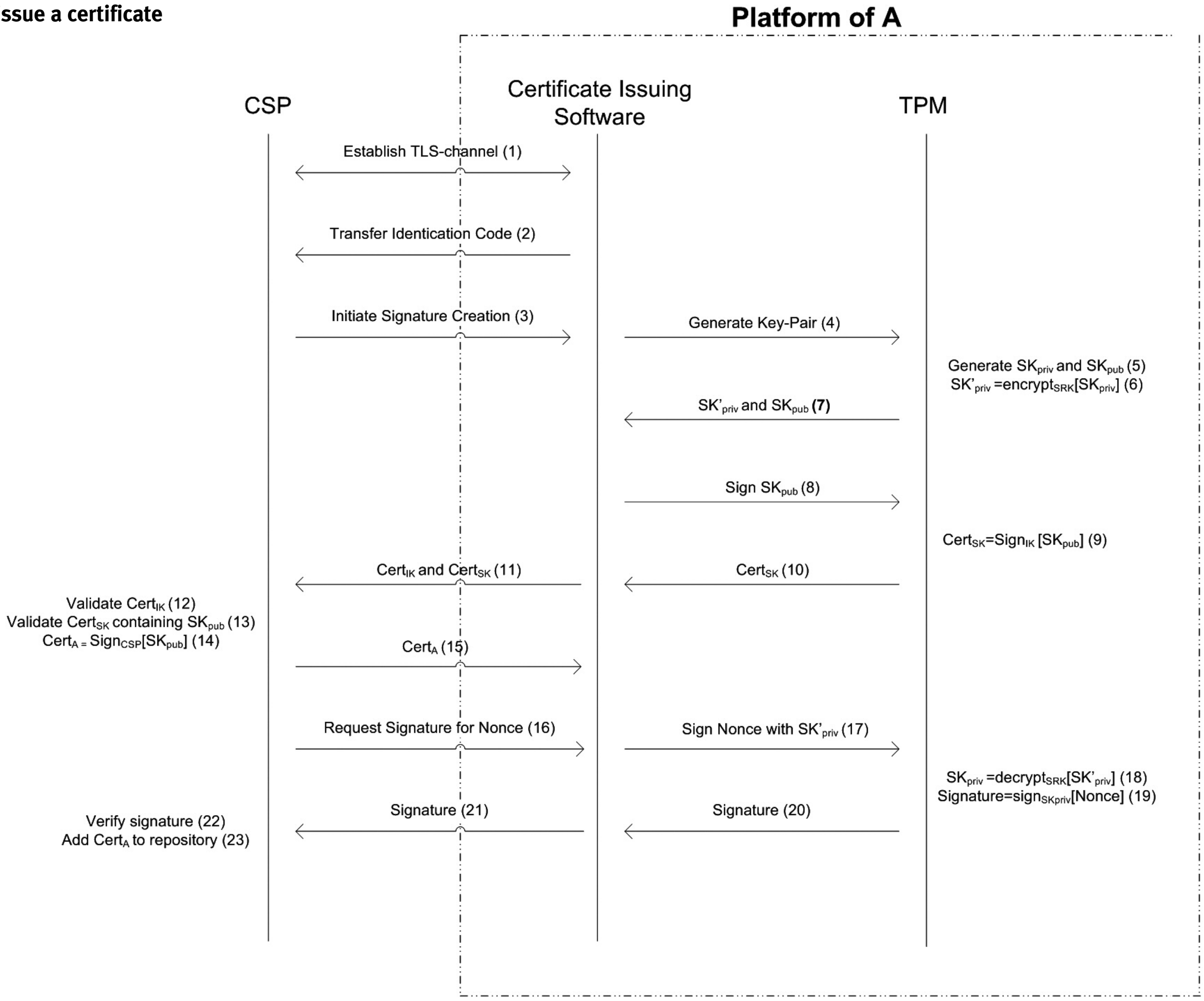
[22] *See also annex III(1)(a) EU Directive.*

[23] *See also annex III(1)(c) EU Directive.*

[24] *Bundesnetzagentur, Statement for electronic signatures, 2.1.2006, Bundesanzeiger No. 58, 23.3.2006, 1913 ff.*

[25] *Federal Ministery of Justice, Verordnung zur elektronischen Signatur, 16.11.2001, http://bundesrecht.juris.de/sigv_2001/index.html.*

Figure 1: Simplified protocol to issue a certificate


Platform of A
CSP
Certificate Issuing Software
TPM
Establish TLS-channel (1)
Transfer Identication Code (2)
Initiate Signature Creation (3)
Generate Key-Pair (4)
Generate SK_{priv} and SK_{pub} (5)
SK'_{priv} =encrypt$_{SRK}$[SK_{priv}] (6)
SK'_{priv} and SK_{pub} (7)
Sign SK_{pub} (8)
$Cert_{SK}$=Sign$_{IK}$ [SK_{pub}] (9)
$Cert_{SK}$ (10)
$Cert_{IK}$ and $Cert_{SK}$ (11)
Validate $Cert_{IK}$ (12)
Validate $Cert_{SK}$ containing SK_{pub} (13)
$Cert_{A}$ = Sign$_{CSP}$[SK_{pub}] (14)
$Cert_{A}$ (15)
Request Signature for Nonce (16)
Sign Nonce with SK'_{priv} (17)
SK_{priv} =decrypt$_{SRK}$[SK'_{priv}] (18)
Signature=sign$_{SKpriv}$[Nonce] (19)
Signature (20)
Signature (21)
Verify signature (22)
Add $Cert_{A}$ to repository (23)

secure signature creation device, and also ensures that the keys are placed into this specific device.

One requirement for the success of this scheme is that the CSP offers a platform that enables secure communication between applicant and the CSP, by using the Transport Layer Security. In this context, it is necessary for the CSP to authenticate itself against the applicant.[26] This is essential, because it is possible that a false person masquerading as the legitimate CSP may present the applicant with what seems like a legitimate certificate to authenticate themselves. Figure 1 shows the CSP and the platform of A (the applicant). The applicant's platform A is split into two components: the TPM, which caries out the cryptographic functions, and the software, which is provided by the CSP.

After the applicant (A) has entered their personal data, they transfer their identification code to the CSP using the certificate issuing software (steps 1 - 3). In the next step, the TPM of A generates a signature key pair SK_{priv} and SK_{pub} using the physical random number generator of the TPM. In accordance with the provisions of § 17(1)(3), this key can be generated on a secure signature creation device - namely the TPM, and does not need to be added externally.[27] This also acts as a

[26] *The applicant must use special software that implements the protocol described in figure 1. This software should validate the certificate and cancel the connection if the certificate is not valid.*

[27] *Alexander Roßnagel, Multimedia und Recht (MMR) 2006, pp 441 (11.07.2006).*

form of self-protection, since this guarantees that the key is protected over its lifetime and is not exposed to third parties. After the private key pair is generated, it is then encrypted with the SRK (step 6 in Figure 1) of the TPM and returned to the user (7). The public part of the signature-key is signed with a so-called identity key (IK) of the TPM (9). This certification proves that the corresponding key-pair is held in the protected storage of a valid TPM and that the signed key is a key that cannot be moved.[28] Identity keys can only sign data that originates from the TPM. Thus, a valid signature of data proves that the data was generated on a TPM and is protected by the TPM's secure storage, in that it is part of the key-hierarchy of the SRK. The identity key is only valid if the TPM has not been tampered with and the TPM is authentic. The IK is an asymmetric key that is generated by a specific TPM key inserted by the vendor. This process takes place before the actual signing key is generated and involves an additional privacy certification authority (CA), which verifies the vendors key and then issues a certificate ($Cert_{IK}$) that belongs to the IK.[29] In the next step (10 and 11), the TPM transfers the certificate of the signature key ($Cert_{SK}$) and the certificate of the identity key ($Cert_{IK}$) to the CSP. The CSP then verifies the authenticity of the signatures and verifies whether IK is a valid identity key (12 and 13). If the verification succeeds, the CSP has confirmation that SK_{priv} is held in the protected storage of a genuine TPM.

Afterwards, the CSP signs the public part of the signature key and issues the corresponding certificate (14), which it adds to his own directory service. This certificate is then transferred to the applicant. Finally, in step 16, the CSP verifies whether the applicant has access to the signature key by requesting a test signature (proof of possession). To create a successful signature, the TPM must decrypt the encrypted private SK key. This is only possible if the correct SRK is stored inside the protected storage of the TPM, and the owner has delivered the correct password for decrypting the SRK.

This kind of sample signature also fulfills the control duties of the CSP. Since the applicant must perform a sample signature, it is guaranteed that the applicant possesses the required knowledge (password) for a signature creation and that this unit is under the control of the person using the password.

Trustworthy initializing software

It is necessary to use an initializing software that reliably enforces the protocol set out above. This software is also responsible for supporting the user during the creation of a secure password. In contrast to smart cards, which often include the use of a counter to prevent more than a set number of attempts to correctly guess the password, the TPM does not provide such a function. The TPM specification requires a mechanism that prevents dictionary attacks, but the specification is not specific on this point, and leaves this to the TPM vendor. As a result, different products exist which differ in their implementation. For example, the STM TPM chip provides a counter to prevent more than a set number of attempts to correctly guess the password. In contrast to smart cards, which prevent further use of the card after several incorrectly entered passwords, the STM TPM chip only increases the reaction time after 15 false attempts.

The generation of a secure password should take place before a signature-key is generated, to ensure that the signature-key is protected by a secure password and to prevent the use of a chip containing an insecure password. The initialization process is important, which means the trustworthiness of the software must be guaranteed. This could, for example, be performed by a boot CD that has been extended by the functions set out above. This software is configured so that it only supports connections to a specific CSP and prevents remote access to the underlying hardware TPM. The CSP must also validate whether the software used for the acceptance of the initial signature reliably enforces this requirement, because it is possible for the applicant to place their signature key into a TPM, which they can only obtain access to remotely. To ensure that a human being has physical access to the TPM, the CSP uses the integrity measurement and reporting functionality provided by the TPM. The initialization software is pre-configured in such a way that the TPM measures all running software components and attests this system state to the CSP. The CSP can then decide via remote attestation[30] whether a trustworthy initialization software is used. If this verification is successful and the protocol shown in figure 1 has been executed, the CSP issues the corresponding certificate and signs the applicant's public key.

[28] *A non-migratable key is an asymmetric TPM signing key which can not be extracted through the platform owner.*

[29] *For more details please refer to the TCG TPM Main specification.*

[30] *Frederic Stumpf, Omid Tafreschi, Patrick Röder and Claudia Eckert, 'A Robust Integrity Reporting Protocol for Remote Attestation', Proceedings of the 2nd Workshop on Advances in Trusted Computing, Tokyo, (1.12.2006).*

The aim of the regulation is to ensure the signatory has the secure signature creation device in their custody, and is capable of preventing unauthorized access to the device.

Knowledge and possession

As described in the preceding sections, the TPM offers the possibility to store and use personal certificates. But it must still be determined whether the signatory is also in in direct possession of a secure signature creation device, and how this fact can be proven to the CSP.[31] The EU Directive requires, pursuant to annex III (1)(c), that the signature key can be reliably protected by the legitimate signatory against the use of others. The provisions of § 15(1) SigVO state, in more detail, that it should only be possible to obtain access to signature keys after the identification of the applicant on the basis of knowledge and possession, or by means of a measurement of a biometric attribute. Since biometric attributes do not provide the same level regarding security, knowledge and possession must be used as the means of identification. The requirement that it should only be possible to obtain access to the signature key if the applicant is successfully identified on the basis of knowledge and possession, provides a reasonable level of assurance that the signature was created by a specific person. Since neither knowledge nor possession on its own are reliable attributes to identify somebody fully, both attributes must exist simultaneously. Only when both attributes are used together, it is argued, can an electronic signature replace a manuscript signature and therefore act as prima facie evidence in trial.[32]

One issue is the meaning of possession in the context of a TPM. The legislation covers smart cards as secure signature creation devices.[33] However, the official statement also mentions special components as secure signature creation devices to be used in mainframe architectures.[34] Since the definition of a secure signature creation device is not very specific,[35] it is not necessary for the secure signature creation device to be portable, as provided for by the provisions of § 15(1) SigVO. The aim of the regulation is to ensure the signatory has the secure signature creation device in their custody, and is capable of preventing unauthorized access to the device. In the case of mobile devices, this custody can be adduced by physically inspecting the device. Unfortunately, it is more difficult to prove that the signatory has sole access to the device and can prevent unauthorized access. In this context, the TPM could be situated in an external environment, and the signatory could obtain access to this device remotely, and protect it with the password. This fact would neither fulfill the requirement of §§ 5(6) and 15(7) SigG nor the protection purpose of § 15(1) SigVO. Therefore, the CSP must verify whether the applicant of an electronic signature has the secure signature creation device in their custody and is capable of preventing unauthorized access. To achieve these properties, it might be necessary for an employee of the CSP to physically attend the applicant's premises to confirm possession.

The use of a password implies that the signatory has control of the secure signature creation device. This does not exclude the creation of signatures on remote devices, if the signatory can prevent unauthorized access to the signature creation device by protecting it physically.

Conclusion

The Trusted Platform Module offers, from the technological point of view, the possibility to use and store personal certificates and their corresponding keys. In the realm of the EU Directive, it can serve as a secure signature creation device. In Germany, to create qualified signatures with the TPM, the TPM must be approved as a secure signature creation device according to § 17(4) SigG. Furthermore, the TPM must

[31] *It should be noted that the protocol described in this article only proves that the generated keys are generated on a secure signature creation device, and not whether the applicant is really the one who initiates the protocol.*

[32] *Alexander Roßnagel and Stefanie Fischer-Dieskau, Neue Juristische Wochenschrift (NJW) 2006, pp 806 (11.07.2006).*

[33] *S. z.B. Bundestags-Drucksache 14/4662, 21, 29, 30; Official statement to SigVO, 27.*

[34] *Official statement to SigVO, 27.*

[35] *According to the provisions of § 2(10) SigG.*

be protected against unauthorized access and be in the signatory's direct possession and secured with an additional method of proving possession. If the TPM is to be used as a signature creation device, it is necessary that the TPM implements the protocol set out in this article, which enables a qualified certificate to be issued to a specific TPM signing key. Based on the high availability and low cost of a TPM, it can reduce the costs involved in creating signatures and possibly act to increase the use of secure signature creation devices.

Frederic Stumpf studied computer science at the Technische Universität Darmstadt. He is working as a research assistant and a PhD student in the IT security group of Prof. Dr. Claudia Eckert. His main research lies in the area of IT Security and covers trustworthy system architectures and attestation protocols.

Markus Sacher, lawyer, is a member of the Project Group Constitution Compatible Technology Development (Provet) at the University of Kassel, and is working on the interdisciplinary research project TrustCaps. He is doing his PhD thesis in the field of trustworthy e-commerce.

Professor Dr. Claudia Eckert holds the chair for IT Security at Technische Universität Darmstadt. She is also the director of the Fraunhofer Institute for Secure Information Technology and co-founder of the Darmstadt Centre for IT Security. The main focus of her research is in IT Security and computer networks.

Professor Dr. iur. Alexander Roßnagel holds the chair for public law, focusing on technology and environmental law at the University of Kassel. He also leads the project group for constitutional compatible technology design (provet); is the academic director of the Institute of European Media Law (Saarbruck) and Vice-President of the University of Kassel.