AuthentiDate®

White Paper

Electronic time stamps

Legally anchored security
for electronic business processes of all kinds,
also as a supplement to electronic signatures

AuthentiDate International AG
Rethelstraße 47
40237 Düsseldorf / Germany

Tel.   +49 (0)211 – 43 69 89 0
Email   info@authentidate.de
Web   www.authentidate.de

(hereinafter termed AuthentiDate)

Effective date of the documentation: February 2009, Version 1.2

Please send any questions and suggestions to the above contact address.

Contents

1.   Introduction

As early as July 1997, the first German Digital Signature Act (SigG) and the Digital Signature Regulations (SigV) defined the framework conditions for electronic signatures and electronic time stamps. After publication of the European Union Digital Signature Directive in December 1999, the German framework conditions were revised in accordance with the EU directive and resulted in the revised version of the German Digital Signature Act of May 2001. Apart from minor changes[1] this version still forms the basis for the preparation and use of qualified signatures and time stamps.

The present White Paper "Electronic Time Stamps" describes the legal framework conditions and technical requirements for the creation of electronic time stamps and also examines the differences between qualified and non-qualified time stamps, for differentiation purposes termed "other time stamps" below.

It explains how qualified and other time stamps are technically implemented. In addition, the White Paper demonstrates how the different implementation measures can affect compliance issues, legal probative value and cost structures.
Moreover, this White Paper presents examples of current application scenarios for electronic time stamps.

---

[1] Amendment of SigG in February 2005

2.   Executive summary

Companies, authorities and organisations of all kinds throughout the world are increasingly generating their processes electronically for purposes of optimisation, cost reduction and speed. Thus, existing paper-based processes are being replaced by electronic processes and new processes made possible through the use of digital information und communication.

These new, improved processes (using electronic information) are subject to the same statutory provisions, compliance and protection requirements, as traditional paper-based processes. In order to meet these requirements, both paper-based and electronic information has to be protected, among other things, against manipulation and loss. In order to be able to assess the observation of compliance requirements in a professional environment, proof of integrity, completeness and confidentiality are often the main criteria.

Electronic time stamps can deliver this proof of integrity and completeness in a way that is simple, legally secure, permanent, inexpensive and, on request, anonymous.

A time stamp is a value in a defined format which allocates an event (for example the dispatch or receipt of a message, the modification of data, etc.) to a point in time. The purpose of a time stamp is to make clear for people or computers when such events occurred.

The term 'time stamp' also designates a certificate that an electronic document was available to the issuer of the time stamp at the time specified. They are essential for the use of electronic signatures in legal relations. The German Digital Signature Act governs the requirements for issuing **qualified time stamps** - an especially advanced form of such certificates which ensures that the valid legal time is recorded, and excludes the possibility of forgeries and falsifications. In the procedures used today, the qualified time stamp includes a hash value for the document certified and the current time designation (date and time), and is furnished with the issuer's qualified electronic signature.
Source: WIKIPEDIA (translated from the German)

A time stamp is an electronic certificate which states when certain data existed. It thus documents the "when" and "what". An electronic signature, often referred to as personal signature, documents the "who" and "what". In contrast to an electronic signature, a time stamp is not bound to people and their actions. It can thus be integrated much more simply and also fully-automatically into electronic processes.

Electronic time stamps can thus provide considerable benefits for companies, authorities and organisations by enabling electronic processes to be introduced cost-effectively and securely <u>without</u> neglecting the necessary security with regard to the observation of statutory provisions, traceability and compliance.

A special status is held by what are termed qualified time stamps from accredited providers. This type of time stamp enjoys special legal protection (through the Digital Signature Act) and is thus able to guarantee even comparatively unprotected electronic data reliable, long-term protection for at least thirty years.

Special legal and technical requirements apply to the creation of this type of time stamp. Nevertheless, in comparison with e.g. qualified personal signatures, it is easier to use because the user himself does not need any specific legally compliant hardware or software, and no manual interaction such as PIN entry is required from the user. The qualified time stamp is simply purchased from an officially accredited provider, the "certification service provider". In this way, this provider's qualified time stamp becomes an easy-to-use "tool" which can be applied to each process step, regardless of location and sector, thus improving its legal security.

High flexibility in conjunction with availability anywhere, any time and in (practically) any amount makes the qualified time stamp a valuable, easy to use tool for the legally secure protection of electronic data and processes.

Time stamps are easier to use than electronic signatures as their application can be fully-automatic and independent of specific individuals, or anonymous.

Qualified time stamps from accredited providers freeze electronic data for at least thirty years in a way that is legally secure and accepted as evidence in court. The probative value applies regardless of sector or process-specific legislation (e.g. Social Security Law, Value Added Tax Act).

"Other time stamps" (non-qualified time stamps) are subject to the free consideration of evidence and require special proof or a specific legal basis for their recognition.

3.   Legal framework conditions

Alongside the qualified electronic signature, the German Digital Signature Act (SigG) also describes the qualified time stamp[2]. In accordance with § 2 (1) SigG, the electronic signature is primarily used for authentication in conjunction with certain data which is linked or attached to the signature. The electronic signature thus documents the "who" and "what". In contrast, in accordance with § 14 (14) SigG, the time stamp constitutes an electronic certificate which states when certain data existed. It thus documents the "when" and "what".
On the issue of international legal aspects cf. ch.8.

3.1.   Probative value of qualified personal signed and qualified time-stamped data

As formulated in FAQ 9 on the Federal Network Agency's website, the German Digital Signature Act lays the groundwork for enabling all legal transactions which are subject to a statutory written form requirement to be carried out in electronic form (with qualified signature).[3]

It should be stressed that a legally compliant electronic reproduction of formerly paper-based processes equivalent to the written form is only possible when using qualified signatures (or time stamps).

Depending on the context in which the personal signature or time stamp is used, sector and/or process-specific legislation, amendments and framework conditions may additionally define the legal probative value of the signatures and time stamps.

Digital Signature Act and Digital Signature Regulations thus define the sector- and process-neutral framework conditions.

What is decisive for the user is that the definitions of the Digital Signature Act and the Digital Signature Regulations are firmly established by law and therefore binding. I.e. a sector- or process-specific law can only refer to a qualified signature or a time stamp in accordance with the Digital Signature Act. It cannot define how this qualified signature or qualified time stamp are to be created, and which security characteristics and probative characteristics thus take effect. This is always uniformly defined by the Digital Signature Act and the Digital Signature Regulations.

A typical example of a process-specific requirement is provided by the current Value Added Tax Act (UStG). § 14 para 3 UStG states that electronic invoices may only be used for pre-tax deduction if they are

---

[2] See § 2 SigG
[3] Cf. FAQ 9 Federal Network Agency www.bundesnetzagentur.de

furnished with a qualified personal signature in accordance with the Digital Signature Act.

A typical example of a <u>sector-specific requirement</u> is provided by the confirmation of the change of medium in the mass recording of payment-related documents by the statutory health insurance funds. Here, among other things the Social Security Law, which governs all of the statutory health insurance funds, states that the use of a qualified personal signature is compulsory if paper documents are destroyed after scanning (mass document recording). This is also monitored by the authority responsible for this specific sector (the Federal Social Insurance Authority - BVA). Details on the use of the qualified personal signature in accordance with the Digital Signature Act can therefore be found in the sector-specific legislation (§ 286 para. 3 of the Social Security Code (SGB V), § 17 of the Social Insurance Accounting Ordinance (SVRV) and § 36, § 40, § 41 of the Social Insurance Accounting and Administration Ordinance (SRVwV) and the respective standing instructions of the Federal Social Insurance Authority (BVA).

3.2. Distinguishing between qualified and other signatures and time stamps

In addition to the "type" (personal signature or time stamp), the Digital Signature Act also describes different "security levels". At least in connection with personal signatures, this is expressed through the supplementary designations "advanced" and "qualified".

Here, the Digital Signature Act differentiates as follows:
- "advanced electronic signatures" (§ 2 no.2 SigG)
  - are exclusively allocated to the signature key holder
  - enable the identification of the signature key holder
  - are generated using means which the signature key holder may have under his sole control
  - and are thus linked to the data to which they refer. Their subsequent alteration can thus be excluded.

- "qualified electronic signatures" (§2 no.3 SigG)
  - are, in addition to the requirements for advanced signatures, based on a qualified certificate valid at the time of their generation and
  - are generated using a safe signature generation unit (signature card).

A typical example of an advanced personal signature is an electronic signature which is generated using a software certificate. The name of the certificate holder, for example, is linked with the software certificate. With the aid of client software, the user can, e.g. electronically sign a document. Since no qualified certificate and no secure signature generations unit is used, this is, at best, an advanced

personal signature. With this advanced personal signature, no probative value is guaranteed[4].

Laws based on the Digital Signature Act such as, for example, the Code of Civil Procedure (ZPO)[5], do <u>not</u> equate the advanced signature with the hand-written signature. Accordingly there is also <u>no legal effectiveness</u> connected with the advanced signature or the signed data.

A qualified personal signature is generated with the aid of tested and validated card readers (smart card terminals), secure signature cards (e.g. T-TeleSec TCOS V3, D-Trust, etc.) and suitable signature application components (signature software). All three components stated must fulfil the requirements of the Digital Signature Act. <u>If even one of the requirements is not fulfilled, no qualified signature can be generated.</u>

The above requirements for secure components etc. also apply, among other things, to electronic time stamps. For these, in accordance with the Digital Signature Act, it is essential that a particularly secure operational environment is established. This operational environment has to be protected by a security concept, access protection and continuous monitoring. For this reason, qualified time stamps can only be issued by service providers accredited (or registered) by the Federal Network Agency.

In contrast to personal signatures, the Digital Signature Act does not distinguish between qualified and advanced time stamps. This means that from a legal point of view, there are only "qualified time stamps" and "other time stamps". There are no further distinctions and gradations in the legal relevance of electronic time stamps.

As soon as even one of the legal requirements is not fulfilled, the signature or time stamp generated is always "<u>not</u> qualified".

This also applies if, e.g. a certain operational environment is prescribed for the generation of the signatures or time stamps. Here the example of the mass generation of personal signatures is relevant. According to the Federal Network Agency, a suitable operational environment with access protection and monitoring, such as a steel cabinet or a computer centre, is an indispensable prerequisite for mass signatures[6]. If this prerequisite is lacking, a qualified signature cannot be generated using the mass signature procedure, even if all other conditions regarding the hardware and software used are fulfilled.

---

[4] Cf. Federal Network Agency website www.bundesnetzagentur.de
[5] See § 371a ZPO
[6] See Federal Network Agency website FAQ 18

The form of a simple signature[7] is not treated in detail in the Digital Signature Act. In general this is deemed to be a signature which is generated without the aid of a qualified or an advanced certificate and also without a signature generation unit. This can, for example, take the form of a footnote under an email. Due to the low legal relevance, the simple signature is not dealt with any further in this white paper.

4. Technical and organisational requirements

4.1. Technical requirements for qualified personal signatures

As shown, in accordance with § 2 of the Digital Signature Act (SigG), the use of appropriate hardware (signature generation unit) and software (signature-application components) is essential for the generation of qualified personal signatures. Both hardware and software have to meet the requirements of the Digital Signature Act. Thus, for example, testing and validation have to be provided for the software in accordance with the Digital Signature Act (SigG validation) or a manufacturer's declaration submitted to the Federal Network Agency and published by it[8]. If the user has the legally compliant hardware and software components, he is able to create qualified personal signatures himself wherever he likes[9]. Put simply, for the generation of a qualified signature, all that is needed is a signature card (secure signature generation unit - SSGU), a certification service provider, a validated card reader and a signature application component (SAC). The signature application component either has to be SigG validated or, alternatively hold a manufacturer's declaration published by the Federal Network Agency[10].

4.2. Technical requirements for qualified time stamps

The hardware and software for the generation of qualified time stamps is also subject to strict requirements. As already explained in Section 3.2, in contrast to qualified personal signatures, qualified time stamps cannot be generated by anybody anywhere. The use of legally compliant hardware and software is not sufficient.

In accordance with § 2 no.14 SigG, a qualified time stamp is a certificate from a certification service provider. It is therefore mandatory that a qualified time stamp be issued by such a provider.

---

[7] See § 2 para. 1 SigG
[8] See §17 (4) SigG and suppl. to this, 1.SigÄndG of 4.01.2005
[9] Process and sector-specific additional requirements, such as, e.g. operational environment in case of mass signatures (see Federal Network Agency website / FAQ 18) are to be taken into account
[10] www.bundesnetzagentur.de

For this, the provider runs a certification service, generally designated as a trust centre. This certification service has to fulfil a range of requirements in accordance with § 4 SigG (see ch. 5).

Certification services are available in two forms; the accredited and the registered certification service. Both are able to issue qualified time stamps. For the user however, there are different legal options for the use of the two forms of certification service. These are shown in Table 1 and explained in ch. 5.

Only certification service providers accredited or registered by the Federal Network Agency can issue qualified time stamps in accordance with § 2 SigG.

4.3. SigG-validation of time stamp software

The use of SigG-validated time stamp software has been much discussed with the aim of enabling qualified electronic time stamps to also be generated outside of the trust centre of a registered or accredited certification service provider, e.g. in a company's own computer centre. Due to the statutory requirements, this is not possible, as is explained in more detail below.

The use of SigG-validated hardware and software alone is not sufficient for the generation of qualified electronic time stamps.

The following simple "rules of thumb" help improve the structuring of the requirements with regard to validations, areas of use and legal validity:

1. It is essential that validated hardware and software for the generation of qualified time stamps be employed in a particularly protected area such as e.g. the trust centre of a certification service provider. This is already stipulated by the Digital Signature Act, which explicitly restricts the generation of qualified time stamps to registered und accredited certification service providers.

2. A validation of hardware and software for the generation of time stamps in accordance with SigG always refers exclusively to the operation and use by a certification service provider. Validations of components for the generation of time stamps outside of the area of employment stated in the validation document are not applicable.

3. If hardware and software is validated in accordance with SigG especially for operation outside of certification service providers, this validation does <u>not</u> refer to the generation of time stamps, because in accordance with the Digital Signature Act, time stamps have to be generated <u>within</u> the trust centre of a

registered or accredited certification service provider. As a rule, such validation in accordance with SigG thus refers to the generation and/or testing of signatures (signature application component).

4. A validation in accordance with SigG for hardware and software for the generation of qualified signatures does not simply also apply to qualified time stamps, as the most important aspect for time stamps - the legally valid time - is not part of the validation of signatures.

5. If, in accordance with SigG, a validation applies to certain framework conditions, such as purpose (e.g. signatures) and place of operation (e.g. particularly protected area), and if even one of these conditions is breached, the validation is fully inapplicable – the rest does not "survive".

5. Selection of the right time stamp

As already explained in chapter 3.2, time stamps are available in different forms. The selection is made on the basis of the individual legal, technical and commercial requirements, and the decision taken as to whether "qualified" or "other time stamps" should or must be used.

In general, before choosing, the following questions need to be answered and then matched with the technical requirements (further sector-specific, individual requirements are also to be checked):

- How long should the legally binding verifiability of the time stamps last?
- How long should e.g. the integrity and thus the completeness of the data on a certain date be legally demonstrable?
    - At least 30 years
    - At least 5 years
    - No legally binding verification necessary; the completeness of the time-stamped data does not need to be demonstrated

- Should the verification of the time stamps also be guaranteed if, e.g. the provider or generator of the time stamps closes his business?

- Should the time-stamped data be admissible as evidence in court; regardless of whether there is specific legislation for the sector or the business process in which the time stamps are used?

- Should the time stamps be usable for subsequent signing (re-signing) in accordance with § 17 SigV?

- Should your own liability risk be reduced and risks transferred to or divided among suppliers, such as e.g. those who generated the time stamp?

The following Table 1 shows the consolidated dependencies between the legal characteristics and the technical implementation in the generation of time stamps.

Feature \ Field of use	Accreditited certification service provider, time stamp service (TSS) in accordance with SigG	Registered certification service provider, time stamp service (TSS) in accordance with SigG	SigG-validated hardware (smart cards of a TSS) + SigG-validated time stamp software * operates outside of a TSS	Secure hardware (HSM–Hardware Security Module) + SigG-validated time stamp software	Standard hardware (server) + SigG-validated time stamp software
Generation of qualified TS in accordance with SigG	yes	yes	no	no	no
Generation of other TS	yes	yes	yes	yes	yes
TS usable as evidence in court in accordance with SigG	yes	yes	no	no	no
TS verifiability legally secured for at least 30 years	yes	no	no	no	no
TS verifiability legally secured for at least 5 years	yes	yes	no	no	no
TS verifiability is also guaranteed in case of "fall out" (e.g. insolvency or closure) of the provider or generator	yes	no	no	no	no
TS suitable for resigning in accordance with § 6 SigG and § 17 SigV	yes	conditional	no	no	no
Federal Network Agency obliged by law to ensure the verifiability of TS in case of "fall out" of TSS	yes	no	no	no	no
Duty to provide cover in accordance with SigG (insurance against financial loss of 2.5 m/TS)	yes	yes	no	no	no

Tab. 1 – Consolidated presentation of time stamp characteristics in dependence on the technical and organisational requirements or areas of use

* Time stamp software can fundamentally be SigG-validated. However, if this is employed outside of a certification service, the SigG validation looses its application.

The areas of use listed in Table 1 are specified in more detail below.

5.1.   Qualified time stamps from certification services

There are fundamentally only two alternative methods of generating qualified time stamps which comply with the Digital Signature Act and are thus legally effective.

   a. In the business (trust centre) of an accredited certification service provider in accordance with the SigG oder

b. In the business (trust centre) of a <u>registered</u> certification service provider in accordance with the SigG

In contrast to qualified personal signatures, the place in which the qualified time stamp is physically generated is of crucial significance. A compulsory prerequisite is the business, i.e. the certified and validated secure spatial environment of a certification service. This is, as already described, generally designated as a trust centre.

Qualified time stamps can only be generated by certification service providers (CSP) accredited or registered in accordance with the Digital Signature Act.

Qualified time stamps always have to be generated in a certified, validated and isolated operational environment (e.g. trust centre).

The operation of a time stamp service for qualified time stamps in accordance with the Digital Signature Act is subject to registration or accreditation at the Federal Network Agency.

Time stamps which are not generated by a registered or accredited CSP are always other time stamps. This depends on the environment and the hardware and software with which they are generated.

5.1.1. <u>Qualified time stamps from accredited certification services</u>

Accredited certification service providers are subject to strict requirements, the fulfilment of which is continuously, i.e. at all times during operation, monitored by the Federal Network Agency[11]. In case of violation, i.e. non-fulfilment of the requirements, operation can immediately be prohibited by the Federal Network Agency.

On the one hand, these high requirements placed on the accredited certification service providers put great demands on those operating the service. On the other hand however, they guarantee the highest level of security available in Germany and Europe for the users and customers who employ their services.

In order to illustrate in which areas these high requirements placed on certification service providers are of benefit to the user or customer, by way of example, several aspects are presented below, which are to be implemented by the certification service providers in accordance with § 4 SigG.

---

[11] See §4 para.4) SigG

Main requirements of accredited certification service providers in accordance with § 4 SigG:

a. Proof of reliability and specialist knowledge
The specialist knowledge is, in particular, demonstrated through the specialist knowledge of the staff. In addition to police clearance certificates, this also requires, among other things, evidence of their knowledge, skills, experience and reliability.

b. Fulfilment of the security requirements by means of a security-concept which is to be practically implemented throughout the entire duration of activity.

c. Provision for coverage
An accredited certification service provider is to take out an insurance policy which protects the users of its services against unforeseeable errors and their financial consequences.

d. Comprehensive testing of the technical and administrative security, (in accordance with § 15 para.1 SigG)

e. Scrutiny and validation of the security concept and its repetition at regular intervals, (in accordance with § 15 para.2 SigG)

The users derive two main advantages from the accreditation:

1. In accordance with § 15 para.6 SigG, the Federal Network Agency always ensures that the processing of contracts concluded by the certification service providers is enabled throughout the statutory term. This means:
qualified time stamps from an accredited certification service provider continue to be verifiable even in case of cessation of the business activities, withdrawal of accreditation or insolvency.

2. In accordance with § 4 SigV, an accredited certification service provider has to ensure the verifiability of the qualified certificates for at least 30 years after expiry of the validity of the respective certificate. Qualified time stamps from accredited certification service providers are thus verifiable at least 30 years after time stamping. That means:
Qualified time-stamped data from accredited providers can be used as legally compliant evidence for at least 30 years.

In particular, this security – even in case of discontinuation of business or insolvency – makes the qualified time stamp from an accredited provider a valuable commodity with a high investment security. Its use is therefore especially suited to long-term legally secure data.

At this point it should be noted that for accredited certification services, the legislature prescribes at least 30 years verifiability for certificates and/or time stamps "if necessary". Since at the generation of a certificate or time stamp as a rule the "necessity" cannot be excluded for the next 30 years, this obligation exists de facto for all certificates and time stamps generated.

In addition, it should be noted that the qualified time stamps generated in a TrustCenter are differentiated by intervals even smaller than a second. By means of pagination, data which is time-stamped within the same second is differentiated and paginated according to the time of receipt of the time stamp request at the trust centre.

5.1.2. Qualified time stamps from registered certification service providers

Qualified time stamps from registered certification service providers only partially fulfil the requirements stated in 5.1.1. They therefore also do not bear the Federal Network Agency seal of approval. Fundamentally, they fulfil the requirements (a) to (c), i.e. proof of reliability and specialist knowledge, security concept and coverage provision.

Registered certification service providers are not subject to <u>any</u> comprehensive verification of the technical and administrative security or <u>any</u> verification and validation of the security concept or its repetition.

For users, in comparison to accredited providers, this means two significant restrictions:

1. In the event that the registered certification service provider closes his business or becomes insolvent, there is no legal security, that these are still verifiable. The verifiability can thus lapse from one day to the next without the user noticing. The user then has no way of demonstrating the integrity of his data stock at a certain time, or securing it subsequently.

2. In accordance with § 4 para.1 SigV, certificates from registered certification service providers only have to be verifiable for five years after expiry of the certificate. Regardless of the provider's business activity, the time-stamped data can thus only be used as evidence where applicable for a maximum of five years after expiry of the certificate. Since qualified time stamps are used especially in areas such as long-term data integrity, long-term archiving and re-signing, the use in these areas is only possible or practical to a very limited extent.

5.1.3. Verification of qualified time stamps

Special importance is attached to the verification of both personal signatures and time stamps. The generation of a signature or time stamp alone cannot bring about the probative value of electronic data. The electronic data can only be used as evidence if it can be demonstrated that the signature or the time stamp is correct using a procedure which is just as legally secure and which meets the statutory requirements.

For personal signatures, the criteria of a personal signature in accordance with § 2 SigG are to be verified, i.e. authenticity and integrity of the data.

For time stamps, in accordance with § 2 SigG, the certification of the time/date is to be verified in connection with the integrity of the electronic time-stamped data.

As described in ch. 5.1.1., qualified time stamps from accredited providers have a special status when it comes to sustaining the verifiability.

Qualified time stamps from accredited certification service providers are verifiable for at least 30 years after the end of the year in which the validity of the certificate expires. Regardless of whether the certification service provider is still accredited at this time or still in business at all. This period is stipulated by the Digital Signature Act and is guaranteed by self-declaration/commitment on the part of Federal Network Agency. This ensures a very high investment security for all users. Their time-stamped data can be used as legal evidence for at least 30 years.

In contrast, for qualified time stamps from **registered certification service providers, there is a legally prescribed maximum verifiability of five years** from the date of expiry of the certificate. However, this period is not guaranteed and can also end earlier at any time e.g. through cessation of the service provision.

Since, for registered certification service providers, the Federal Network Agency is not obliged to ensure verification of the certificates used for at least 30 years, in case of a discontinuation of business or insolvency of the registered provider, as a rule, verification of the time stamp is no longer possible.

Thus, a time stamp from a registered time stamp service is more suited to short-term use, which does not require guaranteed verifiability for months or years.

5.2.   Other time stamps

Other time stamps are provided in practice by various technical systems and organisational solutions. The options are virtually unlimited. It is the user's responsibility to choose according to cost and practical reasons.

All options described below have in common that the other time stamps "produced" are not legal compliant within the meaning of the Digital Signature Act. I.e. admission in court is subject to the free consideration of evidence on the part of the respective court or judge.

Below, some of the solutions discussed on the market are outlined and briefly evaluated in terms of practicality, performance and administrability.

5.2.1.   SigG-validated hardware, smart cards of a CSP and SigG-validated time stamp software

As explained under 4.3., qualified time stamps cannot be generated through the use of SigG-validated hardware, smart cards and SigG-validated time stamp software outside of a certification service. This applies regardless of whether the time stamp software is SigG-validated or not. I.e. this option only enables the creation of "other time stamps".

As SigG-validated hardware, e.g. the use of external USB-connected card readers in the 19" RACK from the company Reiner SCT is possible. If the performance of such systems is to be increased, this can be made infinitely scalable by adding additional card readers or slots. Other additional hardware would not be required.

If, instead of external systems, SigG-validated hardware is used with <u>integrated</u> card slots, it should be borne in mind that the performance of the system cannot be increased infinitely and as desired. This requires the installation of a further system as soon as the number of card slots is exhausted.

Fundamentally, when using time stamp systems that employ signature cards, the speed of the signature card is always the limiting factor when it comes to the throughput of the entire system.

Due to their low performance and comparatively high costs, time stamp solutions which employ signature cards are only suitable for the generation of "other time stamps" to a limited extent.

5.2.2. Hardware Security Module (HSM) and SigG-validated time stamp software

Since to date none of the HSMs available on the market have a legitimate validation in accordance with SigG, this version is only capable of generating "other time stamps" however, with a particularly high throughput.

HSM solutions are currently available on the market (nCipher, SafeNet, Utimaco, etc.) with a throughput of over 250 transactions per second. As a rule, these high-performance HSM systems are operated together with time stamp software and are thus able to produce other time stamps in high numbers.

Since as a rule only the time stamp software is centrally administered and no individual smart cards need to be procured and administered, in operation with time stamp software, HSMs are marked out by their high throughput and simple administration.

5.2.3. Standard server and SigG-validated time stamp software

Instead of having all cryptographic operations carried out by a dedicated HSM, SigG-validated time stamp software can also be installed and operated alone on any server (IBM, Dell, HP, etc.). In this way too, "other time stamps" are generated. In contrast to the use of an HSM, this results in limitations in throughput since the processors of a standard server system are not optimised for cryptographic operations. The security of this variant is comparatively low as the private keys of the certificates used are only minimally protected. It therefore lies within the free consideration of evidence by the judge whether he assigns an other time stamp based on an HSM a higher probative value than a time stamp based on a standard server. In both cases, there is no legal compliance within the meaning of the Digital Signature Act.

The advantages of using time stamp software on a standard server are the low costs of the standard server compared with purchasing an HSM, and the high scalability compared to time stamp solutions using signature cards. The disadvantage is the comparatively low security.

5.2.4. Verification of other time stamps

For the verification of other time stamps, no specific legal requirements apply. Conversely, this means that since there are no statutory provisions to be observed, there is also no statutory security for the

user as to how long a verification of other time stamps has to be possible for. This may even cease soon after generation, and the user can derive absolutely no security from the time-stamped data.

The verifiability of other time stamps is not established by law and not guaranteed. It can end unexpectedly.

The user therefore has to ensure for himself that all other time stamps remain verifiable for the period necessary.

5.3. Cost-benefit considerations

What kind of technology should be used always depends on the respective business process and objectives which are to be pursued through the use of signatures and time stamps.

In some processes it may be sufficient to achieve improved traceability and thus risk minimisation by using other time stamps. From a compliance point of view, and to avoid liability risks, the use of qualified time stamps is, however, to be favoured in a multitude of processes.

The benefits of qualified time stamps are particularly the anonymous, fully automatic use in conjunction with the unique legal security and long-term verifiability (of accredited services).

In the cost-benefit analysis, the costs of qualified time stamps are generally accounted as transaction costs per time stamp. The rationale for this is that each qualified time stamp from a certification service provider is produced individually "on demand". Thus each qualified time stamp draws on resources, e.g. in the form of band widths and computing power.

At the same time, however, each qualified time stamp thus produced also includes an individual service generated for the user, i.e. the legally secure documentation of the user's electronic data. This process is comparable with the work of a notary who carries out the legally secure documentation of a file for his client. The notary too charges on a "transaction basis".

The use of time stamps can be significantly optimised. This is important for the cost-benefit analysis. Thus, by means of corresponding organisational measures and process design, the number of qualified time stamps can be considerably reduced in many cases without having to forgo the legally guaranteed preservation of evidence.

One possible method of transaction and cost optimisation is the formation of a group or "batch". I.e. documents or data are pooled in a special way in a group ("batch") and frozen using a unique qualified time stamp so that they are legally secure. The integrity of each

individual document within the group at a certain point in time can thus be legally securely demonstrated at low cost by means of one single qualified time stamp. Cf. ch. 7.2 "Re-signing".

6. Combination of personal signatures and time stamps

6.1. Signatures with and without time stamp

In many processes, personal signatures and time stamps are combined in order not only to be able to legally securely demonstrate authenticity and integrity, but also to document the time and date of signature generation and/or filing of the signed data in a way that is admissible as evidence in court.

In this context, the question often arises as to whether in such combined cases the quality (the legal level) of the signature and the associated time stamp should be identical. In other words, the question is whether qualified personal signed data should subsequently be combined with other time stamps and vice versa.

Fundamentally, not only in the context of signatures and time stamps, there is a simple rule concerning probative value and security:

The legal probative value of the entire process is always as strong as the weakest link in the entire process chain.

If you use e.g. qualified personal signatures to legally securely establish which member of staff generated a document with a certain content, and combine this with an other time stamp, the documentation of the process as a whole (who, what, when) is not fully legally secure in accordance with the Digital Signature Act. The evidence for "who and what" is correctly documented in accordance with the Digital Signature Act by qualified signature, however the "what and when" is only documented by an "other time stamp". This is subject to the free assessment of evidence – thus the time and date of the document's generation and signature are not one hundred percent securely documented.

The following example illustrates why qualified personal signatures should, as a rule, be combined with an "equivalent" qualified time stamp.

All personal signatures alone, whether advanced or qualified, include a legally binding time/date specification. The use of a wrong time/date specification in the signature can result in misuse.

Thus, e.g., the following case is always possible:
Mr. Paul Schmidt, a keen motor enthusiast, buys a car in the Internet. After agreeing with the seller, Mr. Peter Miller, on the vehicle, delivery and price, Mr. Miller, sends him a purchase contract per email. The contract is a PDF document which already bears Mr. Miller's qualified signature - with the request for counter-signature.

However, Mr. Schmidt is not sure if his bank will finance the vehicle, and at the same time, he does not want to pass up the opportunity. So he sets the date on his computer two days ahead and signs the contract on his PC by qualified signature. Then he sends the document back to Mr. Miller.

The next day, Mr. Schmidt talks to his bank, and is told that the loan unfortunately cannot be granted. Mr. Schmidt is very distressed – and is now forced to cancel the contract he had bindingly concluded the day before.

Now the trick with the clock pays off. Mr. Schmidt simply phones the signature card issuer and says he has lost his card and it should be blocked straight away. The next day Mr. Miller phones to sort out the delivery and payment details. Mr. Schmidt explains to Mr. Miller that the contract is unfortunately invalid and that he is not willing to fulfil his part of the deal.

Mr. Miller is very upset, insists on his contract and checks the security of Mr. Schmidt's signature. The verification shows that the signature was affixed after the card had actually been blocked. Thus the electronic signature and the contract are invalid. Mr. Miller now only has the very lengthy and complicated option of proving that Mr. Schmidt had electronically signed the contract on an earlier date than that shown on the signature.

The above example shows that only a combination of qualified signature und qualified time stamp can provide for the legally secure recording of such processes independently of the IT infrastructure used. By using a qualified time stamp, the documentation of the time and date of the signature generation would have been legally secure. It would have been possible to prove at any time that the certificate had been withdrawn and blocked after signature generation.

Without immediate verification, the signature alone – without time stamp –provides no security with regard to the time of its creation. The time stamp is thus an important supplement to the signature.
Since qualified time stamps can only be generated by officially accredited (registered) service providers, intentional or

unintentional time manipulation, such as e.g. resetting the client's system time for the signature generation, are not possible.

6.2. Time stamps reduce compliance risk

When using qualified time stamps, also without signatures, the picture is altogether different.

Here too, the entire chain of evidence is, of course, only as strong as the weakest link in the chain. However, the use of time stamps with and without signatures makes a great deal of sense in certain areas of application.

The qualified time stamp legally documents the integrity of the data at the time that this was submitted to the certification service provider. Since, as explained in 5.1, the qualified time stamp from an accredited certification service provider cannot be abused through intentional or unintentional misconduct, at least the documentation of the integrity of the data and the time of submission to the service provider are always legally secure.

Here, it should also be noted that on generating a qualified time stamp, accredited certification service providers immediately archive the time stamp, including the hash value, for at least 30 years. In this way, it is also always possible to provide evidence over a long period.

The application cases for time stamps are numerous and extremely varied. With qualified time stamps, anonymous, system-related data, such as e.g. the log files of an SAP system or a hospital information system, can be sealed in a way that is legally secure.

In other cases, with the aid of qualified time stamps, the completeness of data can be documented independently of a personal signature in a way that is both legally compliant and capable of use as evidence in a court of law (see ch. 7.1 Mass document recording).

When it comes to important compliance aspects such as e.g. the traceability of electronic transactions at a given moment, the use of qualified time stamps, also in combination with advanced personal signatures, makes extremely good sense. In long-term electronic archiving, also without personal signatures, qualified time stamps are able to document the integrity of the data over a long period with absolute certainty.

The use of qualified time stamps is simple and fully automatic. They protect the integrity of the data over a long period and allow for long-term, secure, chronological traceability of business transactions.

7. Application scenarios for qualified time stamps

7.1. Legally secure documentation of the time/date of recording and the completeness of scanned documents

More and more sectors are using qualified personal signatures to make documentation of the change of medium within a scan process legally secure. At every scanning workplace, signature hardware and software (signature generation unit and signature application component) are installed in accordance with the Digital Signature Act. The scan operator affixes a personal qualified signature to the electronic copy which is generated by scanning the paper documents. With his personal signature he validates the consistency of the paper documents and the electronic copy.

In general, the signed data from the scanning process is electronically archived in the long-term. Typical examples are vouchers at health insurance companies and medical records in hospitals. Here, the use of qualified time stamps with qualified personal signature provides a meaningful supplement to the confirmation of the change of medium. The qualified time stamp provides secure legal evidence as to which data from the scanning process was available and archived at a dedicated time/date. Adding or deleting data is not possible without destroying the time stamp and thus making it invalid. The legally secure time stamp thus takes over an important function in providing time-based evidence of the integrity and completeness of the data independently of the qualified personal signature.

It is crucial that the legally secure "freezing" of the data and thus the legal effectiveness is carried out independently of upstream processes such as here the scanning.

This also applies if the use of the qualified personal signature at the workplace of the scanner operator is not expressly required by law. In this way, e.g., patient records in hospitals receive qualified personal signatures when scanned in order to confirm the change of medium. This is done in accordance with the rules for health insurance companies[12]. Precisely here, the use of qualified time stamps following the scanning process makes good sense.

By using qualified time stamps after the scanning process, it later cannot be disputed that this data was added to the archive and thus was complete and had a certain content at a dedicated time. Conversely, data, e.g. additional medical records, cannot be added surreptitiously at a later date in order to manipulate patient data.

This example illustrates the demonstrable increase in security by combining qualified time stamps with (qualified) personal signatures. In

---

[12] See ch. 3.1

this way, complete traceability is also provided for electronic processes, for which there is no individual, dedicated legal provision.

Naturally, in these cases too, the number of qualified time stamps can be significantly reduced by means of appropriate process design, e.g. formation of batches. In this way, an economically attractive solution is always guaranteed.

7.2.　Re-signing and over-signing

Qualified signatures and time stamps are instruments for the short, medium and long-term securing of electronic data. Due to technological progress, technologies with which qualified signatures and time stamps are generated have to be continuously monitored and the security requirements raised if necessary. For this reason, the Federal Office for Information Security (BSI) carries out an annual assessment of the cryptographic algorithms and key lengths. This results in a recommendation for algorithms and key lengths with temporal validity forecasts. The Federal Network Agency takes up this recommendation and, based on this, publishes an overview of the appropriate algorithms, key lengths and their validity periods. Thus, up to 31. 12.2007, the algorithm SHA1 and the key length RSA1024 were valid and permissible for qualified signatures and time stamps. Currently, among others, the algorithm SHA256 and the key length RSA2048 are classified as valid and secure.

These algorithms and key lengths are to be used to generate legally compliant qualified signatures and time stamps in accordance with the German Digital Signature Act.

In so far as algorithms and/or key lengths are classified as no longer sufficiently secure, data which has already been signed needs to be resigned or oversigned. In accordance with the Digital Signature Regulations,[13] qualified time stamps have to be used for this. Fig. 1 shows an example in which forgery possibilities occur through the weakening of the hash algorithm or the key length. These forgery possibilities are eliminated by means of re-signing using a qualified time stamp.

---

[13] See § 17 SigV
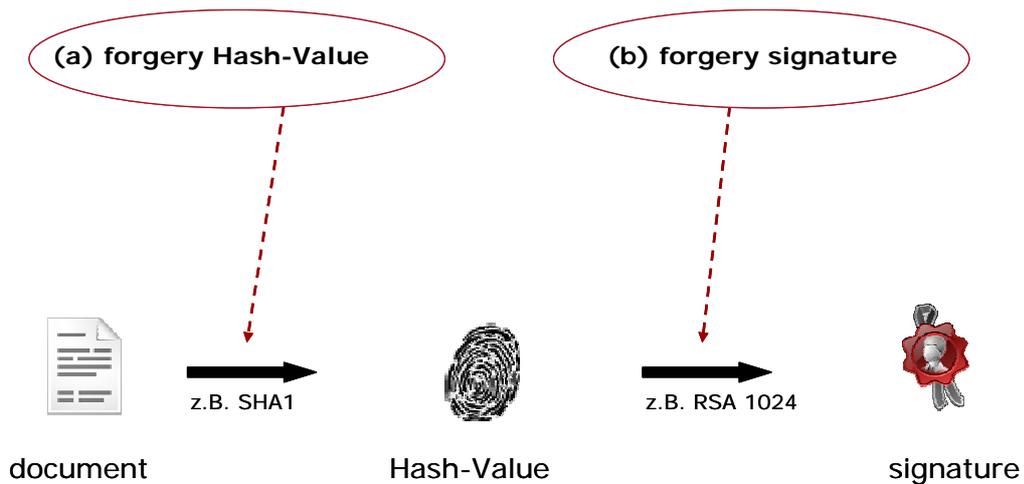
Fig. 1 – Example presentation: forgery possibilities due to weakening of the hash-algorithm and key length

Which data has to be resigned and which methods can be applied depends on whether only the key lengths become insecure or whether key lengths and hash algorithm are both insecure.

In the past, different methods for re-signing developed. Alongside the statutory requirement, the choice of method often depends on the requirements of the archive system employed by the user.

In assessing the different methods, besides the economic aspect, the technical implementation is also a major factor for consideration. Thus, it is imperative that a method for re-signing protects not only the key length (RSA1024, RSA2048), but also the hash algorithm (SHA1, SHA256, SHA512). Methods that only take one aspect into account are therefore not advisable. With such solutions, the future work of re-signing can rapidly become inestimable.

As an example, fig. 2 sketches a method in which the probative value of signed data is kept legally compliant by means of re-signing using a qualified time stamp from an accredited trust centre, both when changing the hash-algorithm, and also the key length.
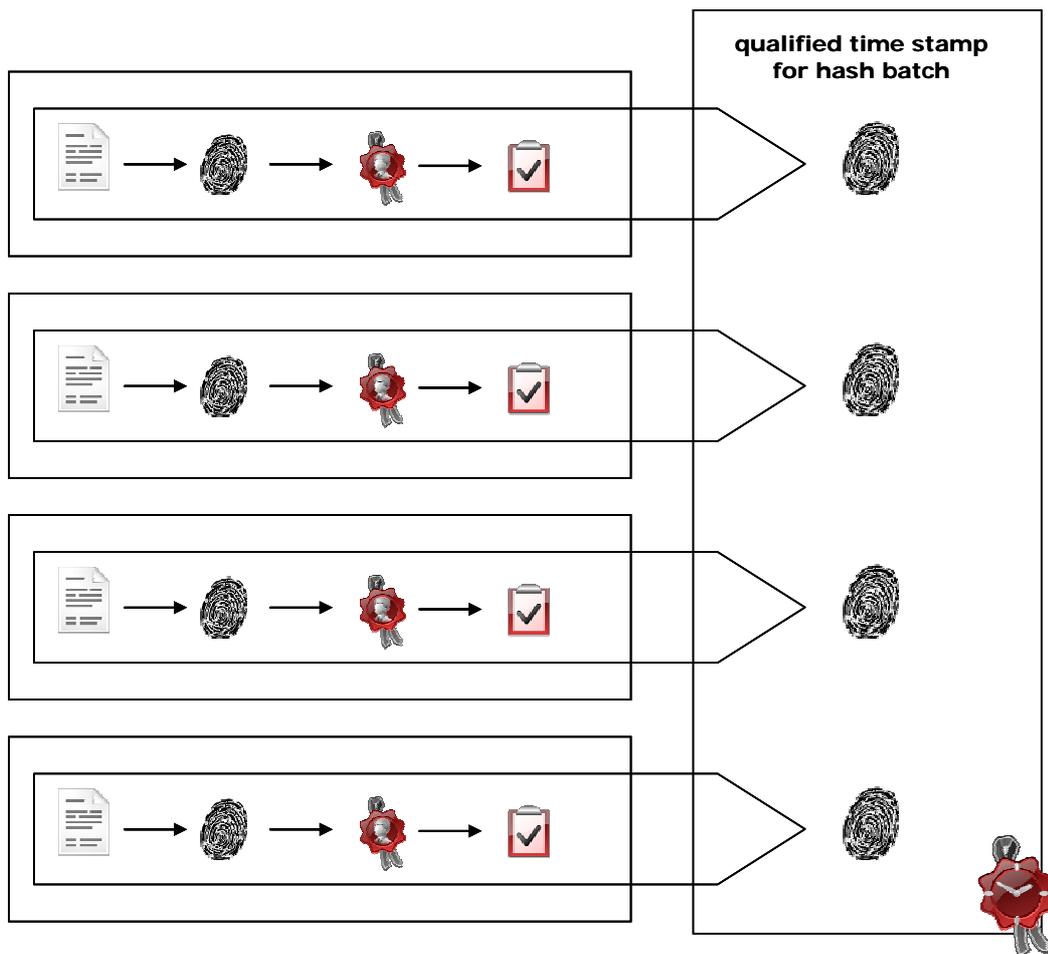
Fig. 2 – Example presentation of re-signing using the batch method

By forming groups or batches, at the same time, the number of qualified time stamps can be greatly reduced.

Such methods were already successfully put into practice at the end of 2007 when the hash-algorithm and the key lengths were changed. In this way, the probative value of many millions of signed data records was very efficiently secured using comparatively few qualified time stamps.

8. International aspects

Hardly any business processes in today's world can be carried out on a purely national level. It is therefore essential that electronic business processes are also oriented around internationally recognised framework conditions.

The German Digital Signature Act in the version of May 2001 implemented the international framework conditions of the EU Digital Signature Directive (2001/115/EG) of December 1999 in national law. Qualified signatures and time stamps which comply with the strict requirements of the German Digital Signature Act therefore also fulfil the requirements of the EU Digital Signature Directive. Electronically signed or time-stamped data can thus also be used as evidence in the international field.

In non-EU countries, e.g. Switzerland, separate regulations apply, but many can be implemented using the technologies available in Germany. The same applies to the U.S.A. Here, the ESIGN Act and the framework conditions of the American Bar Association (ABA) form the necessary foundations for signatures and time stamps.

9.   About AuthentiDate

AuthentiDate International AG
(with its registered office in Germany, Düsseldorf) was accredited in November 2001 by the German Federal Network Agency (formerly the German Regulatory Authority for Telecommunications and Post) as the first accredited certification provider focusing on qualified time stamps in compliance with the new German Signature Act and European Directives. The time stamps supplied by AuthentiDate International AG thus offer the very highest legally recognised protection for all electronic data in the form of qualified electronic signatures with provider accreditation.
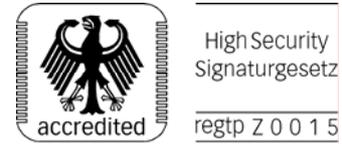
Qualified time stamps from AuthentiDate International AG also fulfil the requirements of the EU Digital Signature Directive. They can therefore also be used internationally for legally secure electronic processes.

AuthentiDate Deutschland GmbH, a wholly-owned subsidiary of AuthentiDate International AG, provides and develops standalone, manufacturer-independent software solutions for the integration of time stamps and personal signatures in all kinds of business processes. Here, both qualified and advanced signatures and time stamps can be used.

Internationally leading
AuthentiDate products are used by medium-sized companies and groups in practically every sector. All technologies are also available as services. This means that signature and time stamp services can be fully outsourced on request.

AuthentiDate has also contributed its expertise in the area of qualified time stamps in setting up time stamp services outside of the EU; for example an accredited time stamp service has been set up and realised in Switzerland using AuthentiDate products.

Inventor of the mass signature
AuthentiDate is the inventor of the central, qualified mass signature, and has established this solution internationally, for example in the context of electronic invoicing.

As a pioneer on the signatures market, the company set up the first signature verification service available worldwide. It is multilingual, user-friendly and can be used around the clock, 365 days a year, anywhere in the world, without any additional software.

More than half of the statutory health insurance companies in Germany use AuthentiDate signature solutions to digitize and archive payment-

related documents. Almost all the common DMS, archive and scan providers have integrated the AuthentiDate signature products as standard.

Globally unique & legally compliant
All AuthentiDate signature products meet the strict requirements of the German Digital Signature Act, the EU-Digital Signature Directive and US-American guidelines.

The AuthentiDate signature technology is globally unique. The wholly operating system-independent, legally compliant, future-oriented SOA (Software Oriented Architecture) and SaaS (Software as a Service) architecture enables the first distributed client-server signature processes. The flexible JAVA architecture enables the mapping of all current and future cards and standards, such as eCard API from the BSI, eHealth/eGK formats and processes, ERS and long-term archiving.

AuthentiDate is the specialist for:

- Qualified & advanced signatures
- Qualified & other time stamps
- Organisation certificates
- Simple, luxury, stacking & mass signatures
- Signature client components
- Web services (software as a service)
- Certified signature products
- Signature products for service providers & system providers

Further information under www.authentidate.de

10.　List of abbreviations

Fig.	-	figure
AG	-	Aktiengesellschaft – joint stock company
BNetzA	-	Bundesnetzagentur - Federal Network Agency
EU	-	European
GmbH	-	Gesellschaft mit beschränkter Haftung – private limited company
SAC	-	signature application component
SSGU	-	secure signature generation unit
SigG	-	Digital Signature Act
SigV	-	Digital Signature Regulations
Tab.	-	table
e.g	-	for example
CSP	-	certification service provider
TS	-	time stamp

11.　Glossary

Accreditation
Term used in conjunction with the Digital Signature Act to designate a certification service provider which provides its services in accordance with the provisions of the Digital Signature Act and Digital Signature Regulations and undergoes corresponding verification by the Federal Network Agency (BNetzA). (See also "certification service providers")

Authenticity
The proof of authenticity of electronic data designates proof that the data is genuine (see also "integrity") and the unambiguous assignment to author, generator and/or sender.

Batch
The compilation and combined processing of several data records.

Client
Computer at an individual workstation which can access software and data which is centrally available at another point in the company (e.g. on a central server, archive systems etc.).

Common PKI

Common PKI is a common specification from the association TeleTrusT and the T7 group for electronic signatures, encryption and PKI. The main objective is, by means of Common PKI, to generate the conditions for international standardisation and interoperability for applications in the areas stated. Until recently, Common PKI was termed ISIS-MTT.

CRL
Abbreviation for the English term: Certificate Revocation List
List generated and published by the "certification service provider" and which shows which certificates which have been blocked (revoked) by the certificate holder.

Electronic signature
In common parlance also frequently termed "digital signature". Designation from the German Digital Signature Act and the EU Digital Signature Directive. An electronic signature is comparable with an electronic autograph[14]. It is generated through the use of "private keys". The process for generation of an electronic signature can be portrayed in simplified terms as follows: by using a certain mathematic algorithm, a "HASH value" is established for the data to be signed. This "HASH value" is encrypted using a "private key". The corresponding "public key" is issued in the form of a "certificate" which also includes information on the originator of the signature. The encryption of the "HASH value" in conjunction with the corresponding certificate is termed an electronic signature. All these processes run automatically through corresponding software programs.
See also "advanced signature" and "qualified signature"

Decryption
Process which uses mathematical algorithms and "private keys" to make electronic data readable and processable again. In its encrypted form, the data cannot be accessed or amended by unauthorised third parties. The data can only be returned to its original form by the owner of the corresponding "private key".

Finger print
Often used as a synonym for "HASH value".

Advanced signature
An "advanced signature" is a signature which is generated with the aid of "advanced certificates". Data with an advanced signature – as against data with a qualified signature – is not legally secure.

---

[14] Translator's note: the German text differentiates between "Signatur" and "Unterschrift". This distinction is difficult in English, as we only have one common term: signature.

Secret key
See "private key"

Hash value
Mathematic value (check sum) generated from an electronic file by applying an arithmetic operation (mathematic algorithm). A hash value maps a clear link to the electronic original. Furthermore, a hash value cannot be used to reconstruct the underlying file. In general, for his purpose, hash algorithms are used which have been approved by the Federal Network Agency (BNetzA) and classified as secure (e.g. SHA-512, RSA 2048)

HSM
Abbreviation for the English term: Hardware-Security-Module
An HSM is hardware which allows the cryptographic key to be kept in a particularly secure form. In addition, the hardware also enables the use in more complex applications, e.g. as a server. An HSM is comparable with an oversized smart card, which can also take on other functions alongside the storage of the private and public keys.

Integrity
The proof of integrity of electronic data refers to the proof that this is complete and unaltered.

ISIS-MTT
Previous designation for Common PKI. See Common PKI.

JAVA
Programming language which enables high flexibility and interoperability. With the aid of JAVA, e.g. applications can be developed which, through the use of a virtual machine, are capable of running independently of the operating system and Internet browser.

Public key
The part of a pair of cryptographic keys which is publicly known and freely accessible. The public key is also used to encrypt data and pass it on to a certain person in encoded form. Only this person can then decode the data using the corresponding "private key" known only to him.
See also "private key"

OCSP query
OCSP is the abbreviation for the English term: Online Certificate Status Protocol

Possibility for querying the status of certificates. By using this online query, it is possible to check e.g. whether a certificate has been blocked by the user or has expired.

PGP

Abbreviation for the English term: Pretty Good Privacy
Program for encryption/signature of data using "public" and "private keys" on the basis of a "Web of Trust", i.e. mutual recommendation of the trustworthiness of a participant. PGP certificates are therefore not issued by accredited certification service providers and therefore do not provide any possibility for generating legally secure signatures in accordance with the German Digital Signature Act.

PKCS

Abbreviation for the English term: Public Key Cryptography Standards
Designation for various industrial standards (e.g. PKCS#6, PKCS#7 etc.) which have become well established on the general market.

PKI

Abbreviation for the English term: Public Key Infrastructure
Technical infrastructure which enables asymmetric cryptographic technologies to be launched and operated in companies. Here the corresponding cryptographic keys (see also "private key" and "public key") are also employed. PKI solutions typically include components for the application, generation, administration, roll out and operation of certificate-based infrastructures on the basis of asymmetrical keys. Application fields for PKI-based solutions are the "electronic signature" and "encrypting/decrypting" of electronic documents.

Private key

The part of a cryptographic pair of keys which is only known to or accessible to the person who generates a signature and thus electronically signs electronic data. The private key is also used to make encrypted data intended only for one certain person, capable of decryption by that person.
See also "public key"

Qualified signature

A qualified signature is an "electronic signature" generated on the basis of a qualified "certificate". If the qualified "certificate" originates from an accredited "certification service provider", and if a secure "signature generation unit" is used for its generation, electronic data signed using the qualified signature is legally secure.
See also "advanced signature"

Signature

See "electronic signature"

Signature application component

For the generation of a qualified signature, suitable signature software is required. This is termed a signature application component (SAC). So that the qualified signature is legally secure and thus equivalent to the hand-written signature, the SAC has to meet the requirements of the Digital Signature Act and the Digital Signature Regulations. This proof of the quality of the SAC can e.g. be furnished by validating the SAC in accordance with the Digital Signature Act (SigG validation).

Signature generation unit

Along with the signature software, suitable hardware is also required for the production of legally compliant, qualified signatures. I.e. both the signature card (smart card), and the card reader used have to meet the requirements of the Digital Signature Act and the Digital Signature Regulations. This can also be demonstrated by means of validation in accordance with the Digital Signature Act (SigG validation).

Signature verification

The signature verification includes two different verification procedures or kinds of verification. These are mathematic verification ("integrity") and the verification of the certificates ("authenticity" and validity). For the mathematical verification, corresponding software is used to check that the hash value of the document signed matches the hash value of the signature corresponding to the document and that the signed document was therefore not modified after generation of the signature. For the verification of the certificate, corresponding software is also used to establish whether the certificate was valid at the time of the signature generation, and the quality of the signature ("advanced", "qualified") is also determined.

Smart card

"Signature generation unit" that serves to store certificates securely in the form of a chip card.

SSL

Abbreviation for the English term: Secure Sockets Layer
Possibility for secure and encrypted communication via the Internet by exchanging certificates using a certain transmission protocol. Frequently used in the communication of a single computer via the Internet with a server, e.g. for banking transactions.

Trust centre

In conjunction with the Digital Signature Act, the term trust centre designates a trust-worthy agency which normally offers services in accordance with the strict requirements of the Digital Signature Act and the Digital Signature Regulations such as e.g. issuing certificates, issuing qualified time stamps, providing information on the status of certificates.

Encryption

Technical procedure which uses "public keys" and "private keys" to protect electronic data. The encryption protects the data against third party access and manipulation.
(See also "PKI")

X.509

Standard format for certificates on the basis of asymmetrical cryptographic procedures.

Time stamp

"Special form" of the electronic signature. Electronic certificate showing that the data signed with the time stamp existed in the form signed at the time/date of signing. The time stamp in accordance with the Digital Signature Act freezes the data making it legally secure.

Certificate

There is a distinction between software-based certificates and hardware-based certificates.
If a certificate is issued as a software certificate, the private and public keys are installed directly as software on a computer. Signatures issued with the software-based certificates cannot generate legally secure electronic data.
If a certificate is issued as a hardware-based certificate, the necessary keys are provided on hardware, e.g. in the form of a smart card. If the certificates or the smart card are issued by an accredited "certification service", "qualified signatures" can also be generated using the qualified certificates contained on it. In this way, these certificates can also be used to generate legally secure electronic data.

Certification service provider

A provider that operates a service in accordance with the German Digital Signature Act (and Digital Signature Regulations) and the EU Digital Signature Directive. Services are offered such as e.g. issuing certificates, issuing qualified time stamps, providing information on the status of certificates.

12. Legal disclaimer

The present white paper contains exclusively non-binding technical and legal information. Errors excepted. Binding technical statements on the individual products specified in this document are to be taken exclusively from the respective product specifications.

AuthentiDate is not liable for the up-to-dateness, correctness, completeness or quality of the information contained in this document. Liability claims based on damages of a material or immaterial nature caused by use or disuse of the information presented here or through the use of erroneous and incomplete information are fundamentally excluded.

Legal statements are on no account binding. In case of deviations to contractual documents relating to this document or AuthentiDate's general terms and conditions, the contractual documents or AuthentiDate's general terms and conditions always have priority over this document.