SAPERION whitepaper

Electronic Signature

This white paper essentially describes and deals with the following points:

The challenge

+ In the course of increasing electronic communication, electronic signatures are becoming more attractive. Great potential savings can also be achieved by switching from paper-based over to fully electronically processed business processes, avoiding media interruptions.

The solution: the content of this white paper

+ Part 1: the first part of this white paper deals with the basics of the electronic signature. In addition to the differences between the simple, advanced and qualified electronic signature, the legal conditions will also be looked into, as well as time stamp signatures. The potential for savings is explained on the basis of typical applications such as electronic invoices or company-internal release processes. The basics will be rounded off with the criteria for the procurement of components such as chip cards, card-reading devices and signature application software for the case of qualified signatures, the responsibility of the Bundesnetzagentur (the federal network agency) for regulations to do with German law on signatures and the use of biometric processes. Subjects such as interoperability of components from various manufacturers and re-signing in the context of weakening signatures for long-term archiving are also dealt with.
+ Part 2: The second part focuses upon the signature functions implemented in SAPERION for the different application functions; such as batch signing as a confirmation of the correct format transition of the paper document into the electronic image upon scanning, the automated verification of signed documents when importing to SAPERION, or the signing of individual documents during release into a workflow. SAPERION has integrated the signature application components of the partners AuthentiDate AG and secrypt GmbH. The individual functions are compared in tables, for deciding which of the two products is the right one for the specific case. Finally, we look at the application of the signature solution from the company signotec GmbH, which uses biometrics-based, advanced signatures.

The authors

+ The author Dr. Martin Bartonitz has been dealing with the subject of business process management since 1992. Since 2004, he has been the Product Manager responsible for the subjects of workflow, signatures and in-bound messages at SAPERION AG.
+ The author Sascha Windisch has been dealing with the subject of documentation management since 1997. He has worked for three years at one of the leading manufacturers of signature applications and is currently senior Consultant at the SAPERION partner maxence GmbH.

Content

Introduction

Electronic signature as signature of electronic documents

Aims Of Electronic Signature

The aim of electronic signature is the availability of an electronic counterpart to the signature from one's own hand on a paper document in the case of an electronic document. This requires the technological means as well as a legal basis and the organisational framework arising from these. In 1993, the European Parliament ratified a directive with common conditions for electronic signatures, which was last amended in 1999. In Germany, this directive was first implemented in 1997 via the signature law (SigG) and a further signature ordinance (SigV) that added details. Following this, more than 2,000 passages were adjusted in the most varied of legal texts in order to bring manual signatures in line with the electronic ones. Supplementing the written form, which continues to mean the document in paper form, the text form has been introduced; i.e. in the cases where the text form is permitted, a document can also be electronically signed.

Advantages Of The Electronic Signature

Advantages:

+ avoidance of interruption in media
+ electronically signed documents can be sent directly by e-mail
+ reduction of costs by up to 72%

The major advantage in the use of the electronic signature lies in the avoidance of the media break that is necessary in the handling of business processes, if the electronic document is printed for the purpose of a manual signature and if necessary then scanned and stored in an electronic archive. If electronic documents are signed electronically then they can also be sent directly by e-mail in this form; both the sender and recipient can here reduce costs enormously, by on the one hand doing without enveloping and postage, and on the other hand being able to dispense with the electronic document gathering with the capturing of index data. A study on behalf of the EU Commission ("Study on the requirements imposed by the Member States, for the purpose of changing taxes, for invoices produced by electronic or other means") showed in 1999 that in the specific case of invoice handling 72% of the costs can be saved.

Fig. 1: Chip-card for the production of the electronic signature.

Fig. 2: class 3 card-reading device with inserted chip-card

Because an electronic document can be easily altered without this being noticed, in comparison with a paper document, particular precautions must be taken. These measures ensure that the text set (message) has not been altered or tampered with since its signature (integrity), that authenticity can be ascertained at any time and that the declaration of will cannot be disavowed (non-repudiation).

In a nutshell, the technology of the electronic signature creates the necessary trust between two business partners for exchanging electronic documents.

Forms Of The Electronic Signature

Three forms of electronic signature: simple, advanced & qualified electronic signature

Due to the variation in the degree of trust that is necessary for electronic documents, three forms of signature are anchored in German taxation law:

+ simple electronic signature
+ advanced electronic signature
+ qualified electronic signature

Simple Electronic Signatures

Simple signature:

solely information on the sender

The simple signature is purely information about a consignor e.g. the typical signature at the end of an e-mail. It is entirely permissible for a scanned-in signature to be used for this. This form of signature has only very slight conclusiveness in Germany, but in the USA it is mostly sufficient in many cases.

Advanced Electronic Signature

Advanced signature:

cryptographic software process with a key pair

The advanced signature offers greater conclusiveness due to the cryptographic software process used with a pair of keys. German partners can agree on this form of signature for the exchanging of the majority of business documents (about 95%). The signature here is in the form of a signature file accompanying the document. This signature file is produced by means of the private key of the signatory together with a certificate identifying him. In most cases, the recipient has already received the certificate before and can check whether the document has arrived with its integrity intact and whether the sender was really the person who signed it.

The key pair can also be used for the encryption of the message before sending. The sender encodes the message with the public key given to him by the recipient. The recipient decodes the message with his private key, i.e. only he can read the message.

The key pair can be produced with free software packages. For safety, the certificate should be handed over at a private meeting together with the public key. There is a range of certificate providers who offer software certificates free of charge for e-mail sending and which can check the identity of a certificate holder several times via a so-called network of trust by means of solicitors, e.g. Thawte.

Qualified Electronic Signatures

Qualified signature:

is produced with hardware and software components on the basis of a certificate which is issued by a CSP.

Unlike the advanced signature, the qualified signature must be produced by means of particular hardware (chip-cards and reading device) and software as well as a certificate from a reliable authority, a certificate service provider (CSP). The certificate service providers make available the necessary certificates per person and deliver these together with the personal chip-card. A distinction is also made between accredited and non-accredited providers. The accredited providers ensure a 30-year safekeeping of the certificates instead of 5 years. In the case of a change in service provider, the Bundesnetzagentur, as the highest certification authority in Germany, takes care of the changeover.

As the private key only exists once and that is in the form of hardware-based coding on the chip-card, this key pair is not suitable for exchanging encoded e-mails. If the card is lost, the encoded e-mails can no longer be decoded.

Due to the very high requirements made of the components to be used and the processes for the production of the certificates, qualified signed documents have the highest conclusiveness. The code of civil procedure regards signatures signed in this way as prima facie evidence, i.e. the judge must acknowledge the document as evidence, if there is no serious doubt that the declaration was made by the owner of the signature key (§ 371a ZPO [German Code of Civil Procedure]).

In addition to the signatures with the person-specific certificates, there is also the qualified time-stamp. While the person-specific signatures settle the matter of "Who has what?", the time stamps settle the matter of "What was produced when."

Person-specific signatures: by means of a chip-card reader connected to the local computer

Time Stamp For The Settling Of The Point In Time Of The Signature

Person-specific signing with the chip-card is carried out at the local computer of the signatory by means of the connected chip-card reader. The time used here is the one set on the computer, i.e. there is possibly a gap in security here. The recipient cannot recognise whether or not the signatory has worked on a computer that had the correct time set. One cannot assume that the document was signed by an employee of a firm that makes sure that the times set on the computers cannot be manipulated. It is thus not ensured that the signing took place in the period of validity of the certificate. To make sure of the time, it is therefore sensible to also embed a qualified time stamp in the signature at the same time. This time stamp is requested over the Internet by a time stamp service that "qualifiedly" ensures the correct time.

Documents requiring The Written Form

There is a range of documents for which the written form (paper and manual signature) continues to be obligatory. Here are some examples:

+ consumer loan contracts (§492 para. 1 clause 2 BGB)
+ termination of employment relationship (§623 BGB)
+ granting of a work reference (§630 clause 3 BGB)
+ certificate of bond (§766 clause 2 BGB)
+ promissory note (§780 BGB)
+ acknowledgement of debt (§781 BGB)

if notarial certification or authentication is required, the electronic form is insufficient (e.g. property transactions).

Factors Promoting The Signature Market

The market for qualified signatures is growing – the general spread is being encouraged by a number of important projects.

Even if the European signature directive was ratified in 1993, it must now be stated that the market for qualified signatures still continues to have difficulties. Reasons given frequently for this are the complexity of the process and the acquisition costs. This is still certainly true of private use. In addition, private individuals buy what they can use frequently. This situation is unfortunately not yet sufficient. There are now, however, a number of important projects that will lead to a general spreading of the use of this technology in the private sphere in Germany as well. The most interesting are listed below. Some of these have already been implemented, and others will soon lead to the spread of signature cards.

Laws And Ordinance

There are now a number of ordinances that either stipulate the use of qualified electronic signatures, e.g. if the safekeeping of paper after scanning is to be avoided.

In the following, it is intended to discuss the most important, including laws and ordinances promoting the signature market.

+ § 14 para. 3 turnover tax law

This law stipulates the use of a qualified signature if an invoice is exchanged electronically and the pre-tax is to be deducted. The sender must have the agreement of the recipient. Toleration is also sufficient.

+ Ordinance for the alteration of the law on local authority cash of 12th May 2003 (Nds.GVBl. p. 193) Lower Saxony (similar in other federal states of Germany)

This ordinance stipulates the use of the qualified signature for the releasing of so-called electronic invoices.

+ §110b judicial communication law (JKomG) – electronic document-keeping and §110a of the code of social law (SGB) and § 36 of the Administrative Procedure Act.

These laws permit the destruction of scanned documents if these have been qualifiedly signed, immediately after being scanned, with the annotation that the scanned document corresponds to the one on the screen.

+ §3a Administrative Procedure Act (VwVfG) and §36a of the code of social law (SGB).

These laws permit electronic communication with others if the documents have been qualifiedly signed.

+ The amendment to the Law on Waste Recovery and Disposal Records (NachwV) concerning the Recycling and Waste management Law (KrW-/AbfG).

The ordinance stipulates an electronic authentication procedure (eANV) that is as far as possible paper-free, using qualified electronic signatures (NachwV, paragraph 4). This electronic verification management is obligatory for the documentation of the disposal of wastes that require particular monitoring (materials that will be hazardous). From February 2010, the waste disposal companies, waste producers and transporters must keep all documents electronically and also sign them with a qualified electronic signature. Insiders are assuming that this procedure will in future be extended to all other sorts of waste.

Examples Of Signature Applications For Private Individuals

Purchasing the infrastructure will become more worthwhile with the growth in the possible applications of electronic signatures.

The more applications exist for the use of electronic signatures, the more worthwhile it will become to purchase the necessary infrastructure. The introduction of electronic signatures is frequently compared with the introduction of the telephone in Germany. It took 20 years before there were more than 100 telephones in operation. Afterwards the number increased rapidly. That is why it is important to look at the applications and components that are already available in order to assess readiness for the market.

+ The money card (account-dependent as well as account-independent) is prepared for the use of the electronic signature.
+ ELSTER - the electronic exchanging of tax data in the tax office was originally designed for the use of the qualified signature. A form of the advanced signature is now also permitted.
+ The E-service of the German annuity insurance offers the option of direct access to one's own annuity account by means of the signature card, in order e.g. to call important planning data for additional private retirement provision.
+ The electronic health card (eGK), which was already to have been introduced in 2006, and is currently only undergoing the first trial test, is prepared for the use of the electronic signature. Among other uses, doctors should be able to sign prescriptions using this card.
+ The electronic personal identification that is to be introduced in October 2008, is prepared for the use of the electronic signature.
+ The job card that every unemployed person will in future receive for the purpose of quicker processing, will be prepared for the use of the electronic signature.

Details Of The Signature Process

This chapter describes the processes of signing for the two types of qualified signature, the person-specific signature with a personal certificate and the time stamp, as well as everything worth knowing about qualified signatures.

Person-Specific Signatures

Signing requires a chip-card with the personal key and the certificate identifying the signatory, a certified card- reading device of at least class 3 with drivers and a piece of software that calls up the signature routines on the chip via the card-reading device. The process of signing is as follows:

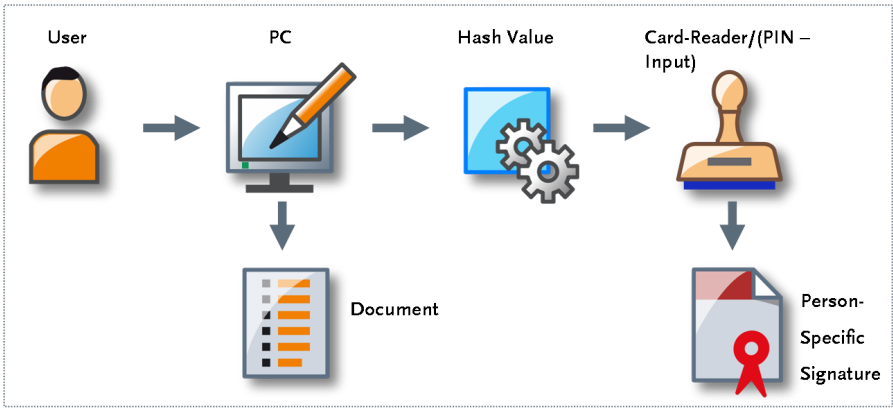

Fig. 3: Signing with the chip-card

The user calls the signing via a function in his application or via a context menu in the file explorer. The software here receives the document and thus forms a so-called fingerprint of the document. Technically, this is a hash value taking up a few bytes. This fingerprint is sent to the chip via the card-reading device. The user is then asked to enter his 6-figure PIN. If this is successfully carried out, the chip encodes the hash value by means of the personal key on the card. On the card there is also the certificate of the user, which is now sent back to the software together with the encoded hash value. This data is then written into a so-called signature container (format is CMS or PKCS#7) together with the information of the system time of the computer.

This container

+ can either be made available as an accompanying (escorting) additional file or
+ the document itself is entered into the container
+ it is itself integrated into the document (e.g. with PDF and TIFF formats).

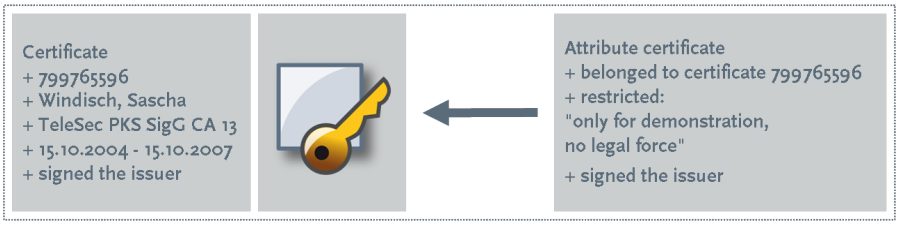

Fig. 4: Certificate and optional attribute certificate

The certificate contains the public key, the serial number, the name of the key owner, the name of the issuer of the certificate, and the valid areas of its use and is itself electronically signed by the issuer. In addition, an attribute certificate supplementing the certificate can be installed on the card, if the legal transactions to be carried out are to be restricted. This information is kept in the standard format X509v3 and/or RFC 3280 respectively.

Signing equipment

+ chip-card with personal key
+ certificate identifying the signatory
+ card-reading device of at least class 3 with driver and software

Contents of a certificate:

+ public key
+ series number
+ name of the key owner
+ valid area of use
+ signed by the issuer himself

The card-reading device being used must have had its compliance with § 3 of the signature law confirmed by the Bundesnetzagentur and correspond to at least class 2 (secured number block). Class 3 also has a small display, via which the device can communicate with the user regarding his use.

BNetzA confirms the certificates of the certificate service providers with the root certificate.

The Bundesnetzagentur, BNetzA for short, is the authority responsible for control of and adherence to the rules anchored in the German signature law and its accompanying signature ordinance. With its root certificate, it confirms the certificates of the certificate service providers, which in turn, by means of its certificate, confirms the certificates it issues to people (certification chain).

A confirmed manufacturer clearance must be published on the web site of the BNetzA for the software being used, the so-called signature application. Signature applications that are certified in accordance with "common criteria" - common criteria for the checking and evaluation of the security of information technology - of the Federal Office for Information Security (BSI) offer the highest degree of security.

The securing of the personal signature with a card together with a PIN follows the principle of "possession and knowledge". The personal key for signing only exists on the chip card that is in the individual's personal possession and only the owner himself knows the PIN. When the PIN is entered, which is once again explicitly requested on the screen or on the display of the card-reading device, there is the typical pause before the declaration of intent, as also occurs with a manual signature. This pause gives time to consider whether to really make this declaration of intent, and thereby supports the non-repudiation of the signature, to the benefit of the recipient of the paper, which then also builds up the necessary "trust" in the transaction.

The costs for acquiring a chip-card including the signature application are about 230 to EUR 200 for private use, and about EUR 250 to 300 per workplace for occupational use. In the case of batch signing, as in the case of outgoing invoices, corresponding server software is necessary, which starts at about EUR 2,000 and is even to be found in the lower 5-figure range with increasing requirements regarding quantity and processing.

Time Stamp

The user frequently produces time stamp signatures in the background of the workflow without noticing it.

The process of signing with a qualified time stamp is mostly performed automatically in the background in a workflow, so that the user himself does not notice it. For example, incoming and outgoing fax documents are often time-stamped.

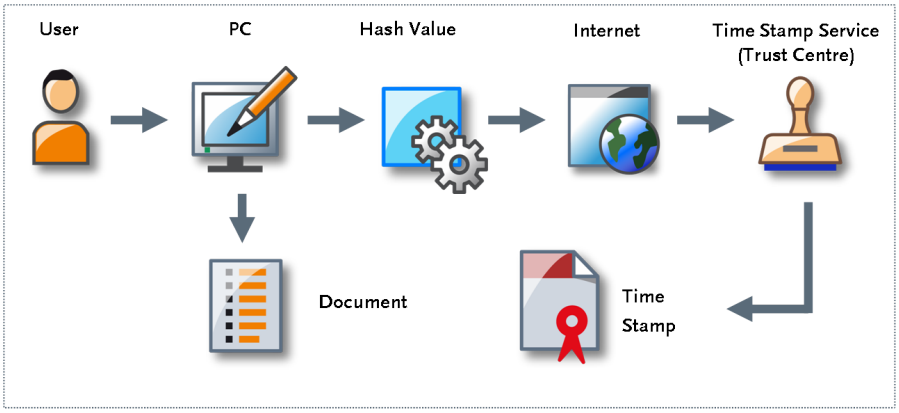

Fig. 5: signing using a time stamp over the Internet

As with the person-specific signature, the signature application produces a fingerprint (hash value) for the document. This is now sent via the Internet to the time-stamp service of a certification service provider (trust centre), which encodes the hash value using a chip-card (parallel operation with several cards), adds the information on the precise point in time in the already-mentioned signature container, and sends it back.

The costs of a time stamp are between 3 to 30 cents per signature depending on the quantity.

Biometric Signatures

Biometric signature process: globally more frequently used, still "only" classed as advanced in Germany.

The so-called signatures based on biometric values are taking on an exceptional status in Germany. Whereas these processes are used substantially more, all over the world, they are still insufficiently anchored in law in Germany. They are not explicitly dealt with in the German signature law and thus do not attain the highest authority as regards conclusiveness, i.e. they are "only" advanced signatures.

Biometric signatures are produced by encoding the hash value with measurable personal characteristics of the initiator. That could be features of thumbprints or of the iris of the eye. The signature is considerably more frequently made with a so-called pen pad, that is known to those who have accepted a parcel from DHL or UPS.

In addition to the writing, the pen pads also record the speed, acceleration and pressure. It is virtually impossible to forge a signature.

Unfortunately, there are not yet any standards at all regarding the storage of the characteristics or necessary, accredited safe-keepers of the original signatures for the purpose of online verification, so this process will not be permissible for qualified use even in the medium-term future. It is, however, to be expected that they will in Germany at least be recognised as advanced signatures. The competence centre for electronic signatures within the VOI (association for organisational and information systems) is currently making efforts to get an appropriate amendment made to the signature law.

Verification Of Qualifiedly Signed Documents

Verification is for information about the integrity of the document, authorship and date of the signature.

The verification of a signed document has the task of giving information about the current integrity of the document, about the originator and the date of the signature, and about whether or not the certificate being used was still valid at the time of the signature and was not blocked.

The verification itself usually takes place in several stages. First of all, the integrity of the signature container itself is checked. Then the integrity of the document is ascertained. In this procedure, the encoded hash value is decoded by means of the public key contained in the signature container, and compared with the newly calculated hash value (same algorithm) of the document. If both are the same, the document has not been altered.

The originator is then ascertained. From the next step, it is necessary to make direct enquiries with the certification service provider responsible for the certificate being used, i.e. access to the Internet is required. It is now checked whether or not the certificate is known, and that the certificate was not blocked at the time of signing. As a final check, the correctness of the certificate chain is checked according to the chain model (Microsoft applications check e.g. according to the shell model).

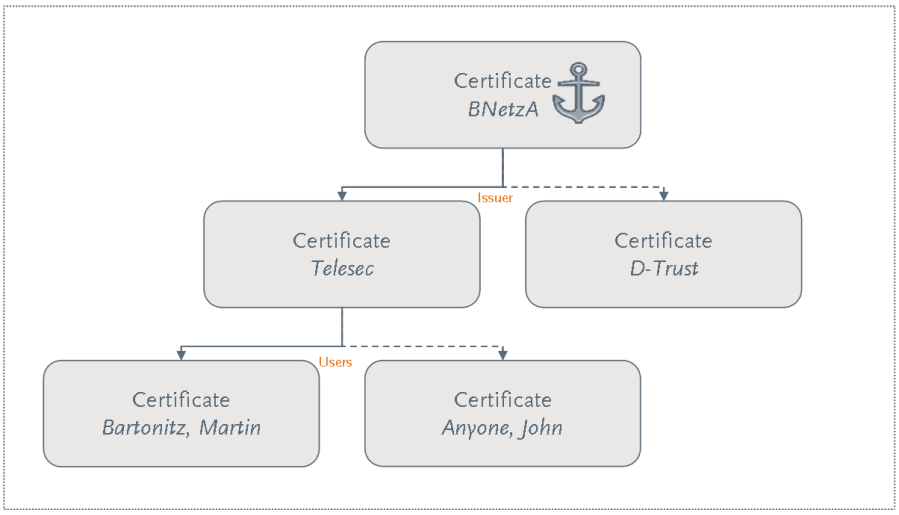

Fig. 6: hierarchical presentation of a certificate chain

Stages of verification:

+ integrity check of the signature container
+ ascertaining of the document's integrity
+ ascertaining of the originator
+ check that the certificate is known
+ checking that signature is in area of validity
+ checking of the certificate chain

The graphic above shows a certificate chain. In Germany there are mostly only three levels from the root instance of the Bundesnetzagentur to the user, here Martin Anyone, via one of the certificate services providers, here Telesec.

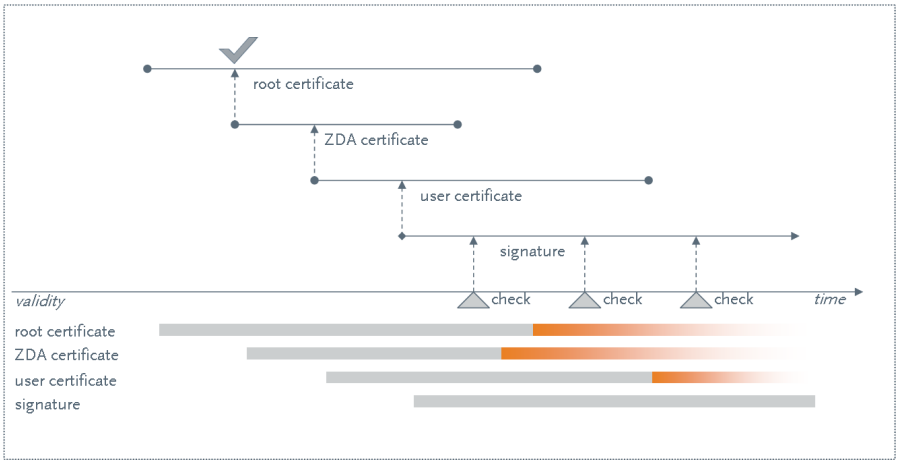

Fig. 7: Verification according to the chain model (German signature law)

To check whether the signature is valid, a check is made according to the chain model at every checking interval, to see whether the user certificate was valid at the time of the signature, whether the CSP certificate was valid at the time that the user certificate was issued and whether the root certificate was valid at the time that the CSP certificate was issued.

When the shell model is used, a signature already loses its validity as soon as one of the validity times of one of the certificates involved is reached at the time of signing.

The enquiries to the certificate service provider are made via a so-called OCSP Request. An OCSP response comes back. Most signature applications enter the data of the OCSP responses and all further verification results into an XML file or into a PDF/A formatted file that is easier for lay people to read, and send this back as a total result. OCSP here stands for Online Certificate Status Protocol, which itself adds the http protocol.

Things Worth Knowing About The Chip Card

Requesting A Chip Card

Post-identification procedure for ascertaining the identity of the person who requested a chip-card

If a person requests a chip card with a qualified signature, the certificate service provider must make sure that the person is also the one that he says he is. During the first few years, it was necessary to appear in person at specially set-up registration offices for this. The application was made there upon the presentation of personal identification. Because this procedure was too awkward and thus hindered the acceptance of electronic signatures, it has now been replaced by the post-identification process. In this, the application is either made directly electronically, or sent in on paper. The identity of the person is ascertained by a postal official at a selected post-office counter.

If a card is requested for several employees in a company then it is practical to have a representative of a CSP come who supports the application and also confirms the identity straight away on the spot. The D-trust is now in the position to carry out the issuing of cards on the spot.

Duration Of Validity Of A Qualified Certificate

Electronic signatures outside the validity period of the certificate are not legally valid

The certificate issued for a person by the certificate service provider is located on the chip of the signature card. The certificate shows the name of the person as well as the duration of the card's validity. If an electronic signature has been produced outside this period of validity, then it has no legal force.

Restriction Of Use

The certificate can also contain a restriction, e.g. "The cardholder is only authorised to sign invoices up to the amount of 1,000 EURO." If a higher amount is shown on the document, then the signature is not legally valid in this case either.

Security Measures Upon The Loss Of The Chip Card - Blocking

Certificates can be restricted

The chip card is especially protected for the eventuality of loss, provided the Pin for it has not also been stolen. The chip self-destructs if the incorrect PIN is entered three times in a row.

Chip self-destructs when the wrong PIN is entered three times.

Even if the owner of the stolen card is certain that the PIN is known only to him, it is still recommended to have the card blocked at the issuing certificate service provider (CSP). The CSP keeps the corresponding information in a blocking list accessible via the Internet. Blocking can also be requested by a company for an employee leaving the company.

Certificate Service Provider

Accredited certification service providers are checked by BNetzA regarding the adherence to security criteria

The certificate service provider must also be registered with the BNetzA. The BNetzA has checked the accredited provider regarding adherence to the security criteria, such as registration of the owner of the certificates and the system being used for producing and storing the certificates.

In Germany, the following providers were accredited as of August 2007:

+ Produktzentrum TeleSec of Deutsche Telekom AG, 17/1998
+ Bundesnotarkammer, 12/2000 (national association of notaries)
+ DATEV eG Zertifizierungsstelle, 03/2001
+ D-Trust GmbH, 03/2002
+ Deutsche Post Com GmbH Geschäftsfeld Signtrust, 07/2004
+ TC TrustCenter GmbH, 05/2006

  The certificate service providers named above are in addition also accredited for the production of so-called qualified time stamps. There is currently one accredited provider who only provides the service for the production of time stam
+ AuthentiDate International AG, 11/2001

Interoperability

CSPs organise in T7 with the ISIS-MTT standard

At the point in time at which the German signature law was ratified, the certificate service providers at the time made chip cards and public key infrastructures (PKI) available that were communicated with in different ways and were thus incompatible with each other. Because this situation has been recognised by all CSPs as an obstacle to acceptance, they organised themselves under the name T7 (T for trust centre and 7 for the number of founding members) and specified the standard ISIS-MTT (Industrial Signature Interoperability Specification MailTrusT), that was passed in the version 1.0 in 2001 and expanded most recently in 2004 with version 1.1.

ISIS-MTT specification:

takes into account all business-relevant electronic signatures

The ISIS-MTT specification takes into account all business-relevant electronic signatures, up to qualified electronic signature, which can meet the form regulations of private and administrative law. As well as this, the specification also contains security functionalities for secure e-mail, with various levels of security and compatibility at the internationally accepted standards. The rapid availability of interoperable security products is hereby made possible at the level of the certificate service providers as well as at the user level (client side). The following contents have been defined:

Part 1: certificate and CRL profiles

Part 2: PKI management

Part 3: message formats

Part 4: operational protocols

Part 5: certificate path validation

Part 6: cryptographic algorithms

Part 7: cryptographic token interface

Part 8: XML signature and encryption message formats

Profile: SigG-conforming systems and applications

Profile: optional enhancements to the SigG profile

This standard led very swiftly to standardisation in Germany and facilitated the laboratory-work of the manufacturers of the signature applications, when a further card was to be supported.

It is, however, not yet clear whether the specification still allows for a range of variations, i.e. the cards still show slight differences. It therefore continues to be necessary for the manufacturer of the signature application to explicitly issue a release for the supporting of one of the cards or OCSP services. The time before support has now become very short.

Each application must be integrated separately as their calling is not standardised.

There is still another aspect of interoperability: signature applications are addressed from other applications such as document management systems, workflow systems, ERP, CRM or even groupware. Unfortunately, the calling of the signature applications themselves is not yet standardised. That is why each application must be integrated separately. In future, it would be desirable if the signature applications could be communicated with via a similar interface, similar to databanks using SQL.

Signatures Embedded In Documents

Signature containers can be embedded in documents

As described above, it is possible to embed the signature container in documents. This procedure offers advantages and disadvantages. The advantage is that unlike having an accompanying signature file there is only one file to manage. Unfortunately, it is not then possible to recognise from the file itself whether or not it has been signed. A further problem is that the file is in principle being altered by the addition of the file. In the case of PDF documents, there are some standard mechanisms that make it possible to bring embedding under control. Adobe Reader also offers flawless verification within the application, from version 8 upwards. This verification does not, however, conform to the signature law as checking is performed according to the shell model and the signature is declared no longer valid as soon as the validity date of the certificate has elapsed. As shown further above, signature according to the chain model continues to be a valid model for checking in signature law.

SAPERION recommends the use of accompanying signature files, even if new versions of PDF/A are orientated towards the ISO standard.

The PDF/A format has also been accepted into the ISO standard for long-term archiving. In the standard this format does not yet provide for the use of signatures but does not in principle prevent them from being used as attachments, i.e. strictly speaking, signatures embedded in PDF/A do not meet the ISO standard. It is only with the next version of PDF / A that a standard for the safekeeping of signatures will be taken into account. Whether this will then correspond to process currently on the market remains to be seen. That is why SAPERION recommends the use of accompanying signature files.

Re-signing Before Weakening Of Conclusiveness

Documents must be re-signed in order to retain their legal force, if BNetzA classes the algorithms being used as weak

A subject still being energetically discussed in connection with signed documents is their re-signing, also called post-signing, when the requirement arises according to § 6 SigG. This requirement always comes into force when BNetzA classes one of the algorithms used in signing as being weak from a particular point in time onwards. In the present state of affairs, it is not yet clear which other documents come under this "requirement". To date, there has been no official statement regarding this, only expert opinions from individual solicitors. So every company must check for itself whether or not this requirement applies to their documents. According to a literal interpretation of the text of the law, the requirement to sign all documents again, if their authority is to be retained, seems to exist when e.g. it seems highly likely that a conflict might arise. A detailed treatment of this subject can be found in the book "Beweiskräftige elektronische Archivierung - Bieten elektronische Signaturen Rechtssicherheit?" (legally conclusive electronic archiving - do electronic signatures provide legal certainty?) by Roßnagel and Schmücker.

There are a number of opinion-formers, such as e.g. Dr. Ulrich Kampffmeyer, publisher of the relevant Project Consult Newsletters with information on the ECM market, and Oliver Berndt of B&L Management Consulting GmbH, who are of the view that e.g. no requirement exists for signing documents again that have been kept in an electronic archive certified to GoB (principles of correct accountancy) by an auditing institute. The electronic archives have the task of protecting the documents kept in them against changes, i.e. one should be able to assume that a document in an archive cannot be changed even if the algorithm has become weak. Renewed signing should only be necessary at the point in time at which it leaves the archive again.

Attack Scenario And Protective Measures

Signatures are becoming weaker due to faster computers and knowledge of algorithms

As already described above, a document signed with a qualified signature possesses the high value of prima facie evidence. Unfortunately, the algorithms used for signing become weaker in time. At the time of signing, these algorithms must have the status of being safe, i.e. it is assumed that nobody is at present in the position to either generate another document that produces the same high hash value (e.g. signing off a sum of 1,000,000 EUR instead of 1,000 EUR) or simulates the private key.

Because computers are becoming faster and faster over time and the knowledge of algorithms is also increasing, the signatures become weaker. Each year, the BSI evaluates how strong the algorithms are, and BNetzA makes the final decisions and publishes the results. In April 2007, an algorithm was for the first time classed as weak at the start of the following year. This was the algorithm for the encoding of the hash value with the designation RSA and a key length of 1024 bits, as was still used on all common chip-cards in mid-2007. The certificate service providers will deliver a new generation of cards by the end of 2007, which will now use a key length of 2048 bits for the RSA algorithm. These cards will in turn also be used for the production of time stamps in the trust centre.

Protective Measures

The following measures must be carried out if it is announced that the encoding algorithm for the production of the signature on the card has become weak:

1. The certificate service providers must issue new cards by the point in time of the weakening, which must then be used for signing instead of the old cards.

2. The signature applications must be replaced with a new version.

3. All documents signed with the old cards must - if necessary - be signed again.

Exceptional Rule: Electronic Invoices

Electronically signed invoices for tax audits do not have to be re-signed.

The Federal Tax Office does not see a requirement for re-signing in the case of electronically signed invoices for the performance of the tax audit. On the one hand, the signed invoices must be verified before processing, and, on the other, the audit report must also be archived together with invoice and signature. Neither is there a requirement in the context of a conflict, because the conflicting parties will have achieved an agreement after six weeks at the very latest in the case of incorrect invoices.

Cryptographic Applications In SAPERION

Since 1997, SAPERION AG has been providing extensive cryptographic functions for the encoding and signing of documents on Windows via Option Security. The functions used in this are provided with the operating system in connection with the so-called Microsoft Crypto API.

SAPERION encodes and signs via Option Security using Windows with the functions of Microsoft Crypto API.

Encoding

The user can also encode a document for increased protection against unauthorised access over and above the usual access rights. He can here use a further password for later decoding.

Advanced Signing

If the state and release procedure of a document are to receive a higher conclusiveness, then the releaser can sign the document and also enter an appropriate comment.

These processes are based upon software algorithms from various manufacturers (e.g. Microsoft or Infineon), which can be activated via the Crypt API. If the user calls a cryptographic function for the first time, then a key pair is produced. The private key is kept safe in the Microsoft Crypto Store, while the public key is managed on the SAPERION broker server. If a document is signed then a hash value is produced via the selected algorithm for the document and encoded with the private key on the broker server and then sent to the document on the SAPERION document server. For the later verification of the document, the hash value is in turn generated, and the saved encoded hash value is decoded again with the public key and compared with the new one.

Increasing conclusiveness using an advanced signature

This process corresponds to the advanced signature according to German signature law and is in most cases enough to increase conclusiveness. The functions described here based on Microsoft Crypto API are restricted to a) the use of an operating system from Microsoft and b) use only within SAPERION. The keys and signatures can currently not be exported in a standard cryptography format.

These restrictions are mostly dispensed with in cases of the use of manufacturer-declared, signature application components, integrated into SAPERION, produced by SAPERION partners and the use of which is described in the following.

SAPERION, different uses for qualified signatures

This chapter describes the essential uses for the application of qualified electronic signatures. SAPERION here uses the signature application components produced by the partners AuthentiDate AG and secrypt GmbH.

Confirmation of the format transformation from paper to the electronic image

A series of regulations demand that documents should be qualifiedly signed directly after scanning and a random sampling test, if they are to be destroyed after scanning. For this, SAPERION offers the function of batch signing in the in-tray. After confirmation of the random sample, all documents in the in-tray are signed simultaneously after the one-off entry of the PIN into the card-reading device.

SAPERION uses components from AuthentiDate and secrypt GmbH for qualified electronic signatures.

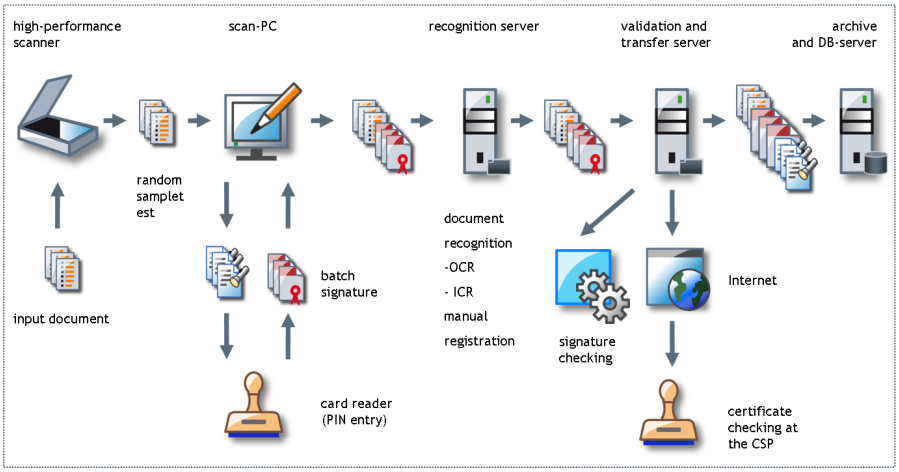

Fig. 8: possible course of the document recording with batch signing and automatic Index recognition

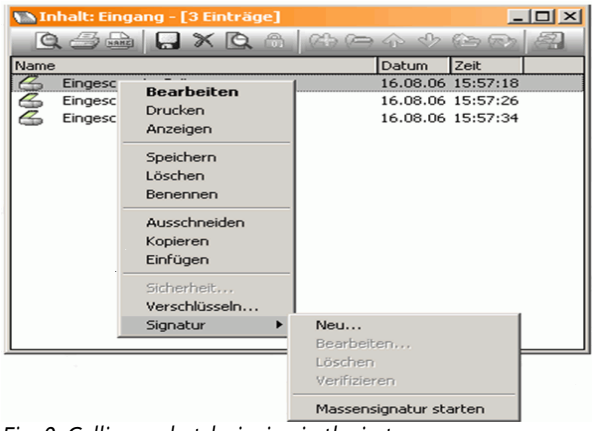

Fig. 9: Calling up batch signing in the in-tray

SAPERION can sign documents of a time-stamp in the in-tray

For security reasons, the scan workplaces may not be connected with the Internet, i.e. the archiving, together with the verification that is required for access to the Internet, must be carried out at another computer.

As an alternative to SAPERION Scan Client, documents can also be recorded via other scan systems that allow a transferral of the documents to the in-tray. For example, SAPERION ReleaseScript for KOFAX Ascent Capture is in a position to save the documents of a scanning batch together with the index data in various in-trays. The documents can then be signed here in the batch process.

Manual Batch Signing Of Outgoing Invoices In Small Quantities

Another possibility is accepting outgoing invoices that have only just been produced into the in-tray. These can then also be signed and archived together in one go. The documents can then be sent by e-mail, together with their signatures, to the addressee, who is known to SAPERION due to the transferral of index data.

Automatic Batch Signing Of Outgoing Documents In Large Quantities

Large quantities of outgoing invoices as an example of mass-signing

Outgoing invoices in larger quantities are an example of the signing of masses of documents together. In this case, the signing is carried out via a signer server that stands in a specially secured room. Only the cardholder, usually the manager of financial accounting, has access to this signer server. Where there are large amounts of documents that must be signed each day, several chip-cards are used in parallel. The chip cards are usually activated for the day in the morning and then the server room is closed off by the chip-card-holder.

Sending invoices by e-mail by the signer server and document transferral to SAPERION for archiving

This procedure is typically carried out close to the invoice-document-producing ERP system before SAPERION is contacted. The signer servers themselves then send the invoices by e-mail and then transfer the documents to SAPERION for archiving.

Co-signing And Counter-signing In The Company's Internal Workflow

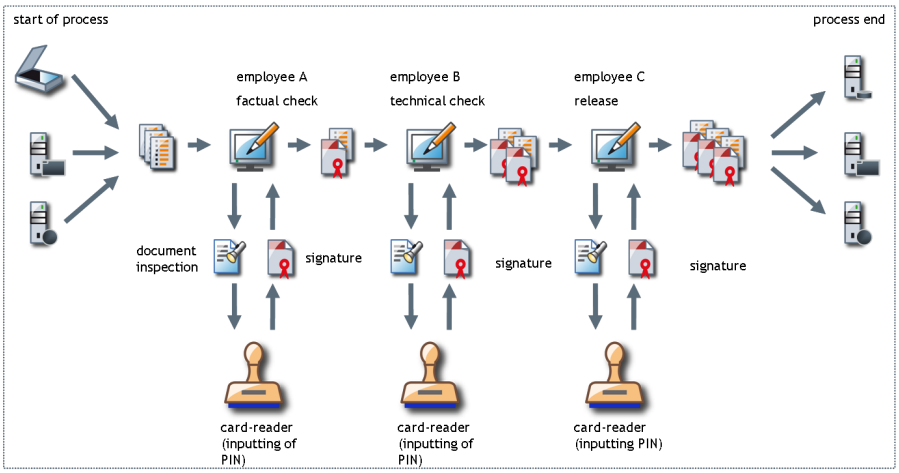

Fig. 10: signing in the workflow

Advanced signature for co and counter-signing in the company-internal workflow

An advanced signature is usually sufficient for co-signing and counter-signing in the company-internal workflow. There are, however, also applications that make a higher degree of conclusiveness desirable. These are mostly cases in which a lot of money could be lost in the event of a claim. This is the case, for example, in the testing of blood products that must be performed by blood-donation services, and where proof of correct testing can save a lot of money if a recipient of the blood product then becomes seriously ill. Or in the field of aircraft construction, when important component descriptions are released. In these cases, it is sometimes necessary for several signatures to be obtained. SAPERION makes it possible to sign a container document (structure document) as a whole as well as every individual document in the container. If the documents are later to be exported with their signatures, individual signing is to be recommended. Each document can be signed several times and also be provided with a comment. In this way, the co-signing and counter-signing can be carried out within workflows.

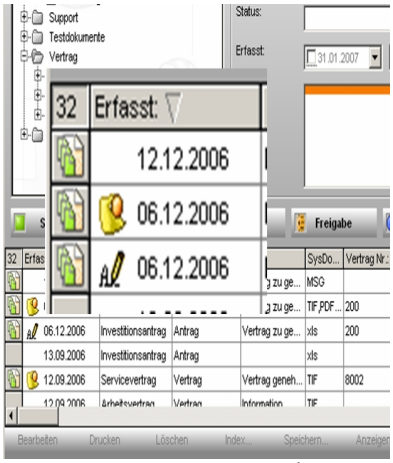

Fig. 11: An existing signed document is shown in the results list with a pencil icon

Signing of container documents and individual documents in the container by SAPERION

Automatic Time Stamping

In the cases in which only the content of a document is to be confirmed at a particular point in time, this can be signed with a time-stamp in a work-step at the SAPERION server. The signing service must have access to the Internet for this.

Manual Time Stamping

The user himself can call time stamping manually. This can take place in two ways. Either the document itself receives a time-stamp or a setting can be made at the client, in which a time-stamp is to be embedded in the signature file as an attribute during the person-specific stamping.

Whereas pure time stamping is carried out via the signature application components on the SAPERION server, in the second case the time-stamp is requested at the workplace, i.e. access to the Internet is necessary.

Making sure of the what and WHEN by means of time stamps

Automatic Verification Of Incoming Documents

SAPERION is able to automatically verify incoming signed documents during archiving via importing or during the use of the API. In the case of successful verification, the verification data are archived together with the document and - if necessary - its accompanying signature file. All other documents are diverted to the open tray for further checking. The SAPERION solution thus meets the GDPdU regulations. These specify that verification must be carried out before the processing of an electronic incoming invoice and that the reserves must be stored for the later tax audit.

Automatic verification of external, signed documents during archiving using SAPERION

SAPERION solution meets GDPdU regulations

Verification Report	
Signature Information	
Authenticity:	Intact
File Integrity: Level Requested: Level Reached: Warning:	Intact Signature Signature Algorithm will become weak soon: 1.2.840.113549.1.1.1,1024; it is strong enough until Tue Jan 01 00:00:00 CET 2008: please make sure that you have time-stamped the data before that date.
Signature Details	
Verification Time:	14.06.2007 06:42
Signature Algorithm:	1.2.840.113549.1.1.1 RSA encoding
Key Length:	1024
Key valid until at least:	31.12.2007 23:00

Fig. 12: example of a verification report (extract)

Prospects For 2008

In future, the interfaces for the SAPERION solutions e-mail Lifecycle Management For Exchange and also for Lotus Notes will automatically recognise the presence of a signed document in an e-mail and thereby be able to automatically cause verification during archiving.

Export And Sending Of Signed Documents

Export capability for signed documents in the event of legal disputes

In the event of a legal dispute the archived, signed documents can be exported or transferred straight away as an attachment by dragging and dropping into the MAPI e-mail client. The documents can alternatively be sent by programming by SMTP.

Due to this exporting capability, the judge does not first have to call in an expert who assesses the legitimacy of the document in question on the system.

Prospects 2008

At present, the signing and verification functions can only be called within the standard client. In the course of 2008 these functions will also be made available in the HTML client.

Details On The Partner Solutions

AuthentiDate AG

AuthentiDate AG is one of the leading manufacturers of signature applications on the international market. Because Germany has set the highest standards with its signature law, the solutions for qualified signatures meeting SigG are also developed in the German branch. AuthentiDate specialises purely in solutions for qualified signatures, which are integrated by partners via an API. The signature routines are Java-based and can thus be used regardless of the platform. In addition to these solutions, AuthentiDate also operates an accredited time-stamping service.

AuthentiDate provides solutions for qualified signatures

secrypt GmbH

Unlike AuthentiDate, which restricts itself to the field of qualified signatures, secrypt GmbH, based in Berlin, also deals with advanced signatures. On top of this, secrypt is also one of the few manufacturers that support all the cards of the German Trust Centre as well as a range of cards from our neighbouring nations. The signature server can support various signature processes in parallel. This is especially important for companies who do a lot of business with countries abroad and must therefore sign outgoing invoices in connection with the statutes of the foreign states in question.

Secrypt offers solutions for qualified and also advanced signatures.

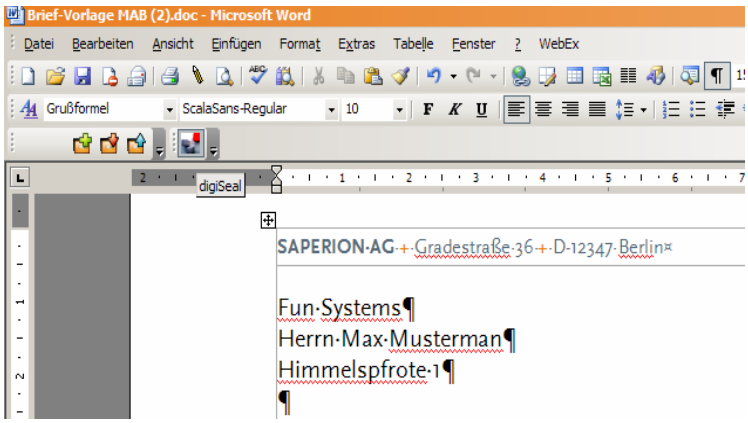

Fig. 13: Signing from Word via the digiSeal icon

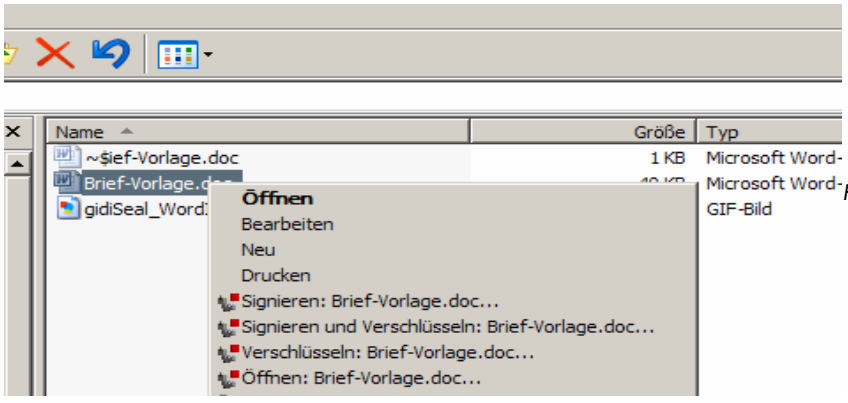

Fig. 14: Calling signing via the context menu in MS File Explorer

Unlike AuthentiDate, secrypt offers a signature client with its own user interface, with its product digiSeal office. This can, therefore, also be used outside SAPERION and represents a further benefit for our customers.

Comparison Of The Signature Functions In Combination With The Partner Solutions

Function	Only SAPERION	AuthentiDate	Secrypt
Independent signature client incl. integration into MS Explorer & MS Word			x
Advanced signature in "closed" SAPERION	x		
Accompanies advanced signature			x
Accompanies qualified signature		x	x
Qualified signature embedded in TIFF		x	
Advanced and qualified XML signature (XML DSig and XAdES)			x
Advanced and qualified 2D barcode signature (for secure paper printout)			x
Qualified signature embedded in PDF			x
Multiple signing of a document	x	x	x
Programmed start of the signature dialogue	x	x	x
Programmed verification	x	x	x
Automated verification during importing		x	x
Export (saving and e-mail)		x	x
Batch-signing (qualified)		x	x
Verification report saved in XML		x	x
Verification report in PDF (Q1/08)		x	x
Verification report displayed in HTML		x	
Secure viewer (TIFF)			x
Supporting of all signature cards of German CSPs			x
Signing with Aladin e-tokens via PKCS#11 interface			x
Time-stamping (manual and automatic)		x	x
Time stamp integrated into signature		x	x
Tool for card configuration			x
Platform-independence (Java, HTTPS)		x	(Windows)
Index interface			x
Programming interface (C-API)			x
Programming interface (HTTPS)		x	
STMP connector			x
Automated document encoding with password or certificate			x

Signotec GmbH

There is a further signature solution that has been realised by two partners in the context of SAPERION, and which is described here briefly. The solution is based upon the signotec application "Signing Suite" for the simultaneous manual and electronic signing of PDF or TIFF documents. It consists of the "eDocPrinter", a virtual PDF printer, and "SignoSign", a programme for the safe signing of PDF documents with an advanced electronic signature.

Fig. 15: Manual signature with a pen pad

With the signotec suite, electronic documents can be signed by pen pad and archived directly in SAPERION.

With the signotec suite, electronic documents can be signed by pen pad and then archived directly via an interface in SAPERION. In this process, the characteristics of the handwriting are recorded and also saved in the respective document. The procedure is regarded by a number of experts as more secure than the conventional signature on paper. This is because the typical and individual features of the signatory can be better analysed than with a signature on paper. The process is used especially frequently by banks because very few customers currently have a signature card. The customer can sign directly on the pen pad and the legally signed document is fed directly into the rest of the electronic workflow without a change of media. Apart from financial services, the use of the solution is also practical anywhere where approval processes are operated that require a signature and an efficient workflow, such as in industry and health services.

Availability and handling are frequently mentioned advantages of this technology. There are no cards to be lost or passed on to third parties without authorisation, i.e. the signature is absolutely personal and neither is there a PIN that can be forgotten.

Conclusion

- SAPERION offers a large number of functions for everything to do with the application of electronic signatures. Starting with the encoding of documents for added protection against unauthorised access, to signing in workflows to the securing of authorship, to the long-term safekeeping of signed documents that come into the company from outside, whether it is by paper or e-mail.
- A series of SAPERION standard functions can be used for encoding and advanced signing, which is sufficient for 95% of business documents. In the case of qualified electronic signatures with the highest level of conclusiveness, SAPERION can be supplemented by functions based on partner products from the companies AuthentiDate and secrypt.
- Many processes that up until now required the printing of electronic documents onto paper can be performed more efficiently, and therefore more cheaply, within SAPERION and then provided with a manual signature. Particularly in the case of electronic invoices, it has been proven that up to 70% of the process costs can be saved.
- In addition to the person-specific signature, which allows one to prove WHO has signed WHAT, documents can also be signed using a time stamp. This also allows one to later verify WHEN WHAT was signed.
- In the vent of a conflict, the signed documents managed in SAPERION can simply be transferred to the e-mail client by dragging and dropping in order to send these to third parties for inspection and external examination.
- For the purpose of the destruction of paper after scanning, all the documents in a batch can be confirmed, regarding their correct conversion into images, by means of so-called batch signing. For this, the PIN must only be entered once for the release of the chip-card, and then all the documents in the batch are signed.
- The company signotec offers the solution for processes that involve people who do not possess a chip-card, e.g. private customers of banks and insurance companies. In this solution, manual signatures can be recorded by pen pad and integrated into a PDF document as an advanced electronic signature.
- For long-term safekeeping, SAPERION offers the option of having signed documents quickly and cheaply re-signed if the Bundesnetzagentur announces that this is necessary.

The Advantages Of An Electronic Signature

+ Electronic signatures create the necessary trust in the electronic exchanging of business letters. Unlike with a paper document, the recipient of a signed document can himself at any time ascertain whether or not the document has been altered since the declaration intent, who the actual author was and whether the document was signed with legal effect.
+ Qualifiedly signed electronic documents have greater conclusiveness than paper-based documents due to the new rules in the code of civil procedure. The judge must recognise such a document as proof (prima facie evidence), whereas a paper document is subject to the discretionary acknowledgement of the judge, and thus of his own judgement.
+ The creation of the necessary trust and the equalisation of legal status between electronic signatures and manual ones (text form) provide the necessary conditions for avoiding the interruption caused by moving from one media to another. Business processes can now be performed entirely electronically, i.e. paper printouts for manual signature and the subsequent expensive postage are no longer necessary. The recipient can also reduce costs greatly. The time-consuming and therefore costly opening of letters, sorting, scanning, manual indexing or alternatively automated recognition of data such as e.g. the sender and the recipient is dispensed with when documents are received electronically by e-mail.
+ In the case of incoming invoices, up to 70% of procedural costs can be saved, especially when all invoice data can still be read by computer as in the EDI process. In this case, a substantially lower error rate is achieved than could ever be achieved using scanning and automatic analysis.
+ With the electronic signature, the format conversion when scanning from paper document to electronic image can also be made secure. This procedure is now already demanded by regulations for e.g. social insurance providers and hospitals, when the paper documents are to be destroyed after scanning. In this way, the costs of conventional archiving can be dispensed with.

Glossary

BNetzA

Abbreviation for Bundesnetzagentur, responsible authority according to the signature law. BNetzA produces the root certificate with which it signs the certificates for the CSPs. The BNetzA also secures the further use of the PKIs of CSPs, if the latter cease operation.

SigG

Abbreviation for the German signature law.

SigV

Abbreviation for the signature ordinance for detailing of SigG

ISIS-MTT

ISIS-MTT is a profile on internationally widespread and recognised standards for electronic signatures, encoding and public key infrastructures. In October 2001, the ISIS-MTT specification (last published version 1.1 of 16.03.2004) was passed by T7 and TeleTrusT together. Because signature application providers as well as trust-centre operators were involved in the drawing-up of the specifications, ISIS MTT is supported by the leading German product-developers and solution providers for e-business and e-government.

text form

The text form has been introduced into German law in addition to the written form. Where the text form is demanded in laws, ordinances or contracts, then a qualifiedly signed electronic document can be used as an alternative to a paper document.

manufacturer declaration

Every signature application that is used to produce qualifiedly signed electronic signatures must be declared to the BNetzA by the manufacturer. After an appropriately positive checking of the applications regarding their safety, the declarations are confirmed and published on the website of the BNetzA.

OCSP

Abbreviation for Online Certificate Service Protocol, for checking whether a certificate was still valid at a particular point in time and was not blocked.

CSP

Abbreviation for certificate service provider, who upon request delivers the chip-cards together with the private key and the certificate after checking identity, and holds the certificate in safe-keeping for 5 – 30 years. In the latter case, the CSPs must have themselves certified by the BNetzA.

PKI

Abbreviation for Public Key Infrastructure, which is required by the CSPs for the production and administration of key pairs and of the certificates and blocking lists for the application of the electronic signatures.

PKCS

Abbreviation for Public Key Cryptography Standards and designates a series of cryptographic specifications. These were developed from 1991 by RSA Laboratories in cooperation with others. The aim was to accelerate the spreading of Public Key Cryptography.

shell / chain model

The two models are used for checking the validity of a signature. The SigG demands checking in accordance with the chain model, whereas e.g. the shell model is used in America and thus in products of this country.

BSI

Abbreviation for the Federal Office For Information Security, which determines the criteria for the safety of all technical components that are required for the production of a qualified signature (chip-card, card-reading device, software), and also annually evaluates the strength of the algorithms that are used for the production of signatures.

FAQs About Signatures

+ **What do I need to pay attention to if I want to make qualified electronic signatures?**

All application components are subject to stringent, trust-building criteria:

1.The signature card must be certified to Common Criteria.

2.The issuing trust centre must have declared itself (5 years safe-keeping of the certificates), or is accredited (30 years safekeeping)

3.The card-reading device must correspond to security class 2 or 3 (safe number block for PIN entry). Class 3 also has a display.

4.The signature software must be manufacturer-declared.

On the website of the BNetzA one can find out which trust centres and components may be used

+ What type of signature must be used to sign electronic invoices?

With the qualified signature, issued by a trust centre that does not necessarily have to be accredited.

+ Do electronic invoices that are exchanged within the group of companies also have to be signed with a qualified signature?

Yes. Although the UStG does not go into this explicitly, it does not specify it as an exception either.

+ What do I have to do if I receive an electronic document and want to deduct the pre-tax?

Before the start of processing, the signature must be verified with regard to the invoice. The resulting report must be held securely in safekeeping together with the document and signature file (if accompanying) in accordance with the GoB and GDPdU (for the purpose of the tax audit).

+ Must I accept an electronically signed invoice?

No. I can demand that a paper invoice be sent. If I do not react, this is my tacit consent. If I cannot present the verification report at the tax audit, I must pay the withheld pre-taxes afterwards.

+ Why do I need a signature card?

The signature law (SigG) requires a chip-card for qualified signatures. The usage of this chip-card corresponds to the principle of ownership and knowledge. I own the unique personal key with which the signature is generated and I am the only one who has the PIN for making the signature. Entering the PIN ensures the necessary pause before the declaration of intent: "Do I really want to sign this document?" Additionally, the non-repudiation of the signed document is also ensured.

+ What documents must be signed with a qualified signature?

All documents for which the text form is required can be signed with a qualified signature. All documents requiring the written form must however continue to be signed manually.

+ What must be kept in mind when a large number of invoices are to be signed during the day?

In this case, a signer server should be used that can communicate with signature cards. The owner of the cards releases these for a certain time and then shuts off the room (and/or box) so that no unauthorised person has access to the cards (strong process coupling).

+ Must I sign every invoice individually?

No. The invoices can be combined in one file, which is then signed.

+ In the case of important documents such as contracts, which have been signed by a third party, can I scan the document, give the scanned document a qualified signature and then destroy the paper?

In the area of social insurance providers, there is an ordinance that permits this procedure. Legal practitioners, however, point out that documents that are explicitly documentary lose their documentary character when they are converted into the electronic copy. The justification for this is that the manual signature on paper is three-dimensional whereas the copy has only two dimensions. Due to this, information is supposedly lost that is important for an expert on documents.

+ What evidentiary value does a qualified, signed document possess?

This document has a higher level of conclusiveness than manually signed documents. According to the German code of civil procedure they are regarded as prima facie evidence, i.e. the judge must recognise the document as evidence unless the opposing party can name cogent reasons not to accept it as such.

+ •What should one pay particular attention to in relation to signatures embedded in PDF documents?

If signatures are embedded in PDF files then this document certainly no longer corresponds to the PDF / A format.

Embedded signatures have the disadvantage that it cannot be recognised from outside that a signature is contained. The advantage is that unlike an accompanying signature file the signature cannot be lost.

Although the PDF reader can check advanced signatures, in the case of qualified signatures, a special piece of software must be used. Adobe checks in accordance with American regulations using the shell model, whereas the German signature law requires the chain model. SAPERION recommends the use of accompanying signature files.

It is planned to expand the PDF / A format in 2008 to include signatures.

+ What is to be kept in mind when electronic invoices are being exchanged with companies in other countries?

The laws of the destination country are always to be adhered to, i.e. foreign companies must observe the German law on turnover tax and the German signature law, i.e. appropriate technologies must be used for producing the signatures.

+ What must I do if I have lost the card and/or if I no longer want to / should not use it?

In principle, a lost card is nothing critical, as the card will destroy itself after a third failed attempt to enter the PIN. It is nevertheless recommended to contact the trust centre that issued the card and to request that the card be blocked. In this way, if someone later tries to sign using the card, it can be ascertained during the verification of the signature whether or not the card was used before or after blocking.

+ Which signature solutions has SAPERION integrated?

Available since 2003: AuthentiDate SLMBC Module (eArchive, eSign Client, Scan Signature, eTimestamp)

From version 5.7 SP1: secrypt digiSeal office, digiSeal office pro, digiSeal server

+ Can SAPERION also hold signed documents in safekeeping without the use of the signature solutions?

Yes, but no graphic markings for the visualisation of an existing signed document are shown.

+ Does SAPERION offer a solution for post-signing?

Yes, SAPERION combines all documents and signatures that are saved on a medium into a hash tree, in accordance with ArchiSig. The hash tree is then signed with a time stamp. With this procedure, between 100,000 and 800,000 objects can be processed within an hour, depending on the storage technology.

+ **When must a document be post-signed?**

Post-signing is sometimes necessary if one of the two algorithms that were used for producing the signature are classed as weak by the Bundesnetzagentur. Here it is to be ensured that the post-signing takes place before the point in time at which the algorithm becomes weak. Post-signing applies to all documents that are intended to retain the high level of evidentiary value of prima facie evidence. SAPERION is of the opinion that the post-signing of documents that are held for safekeeping in a GoBS-conformant archive is superfluous. In legal practice, however, there are no such exceptions. It is to be hoped that an amendment of the signature law will bring some relief in this connection.

+ Must electronic invoices also be post-signed when required?

No, the responsible federal office has expressly forbidden post-signing.

+ If I now use the signature solution of SAPERION, when should I expect to have to post-sign?

At present algorithms are used that the BNetzA expects to remain strong until 2014.

+ Why was post-signing accepted into the law?

If algorithms become weaker, there could be offenders who either forge a document or could forge a signature. So that this risk is minimised, the Federal Office For Information Security examines the strength of the algorithms each year.

+ Can I also use my signature card to encode my e-mail messages?

That is not recommended. The encoding of a message is always carried out with the public key, i.e. your business partner acquires the public key from e.g. your trust centre, encodes the message and sends it to you. You now decode it with your private key. Because this key is only on the card once and it is not possible to replace the card with one with precisely the same key, you would no longer be able to decode any of your encoded messages or documents. It is therefore recommended that so-called software-based certificates be used for the safer transferral of messages. You can make and safely store a duplicate.

+ What are the advantages and disadvantages of the signature solutions from AuthentiDate and secrypt?

AuthentiDate has been active in the signature market for years and has a strong American parent company.

In addition to supporting qualified signatures, secrypt also offers the use of advanced signatures, using e.g. the e-token from the company Aladin.

With digiSeal office secrypt offers an autonomous Client which can also be used outside of SAPERION.

secrypt can embed signatures in PDF and also verify them.

secrypt supports almost all German and Austrian signature cards. At present, AuthentiDate only supports the card from Telesec. secrypt produces a country-specific, XML-formatted verification report that can also be read by a layman.

Notes

Disclaimer

Through the presentation of the software in this Whitepaper or any public statements or advertising by SAPERION or by its employees or distribution and marketing partners no representations or warranties about the software or services by SAPERION may be dervied. For the state of the delivered software, the respective technical documentation of the software which can be inspected on request prior to the conclusion of any contract and which is valid on delivery is decisive. SAPERION therefore expressly disclaims any further representations or warranties of the software.

Additional Information

SAPERION AG
Steinplatz 2
10623 Berlin, Germany

phone.: +49 30 600 61-00
fax.: +49 30 600 61-500

sales@saperion.com
www.saperion.com

SAPERION (Switzerland AG
In der Luberzen 19
CH-8902 Urdorf-Zürich, Switzerland

phone.: +41 44 735 46-00
fax.: +41 44 735 46-10

international@saperion.com
www.saperion.com