

LEGAL STATEMENT¹

COMPLIANCE OF CoSIGN WITH REQUIREMENTS OF THE ELECTRONIC SIGNATURE LAW IN GERMANY

MADE FOR

ALGORITHMIC RESEARCH (AR)

FRANKFURT/ GERMANY
JANUARY 2005

WALDECK RECHTSANWÄLTE PARTNERSCHAFTSGESELLSCHAFT
BEETHOVENSTRASSE 12-16, 60325 FRANKFURT AM MAIN

¹ Waldeck Rechtsanwälte Partnerschaftsgesellschaft (Legal Advisor) acts as an independent expert and is not representing AR. Legal Advisor gives no binding legal opinion and accepts no liability for damages or financial loss of AR or third Parties, especially because of any use of CoSign or any business decision founding on this legal statement. The legal statement is based on the information provided by AR which is available on the website www.arx.com and the user manual provided by AR. This information has not been proved by WRA. The statement is for internal use of AR and does not claim to cover all legal requirements.

DIRECTORY

| | |
|---|-----------|
| 1. PRODUCT INFORMATION | 3 |
| 2. LEGAL RECOGNITION AND LEGAL EFFECTS OF ELECTRONIC SIGNATURES | 4 |
| 3. BASIC REQUIREMENTS OF GERMAN SIGNATURE LAW FOR ELECTRONIC SIGNATURES..... | 4 |
| 4. CLASSIFICATION OF ELECTRONIC SIGNATURES CREATED BY COSIGN | 6 |
| 5. ELECTRONIC SIGNATURES CREATED AUTOMATICALLY BY COSIGN..... | 7 |
| 5.1 AUTOMATIC CREATION/ BATCH SIGNING UNDER GERMAN LAW | 7 |
| 5.2 QUESTIONS DISCUSSED - COSIGN'S SOLUTIONS..... | 8 |
| 6. SUMMARY | 12 |
| | |
| AUTHORS OF THIS STATEMENT | 13 |

1. PRODUCT INFORMATION²

CoSign is an electronic-signature solution that is quick to deploy, offering all the components of an electronic-signature solution while requiring virtually zero-management. CoSign delivers an innovative solution for electronically signing documents, files, forms and transactions.

Based on standard PKI technology, CoSign ensures signer authenticity, data integrity, and non-repudiation of documents. CoSign offers the possibility to create non-forgable electronic signatures that cannot be duplicated and altered unnoticed. The recipient of an electronic signature created by a CoSign-User is able to prove integrity of the electronic document as well as authenticity of the CoSign-User and the document's content.

With its unique centralized approach for managing private keys and built-in integration with the organization's existing User-Management-System, CoSign eliminates additional overhead expenses that are common with other solutions. CoSign can be integrated with leading User-Management-Systems, including Microsoft Active Directory and Novell/ NDS. This integration ensures no overhead in managing the electronic signature system and the signature credentials, particularly with regard to the private keys of users. CoSign also supports a wide range of third party applications, e.g. Microsoft Word, Adobe Acrobat, ERP (SAP) and several web applications. Additional features in CoSign include support for high-volume batch signing without individual intervention.

Private keys and other necessary signature credentials are stored in a secure environment on the CoSign-Appliance. Users are able to sign only if they are part of the system and members in the user list which can be administrated from a standard User-Management-System over a management console. If a user is authenticated, e.g. by Password, PIN, a private token or by biometrics, he may send a signing request to the secure CoSign-Appliance which includes the document-hash. CoSign signs the document hash using the authenticated user's private signing credentials. After the signature process takes place on the secure CoSign-Appliance, the signature is sent back to the user. To avoid unauthorised users from creating a signature with the signature credentials of another user, CoSign ensures exclusive access between the user's computer and the secure CoSign-Appliance.

² All Statements regarding technical features of CoSign are based on information provided by AR. Technical features have not been proved by Legal Advisor.

2. LEGAL RECOGNITION AND LEGAL EFFECTS OF ELECTRONIC SIGNATURES

The starting point of the legal recognition and the legal effects of electronic signatures under German law is the German Electronic Signature Act (Signaturgesetz) and the Signature Regulation which specifies the Signature Act (Signaturverordnung). Both, the Electronic Signature Act and the appropriate Electronic Signature Regulation transform the European Directive for Electronic Signatures 1999/93/EG (Directive). According to Reason 21 and Article 5, Section 2 of the Directive, it is prohibited to deny the legal effects of an electronic signature just because of its electronic form. This non-discrimination rule has been adapted to the German Signature Law, which means that all kinds of electronic signatures are legally recognized in Germany.

Moreover, electronic signatures can have certain legal effects if they reach a defined security standard. The fundamental legal effects under German Law are the substitution of a handwritten signature with an electronic signature and the facilitation of giving evidence in court with an electronic signature. Basically, not every electronic signature has these or other defined legal effects, even though it is prohibited to deny the legal recognition in principle for the sole reason of the electronic form. Legal effects under German Law like the substitution of a handwritten signature (§ 126a BGB) and the facilitation of giving evidence (§ 292a ZPO) require at least “qualified electronic signatures” under the German Signature Act. Regardless of the security level, it is always legal to prove authenticity and integrity of an electronic document in court with other forms of electronic signatures.

Furthermore, the effects of electronic signatures always depend on the context and the legal framework in which an electronic signature is used. For some special situations several German regulations outside the electronic signature law require advanced electronic signatures (e.g. § 87a Abs. 6 AO) or qualified electronic signatures (§ 14 Abs. 3 UStG).

3. BASIC REQUIREMENTS OF GERMAN SIGNATURE LAW FOR ELECTRONIC SIGNATURES

The basic requirements of German electronic signature law have to be judged taking into consideration two Laws, the Electronic Signature Act and the Electronic Signature Regulation which specifies several articles of the Signature Act. The Signature Regulation contains technical and organisational requirements for certification authorities as well as for producers of electronic signature-devices.

Especially for creating electronic signatures, the Signature Act and the Signature Regulation contain requirements for several defined security standards. The German signature law regulates three security standards for electronic signatures. The starting point is the simple “electronic signature” which Article 2, No. 1 of the Signature Act defines as data in an electronic form which is attached or logically connected with other electronic data and which serve to authenticate the signer. Higher standards are advanced electronic signatures and subsequently, qualified electronic signatures³, each of which have more requirements than the previous signature standard.

To create advanced electronic signatures under Article 2, No. 2 of the Signature Act it is additionally necessary that the electronic signature is uniquely linked to the signatory (a), enables to identify the signatory (b), was created with means that the signatory can maintain under his sole control (c) and is linked to the data to which it relates in a way that any subsequent change of the data is detectable (d).

To create qualified electronic signatures Article 2, No. 3.a of the Signature Act requires additionally the use of “qualified certificates” at the time of creation of the signature. Article 2, No. 3.b requires the creation of qualified signatures with a “secure signature-creation device”. Such a secure signature-creation device can be both, software or hardware-unit to store and to use the private signature key (Article 2, No. 10 of the Signature Act).

Furthermore, requirements for the secure signature-creation device are regulated in Article 17, Section 1 of the Signature Act and in Article 15, Section 1 of the Signature Regulation. Article 17, Section 1 of the Signature Act requires the secure signature-creation device to be protected against “unauthorised use” of the signature key. Article 15, Section 1 of the Signature Regulation specifies this term and requires the secure signature-creation device to be constructed in a way that ensures the signature key to be used only after identification of the signatory by “possession” and “knowledge” or possession and one or more biometric characteristics.

Because the secure signature-creation device is defined as a “soft- or hardware-unit” under Article 2, No. 10 of the Signature Act, there is no legal concept under Article 2 No. 10 that requires solely a hardware solution like smartcards. Because the secure signature-creation

³ Further on, a Certification Authority (CA) can be accredited by the RegTP under Art. 15 of the Signature Act. Qualified electronic signatures which use a certificate from such a CA have special legal effects but are still qualified electronic signatures.

device can also be a software-unit it is not forbidden by law to create qualified electronic signatures with software solutions or combined soft- and hardware solutions.

4. CLASSIFICATION OF ELECTRONIC SIGNATURES CREATED BY CoSIGN

Looking at the product information and the legal requirements under Article 2, No. 1, 2 and 3 of the German Electronic Signature Act, CoSign is also designed to create advanced or qualified electronic signatures.

Article 2, No. 1 of the Signature Act requires for an electronic signature data in an electronic form which is attached or logically connected with other electronic data and which serves to authenticate the signer. CoSign establishes a logical connection between an electronic document and the belonging signature by building a unique document hash. By encrypting the document hash with the private user key and by attaching the signature to the electronic document, CoSign creates an electronic signature which enables an authentication of a user because it can be decrypted only with the public user key that belongs to an identifiable user. Thus CoSign fulfils those requirements.

To create advanced electronic signatures under Article 2, No. 2 of the German Electronic Signature Act additional requirements have to be fulfilled. The fundamental requirements are that the electronic signature is uniquely linked to the signatory, enables identification of the signatory, was created with means that the signatory can maintain under his sole control and is linked to the data to which it relates in a way that any subsequent change of the data is detectable. Electronic signatures created by CoSign are uniquely linked to the signatory because the private keys which are used to encrypt the document hash are linked to a known CoSign-User and because the user keys are also unique. Therefore, the signature also enables the identification of a user. The user maintains the means to create a signature under his sole control because he has an exclusive access to his private signature key which is stored on the secure CoSign-Appliance and by having to authenticate before signing. Finally, electronic signatures created by CoSign cannot be duplicated and altered unnoticed because CoSign uses a secure hash algorithm and a secure RSA algorithm to encrypt the document hash. Therefore, CoSign is designed to fulfil requirements for advanced electronic signatures.

Moreover, CoSign can be used to create qualified electronic signatures under Article 2, No. 3 of the German Electronic Signature Act if it additionally uses a valid qualified certificate at the

time of creation of the signature as well as a secure signature-creation device. The secure signature-creation device has to comply with generally accepted standards like CWA 14169 of the Common Criteria.

5. ELECTRONIC SIGNATURES CREATED AUTOMATICALLY BY CoSIGN

Where advanced or qualified electronic signatures are required by law or by an agreement, CoSign is designed to create such electronic signatures. Furthermore, the creation of - especially qualified - electronic signatures has to proceed in many cases in an automatic mass-process to be economic.

5.1 AUTOMATIC CREATION/ BATCH SIGNING UNDER GERMAN LAW

It is generally possible to create electronic signatures automatically under the German signature law. The motivation of the legislature for the Signature Act in 1997⁴ as well as in 2001⁵ was to give an opportunity to create automatic signatures for mass-processes. The possibility of automatically creating electronic signatures has been the intention of the legislature from the very beginning of the signature law. One sub-topic of the automatic creation of electronic signatures by a machine is high-volume batch signing.

However, the German signature law includes no special regulations for the automatic creation of electronic signatures. Basic requirements of the German signature law for secure signature-creation devices are regulated in Article 17 of the Electronic Signature Act and the Electronic Signature Regulation which specifies this Article. Moreover, the Electronic Signature Regulation contains just technical and organisational requirements for producers of signature-devices.

At present there is no indication that a future reform of the German signature law will lead to new regulations for automatically created signatures. Therefore, several potentially problematic issues under German signature law are still under discussion by scientists and lawyers.

⁴ BT-Drs. 13/7385, 27 und BR-Drs. 966/96, 29.

⁵ Art. 15 Section 2 of the Official Substantiation of the Signature Regulation, 28; also www.regtp.de, FAQ18; The Official Substantiation of the Signature Act 2005 includes no changes, BT-Drs. 15/3417 v. 24.6.2004.

5.2 QUESTIONS DISCUSSED - CoSIGN'S SOLUTIONS

The following contains a brief discussion and an overview of several of the potential problems with the automatic creation/ batch signing of qualified signatures.

- **AUTHENTICATION BEFORE SIGNING**

One question that has been discussed since the evaluation of the Electronic Signature Act is whether there is a requirement for an authentication for each single signature at all, as there are no rules in the Electronic Signature Act or in the appropriate Signature Regulation. An important indication of the legislator's motivation is set down in the official substantiation to Article 15 of the Electronic Signature Regulation.⁶ The legislator assumes secure signature-creation devices to be constructed in a way that regularly offers a user the option to authenticate before each single signature or to authenticate once before creating a certain number of signatures or before the creation of signatures within a certain timeframe. Therefore, the creation of more than one electronic signature after a single authentication process is legal, if the automatic process ensures protection against misuse. Because there are no detailed regulations about the amount of signatures created after a single authentication or about the timeframe, requirements have to be defined in each individual case (e.g. one company using CoSign may decide to allow X automatic signatures before requiring authentication, another company may allow Y minutes to pass before requiring authentication). The requirements depend on the individual context and the need for security.

CoSign solves the discussed requirement by giving a company using CoSign the chance to change the default set-up in the system. If the set-up in CoSign is set in such a way, that a user needs to be authenticated for each signature, CoSign fulfils the legal requirement. Alternatively, CoSign can also fulfil the legal requirement if it is configured in a way that creates user signatures up to a certain amount or within a certain timeframe after a single authentication, taking into consideration the individual context.

⁶ Art. 15 Section 2 of the Official Substantiation of the Signature Regulation, 28; also www.regtp.de, FAQ18.

- **PROTECTION AGAINST UNAUTHORIZED USE**

Another question discussed is the requirements for the secure signature-creation device under Article 2, No. 10, Article 17 of the Electronic Signature Act and Article 15 of the Electronic Signature Regulation. Qualified electronic signatures have to be created with a secure signature-creation device. This signature-creation device can be both soft- or hardware-unit (Art. 2 No. 10).

One of the requirements under Article 17, Section 1 for the secure signature-creation device is to avoid “unauthorized use” of the user’s private signature key. This requirement is specified in the Electronic Signature Regulation under Article 15, Section 1. Article 15 demands the possibility of using the private signature key only after an identification by “possession” and “knowledge” or by possession and one or more biometrical characteristics, in order to protect against unauthorized use of the private signature key. The criteria of possession and knowledge specify the criteria of protecting against unauthorized use. In fact, those criteria led to a discussion whether possession means the physical possession of e.g. a hardware token like a chip card or if a logical possession of the signature key is enough. Neither the substantiation of the legislator to Article 17 of the Electronic Signature Act nor the substantiation to Article 15 of the Electronic Signature Regulation say anything more detailed about the meaning of the term possession. The substantiation of Article 15 only clarifies that possession and knowledge are specifications for the protection against unauthorized use.

Because of other requirements of Article 17 of the Electronic Signature Act, which were regularly fulfilled in the past only by hardware tokens like chip cards (e.g. strong protection against copying a key from the secure signature-creation device), the discussion of the term “unauthorized use” led to an interpretation of possession as a physical possession. In fact, there is no intention in the motivation of the legislator for such an interpretation. In contrast with such an interpretation the discussion actually leads to an interpretation of possession as a logical possession, even if this issue is still contentious. It is clear from the position stated that the term possession should just specify the term of protection against unauthorized use at a time, that the legislator just thought about chip cards being a secure signature-creation device because just chip cards give strong protection against copying a key. But clearly, the motivation of the legislator was showing the legal possibility of automatically creating electronic

signatures from the beginning.⁷ Because the substantiation of the legislature is speaking from “mass-procedures”, e.g. electronic invoicing, it is obvious that the private key in such a mass-procedure cannot be in the sole physical possession of a single signatory. Usually the private key in a mass-procedure will be stored outside the reach of one single user as the keeper of the key, e.g. in a special secure room or maybe in a completely different building. In this case the protection against unauthorized use can usually not be guaranteed by the real physical possession of the signature key, but with a secure access to the key and a secure storage.

Basically, a secure access and a secure storage can also be transferred by a software solution or a combined soft- and hardware solution. The possibility of creating qualified signatures in a secure signature-creation device which is a software-unit is explicitly given under Article 2 No. 10 of the Electronic Signature Act. Similar statements to this conclusion are given in the most recent scientific discussion⁸ as well as in a bulletin from the competent authority in Austria⁹ which is a member-state of the European Union that had to transform the European Directive for Electronic Signatures for the term of “sole control” in case of advanced electronic signatures. The competent authority in Austria says explicitly that the term “sole control”, which shall protect against unauthorized use, can be fulfilled without possession of special hardware. Therefore, further security-measures have to be made. Electronic data have to be encrypted and the access to those data has to be secure in order to give the signatory control.

CoSign solves this question by giving exclusive access to the CoSign-Appliance for all users after authentication and by encrypting the private keys on the CoSign-Appliance with a so-called SVMK-key. This key is stored inside a hardware tamper proof device. Once the CoSign-Box is being opened, the tamper device detects this and will erase the SVMK-key making all the keys stored on the hard disk useless since they cannot be read or decrypted.

⁷ BT-Drs. 13/7385, 27 und BR-Drs. 966/96, 29; Art. 15 Section 2 of the Signature Regulation (Official Substantiation).

⁸ Roßnagel/Fischer-Dieskau, MMR 2004, 133ff.

⁹ www.signatur.rtr.at.

- **REFORM OF THE GERMAN SIGNATURE LAW**

The last actual question picked up in this paper is the future meaning of the reform of the German electronic signature law. Because there is a need of having clear regulations for automatically created signatures, the legislator was expected to enact several regulations for the automatic creation. In fact this has not yet taken place. The new Electronic Signature Act 2005¹⁰ just clarifies other problems of law interpretation. It will, however, not include any systematic change or any special regulations for automatically created signatures.

¹⁰ BT-Drs. 15/3417 v. 24.6.2004.

6. SUMMARY

- Although traditionally chip cards provide strong protection against copying a key from the secure signature-creation device and have therefore been accepted as secure signature-creation devices in the past, it is legal to use specially protected software-devices or combined soft- and hardware devices (Article 2 No. 10 Signature Act).
- Electronic signatures created this way are legally recognized and can have certain, defined legal effects. Those effects are mostly regulated outside the signature law.
- It is legal to create advanced and qualified electronic signatures in an automatic mass-process (also batch signing) under German Law.
- The Authors come to the conclusion that a combined soft- and hardware device concept to store signature keys like the concept used in CoSign is basically suitable to be a secure signature-creation device. It has to be protected by security-measures and has to comply with the generally accepted standard for secure signature-creation devices – CWA 14169 of the Common Criteria.
- To ensure necessary authentication before signing, CoSign can be configured in the subscribed way. It is, for example, possible to configure CoSign in a way that enables an obligatory authentication of a user for each signing process. In this case, the question discussed regarding the need of authentication before signing is fulfilled. Alternatively, CoSign can be configured to authenticate a user before creating a certain number of signatures or before creating signatures within a certain timeframe with regard to the individual situation. In this case, CoSign still complies with this requirement of the German Signature Law.
- The Authors come to the conclusion that CoSign can be configured to protect users against unauthorized use of the signature key by giving secure, exclusive access to the CoSign-Appliance, by means of encrypting the access, the signature credentials and the private keys and by the hardware tamper proof device including the SVMK-key.
- It is necessary to use valid, qualified certificates with CoSign in order to create qualified signatures under German law. Based on information given by Algorithmic Research CoSign supports integration of qualified certificates.

AUTHORS OF THIS STATEMENT

The information contained in this statement was provided by Roland Steidle, Attorney at Law with Waldeck Rechtsanwälte Partnerschaftsgesellschaft and by Thomas H. Fischer, M.B.L., Attorney at Law and Partner of the firm. Roland Steidle is specialised in IT/ Multimedia. Until 2003 he was Research Associate with Prof. A. Roßnagel, University of Kassel, who drafted the German Electronic Signature Act 1997 and who was involved in transforming the European Directive for Electronic Signatures into German law. Thomas Fischer is a versed expert in Europe-wide Outsourcing-Projects and IT-Law. His focus is also in encryption and electronic signatures.

For more information about the authors please see www.waldeck-rechtsanwaelte.com.