Security Confirmation for Technical Components

according to §14 (4) of the German Digital Signature Act and §§16 and 17 German Digital Signature Ordinance

debis Systemhaus Information Security Services GmbH
- Certification Body debisZERT -

Rabinstraße 8
D-53111 Bonn, Germany

hereby confirms in accordance with §14 para. 4 Digital Signature Act[1] and §17 para. 3 Digital Signature Ordinance[2], that

Siemens Sign@tor Version 1.0

complies with the requirements described in this document of Article 3 (Digital Signature Act) of the German Federal Act Establishing the General Conditions for Information and Communication Services endorsed August 1, 1997 resp. the Signature Ordinance endorsed November 1, 1997 and can be operated within the effective range of the specified legal regulations when used properly.

The documentation for this confirmation is registered under

debisZERT.02065.TE.03.2001.

Bonn, 6 April 2001 **(signed by Dr. Heinrich Kersten)**[3]

Certification Body

As published in the Bundesanzeiger (Federal Gazette) No. 31 dated February 14, 1998, p. 1787, debis Systemhaus Information Security Services GmbH – Certification Body debisZERT – was licensed to issue confirmations for technical components according to § 14 para 4 of the German Digital Signature Act.

---

1 „Gesetz zur digitalen Signatur (Signaturgesetz – SigG)“ as of 22.07.1997 (BGBl. I., S. 1870, 1872)

2 „Verordnung zur digitalen Signatur (Signaturverordnung – SigV)“ as of 08.10.1997 (BGBl. I., S. 2498 ff.)

3 (added to translated version only:) Security confirmations in the context of the German Signature Act have to be passed by debisZERT to the “Regulatory Authority for Telecommunications and Posts” in German language; only the official German version is manually signed.

This confirmation for registration number debisZERT.02065.TE.03.2001 consists of 7 pages.

Description of Technical Components:

1 Identification and Delivery of the Technical Component

Identification:

- Siemens Sign@tor, Version 1.0

Vendor:

- Siemens AG Austria
  Siemensstr. 82, A-1210 Vienna

Technical requirements:

Installation on industrial standard PC (CPU: Pentium I or higher, USB interface, Internet connection (optional), storage space / hard disk: min.10 MB, main memory: min. 32 MB) with operating system Windows 98 SE, Windows ME or Windows 2000.

Scope of delivery:

- "Sign@tor terminal" (Version 1.0, intelligent chipcard reader with keypad and display and preinstalled software),

- "Sign@tor PC" (Version 1.0, software including installation and update program as well as online help; supplied on CD)

  The following files are contained on the supplied CD:

File name	Size / Bytes	Date
Root Directory		
`Autorun.inf`	63	21.12.00
Directory `Autorun`		
`Ct_signator.dll`	45056	21.12.00
`Installation.txt`	2675	21.12.00
`Setup.exe`	708608	21.12.00
`Setupcd.ico`	766	21.12.00
`Signator.dll`	327680	21.12.00
`Signator.sig`	128	21.12.00
`Signator.tlb`	2724	21.12.00

File name	Size / Bytes	Date
Directory PC		
Instmsia.exe	1511680	12.12.00
Instmsiw.exe	1509632	12.12.00
Setup.exe	83717	12.12.00
Setup.ini	39	22.03.01
Signator.msi	1071616	22.03.01
Directory Drivers		
Signator2000.inf	6492	21.12.00
Signator98.inf	972	21.12.00
Directory Update		
Updatepc.exe	40960	21.12.00
Updateterminal.exe	24576	21.12.00

The files instmsia.exe and instmsiw.exe are installation packages in compressed form. They also contain important online help for the user. Following installation, this is located in the help subdirectory and has the following properties:

Name: sign@tor.hlp, size: 649444, date: 19.03.01,
Name: signieren.hlp, size: 286632, date: 16.03.01.

The scope of delivery of the product **does not** include a suitable **viewer** or suitable **signature chipcard.**

The following chipcards[4] are approved for use with the product from a technical viewpoint:

- Signature chipcard from the Datakom Austria (A-Sign) company with Infineon processor chip and chipcard operating system CardOS / M4.0,
- Signature chipcard from the A-Trust company with Philips processor chip and chipcard operating system Starcos SPK 2.2 + mod.

2 Functional Description

Siemens Sign@tor, version 1.0, consists of the parts Sign@tor PC (software running on a PC) and the external Sign@tor terminal connected to the PC via USB.

Siemens Sign@tor, version 1.0, serves for

---

4 This security certification does not provide any information on the status of the specified chipcards in terms of their conformity with the signature act.

- secure entry of the user identification data (PIN) and transfer of it to a chipcard (not belonging to the product) via the chipcard reader built into the Sign@tor terminal.

- selection of the file to be signed, support of an external viewer (not belonging to the product) for display of the file to be signed, calculation of the hash value for the selected file for communication security, transfer of this file from the PC to the terminal,

- calculation of the hash value for the selected file in the Sign@tor terminal, hash value comparison by the user (display on PC and on terminal display), upon positive comparison forwarding the hash value to the chipcard for generation of the signature,

- starting the signature operation with the chipcard used,

- takeover of the signature and the user certificate, storage of the file including signature and user certificate in PKCS#7-conform data structure on the PC,

- offline check of other signatures,

- secure maintenance of the software (update) on the Sign@tor PC and Sign@tor terminal.

Note: The offline signature check and software maintenance are not the subject of this security confirmation.

3 Fulfilment of Requirements of Signature Act and the Signature Ordinance

3.1 Fulfilment of Requirements

Siemens Sign@tor, version 1.0, fulfils the following requirements of the Signature Ordinance in the scope specified in context with the prescribed technical and organisational operational conditions:

§16 (2), Sent. 4: **The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key.**

§ 16 (2), Sent. 5: **Security-relevant changes in technical components must be apparent for the user.**

The requirement according to §16 (2), sentence 4, is fulfilled by the product in the considered operational environment by the terminal (which is separate from the PC) used for PIN entry with its own separate keypad, display, chipcard reader and integrated software. The identification data is stored permanently only on the chipcard used, disclosure by the terminal is excluded in the operational environment considered.

The requirement according to § 16 (2), sentence 5, is fulfilled by the product to the extent that no security relevant modifications are possible in the operational environment considered.

§ 16 (3), Sent. 1: **The technical components required for display of data for signing must function in such a manner that the signing person can reliably determine what data is to receive the signature; that**

a digital signature is provided only at the initiation of the signing person; and that such initiation is clearly indicated in advance.

§ 16 (3), Sent. 4: **The technical components must permit adequate determination, as necessary, of the contents of signed data or of data that is to be signed.**

§ 16 (3), Sent. 6: **Security-relevant changes in technical components must be apparent for the user.**

Since the product does not have its own display component (viewer), the requirement in §16 (3), sentence 4 is fulfilled only to the extent that *manipulated* display is not possible in the operational environment considered (here particularly exclusive use of trustworthy software on the PC); however, the precautions for the operational environment considered here are alone not sufficient to allow *secure* display according to the Signature Ordinance: Additional requirements must be placed on the display options of the viewers used in order to sufficiently recognise the content of the data to be signed.

The requirements according to §16 (3), sentence 1 are fulfilled by the product to the extent that precise file selection is possible in the operational environment considered (here particularly exclusive use of trustworthy software on the PC), the signature process can be initiated only by the user and this is clearly indicated in advance.

The requirement according to §16 (2), sentence 5, is fulfilled by the product to the extent that no security relevant modifications are possible in the operational environment considered.

3.2 Terms of Usage

Basic considerations

The user documentation and the specifications in this security confirmation contain important information for secure use of the product and are therefore to be followed strictly.

Delivery

After purchasing (and before every installation), it is necessary for the user to check the Sign@tor terminal to ensure that the seal (bonded points) on the terminal's case is not broken.

Installation

Suitable precautions must be made in the operational environment to prevent unauthorised access to the workstation on which Siemens Sign@tor, Version 1.0 is installed.

The Sign@tor terminal and Sign@tor PC must be located in the same room next to one another so that the PC monitor and terminal display are within the field of vision of the user.

It is necessary to ensure that only trustworthy software is installed and used on the PC. Installation of Siemens Sign@tor, Version 1.0 and other (trustworthy) software on the PC in question should be performed only by qualified personnel.

It is necessary to ensure that an up-to-date virus scanner is always installed on the PC and that it is activated at regular intervals, particularly before installation of Siemens Sign@tor, Version1.0.

The Sign@tor terminal software is already installed when the unit is purchased.

It is necessary for the user to perform the initial installation of the software on the PC with the CD provided in the package with Siemens Sign@tor, Version1.0.

The instructions in the user documentation (Sign@tor online help) on procedures to be taken in the event of erroneous installation are to be followed.

The CD must be stored in a secure place, because it is required for reinstallation and for software maintenance.

Operation

Siemens Sign@tor, Version 1.0, has two operating modes, of which only one fulfils the requirements of the German Signature Act. The certified secured operating mode can be recognised after switching on by the message "Ready" on the Sign@tor terminal display.

It is necessary for the user to keep the PIN required for activation of the chipcard confidential. The PIN must be entered only at the Sign@tor terminal.

It is necessary for the user to ensure that only documents without macros are signed. Where applicable, macros which otherwise would also be signed must be removed from documents before signing. Documents referred to with hyperlinks are not signed.

The user should start the signing operation only after ensuring that the hash values indicated on the PC and the terminal display are identical. For this purpose, it is necessary to scroll through all four lines of the hash value on the terminal before starting the signing operation with OK.

The instructions in the user documentation (Sign@tor online help) for procedures to be taken when the hash values do not coincide are to be observed.

The signing operation can be cancelled with the C key on the terminal.

For security reasons, the signed files should always be checked with the function "Check signature offline".

This offline signature check offered by Siemens Sign@tor, version 1.0, is, however, accomplished without checking the certificate validity and therefore does not completely fulfil the legal requirements.

It is necessary to ensure that only trustworthy software is installed subsequently on the PC.

The file name, file size and creation date indicated on the terminal should be considered only as additional information which is not necessarily reliable.

Update

To update the "Sign@tor PC" software, it is necessary for the user to check the signature of the update with the aid of the (old) original CD. For this reason, it is necessary to keep the original CD securely.

The corresponding check is performed automatically by the terminal when the Sign@tor terminal software is updated.

The instructions in the user documentation (Sign@tor online help) on procedures to be observed in the event of an erroneous update are to be followed.

Important note: When the security certified product Siemens Sign@tor, Version 1.0, is updated, it loses its legally conforming status - unless the security of the update or the updated product has been re-confirmed. Information on this is available to the user on the Web sites of the Regulatory Authority for Telecommunications and Posts under www.regtp.de, from the confirmation body under www.debiszert.de or directly from the vendor.

3.3 Validity of Algorithms and Parameters

The following algorithms and parameters are approved for use for legally conforming digital signatures by the Regulatory Authority for Telecommunications and Posts.

- Hash value calculation according to SHA-1, approved until 31 December 2005.

RSA is used as a further mechanism within the scope of the offline signature check and software updates for Sign@tor PC and Sign@tor terminal; because these functions are not the subject of this security confirmation, no mechanisms except SHA-1 are to be taken into consideration concerning approval by the Regulatory Authority.

This security confirmation remains valid until 31 December 2005; however, it can be extended when no new security findings as to the product or its algorithms are present at that time.

3.4 Assurance Level and Strength of Mechanisms

In accordance with the legal requirements, the technical components considered here were successfully evaluated according to evaluation level **E2** and the ITSEC strength of mechanism **high.**

End of security confirmation for registration number debisZERT.02065.TE.03.2001.