Security Target

to reach the

evaluation level
Common Criteria EAL3+

for the

class 2 smart card reader
SPR332

Table of contents

Certification label: CC: BSI-DSZ-CC-0592
SigG: BSI.02117.TE.xx.20xx

1 ST introduction “ASE_INT.1”

The target of evaluation is the SPR332 smart card reader with the firmware version 6.01.

The smart card reader is available with one delivery version:

- SPR332, USB cable option

1.1 ST identification

Title of the Security Target:	Security Target to reach the evaluation level Common Criteria EAL3+ for the class 2 smart card reader SPR332
Version:	1.35
Issue date:	26.08.2009
Document ID:	CCASESPR
Author:	Torsten Maykranz / SCM Microsystems GmbH
Evaluation level:	EAL3 with augmentations, Strength of security functions “high”
Certification label:	CC: BSI-DSZ-CC-0592 SigG: BSI.02117.TE.xx.20xx

Certification label: CC: BSI-DSZ-CC-0592
SigG: BSI.02117.TE.xx.20xx

1.2 ST overview

The SPR332 smart card readers are universal smart card readers with keypad and offer capability for secure PIN entry and for authentic firmware download.

This security target describes the functional and organisational security requirements and procedures for the TOE and its operational environment. They are compliant to the security targets of SigG/SigV:

- No disclosure or storage of identification data
  (§15 paragraph 2 number 1a SigV)
- Recognizability of security technical modifications
  (§15 paragraph 4 SigV)

1.3 Postulate of CC Conformance

The security target with its functional requirements is compliant to the security requirements according to part 2 and in its requirements for assurance compliant to part 3 of Common Criteria (Version 2.3 August 2005) EAL3 with augmentation (ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4). The strength of security mechanism is classified as “high”.

2 TOE description “ASE_DES.1”

The SPR332 smart card reader represents universal smart card reader devices, which can communicate with processor cards compliant to ISO 7816 and EMV2004 through different application interfaces (CT-API [1], PC/SC [3]). The devices work with all smart card transmission protocols compliant to ISO 7816 [4] (T=0, T=1). Data transmission protocols for memory cards (I^2C, 2-wire, 3-wire protocol) are also supported.

SPR332 readers have a keypad with silicone keys, in order to guarantee a secure PIN entry. The keypads include the numeric keys “0” to “9” as well as the keys “Clear” (yellow), “Confirmation” (green) and “Cancel” (red). The reader recognizes the commands sent by the host, which is typically a PC, and inserts the numbers entered over the keypad as a PIN to the appropriate places of the command to the smart card. Only the fact that a numeric key has been pressed is communicated to the host. This causes the host application to display to the user that a key is pressed and how many numbers of the PIN have been actually entered. The PIN never leaves the reader towards the host.

The readers can be used at all host systems that possess a USB interface. They are used as accessories in the PC surrounding field. The current supply is made by the USB bus.

On the host side the application interfaces are made available as CT-API and PC/SC, which can be used for all types of smart cards. All functions at the interfaces are illustrated for CT-API in accordance with [1] and for PC/SC in accordance with [3]. Further interfaces (such as OCF) are in planning.

The SPR332 smart card reader does not possess any functionality that works without connection to a host. It must generally be operated at a host.

Details on available host software such as drivers, libraries and tools are available in the user manual of the SPR332.
The driver software is not included in this evaluation. The TOE ends at the USB interface to the host computer. Installation software including drivers, manual and tools (such as the tool to verify the firmware version) can be downloaded from: http://www.scmmicro.com/security/pcs_product_drivers.html.

SPR332 smart card readers are usable in many market segments because of their multi-functionality. As class 2 readers [5], the SPR332 readers are also able to enter identification data (PIN) and convey it securely to secure signature production units (signature smart cards) according to §2 number 10 SigG; therefore the readers can also be used for applications in accordance with signature law and signature regulation [6], [7]. Moreover, they can be used for the transmission of the hash value from the application to the signature card and for the provision of a signature from the card for use in signature applications. Thus, they represent a partial component for signature applications, which require a security confirmation to be able to be used for qualified electronic signatures under §2 number 3 SigG. For the use of the TOE in accordance with SigG/SigV, only signature applications and smart cards can be used that were evaluated and confirmed in the SigG context. SPR332 smart card readers fulfill the special requirements under §15 paragraph 2 number 1a (no disclosure or storage of identification data) and paragraph 4 (recognizability of security-relevant changes) to SigV.

The following list of supported instruction bytes for the secure PIN input must be used by the applications and be supported by smart cards in accordance with the specification. Non-supported instruction bytes will be rejected with a qualified error message:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-4): INS=0x24
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-4): INS=0x2C
- UNBLOCK APPLICATION (EMV2004): INS=0x18

The SPR332 smart card reader family offers secured firmware download, in order to be prepared for future requirements. The verification of a signature of the firmware with the asymmetrical RSA algorithm and a bit length of 2048 guarantees the integrity and authenticity of the firmware during the loading of the firmware into the smart card reader. The manufacturer SCM Microsystems ensures the secure generation and administration for the production of the necessary secure signature key. SCM guarantees that each new version of the TOE receives a new version number and thus is clearly identifiable.

The user may download actual firmware versions of SPR332 from SCMs web site (http://www.scmmicro.com/security/pcs_product_drivers.html) together with a Windows tool to download the new firmware to the smart card reader.
SCMs web site clearly states during the download of firmware if the respective firmware is CC certified or not.
If a non CC certified firmware version is loaded to the TOE, the smart card reader loses the CC certified and SigG/SigV confirmed status.
A software tool is provided with which the user can control the version number of the TOE to correspond with the confirmed firmware version.

The housing is sealed by means of a falsification secure security sticker, which will be destroyed during removal and thus can be used only once. The seal is compliant to the technical guidline [BSI 7586] with security level 1 and manufactured by “wilkri etiketten”.

The Common Criteria certification report of SPR332 is available at http://www.bsi.de and the SigG/SigV compliance confirmation at http://www.bundesnetzagentur.de.

Certification label: CC: BSI-DSZ-CC-0592
SigG: BSI.02117.TE.xx.20xx

SPR332 smart card readers demonstrate different operating conditions by means of two LEDs and a buzzer as follows:

	LED1 (green)	**LED2 (orange)**	**Buzzer*2**
Just after power on Just after DFU*1 operation	OFF	OFF	740Hz / 25ms
Reader powered	0.5s ON 4.5s OFF	OFF	OFF
Smart card powered	ON	OFF	OFF
Smart card communication	500ms ON 500ms OFF	OFF	OFF
Secure PIN entry mode	ON	500ms ON 500ms OFF	Diff. sounds for each keys 0-9 2400Hz / 25ms Clear 1100Hz / 25ms Cancel 1100Hz / 25ms OK 1100Hz / 25ms PIN Success: 900Hz / 100ms 1200Hz / 100ms PIN Fail 300Hz / 100ms
PIN entry successfully completed, Smart card powered	ON	ON	OFF
PIN entry successfully completed, Smart card communication	500ms ON 500ms OFF	ON	OFF
Smart card communication Error	100ms ON 100ms OFF	Previous state	OFF
Self test during boot of SPR332 failed	100ms ON 100ms OFF	Previous state	OFF
Firmware upgrade running	OFF	ON	OFF
Firmware upgrade failed	OFF	32ms ON 32ms OFF	OFF
BootROM mode	ON	ON	OFF
Diagnostic mode	250ms ON 250ms OFF	250ms ON 250ms OFF	depends on test function

*1 Device Firmware Upgrade *2 can be disabled by host application

Certification label: CC: BSI-DSZ-CC-0592
SigG: BSI.02117.TE.xx.20xx

3 TOE security environment “ASE_ENV.1”

This chapter describes the security aspects of the environment in which the TOE is used, those values that can be protected and the acting subjects (like users and attackers). Moreover, the organizational security precautions and references to the secure use of the TOE are represented.

The values that can be protected are identification data (PIN) of the user as well as the firmware and hardware of the smart card reader itself.

The threats of the TOE by an attacker are:

- Uncovering identification data
- Security-relevant changes in the equipment

An attacker with high offensive capability cannot uncover identification data from the TOE. The firmware guarantees that the commands for verifying and modifying the PIN are recognized and worked on by the security function “Secure PIN entry”. This security function ensures that the PIN input is passed on surely over the keypad of the smart card reader to the smart card, without the possibility to be spied out by the host computer.
The storage areas of the PIN data are reworked by the firmware, so that no attack on stored data is possible.
The requirements of the environment of the deployment are formulated in a way that the user must be able to enter his or her identification data unobserved.

The falsification secure security seal guarantees the recognition of security-relevant changes.

3.1 Assumptions

The SPR332 smart card readers are suitable both for the office and for private use. Due to multi-functionality, the readers can support additional uses beyond signature applications, such as secure home banking.

The end user is informed about his or her responsibility during the use of the TOE:

A_USER.VERSION:

It is assumed that the user verifies routinely with a software tool provided by the manufacturer, whether the version number of the TOE agrees with the confirmed version, before use of the smart card reader.

Applications in accordance with §2 number 11 SigG should verify automatically that only confirmed versions of the TOE are used, in order to remove this task from the end user.

A_USER.UNOBSERV:

The user must enter his or her identification data unobserved.

A_USER.KEYPAD:

It is assumed that the user enters his or her identification data using the keypad of the TOE.

A_USER.LED:

While the PIN is being entered on the keypad of the reader, the status of the LED verifies that the mode of the secure PIN input is active.

A_USER.SEAL:

The user routinely has to examine that the security seal is intact.

A_USER.STORE:

The rules to the secure keeping and non-proliferation of the PIN are communicated to the user by the publisher of the smart card.

A_USER.USAGE:

The TOE is laid out for use in private and office environments.
In an office environment, the SPR332 smart card reader should be arranged in such a way that the usage is avoided by unauthorized users. That means that the smart card reader is set up in such a manner that its usage is possible for authorized persons only and that a working environment protected from manipulation attempts has to be guaranteed.
An unobserved input of identification data (PIN) is to be ensured by suitable measures at the place of work.

A_USER.ISO_EMV:

For applications requesting a secure PIN input the user has to use only processor smart cards compliant to ISO 7816 or EMV.

A_USER.FWLOAD:

The user may download firmware versions of the TOE from the Internet site of the manufacturer, the supplier or the distributor as well as from intranet sites of a company.
It is assumed that it is clearly communicated during the download of the firmware from an external source, whether or not the firmware is CC certified.
It is assumed that the user will download CC certified firmware versions only.
It is assumed that the user knows that he or she will loose the CC certified and SigG/SigV confirmed status of the product, if he or she downloads any non CC certified firmware version to the TOE.

A_USER.SIG_APP:

It is assumed that for the use of the TOE in accordance with SigG/SigV, only applications and smart cards that were evaluated and confirmed in the SigG context are used.

3.2 Threats

In the following section, threats are represented that require special preventive measures within the TOE or in its environment. The authors of threats are identified and described by attacks and attacked values. The motivation of the attacker is to spy the PIN of the user. It is assumed that an attacker should have very good knowledge in electronics and software.
The attacker could use the following weak points of the TOE:

- the interface between readers and smart card
- the keypad for the PIN entry
- the firmware download

Opportunity for attack is offered, if the TOE is unobserved by the user or if the user is careless during PIN entry.

The PIN as identification code of the user represents a personal secret. An attacker has two possibilities to uncover this secret:

T.REVEAL:

The attacker could try to intercept the communication between host and smart card and/or smart card reader over a Trojan horse (virus), if the PIN is entered into the host equipment. Or the attacker could try to attain a PIN code outside of the commands planned for it.

T.STORE:

Storage of identification data:
Storing identification data in the TOE also poses a danger of attack because these data could be obtained from the TOE by an attacker, if the attacker came into the possession of the TOE and would have the technical facility.

Security-type modifications give the opportunity to an attacker to obtain identification data in the TOE and arrive thus in possession of the PIN:

T.DOWNLOAD:

By manipulations during the download, a modified or unauthorized firmware could be loaded into the reader, which could contain capabilities for uncovering the PIN.

T.SEAL:

By manipulation of the seal and following manipulation of the hardware after opening the reader the attacker can intercept the communication between reader and smart card.

3.3 Organisational security policies

There are no organisational security policies intended for this TOE.

4 Security objectives “ASE_OBJ.1”

4.1 Security objectives for the TOE

The SPR332 smart card reader serves to get the identification data (PIN) from the user. The basic security objectives for the TOE are:

O.REVEAL:
The TOE does not reveal any identification data.

O.TRANSFER:
The TOE guarantees that the PIN is only transferred to the smart card.

O.INS_BYTE:
The TOE guarantees that the PIN is transferred to the smart card only using PIN commands with specified instruction bytes.

O.SIGNAL:
The TOE guarantees that the secure PIN entry mode is clearly signaled to the user.

O.STORE:
The TOE does not store any identification data.

O.DOWNLOAD:
The TOE guarantees that newly downloaded firmware will be accepted only if integrity and authenticity are successfully verified.

O.SEAL:
The TOE guarantees that the user may be alerted to security critical modifications by changes made to the security seal.

4.2 Security objectives for the environment

The security objectives for the environment correspond in a general manner to those under 4.1 specified:

OE.UNOBSERV:
The user must be able to enter his or her identification data unobserved.

OE.KEYPAD:
The user must enter his or her identification data using the keypad of the TOE.

OE.LED:
The user must examine the status of the LED during PIN entry on the keypad of the reader to check that the mode of the secure PIN input is active.

OE.ISO_EMV:
For applications requesting a secure PIN input the user must use only processor smart cards compliant to ISO 7816 or EMV.

OE.USAGE:
The TOE should to be used in non-public, private and office environment only. An unobserved input of identification data (PIN) is to be ensured by suitable measures at the place of work.

OE.STORE:
The user may not store his or her identification data unsecured outside the secure smart card.

OE.SEAL:
The user must examine regulary before use that the security seal is intact.

OE.VERSION:
In regular intervals the user must verify that the version number of the TOE agrees with the confirmed version. The user uses a software tool provided by the manufacturer, supplier or system integrator.

Applications in accordance with §2 number 11 SigG should verify automatically that only confirmed versions of the TOE are used, in order to remove this task from the end user.

OE.FWLOAD:

The user may download firmware versions of the TOE from the Internet site of the manufacturer, supplier or distributor as well as from intranet sites of a company.
It must be clearly communicated during the download of the firmware from an external source whether or not the firmware is CC certified.
The user should download CC certified firmware versions only.
The user has to be informed that he or she will lose the CC certified and SigG/SigV confirmed status of the product, if any non CC certified firmware versions are downloaded to the TOE.

OE.SIG_APP:

For the use of the TOE in accordance with SigG/SigV, only applications and smart cards that were evaluated and confirmed in the SigG context may be used.

4.3 Dependencies: requirements SigG/SigV – security objectives

In the following table the required security requirements of SigG/SigV are referenced to the security objectives of Common Criteria.

Law / order	Text of law	Security objectives	Description
§15 paragraph 2 number 1a SigV	Signaturanwendungs-komponenten nach §17 Abs. 2 des SigG müssen gewährleisten, dass bei der Erzeugung einer qualifizierten Signatur die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden. (Signature application components pursuant to Section 17 (2) of the Signatures Act must ensure that, when producing a qualified electronic signature the identification data are not disclosed and are stored only on the relevant secure signature creation device)	O.REVEAL	The TOE guarantees that the PIN does not leave the reader toward the host.
		O.STORE	The TOE does not store any identification data.
		O.SIGNAL	The TOE guarantees that the secure PIN is clearly signaled to the user.
		O.TRANSFER	The TOE guarantees that the PIN is only transferred to the smart card.
		O.INS_BYTE	The TOE guarantees that the PIN is transferred to the smart card only using PIN commands with specified instruction bytes.
		OE.LED	The user must examine the status of the LED during PIN entry on the keypad of the reader to check that the mode of the secure PIN input is active.
		OE.KEYPAD	The user must enter his or her identification data using the keypad of the TOE.

§15 paragraph 4 SigV	Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar sein (Security-relevant changes in technical components pursuant to subsections (1) to (3) must be apparent for the user)	O.SEAL	The TOE guarantees that the user may recognize security critical modifications by the security seal.
		O.DOWNLOAD	The TOE guarantees that newly downloaded firmware will be accepted only if integrity and authenticity are successfully verified.
		OE.SEAL	The user must examine regulary before use that the security seal is intact.
		OE.VERSION	In regular intervals the user must verify that the version number of the TOE agrees with the confirmed version.
		OE.FWLOAD	The user should download CC certified firmware versions only.

5 IT security requirements “ASE_REQ.1”

5.1 Functional security requirements of the TOE

FCS Cryptographic support:

SFR.FCS_COP.1_RSA: Cryptographic operation
The TSF shall perform a secure firmware download by means of decoding and verification of signed data in accordance with a specified cryptographic algorithm by RSA and cryptographic key sizes of 2048 bit length that meet the following:
Norms PKCS #1 Ver. 1.5, section 10.2 and ISO/IEC 14888-2:2008, section 6.

The verification of a signature of the firmware with the asymmetrical RSA algorithm and a bit length of 2048 in connection with SFR.FCS_COP.1_SHA guarantees the integrity and authenticity of the firmware while loading the firmware into the smart card reader.

SFR.FCS_COP.1_SHA: Cryptographic operation
The TSF shall perform a secure firmware download by means of decoding and verification of signed data in accordance with a specified cryptographic algorithm by SHA-256 and cryptographic key sizes, which are here not relevant, that meets the following:
Norms FIPS180-2 and ISO/IEC 10118-3

The verification of a signature of the firmware based on a 256-bit hash value in accordance with SHA-256 and in connection with SFR.FCS_COP.1_RSA guarantees the integrity and authenticity of the firmware while loading of the firmware into the smart card reader.

FDP User data protection:

SFR.FDP_ACC.1: Subset access control
The TSF shall enforce the smart card reader access policies *on* the subjects:

- **S.USER:** User through the keypad interface
- **S.PC:** PC through the USB interface
- **S.ICC:** Smart card through the card reader interface

the objects:

- **OB.PIN:** PIN
- **OB.LED:** Two LEDs
- **OB.FW:** Firmware

and the operations covered by the SFP:

- **OP.P_ENTRY:** PIN entry
- **OP.P_VERIFY:** Verification of the PIN
- **OP.L_CONTROL:** Control of the LEDs
- **OP.F_DOWNLD:** Download valid signed firmware

Connections: subjects - objects - operations

	S.USER	S.PC	S.ICC
OB.PIN	**OP.P_ENTRY**		**OP.P_VERIFY**
OB.LED		**OP.L_CONTROL**	
OB.FW		**OP.F_DOWNLD**	

The subjects S.* are accessing the objects OB.* by the operations OP.*.

SFR.FDP_ACF.1: Security attributes based access control
FDP_ACF.1.1:
The TSF shall enforce the smart card reader access policies *to objects based on* the identity of the object.

The TSF must enforce the
subjects:
- User through the keypad interface
- PC through the USB interface
- Smart card through the card reader interface

objects:
- PIN
- Two LEDs
- Firmware

and operations:
- PIN entry
- Verification of the PIN
- Control of the LEDs
- Download valid signed firmware

The identity of the objects is sufficient as security attribute, since the objects are attainable only over defined interfaces of the TOE and for each interface only one subject is defined.

FDP_ACF.1.2:
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The PC (S.PC) sends commands on behalf of the application to the reader, which causes the TOE to then only cause the LEDs (OB.LED) to display the secure indicator mode (OP.L_CONTROL) and to pass the entered PIN (OB.PIN) to the smart card, if:

1.) the commands to the smart card reader are recognizable on the basis of their command structure in accordance with CCID [8] as such for verifying or modifying the PIN, and in addition
2.) a command with one of the following instruction bytes, which can be passed on to the smart card, is contained:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-4): INS=0x24
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-4): INS=0x2C
- UNBLOCK APPLICATION (EMV2004): INS=0x18

The PIN (OB.PIN) must be entered by the user (S.USER) at the keypad of the TOE (OP.P_ENTRY).

The PIN (OB.PIN) may be sent only over the card reader interface to the smart card (S.ICC) for verification of the PIN (OP.P_VERIFY).

The download of a new firmware (OP.F_DOWNLD), initiated by the PC (S.PC), may be only accepted, if the integrity and authenticity of the firmware (OB.FW) were successfully verified on the basis of its signature with the asymmetrical RSA algorithm and a bit length of 2048.

FDP_ACF.1.3:
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:
None.

FDP_ACF.1.4:
The TSF shall explicitly deny access of subjects to objects based on (*the*)
No further rules.

SFR.FDP_RIP.2: Full residual information protection
The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from *all objects.*

A memory rework of the buffer for the transmission of the PIN from the keypad to the smart card is realized with the power-on procedure, after transmission of the command to the smart card, after pulling the card, in the case of abort by the user, with a timeout during the PIN input and after defined resetting commands initiated by the host.

FTA TOE access

SFR.FTA_TAB.1: Default TOE access banners
Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

During execution of the function “Secure PIN entry” the orange LED is switched into the flashing mode.

After transmission of the PIN to the signature component (smart card) and confirmation by the smart card with the status byte SW1=0x90 the orange LED is turned on.

A disturbance of the card reader caused intentionally or due to a technical failure is indicated to the user by fast flashing the green LED.

Invalid data are rejected. An error message is transferred to the host.

FPT TOE material protection

SFR.FPT_PHP.1: Passive detection of physical attack
The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
The TSF shall provide the capability to determine whether physical tampering with the TSF’s devices or TSF’s elements has occurred.

The housing is sealed by means of a falsification secure security sticker, which will be destroyed during removal and thus can be used only once. Thus the user can recognize by the condition of the safety seal that no manipulations at the hardware were made.

5.2 Minimum strength of TOE security objectives

By the use of the algorithms RSA and SHA-256 in the security function SF.SECDOWN, the TOE offers protection against high offensive capability and fulfills the minimum strength of functions "high", as demanded in SigG.

5.3 Assurance requirements of the TOE

The requirements for the aimed evaluation assurance level 3 with augmentations are listed in table 6.4 Common Criteria part 3 as follows:

Assurance class	Assurance components
Class ACM: Configuration management	ACM_CAP.3 Authorisation controls ACM_SCP.1 TOE CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification ADV_HLD.2 Security enforcing high-level design ADV_RCR.1 Informal correspondence demonstration ADV_IMP.1: Subset of the implementation of the TSF ADV_LLD.1 Descriptive low-level design
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Class ALC: Life Cycle Documents	ALC_DVS.1 Identification of security measures ALC_TAT.1: Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: high-level design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing sample
Class AVA: Vulnerability assessment	AVA_MSU.3: Analysis and testing for insecure states AVA_SOF.1 Strength of TOE security function evaluation AVA_VLA.4 Highly resistant

5.4 Security requirements for the IT environment

There are no security requirements for the IT environment.

6 TOE summary specification “ASE_TSS.1”

6.1 TOE security functions

To realize a qualified electronic signature it is necessary that the user identifies himself or herself to the signature application. This could be done for instance using a PIN of his or her signature card.
The private PIN code has therefore to be protected.
The PIN data should be stored in the smart card reader only as long as the corresponding command is sent to the smart card or until the smart card is removed.

The security specific functions to ward off any threats and reach the security objectives are listed below:

SF.PINCMD:

The firmware in the reader checks the commands sent to the reader by means of the command structure compliant to the USB smart card reader specification.
If the commands for Verification or Modification of the PIN are recognized and if the command, which has to be forwarded to the smart card, contains one of the following instruction bytes:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-4): INS=0x24
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-4): INS=0x2C
- UNBLOCK APPLICATION (EMV2004): INS=0x18

it will be switched into the mode for secure PIN entry over the integrated keypad.

The security function SF.PINCMD recognizes the command for PIN entry, sent by the host software, and inserts the PIN data entered over the keypad to the corresponding place in the command to the smart card. As well, only the fact that one of the numeric keys is pressed is reported to the host.

This information is used by the host application to show the user with "*" the progress of PIN entry.
During the PIN entry the corresponding LEDs display the mode of secure PIN entry.
Even a determined attacker with significant technical capabilities cannot bypass the security functions, as based on the implementation there is no possibility to manipulate the processing of the PIN commands in the TOE. An attacker can not influence the program flow of SF.PINCMD in the TOE which guarantees the protection of the PIN data.
The exchange of the PIN takes place only between smart card and TOE over the card reader interface. This interface is inside the TOE and from manipulation protected by the security seal.

SF.CLMEM:

The memory area for the PIN data will be reworked after transfer of the command to the smart card, after removing the card, after cancellation by the user, after a timeout during PIN entry, during switch on process and after defined reset commands from the host.
Even a determined attacker with significant technical capabilities cannot bypass the security functions, as based on the implementation there is no possibility to manipulate the rework of the memory area in the TOE. An attacker can not influence the program flow of SF.CLMEM in the TOE which guarantees the erasing of the PIN data in the internal memory of the TOE as described above. An evasion of SF.CLMEM would be only possible if a manipulated firmware would be loaded, which is however not possible due to SF.SECDOWN.

SF.SECDOWN:

The verification of a signature of the firmware with the asymmetric RSA algorithm and a bit length of 2048 guarantees the integrity and authenticity of the firmware during loading of a new firmware into the smart card reader.
The hash value over those firmware, which will be loaded, is determined based on the algorithm SHA-256 with a length by 256 bits. The verification of the integrity and authenticity takes place in the TOE via comparison of the determined hash value and the hash value as a component of the decoded signature. The public key for this operation is stored in the TOE.
Even a determined attacker with significant technical capabilities cannot bypass the security functions, as based on the implementation there is no possibility to get the private key to manipulate the TOE.
As the probability of guessing or calculating the key is negligible, SF.SECDOWN is fulfilling the minimum strength of functions "high."

6.2 TOE security measures

The housing is sealed by means of a falsification secure security sticker, which will be destroyed during removal and thus can be used only once.
Thus the user can recognize by the condition of the safety seal that no manipulations at the hardware were made.

6.3 Assurance measures

The assurance measures are reflected by the following documents of the manufacturer.

- Configuration management
- Delivery and operation
- Development:
  - Informal functional specification
  - Security enforcing high-level design
  - Informal correspondence demonstration
  - Descriptive low-level design
  - Subset of the implementation of the TSF
- User guidance
- Life cycle support / Identification of security measures
- Test documentation
- Vulnerability assessment

7 PP claims “ASE_PPC.1”

The present Security Target is not aiming at fulfillment of a PP.

8 Explanation

8.1 Explanation of the security target

These chapters furnish the proof that the security target is complete and result coherently in a consistent whole, which corresponds to the security objectives.
The SPR332 smart card readers fulfill the requirements under §15 paragraph 2 number 1a (no disclosure or storage of identification data) and paragraph 4 (recognizability of security-relevant changes) to SigV.

8.1.1 Connections: assumptions – security objectives, threats – security objectives

Assumptions	Security objectives	Comments
A_USER.LED	OE.LED	During PIN entry on the keypad of the reader the status of the LED has to be verified, that the mode of the secure PIN input is active.
A_USER.VERSION	OE.VERSION	By means of a software tool it is to be checked in regular intervals that the version number of the TOE agrees with the confirmed firmware release. Applications in accordance with §2 number 11 SigG should automatically verify that only confirmed versions of the TOE are used, in order to remove this task from the end user.
A_USER.SEAL	OE.SEAL	The user regularly has to examine that the security seal is intact.
A_USER.STORE	OE.STORE	The rules to the secure keeping and non-proliferation of the PIN are communicated to the user by the publisher of the smart card.
A_USER.USAGE	OE.USAGE	The operational area of the TOE is clearly defined with home and office applications.
A_USER.UNOBSERV	OE.UNOBSERV	The user must enter his or her identification data unobserved.
A_USER.KEYPAD	OE.KEYPAD	The user must enter his or her identification data using the keypad of the TOE.
A_USER.ISO_EMV	OE.ISO_EMV	For applications requesting a secure PIN input the user must use only processor smart cards compliant to ISO 7816 or EMV.
A_USER.FWLOAD	OE.FWLOAD	The user will download CC certified firmware versions only.
A_USER.SIG_APP	OE.SIG_APP	For the use of the TOE in accordance with SigG/SigV, only applications and smart cards that were evaluated and confirmed in the SigG context, may be used.

Threats	Security objectives	Comments
T.REVEAL	O.REVEAL	The TOE guarantees that the PIN does not leave the reader toward the host.
	O.SIGNAL	The TOE guarantees that the secure PIN is clearly signaled to the user.
	O.TRANSFER	The TOE guarantees that the PIN is only transferred to the smart card.
	O.INS_BYTE	The TOE guarantees that the PIN is transferred to the smart card only using PIN commands with specified instruction bytes.
	OE.USAGE	The TOE has to be used in non public but private and office environments only.
	OE.SEAL	The user must examine regulary before use that the security seal is intact.
T.STORE	O.STORE	The TOE does not store any identification data.
	OE.STORE	The user may not store identification data unsecured.
T.DOWNLOAD	O.DOWNLOAD	The secure firmware download guarantees that the TOE cannot be changed without authorization.
	OE.FWLOAD	The user should download CC certified firmware versions only.
T.SEAL	O.SEAL OE.SEAL	The user can recognize by the condition of the security seal that no manipulations at the hardware were made.

- By using a "Trojan horse", an attacker could try to spy the PIN entered by the user. Since the PIN will be transferred only within the TOE directly to the smart card, it is not possible to spy the PIN with such "Trojan horses".
- An attacker could try to modify the firmware to read out the PIN. Since the TOE accepts only a correctly signed firmware for the download, loading a manipulated firmware is not possible.
- An attacker could try to open the TOE and manipulate it in such a way that the PIN could be read out. Since the TOE is sealed and the user is able to examine the sealing before each use, a manipulation of the TOE is already identifiable from the outside by the user.

The security objectives are suitable to counter the identified threats to security.

8.1.2 Cross references: threats – security objectives of the TOE

	T.REVEAL	T.STORE	T.DOWNLOAD	T.SEAL
O.REVEAL	√			
O.STORE		√		
O.SEAL				√
O.SIGNAL	√			
O.TRANSFER	√			
O.INS_BYTE	√			
O.DOWNLOAD			√	

8.1.3 Cross references: assumptions/threats – security objectives of the environment

	OE. UN OBSERV	OE. KEY PAD	OE. LED	OE. FW LOAD	OE. SIG_APP	OE. ISO_ EMV	OE. USAGE	OE. STORE	OE. SEAL	OE. VER SION
A_USER. UNOBSERV	√									
A_USER. KEYPAD		√								
A_USER. LED			√							
A_USER. VERSION										√
A_USER. SEAL									√	
A_USER. STORE								√		
A_USER. USAGE							√			
A_USER. ISO_EMV						√				
A_USER. FWLOAD				√						
A_USER. SIG_APP					√					
T.REVEAL							√		√	
T.STORE								√		
T.DOWNLOAD				√						
T.SEAL									√	

8.2 Explanation of the security requirements

Together with the security requirements of the environment the TOE corresponds to the security-relevant requirements.

The SPR332 smart card readers fulfill the special requirements under §15 paragraph 2 number 1a (no disclosure or storage of identification data) and paragraph 4 (recognizability of security-relevant changes) to SigV.

The security functions SF.PINCMD and SF.CLMEM for secure PIN input including LED control and memory rework are not directly open to attack due to their implementations.
The secure firmware download corresponds to the requirements according to the minimum strength of the functions “high.”
An attacker with high offensive capability cannot go around the security functions, since he or she cannot attain an access to the security functionality of the TOE.
Thus the TOE is consistent with the security objectives.

The minimum strength of the functions “high” is appropriate and consistent with the TOE security objectives of non-revealing and non-storing from identification data and the recognizability of security-relevant changes.

The minimum strength of the functions “high” is appropriate for the requirements to the assurance, which reflects itself in the requirements going beyond EAL3

- ADO_DEL.2 (detection of modification)
- ADV_IMP.1 (subset of the implementation of the TSF)
- ADV_LLD.1 (descriptive low-level design)
- ALC_TAT.1 (well-defined development tools)
- AVA_MSU.3 (analysis and testing for insecure states)
- AVA_VLA.4 (highly resistant)

The quantity of the selected security requirements forms a mutually support and whole consistent in itself, since all relevant dependence is considered. The formulated requirements of the security policies are a completing part of this security system.

8.2.1 Connections: security objectives – security requirements

Security objectives	Security requirements	Comments
O.REVEAL O.TRANSFER O.INS_BYTE	SFR.FDP_ACC.1 SFR.FDP_ACF.1	The security function of the “Secure PIN entry” guarantees that only approved commands are passed to the smart card.
O.SIGNAL	SFR.FTA_TAB.1	The LEDs of the reader display the mode of the “Secure PIN entry”.
O.STORE	SFR.FDP_RIP.2	A memory rework of the buffer for the transmission of the PIN from the keypad to the smart card is realized with the power-on procedure, after transmission of the command to the smart card, after pulling the card, in the case of abort by the user, with a timeout during the PIN input and after defined resetting commands from the host.
O.DOWNLOAD	SFR.FDP_ACF.1 SFR.FCS_COP.1_RSA SFR.FCS_COP.1_SHA	The verification of a signature of the firmware with the hash algorithm SHA-256 and the asymmetrical RSA algorithm with a bit length of 2048 guarantee the integrity and authenticity of the firmware while loading of the firmware into the smart card reader.
O.SEAL	SFR.FPT_PHP.1	The falsification secure security seal, which will be destroyed during removal and thus can be used only once, guarantees that the user may recognize security critical modifications.

8.2.2 Cross references: security objectives – security requirements

	O.REVEAL	O.STORE	O.SEAL
SFR.FDP_ACC.1	√		
SFR.FDP_ACF.1	√		
SFR.FTA_TAB.1			
SFR.FDP_RIP.2		√	
SFR.FCS_COP.1_RSA			
SFR.FCS_COP.1_SHA			
SFR.FPT_PHP.1			√

	O.SIGNAL	O.TRANSFER	O.INS_BYTE	O.DOWNLOAD
SFR.FDP_ACC.1		√	√	
SFR.FDP_ACF.1		√	√	√
SFR.FTA_TAB.1	√			
SFR.FDP_RIP.2				
SFR.FCS_COP.1_RSA				√
SFR.FCS_COP.1_SHA				√
SFR.FPT_PHP.1				

8.2.3 Dependencies of functional security requirements

	Security requirements	Dependencies	Reference
SFR1	SFR.FCS_COP.1_RSA	*[FDP_ITC.1 or* *FCS_CKM.1]* *FCS_CKM.4* *FMT_MSA.2*	not applicable not applicable not applicable not applicable
SFR2	SFR.FCS_COP.1_SHA	*[FDP_ITC.1 or* *FCS_CKM.1]* *FCS_CKM.4* *FMT_MSA.2*	not applicable not applicable not applicable not applicable
SFR3	SFR.FDP_ACC.1	*FDP_ACF.1*	SFR4
SFR4	SFR.FDP_ACF.1	*FDP_ACC.1* *FMT_MSA.3*	SFR3 not applicable
SFR5	SFR.FDP_RIP.2	*none*	-
SFR6	SFR.FTA_TAB.1	*none*	-
SFR7	SFR.FPT_PHP.1	*FMT_MOF.1*	not applicable

SFR1: SFR.FCS_COP.1_RSA

FDP_ITC.1

- *Import of user data without security attributes*
- No direct dependence for the TOE, since the key is brought in with the manufacturer and delivered with the TOE

FCS_CKM.1

- *Cryptographic key generation*
- A requirement for the development environment of the manufacturer, which is describing the generation of the keys
- No direct dependence for the TOE

FCS_CKM.4

- *Cryptographic key destructions*
- A requirement for the IT environment describing the destruction of the generated private keys
- No direct dependence for the TOE, since this contains only the public key

FMT_MSA.2

- *Secure security attributes*
- No dependence for the TOE, since only one key for the secure firmware download is present, whereby a management of the security attributes can be dropped

SFR2: SFR.FCS_COP.1_SHA

FDP_ITC.1

- *Import of user data without security attributes*
- No dependence, since the hash algorithm does not use keys

FCS_CKM.1

- *Cryptographic key generation*
- No dependence, since the hash algorithm does not use keys

FCS_CKM.4

- *Cryptographic key destructions*
- No dependence, since the hash algorithm does not use keys

FMT_MSA.2

- *Secure security attributes*
- No dependence, since the hash algorithm does not use keys

SFR3: SFR.FDP_ACC.1

FDP_ACF.1

- *Security attribute based access control*
- See SFR.FDP_ACF.1

SFR4: SFR.FDP_ACF.1

FDP_ACC.1

- *Subset access control*
- See SFR.FDP_ACC.1

FMT_MSA.3

- *Static attribute initialisation*
- No dependence for the TOE, since only one key for the secure firmware download is present, whereby a management of the security attributes can be dropped

SFR5: SFR.FDP_RIP.2

No dependencies

SFR6: SFR.FTA_TAB.1

No dependencies

SFR7: SFR.FPT_PHP.1

FMT_MOF.1

- *Management of functions in TSF*
- No dependence for the TOE, since no change of the behavior of the security function is possible, whereby a management of the behavior of the security functions can be dropped

8.2.4 Connections: security requirements – IT environment

There are no security requirements for the IT environment.

8.3 Explanation of the TOE summary specification

8.3.1 Security requirements and security functions

Those in the following represented security functions complement each other and correspond in their cooperating to the security requirements of the TOE. All security requirements are covered by the existing security functions, which complement each other mutually to an overall secure system.

	Security function	**Security requirement**	**Comment**
SF1	SF.PINCMD	SFR.FDP_ACC.1 SFR.FDP_ACF.1 SFR.FTA_TAB.1	The security function guarantees that only approved commands are passed to the smart card. The LEDs of the reader display the mode of the “Secure PIN entry” input.
SF2	SF.CLMEM	SFR.FDP_RIP.2	A memory rework of the buffer for the transmission of the PIN from the keypad to the smart card is realized with the power-on procedure, after transmission of the command to the smart card, after pulling the card, in the case of abort by the user, with a timeout during the PIN input and after defined resetting commands from the host.
SF3	SF.SECDOWN	SFR.FDP_ACF.1 SFR.FCS_COP.1_RSA SFR.FCS_COP.1_SHA	The verification of a signature of the firmware with the hash algorithm SHA-256 and the asymmetrical RSA algorithm with a bit length of 2048 guarantee the integrity and authenticity of the firmware while loading of the firmware into the smart card reader.

8.3.2 Requirements and measures for security

	Measure for assurance	Requirements of assurance	Comment
SM1	Sealing	SFR.FPT_PHP.1	The security requirement against material manipulation of the TOE is fulfilled by the sealing and not by a security function (SF) as a component of the TOE, but ensured by the security measure (SM).

8.3.3 Requirements and measures for assurance

Those in the following represented measures for the assurance correspond to the requirements of the assurance. All requirements to the assurance are covered by the existing measures to the assurance, which complement each other mutually to an overall secure system.

	Measure for assurance	Requirements of assurance	Comment
AM1	Configuration management	ACM_CAP.3 ACM_SCP.1	Authorisation control TOE CM coverage
AM2	Delivery and operation	ADO_DEL.2 ADO_IGS.1	Detection of modification Installation, generation and start-up procedures
AM3	Informal functional specification	ADV_FSP.1	Informal functional specification
AM4	Security enforcing high-level design	ADV_HLD.2	Security enforcing high-level design
AM5	Subset of the implementation	ADV_IMP.1	Subset of the implementation of the TSF
AM6	Descriptive low-level design	ADV_LLD.1	Descriptive low-level design

AM7	Informal correspondence demonstration	ADV_RCR.1	Informal correspondence demonstration
AM8	Guidance	AGD_ADM.1 AGD_USR.1	Guidance
AM9	Life cycle support	ALC_DVS.1 ALC_TAT.1	Identification of the security measures Well-defined development tools
AM10	Test documentation	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	Analysis of coverage Testing: high-level design Functional testing Independent testing – sample
AM11	Vulnerability assessment	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4	Analysis and testing for insecure states Strength of TOE security function evaluation Highly resistant

8.4 Explanation of the PP postulates

At present there exist no protection profiles for smart card readers to the employment in the framework SigG/SigV.

9 Abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CCID	Integrated Circuit(s) Cards Interface Devices
CT-API	Card Terminal - Application Programming Interface
DFU	Device Firmware Upgrade
EMV	Europay, MasterCard, Visa
HBCI	Home Banking Computer Interface
ID	Identifier
LED	Light Emmitting Diode
PC	Personal Computer
PC/SC	Personal Computer / Smart Card Interface
PIN	Personal Identification Number
ROM	Read Only Memory
RSA	Rivest, Shamir, and Adleman Public-Key Cryptography
SHA-256	Secure Hash Algorithm Rev 1. One-way hash
SigG	Signaturgesetz (Signature law)
SigV	Signaturverordnung (Signature regulation)
SPR	Secure pin pad reader
USB	Universal Serial Bus

10 Bibliography

	Reference	Description
[1]	CT-API	Application Independent **C**ard**T**erminal **A**pplication **P**rogramming **I**nterface for ICC Applications Revision 1.1; Deutsche Telekom, GMD, TUV & Teletrust ; 15.04.1999
[2]	CT-BCS	Application Independent **C**ard**T**erminal **B**asic **C**ommand **S**et for ICC applications (MKT-Version 1.0, 15.04.1999)
[3]	PC-SC V 1.0	Interoperability Specification for ICCs and Personal Computer Systems, Revision 1.0, December 1997
[4]	ISO/IEC 7816	Integrated circuit(s) cards with contacts
[5]	Class 2 Definition	Requirements at smart card readers for home use from view of SKO“ V1.0 (09/97) ”SIZ - Informatikzentrum der Sparkassenorganisation GmbH“
[6]	SigG (signature law)	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)
[7]	SigV (signature regulation)	Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), vom 16. November 2001 (BGBL 2001 Teil I Nr. 59, S. 3074–3084) zuletzt geändert durch Art. 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)
[8]	CCID	Chip/Smart Card Interface Devices, Revision 1.00, 2001-03-20
[9]	Common Criteria	Common Criteria for Information Technology Security Evaluation Part 1-3, August 1999
[10]	EMV 2004	Integrated Circuit Card Terminal Specifications for Payment Systems, version 4.1
[11]	BSI 7500	BSI - TL 03400 / BSI 7500: Produkte für die materielle Sicherheit, Juli 2008

	Reference	Description
[12]	BSI 7586	Sicherheitsetiketten, Anforderungen und Prüfbedingungen, Entwurf April 2002
[13]	BANZ	Übersicht über geeignete Algorithmen vom 17. November 2008; Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung; Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
[14]	CC	Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Part 1: Introduction and general model, CCMB-2005-08-001, Part 2: Security functional requirements, CCMB-2005-08-002, Part 3: Security Assurance Requirements, CCMB-2005-08-003.
[15]	CEM	Common Methodology for Information Technology Security Evaluation – Evaluation methodology, version 2.3, August 2005, CCMB-2005-08-004
[16]	FIPS180-2	NIST: FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 und Change Notice 1, Februar 2004.
[17]	ISO10118-3	ISO/IEC 10118-3: Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions, 2nd ed., 2004.
[18]	ISO/IEC 14888-2:2008, section 6	ISO/IEC 14888-2:2008 Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms. Kindly note that RSA is specified in section 6 of ISO/IEC 14888-2:2008
[19]	PKCS #1 Ver. 1.5, section 10.2	RSA Cryptography Standard. Kindly note that Signature Verification process is described in section 10.2