Security Target for KC 1000 SC

Zertifizierung	**ID:**	**BSI-DSZ-CC-0970-V2**
Document	**ID:**	**ASE_KC1000SC**
	Version:	**1.06**
	Status:	**Final**
	Date:	**19.12.2017**
	Prepared by:	**Jürgen Meier**
	Date/Signature:	**19.12.2017**
	Checked by:	**Dr. Philipp Tomsich, Philipp Sehner**
	Date/Signature:	**19.12.2017**
	Approved by:	**Jürgen Meier**
	Date/Signature:	**19.12.2017**

Cherry GmbH
Cherrystraße
D-91275 Auerbach / Opf.

History

Date	Version	Description	Autor
13.05.2014	0.01	Creation	Jürgen Meier
28.07.2017	1.0	Revision after first comments from BSI and further comments from the Evaluation Body	Jürgen Meier
22.09.2017	1.01	ALC_TAT.1 added to Chapter 2.3, Revision after second comment from BSI (ZK V 3.0)	Jürgen Meier
11.10.2017	1.02	Information about Guidance Documentation in Chap. 1.2.2 and 1.3 clarified Chap. 3 and 4 revised	Jürgen Meier
14.11.2017	1.03	Minor changes after commenting by BSI	Jürgen Meier
22.11.2017	1.04	Chap. 4.3.2, Table 8, additional description about AE.3 added. Chap. 1.3 Description about the scope of delivery refined	Jürgen Meier
23.11.2017	1.05	Added packaging version to Part number overview (JK-A0150yy-z-Z-)	Jürgen Meier
19.12.2017	1.06	Added reference to Software Developers Guide	Philipp Sehner

Table of Contents

1. ST-Introduction (ASE_INT)

1.1 ST reference and TOE reference

Titel:	Security Target for KC 1000 SC
Document Version:	1.06
Date:	19.12.2017
Dok. ID	ASE_KC1000SC
File name:	ASE_Security_Target-KC1000SC-V1_06.docx
Author(s):	Dr. Philipp Tomsich, Philipp Sehner, Jürgen Meier
Zert. ID:	BSI-DSZ-CC-0970-V2

The security features outline the functional and organizational security requirements and procedures for the TOE and its operational environment which meet the security objectives “Secure PIN Entry”.

The Target of Evaluation (TOE) is the smartcard keyboard of the KC 1000 SC series with firmware version 2.0.0 and the product index /01.

The target of evaluation is divided into the following product variants:

- JK-A01xxyy-z-Z-

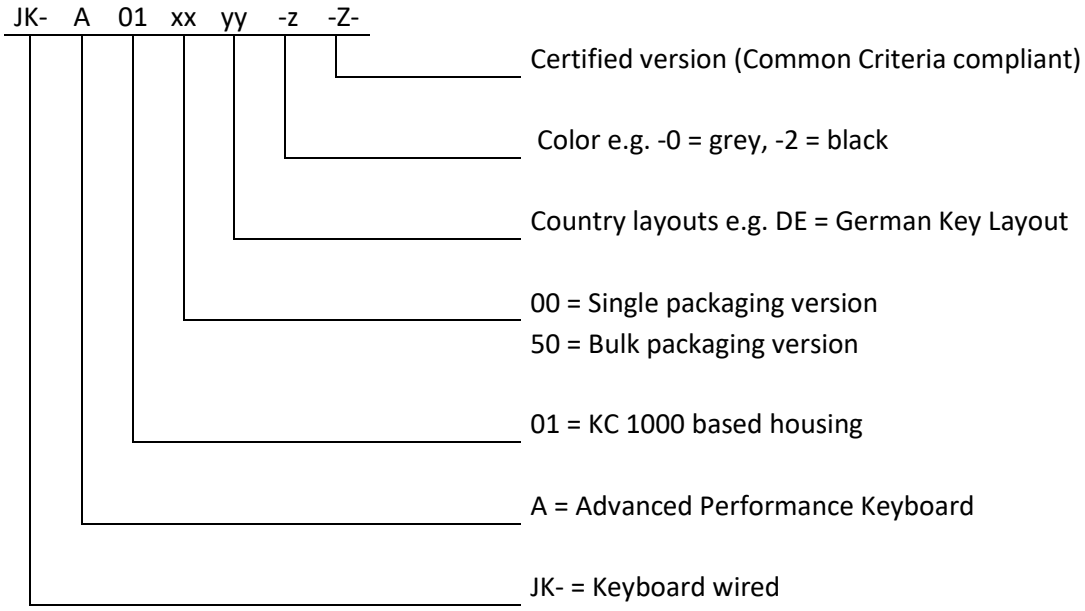
All product variants contain the same firmware to be evaluated.

Theobroma Systems Design and Consulting GmbH designed the firmware for the JK-A01xxyy-z-Z-smartcard keyboard. The driver software is created by HID Global.
Cherry GmbH is the manufacturer, product owner and distributor of the TOE.

Figure 1: KC 1000 SC

Part number overview

The Product name KC 1000 SC covers the part numbers JK-A01xxyy-z-Z-. Below is a brief description of the part number.



The part number is printed at the bottom side of the TOE and is followed by the product index of the TOE. For example, JK-A0100DE-0-Z- /01.

1.2 TOE Overview

1.2.1 TOE major security features for operational use

The TOE ensures the functionality for entering a PIN securely.
The keyboard can be used universally in any smartcard-based applications. Possible applications include:

- Qualified digital signature
- Home banking (HBCI)
- Access control (PC login)

When using the TOE as part of a signature application component for “qualified electronic signature”, The security functionality of the TOE always works effectively irrespective of the application program running it. For secure PIN entry, only the relevant CT command according to [CCID] needs to be used. The used smartcard must be [ISO 7816] and [EMV2000] compliant processor smartcard. For more details about the supported interfaces and protocols of smartcards, see Chapter 1.3.

1.2.2 TOE Type

The TOE is the smartcard keyboard KC 1000 SC with an integrated Class 2 card reader for use in a non-public environment as defined for assumption AE.1 (Chap. 3.1).
The physical boundary of TOE is defined by:

- the hardware
- the keyboard's sealed housing
- the USB interface
- the smartcard interface
- Secure PIN- Entry State LED

The logical boundary covers:

- the firmware of the µC

The Quick Start Guide [6440639], the detailed Operating Instruction [6440640] and the Software Developer's Guide [64410018] are supplied to the user in electronic form. The documents are signed with a qualified electronic signature and are available from the Cherry Support website.

1.2.3 Required non-TOE hardware/software/firmware

The KC 1000 SC smartcard keyboard has no functionality that works without connecting to a host PC. The keyboard must be connected to a PC. A PC is required with a [USB] standard interface for this.
The driver and tools included in the scope of delivery are not part of the TOE.
The following operating systems are supported by the drivers. The operating systems listed are exemplary and not necessarily complete, as fundamentally not required for the secure operation of the TOE.

- Windows 7
- Windows 8 / 8.1
- Windows 10
- Linux

To use the TOE as a secure PIN entry device a corresponding application, e.g. home banking software, is required which use the [CT-API]- or [PC/SC]- Interface of the operating system to set the TOE into the secure PIN entry mode.

1.3 TOE Description

The TOE, the smartcard keyboard KC 1000 SC, features a keyboard with an integrated Class 2 reader that is able to read processor smartcards in line with [ISO 7816] and [EMV 2000] via various application interfaces ([CT-API], [PC/SC] etc.). The keyboard works with all smartcard data transfer protocols according to [ISO 7816] (T=0, T=1). It also supports data transfer protocols for memory smartcards (2-wire, 3-wire protocols).

The smartcard keyboard recognizes the commands for PIN entry transmitted by the host software and inserts the alphanumeric characters (including small letters, capital letters, numbers and special letters) entered as the PIN to the locations occupied by the command on the smartcard. In this process, only the fact that one of the numerical or alphanumerical keys has been pressed is reported to the host. This enables the host application to show the user that he has pressed a key and how many of the PIN digits have been entered so far. The PIN itself never leaves the smartcard keyboard in plain text.
Secure PIN entry mode is signaled to the user by a red LED. The LEDs for indicating the smartcard status are routed up through a light guide to the casing surface.

The following table lists the functions and keys which can be used to processing or confirming a PIN during the secure PIN entry mode.

Function	**Keypad**		**Alphanumerical field**
	Key	**Detailed description**	
Confirms entry	[Enter]	[OK]	[↵]
Cancel	[+]	[CANCEL]	[ESC]
Undo	[-]	[←]	[←]

Table 1: Key configuration

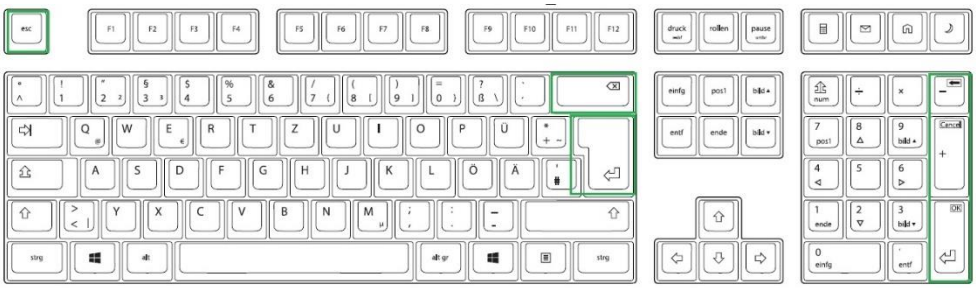


Figure 2: Keys for processing or confirming a PIN

The described Secure PIN entry mode is realized by the implemented security function *SF.1 secure PIN entry,* which is supported by the security function *SF.2 memory reprocessing*. This security function ensures that the memory where the entered PIN is stored temporarily will be reprocessed immediately after usage.

The smartcard keyboard can be used on all host systems that have a corresponding USB interface. Power is supplied via the USB bus.

The CT-API and PC/SC application interfaces can be used for all types of smartcard and is provided by the host-PC. All functionalities at the interfaces are mapped in accordance with the [CT-API] and [PC/SC] specification.

The scope of delivery includes:

- Keyboard with attached USB cable
- Quick Start Guide [6440639] with instructions for installation
- Detailed Operating Instruction [6440640] with instruction for secure use of the product via Cherry website
- Software Developer's Guide [64410018] via Cherry website
- Driver and software tools via Cherry website

Optionally, the software and the user guidance [6440639] and [6440640] provided via Cherry website can also be enclosed on CD with the delivery. But as described under Chapter 1.2.2 "*TOE Type"* only the electronically signed version distributed via Cherry website is valid under Common Criteria aspects and part of the certification.

The interface between host and keyboard is based on the functional scope of the [CCID]. The USB interface represents the physical and logical boundary between the TOE and the host system.

The primary aim is to use the smart card keyboard for "qualified digital signature" applications as a secure PIN entry- device.
Since, as a Class 2 reader, the smartcard keyboard is also able to capture identification data (PIN) and securely transmit this data to secure signature creation devices (signature smartcards) it can also be used for applications conforming to the Regulation (EU) No. 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions [eIDAS]. Furthermore, it transmits the hash value from the application to the signature card and loops back the signature from the card to the signature application.

The following list of supported instruction bytes for secure PIN entry are to be used by the applications and to be supported by the smartcards according to specifications or declined when not supported with an appropriate error message:

- VERIFY (ISO/IEC 7816-4): INS=0x20
- CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x28
- UNBLOCK APPLICATION (EMV 2000): INS=0x18
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C

The housing is sealed with tamper-proof security labels, which self-destruct if removed.
The arrangement of the seals and the TOE housing design makes unauthorized opening impossible without breaking a seal.
This allows the user to check the integrity of the keyboard, which he is also prompted to do.
Security components and data lines are arranged inside the housing in such a way that it is not possible to gain access through existing openings, e.g. the card slot.

Due to the fact, that the Common Criteria component ALC_DEL.1 is not part of the certification, the security review ends with the packaging process at the production line. The delivery of the TOE to the secure environment in which the TOE will be used must be negotiated individually with every single customer. Direct delivery to the user or administrator is preferred.

2. ASE_CCL Conformance Claim

2.1 Common Criteria Conformance Claim

This Security Target and the TOE claim conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3]

Conformance is claimed for Part 2 extended and Part 3 conformant.

2.2 PP Claim

This Security Target claims no Protection Profile.

2.3 Package Claim

The following components claimed for the TOE:

ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1,
ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3,
AGD_OPE.1, AGD_PRE.1,
ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1
ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2,
AVA_VAN.3

This component claim corresponds to the assurance level EAL 3 augmented by the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA.VAN.3 and reduced by the component ALC_DEL.1.

3. ASE_SPD – Security Problem Definition

The following section features the security environment in which the TOE should be used. This covers the security aspects of the environment and the anticipated use of the TOE.
In this context, the assets to be protected and the people involved are explained with respect to the proper use and misuse of the TOE.

The PIN as the identification feature of the smartcard owner, as well as the firmware and hardware of the TOE, must be protected.

Exposing the identification data and security related changes to the TOE are considered to be threats to the TOE by an attacker.

To counteract these threats, mechanisms have been integrated:

- Secure PIN entry is shown by a LED
- Residual information protection by zeroization of memory areas containing sensitive data
- The TOE may only transmit the PIN to the smartcard
- The PIN may only be forwarded to the smartcard via the approved PIN commands
- The TOE is protected by the seal
- The end user is informed of his responsibility using the TOE as PIN entry device.

3.1 Assumptions

In general, it is assumed that the end user is informed about his responsibility while using the TOE. The following assumptions show in detail the responsibilities of the user about a secure use of the TOE.

Assumptions regarding the physical conditions

Assumptions	Description
AE.1	It is assumed that the TOE is used as a smartcard keyboard for the non-public environment only with single and multi-user PCs in the private domain and in the office environment. Any area which is not accessible for the general public is classed as a non-public environment. Such a non-public environment shall ensure that an attacker cannot install or use any equipment to spy on the entered PIN by the use of audio or video recording equipment or at least it enables the user to identify such equipment. Visitors have only controlled access and visitor policies ensure that they don't carry any equipment for audio or video recording. The access of service providers and external employees to the premises is contractually regulated.

Assumptions regarding the personnel conditions

Assumptions	Description
AE.2	It is assumed that the user is convinced of the integrity of the seal before using for the first time, and periodically thereafter, by checking whether any security-related changes to the seals or smartcard keyboard have been made.
AE.3	It is assumed that the user is advised on rules regarding secure storage and non-disclosure of the PIN by the issuer of the smartcard. This includes that the user ensures that the PIN is entered unobserved.
AE.4	It is assumed that the user checks the status of the LED to ensure that the secure PIN entry mode is active, while entering the PIN using the number keypad.

Assumptions regarding the connection options or the connections to other IT systems or products

Assumptions	Description
AE.5	It is assumed that only processor smartcards are used which satisfy the [ISO 7816] and [EMV 2000] specifications. The user or organization which procures the smartcards that will be used with the TOE, must ensure, that the smartcards fulfill the proposed requirements.

Table 1: Assumptions

3.2 Assets

The following assets must be protected by the TOE and its environment.

Assets to be protected	Description
PIN	The PIN as identification code of the user represents a personal secret. The user enters the PIN using the numerical and alphanumerical key area of the TOE. This is then sent to the smartcard by the TOE. The TOE must ensure the confidentiality of the PIN.

Table 2: Assets

3.3 Subjects

The following subjects are interacting with the TOE:

Subject	Description
Attacker	A human or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to gain the entered PIN. The attacker could use the following weak points: - the interface between the TOE and the host- PC, - the electromagnetic emanation Attack attempts can be conducted from outside of the operational environment. The attacker can also try to get physical access to the TOE within the given access possibilities to the operational environment. The attacker has an enhanced-basic attack potential.
User	A user uses the TOE as a standard computer input device for normal office work and also as security device where secure PIN entry is required for example as part of a signature application component. The user is non-hostile and knows the existing guidance documents of the TOE. The user is responsible for the secure operation of the TOE.
Host-PC	A host-PC can be any PC which supports USB devices. The TOE can be used as input device with an integrated class 2 card reader with the host-PC. In addition, the host-PC supports an application with the functionality of PIN verification against a signature card where a class 2 card reader is supported for secure PIN entry.
Smart Card	The user is in possession of the smart card and the corresponding PIN used for e.g. digital signature. The TOE is handling the communication of the smart card in its card slots and an application on the host-PC.

Table 3: Subjects

3.4 Threats

In the following, all threats are considered which are directed against the assets which require specific protection within the TOE or its environment and are relevant for the secure operation of the TOE. The perpetrators of threats are identified and described in terms of attacks and compromised assets.

Threats	Description
T.1	Spy on the PIN entered on the TOE via the interface the TOE is connected to the host PC. The attack may be performed using a malicious application installed on the host PC.
	Adverse effects: The PIN information entered by the user may be compromised.
	Threat agent: Attacker
	Asset: PIN
T.2	Try to provoke PIN entry and obtain the PIN in this way.
	Adverse effects: Obtaining the PIN by provoked PIN entry without active security functions.
	Threat agent: Attacker
	Asset: PIN
T.3a	Manipulation of the TOE into its components (hardware and firmware) or replacing

Threats	Description
	the TOE by a manipulated keyboard to determine the PIN.
	Adverse effects: Obtaining the PIN by manipulation of the hardware or firmware of the TOE to bypass the implemented security functions.
	Threat agent: Attacker
	Asset: PIN
T.3b	Read out the PIN which is stored temporarily in the TOE.
	Adverse effects: Read out the PIN over TOE interfaces or direct after internal processing.
	Threat agent: Attacker
	Asset: PIN
T.4	Writing the PIN in an unprotected area of the smart card to then read it.
	Adverse effects: Direct the PIN to unprotected areas of a smart card.
	Threat agent: Attacker
	Asset: PIN
T.5	Make security-related changes to the TOE by tampering with the security seal.
	Adverse effects: Manipulation the TOE by tampering the security seals to obtain the entered PIN.
	Threat agent: Attacker
	Asset: PIN
T.6	Eavesdropping of the electromagnetic emanation to draw conclusion about the entered PIN by analyses of the recorded signals. The attacker and the attack equipment is located outside the operational environmental of the TOE in an adjacent area.
	Adverse effects: Eavesdropping of the PIN with equipment to record electromagnetic emanation for subsequent analysis in order to compromise PIN information from adjacent areas.
	Threat agent: Attacker
	Asset: PIN

Table 4: Threats

3.5 Organizational Security Policy

No organizational security policy is defined.

4. ASE_OBJ.1 – Security Objectives

The security objectives for the TOE and its environment are defined in this chapter. The following security objectives counteract all identified threats and outline the assumptions.
In chapter 4.1 the security objectives for the TOE are defined, while in chapter 4.2, the security objectives for the environment of the TOE are specified.
Chapter 4.3 presents the correlations between the identified assumptions and threats and the defined security objectives.

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in the following table.

Security objectives for the TOE	Description
O.1	The TOE ensures that the PIN is not stored, except at the time of processing.
O.2	The TOE ensures that secure PIN entry mode is clearly signaled to the user.
O.3	The TOE ensures that the PIN is only transferred to the smartcard.
O.4	The TOE ensures that the PIN is passed on to the smartcard only by means of PIN command with approved instruction bytes.
O.5	The TOE ensures that any security changes to the TOE are recognizable by the security seal.
O.6	The TOE ensures that the electromagnetic emanation cannot be used to simply draw conclusion about the entered PIN.

Table 5: Security objectives for the TOE

4.2 Security Objectives for the Environment

The user is advised on rules regarding secure storage and non-disclosure of the PIN by the issuer of the smart card.
The end user must be informed of his responsibility while using the TOE.
The security objectives for the environment are defined in the following table.

Security objectives for the environment	Description
OE.1	The TOE must be used as a smartcard keyboard for the non-public environment. This comprises that the user is obligated to check the operational environment regularly about installed audio and video recording equipment used for spy attacks on the PIN. It must be ensured that visitors, service providers or external employees cannot install or carry any kind of audio or video recording equipment.
OE.2	The user must check the integrity of the security seal (seal number) and the TOE regularly before using the device.
OE.3	The user must follow the instructions of the card issuer regarding the secure handling of the card and the PIN and ensure that the PIN is entered unobserved.
OE.4	While entering the PIN, the user must check the status of the LED to ensure that the secure PIN entry mode is active.
OE.5	The user may only use processor cards which satisfy the [ISO 7816] and [EMV 2000] specifications.

Table 6: Security objectives for the environment

4.3 Security Objectives Rational

The following table provides an overview for the security objectives coverage. The following chapters provide a more detailed explanation of this mapping:

	O.1	O.2	O.3	O.4	O.5	O.6	OE.1	OE.2	OE.3	OE.4	OE.5
T.1			X								
T.2		X								X	
T.3a					X			X			
T.3b	X										
T.4				X							
T.5					X						
T.6						X					
AE.1							X				
AE.2								X			
AE.3									X		
AE.4										X	
AE.5											X

Table 7: Security objectives coverage

4.3.1 Countering the threats

The threat **T.1** describes that an attacker may try to eavesdrop and log the communication between the TOE and the host system by a malicious tool installed on the host system, to obtain an entered PIN or bypass the security functions. This treat is countered by the objective **O.3** which describes that the PIN will never leave the TOE other than to the corresponding smartcard.
The threat **T.2**, which describes that an attacker can provoke the PIN entry by a program from outside of the TOE is countered by the objective **O.2** and **OE.4**. **O.2** describes that the TOE will signal the secure PIN entry mode clearly to the user and **OE.4** ensures that the user check the status of the secure PIN entry LED while he is entering the PIN to be sure that the secure PIN entry mode is active.
Threat **T.3a** which describes the manipulation of the TOE into its components (hardware and firmware) to bypass the security functions is countered by the objective **O.5** which ensures that manipulation of the TOE is recognizable because of the use of security seals.
It is also assumed, that an attacker can replace the TOE by a manipulated keyboard. The Objective **OE.2** counteracts to this threat, which is an assumption to the operational environment that the serial numbers of the security seals will be checked regularly by the user.
Objective **O.1** which ensures that the PIN will never be stored in the TOE, except during the processing counters the threat **T.3b** which describes the reading of the PIN after PIN entry from memories.
The threat **T.4**, which describes that an attacker could try to redirect the PIN to an unprotected area of a smart card, is covered by the objective **O.4**. This objective ensures that the TOE only accepts PIN commands with permitted instruction bytes.
The threat **T.5**, which describes that an attacker could tamper with the security seal to manipulate the TOE is countered by the objective **O.5** which claims that manipulations of the TOE are recognizable because of the use of security seals.
The threat **T.6**, which describes that an attacker can eavesdrop the PIN by analyzing the electromagnetic emanation is countered by the security objective **O.6** which claims that the electromagnetic emanation cannot be exploited by a simply way.

4.3.2 Covering the assumptions

AE.1	It is assumed that the TOE is used as a smartcard keyboard for the non-public environment.	
	OE.1	The TOE must be used as a smartcard keyboard for the non-public environment.
AE.2	It is assumed that the user is convinced of the integrity of the seal before using for the first time, and periodically thereafter, by checking whether any security-related changes to the smartcard keyboard have been made.	
	OE.2	establish an objective which covers the assumption directly
AE.3	It is assumed that the user follows the instructions of the card issuer regarding the secure handling of the card and the PIN. Thus, it is also assumed that the user ensures that the PIN is entered unobserved.	
	OE.3	establish an objective which covers the assumption directly
AE.4	It is assumed that the user checks the status of the LED to ensure that the secure PIN entry mode is active, while entering the PIN.	
	OE.4	establish an objective which covers the assumption directly
AE.5	It is assumed that only processor smartcards are used which satisfy the [ISO 7816] and [EMV 2000] specifications.	
	OE.5	establish an objective which covers the assumption directly

Table 8: Covering the assumptions

5. ASE_ECD – Extended Component Definition

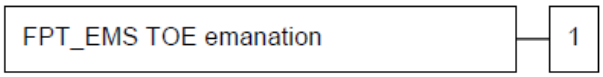
This Security Target uses components defined as extensions to CC part 2.
The defined components are drawn from extended component definition [PP_0068].

5.1 Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data processed by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [CC2].
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

5.1.1 FPT_EMS TOE emanation

This family defines requirements to mitigate intelligible emanations.
Component levelling:



FPT_EMS.1 TOE emanation has one constituent:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

Management: FPT_EMS.1
There are no management activities foreseen.

Audit: FPT_EMS.1
There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Hierarchical to: No other components

Dependencies: No dependencies

6. ASE_REQ – Security Requirements

This Chapter defines the functional requirements and the security assurance requirements for the TOE and its environment.

Operations for assignment, selection, refinement and iteration have been made.

All operations which have been performed from the original text of [CC2] are written in *italics for assignments*, underlined for selections and **bold text for refinements**. Furthermore the [brackets] from [CC2] are kept in the text

6.1 Security Functional Requirements for the TOE

The TOE has to satisfy the SFRs delineated in the following table. The 4th row of the table designates the dependencies of the SFRs.

Nr.	Component	Description	Dependencies
	FDP	**User Data Protection**	
1	FDP_ACC.1	Subset access control	FDP_ACF.1
2	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3
3	FDP_RIP.1	Subset residual information protection	none
	FIA	**Identification and authentication**	
4	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1
	FTA	**TOE access**	
5	FTA_TAB.1	Default TOE access banners	none
	FPT	**Protection of the TSF**	
6	FPT_EMS.1	TOE Emanation	none
7	FPT_PHP.1	Passive detection of physical attack	none

Table 9: Security functional requirement for the TOE

6.1.1 User Data Protection (FDP)

6.1.1.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [*Smart card reader access control policy*] on
[
Subjects:
- *User via key matrix interface*
- *Host- PC via USB interface*
- *Smart card via smart card interface*

Objects:
- *PIN*
- *Secure PIN entry mode LED*

Operations among subjects and objects covered by the SFP:
- *Entry of the PIN*
- *Transfer of the PIN*
- *Control of the secure PIN entry LED*

].

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

6.1.1.2 *FDP_ACF.1 Security attribute based access control*

FDP_ACF.1.1 The TSF shall enforce the [*smartcard reader access control policy*] to objects based on the following:
[
list of subjects:
- *User via the key matrix interface*
- *Host- PC via USB interface*
- *Smart Card via smart card reader interface*

attribute: [none]

objects:
- *PIN*
- *Secure PIN entry mode LED*

Attribute: State of the Secure PIN entry mode LED
].

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 Host- PC (subject) sends via the USB- Interface an explicit command from an application to the smart card interface, whereby the secure PIN entry LED (object) will be triggered (operation) by the TOE. The entered PIN (object) will be send (operation) to the corresponding smart card, if the command structure of the command meets [CCID] and the instruction correlates with one of the following instruction bytes:*
  - *VERIFY (ISO/IEC 7816-4) INS= 0x20*
  - *CHANGE REFERENCE DATA (ISO/IEC 7816-8) INS=0x24*
  - *DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=0x26*
  - *ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8) INS=0x28*
  - *RESET RETRY COUNTER (ISO/IEC 7816-8) INS=0x2C*
  - *UNBLOCK APPLICATION (EMV 2000): INS=0x18*
- *The user (subject) can only enter (operation) the PIN (object) via defined keys of the alphanumeric key area and the numeric pad of the keyboard.*
- *The TOE sends (operation) the PIN (object) to the smart card (subject) in the smart card interface only.*

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
[*No further rules required for the TSF*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
[*No further rules required for the TSF*].

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

6.1.1.3 *FDP_RIP.1 Subset residual information protection*

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects:
[
- *PIN*
- *Secure PIN entry mode LED*
].

Application Note 1: After activation, the forwarding of a PIN command, withdrawal of the smartcard or cancellation, the PIN memory area is zeroized to ensure that no personal identification data or data fragments remain in the smartcard keyboard.
FDP_RIP1.1 for the PIN LED means that the defined switch off the PIN LED is ensured.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.1.2 FIA Identification and Authentication

6.1.2.1 *FIA_UAU.7 Protected authentication feedback*

FIA_UAU.7.1 The TSF shall provide only [*non-PIN placeholder character*] to the user while the authentication is in progress.

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

6.1.3 FTA TOE access

6.1.3.1 *FTA_TAB.1 Default TOE access banners*

FTA_TAB.1.1 Before establishing a user session, the TSF shall **indicate, whether the TOE is in a secure state or not.**

Application Note 2: The state of secure PIN entry mode will be indicated by a red LED.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.1.4 Protection of the TSF (FPT)

6.1.4.1 *FPT_EMS.1 TOE Emanation*

FPT_EMS.1.1 The TOE shall not emit *[information about the timing of the matrix scan during secure PIN entry]* in excess of [*non-useful information]* enabling access to [*none*] and [*PIN*].

Application Note 3: The key matrix scan during the secure PIN entry mode must be scrambled. Therefore, a random number generator must be used to scramble the scan randomly.
The random number as seed for the random number generator must be loaded into the TOE securely.
It must be ensured during the preparative installation procedure of the TOE at production site that a random number from sufficient quality is been used. Evidences have been taken within the scope of the ALC evaluation.

6.1.4.2 *FPT_PHP.1 Passive detection of physical attack*

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

Application Note 4: Based on authentic and tamper-proof security seals affixed over the join between the bottom and top parts of the housing is it possible to reliably establish that the hardware has not been tampered with.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note 5: This can be ensured because the housing cannot be opened without breaking the seal.
The nature (destruction characteristics) of the seal ensures that it cannot be removed and re-attached without damaging it.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.2 Security Assurance Requirements for the TOE

The TOE fulfills the below listed Security Assurance Requirements which represents EAL 3 augmented by the components marked in bold text and reduced by the component ALC_DEL.1. The complete text for these requirements can be found in Part 3 of the Common Criteria [CC3].

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedure
ALC: Life-cycle support	ALC_CMC.3 Authorisation control
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ASE_CCL.1 Conformance claims
ASE: Security Target evaluation	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
	ATE_COV.2 Analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	**AVA_VAN.3** Vulnerability analysis

Table 10: Chosen Evaluation Assurance Requirements

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rational

The following table provides an overview for security functional requirements coverage.

	O.1	O.2	O.3	O.4	O.5	O.6
FDP_ACC.1			X	X		
FDP_ACF.1			X	X		
FDP_RIP.1	X					
FIA_UAU.7			X			
FTA_TAB.1		X				
FPT_EMS.1						X
FPT_PHP.1					X	

Table 11: Security Functional Requirements Rational

The security objective O.1 which ensures that the PIN is not stored, expect at the time of processing is met by *FDP_RIP.1* which defines that the PIN have to be securely deleted when it is no longer used. Security objective O.2 which requires that the secure PIN entry mode is clearly signaled to the user is directly and completely met by FTA_TAB.1 as this SFR requires that the TOE shall be able to indicate, whether it is working in a secure state.

The security objective **O.3** which requires that the PIN will be only transferred to the smartcard is met by *FDP_ACC.1*, *FDP_ACF.1 and FIA_UAU.7.*
FDP_ACC.1 and *FDP_ACF.1* define that nobody is able to read out the PIN from the keyboard.
FIA_UAU.7 supports this objective by providing only asterisk to the application during the user enters a PIN.
FDP_ACC.1 and *FCP_ACF.1* fulfills also the security objective **O.4** which requires the use of approved instruction bytes for PIN processing.
The security objective **O.5** which ensures that any security changes are recognizable is met by *FPT_PHP.1* as this SFR requires that the TOE detected physical tampering.
The security objective **O.6** which ensures that the PIN cannot be observed by simply analyses of the electromagnetic emanation is met by FPT_EMS.1 which defines the TOE doesn't emit timing information during the secure PIN entry mode.

6.3.2 Dependency Rationale

SFR	Dependencies	Support of the dependencies
FDP_ACC.1	FDP_ACF.1	fulfilled
FDP_ACF.1	FDP_ACC.1; FMT_MSA.3	Fulfilled by FDP_ACC.1. See chapter 6.3.3 for FMT_MSA.3
FDP_RIP.1	none	-
FIA_UAU.7	FIA_UAU.1	See chapter 6.3.3
FTA_TAB.1	none	-
FPT_EMS.1	none	-
FPT_PHP.1	none	-

Table 12: Dependencies of the SFR for the TOE

6.3.3 Justification for missing dependencies

The dependency FMT_MSA.3 of FDP_ACF.1 is considered to be not applicable as changes of security attributes is not possible, whereby the management of security attributes is not applicable.
The dependency FIA_UAU.1 of FIA_UAU.7 is considered to be not applicable because user authentication is no objective for the TOE. Therefore, no TSF mediated actions need to be defined as executable without user authentication.

6.3.4 Security Assurance Requirements Rationale

The TOE fulfils the security assurance requirements, as claimed in chapter 2.3.
The following components corresponds to the Evaluation Assurance Level EAL 3 without the component ALC_DEL.1

- ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1,
- AGD_OPE.1, AGD_PRE.1,
- ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
- ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
- ASE_OBJ.2, ASE_REQ.2
- ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
- AVA_VAN.2

This assurance level has been augmented by the component:

- AVA_VAN.3

This component has the following direct and indirect dependencies, which has to be satisfied within the evaluation:

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1 (required by ADV_IMP.1)

The main decision about the Evaluation Assurance Level has been taken based on the fact that the TOE described in this Security Target shall serve as a secure PIN entry device and based on the fact

that the TOE is used in a non-public environment but also needs to provide an adequate level of protection for its assets.

The component ALC_DEL.1 has not been chosen to give the customer the decision about the security measures for the delivery of the TOE to the operational environment.

7. ASE_TSS – TOE Summary Specification

This chapter describes the TOE summery specification under chapter 7.1 as well as the TOE security measures under chapter 7.2. All assurance measures will be described under chapter 7.3

7.1 TOE Security Functions

To sign an electronic document digitally, the user is prompted by the application to insert his signature card. The “digital signature” application must then be activated in the smartcard. To do this, the owner must authenticate possession (signature card) and knowledge (PIN) using his signature card.
The priority here is to protect the personal identification data (PIN).

The TOE provides the user with the security features to protect the identification data (PIN) and to reprocess information carriers (storage areas and LED display).
The implementation of the individual security functions is described below.

Security function 1: Secure PIN entry (SF.1)

The smartcard keyboard is switched to the secure PIN entry mode using an explicit CT command according to [CCID]. This CT command contains the PIN handling agreements and the smartcard command, in which the PIN is integrated at the specified location.
The instruction byte of the smartcard command is used to verify whether this is a PIN command that explicitly expects a PIN to be entered. The table below shows the permitted instruction bytes.

INS-Byte:	Bezeichnung:	Bedeutung	Norm:
0x20	VERIFY	PIN entry	ISO/IEC 7816-4
0x24	CHANGE REFERENCE DATA	Change PIN	ISO/IEC 7816-8
0x26	DISABLE VERIFICATION REQUIREMENT	Activate PIN	ISO/IEC 7816-8
0x28	ENABLE VERIFICATION REQUIREMENT	Deactivate PIN	ISO/IEC 7816-8
0x18	UNBLOCK APPLICATION	Unblock Application	EMV 2000
0x2C	RESET RETRY COUNTER	Unlock PIN	ISO/IEC 7816-8

Table 13: Instructionbytes [ISO 7816]/[EMV 2000]

After changing to the secure PIN entry mode, the key matrix query of the key area switches from a serial scan into a random scan of the single columns of the key matrix.
The entered personal identification data is buffered in the internal RAM of the TOE, so that it can be sent with the PIN command to the smartcard as soon as the entry is complete. PIN entry mode is indicated visually by a red PIN LED until the PIN has been completely entered or the operation is cancelled. The operation is cancelled by withdrawing the card, pressing the Cancel key or exceeding the permitted input time.
The user is shown the progress of the entry, with a non-PIN placeholder character appearing for each alphanumeric character entered. The dummy codes are output via the USB interface, and are then displayed by the corresponding PC application. The process inside the TOE, however, uses the correct PIN.
In the context of the SPD as described in Chapter 3, an attacker with enhanced-basic attack potential cannot manipulate the security features, as the transfer of the PIN is only carried out between the smart card and the TOE on the card reader interface. This is located inside the TOE and is protected against tampering with the security seal.

Security function 2: Memory reprocessing (SF.2)

Communication between the PC system and smartcard is based on the so-called APDUs according to [CCID]. If an APDU is received in the smartcard keyboard via the USB port, it is stored temporarily and then sent to the smartcard. After activation, the forwarding of a PIN command, withdrawal of the smartcard or cancellation, the PIN memory area is reprocessed to ensure that no personal identification data or data fragments remain in the smartcard keyboard. The memory area contains both the PIN and the APDU. Furthermore, the LED for indicating secure PIN entry goes out.
In the context of the SPD as described in Chapter 3, an attacker with enhanced-basic attack potential cannot circumvent this security function, as it is not possible to tamper with the memory reprocessing in the TOE.

7.2 TOE Security Measures (SM.1)

Four authentic and tamper-proof security seals affixed over the join between the bottom and top parts of the housing make it possible to reliably establish that the hardware has not been tampered with. This can be ensured because the housing cannot be opened without breaking the seal.
The nature (destruction characteristics) of the seal ensures that it cannot be removed and re-affixed without damaging it.
A 7-digit serial number on the seal permits it to be uniquely identified.
The seal employed satisfies the requirements of security level 2 as defined by [AIS 48].

8. Rationales

8.1 Rational of the TOE summery specification

8.1.1 Security functions and security requirements

	Security function	SFR	Comment
SF.1	**Secure PIN entry**	FDP_ACC.1 FDP_ACF.1	The smartcard keyboard is switched to the secure PIN entry mode using an explicit CT command according to [CCID]. This CT command contains the PIN handling agreements and the smartcard command, in which the PIN is integrated at the specified location. The instruction byte of the smartcard command is used to verify whether this is a PIN command that explicitly expects a PIN to be entered. The table [**Table 15**] below shows the permitted instruction bytes. The entered personal identification data is buffered in the RAM, so that it can be sent with the PIN command to the smartcard as soon as the entry is complete.
		FPT_EMS.1	After changing to the secure PIN entry mode, the key matrix query of the key area switches from a serial scan into a random scan of the single columns of the key matrix.
		FTA_TAB.1	PIN entry mode is indicated visually by a red PIN LED until the PIN has been completely entered or the operation is cancelled. The operation is cancelled by withdrawing the card, pressing the Cancel key or exceeding the permitted input time.
		FIA_UAU.7	The user is shown the progress of the entry, with a non-PIN placeholder character appearing for each alphanumeric character entered. The dummy codes are output via the USB interface, and are then displayed by the corresponding PC application. The process inside the TOE, however, uses the correct PIN.
SF.2	**Memory reprocessing**	FDP_RIP.1	After activation, the forwarding of a PIN command, withdrawal of the smartcard or cancellation, the PIN memory area is reprocessed to ensure that no personal identification data or data fragments remain in the smartcard keyboard.

Table 14: security functions and security requirements

INS-Byte:	Designation	meaning	Norm:
20_h	VERIFY	PIN entry	ISO/IEC 7816-4
24_h	CHANGE REFERENCE DATA	Change PIN	ISO/IEC 7816-8
26_h	DISABLE VERIFICATION REQUIREMENT	Activate PIN	ISO/IEC 7816-8
28_h	ENABLE VERIFICATION REQUIREMENT	Deactivate PIN	ISO/IEC 7816-8
$2C_h$	RESET RETRY COUNTER	Unlock PIN	ISO/IEC 7816-8
18h	UNBLOCK APPLICATION	Unblock Application	EMV2000

Table 15: Instruction bytes

Security functional requirements	SF.1	SF.2
FDP_ACC.1	**x**	
FDP_ACF.1	**x**	
FDP_RIP.1		**x**
FIA_UID.7	**x**	
FTA_TAB.1	**x**	
FPT_EMS.1	**x**	

Table 16: Security Functional Requirement – Security Functions

8.1.2 Security functional requirements and security measures

	Security Measure	SFR	Comment
SM.1	**Sealing**	FPT_PHP.1	The SFR passive detection of physical attacks is not met by a security function (SF) as an integrated part of the TSF, but is met by the security measure (SM) sealing.

Table 17: Security functional requirements and security measures

9. Annex

9.1 Abbreviations

AP	Advanced Performance
APDU	Application Programming Data Unit
AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria,
CT	Card Terminal
DIN	Deutsches Institut für Normung e.V.
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
eIDAS	Regulation for electronic identification and trust services for electronic transaction
EMV	Europay International, Mastercard, Visa
HBCI	Home Banking Computer Interface
ICC	Integrated Chip Card
ISO	International Organization for Standardization
IT	Information Technology
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PP	Protection Profile
RAM	Random Access Memory
SF	Security function
SM	Security measure
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
US	United States
USB	Universal Serial Bus
M	Maßnahme

9.2 Bibliography

[AIS 48]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 48, Version 1, Stand: 30.04.2015
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 3.1, Revision 4, September 2012
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 4, September 2014
[CCID]	Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001
[CT-API]	Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen CT-API Version 1.1.1 / Juni 2001
[eIDAS]	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[EMV 2000]	EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000
[ISO 7816]	DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands
[PP_0068]	Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01; Version 1.01, July the 22nd 2014
[PC/SC]	Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 2.0, November 1999
[USB]	Universal Serial Bus Specification; Revision 2.0, April 27th, 2000
[6440639]	Quick Start Guide CHERRY KC1000SC – Corded Smartcard Keyboard; 6440639-03, Jul 2017
[6440640]	Operating Instruction CHERRY KC1000SC – Corded Smartcard Keyboard; 6440640-00, Okt. 2017
[64410018]	Software Developer’s Guide KC1000SC 64410018-01, Sept 2017