Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0660-2010

for

## Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01

from

## ZF Electronics GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-0660-2010**

smart card terminal

**Cherry SmartTerminal ST-2xxx**
Firmwareversion: 6.01

| | |
|---|---|
| from | ZF Electronics GmbH |
| PP Conformance: | None |
| Functionality: | Common Criteria part 2 conformant |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 3 augmented by<br>ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 |

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 6 August 2010

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY SOGIS IT SECURITY CERTIFIED MUTUAL RECOGNITION AGREEMENT

Irmela Ruhrmann
Head of Division

L.S.

For components up to EAL 4

This page is intentionally left blank.

# Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

# Contents

# A Certification

## 1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

## 2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

## 2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

## 2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components AVA_MSU.3 and AVA_VAN.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

# 3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0477-2007. Specific results from the evaluation process BSI-DSZ-CC-0477-2007 were re-used.

The evaluation of the product Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 19 July 2010. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: ZF Electronics GmbH

The product was developed by: ZF Electronics GmbH

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

# 4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

# 5 Publication

The product Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01 has been included in the BSI list of the certified products, which is published regularly (see also Internet:

[6] Information Technology Security Evaluation Facility

https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] ZF Electronics GmbH
Cherrystraße
91275 Auerbach

# B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1 Executive Summary

The Target of Evaluation (TOE) is the SmartTerminal ST-2xxx with the firmware version 6.01 and Part No. ST-20xxUxZ-x/xx HWV03. It is a universal smart card reader with a keypad unit, which in whole builds the TOE. The keypad possesses the numeric keys “0” to “9” as well as the keys “Clear” (yellow), “Confirmation” (green) and “Cancel” (red). Additionally the three keys “*”, “.”, and “F” are provided for future functionality.

The TOE can communicate with processor cards compliant to ISO 7816 and EMV2004 through different application interfaces (CT-API, PC/SC). The devices work with all smart card transmission protocols compliant to ISO 7816 (T=0, T=1). Data transmission protocols for memory cards (I2C, 2-wire, 3-wire protocol) are also supported.

The smart card reader realises secure PIN entry functionality over its keypad, whereas the PIN data are only redirected to the connected smart card, but do not leave the TOE in direction to the host computer. The application receives only a signal, that one of the numeric keys was pressed, but not which key.

The reader can be used at all host systems that possess an USB interface. 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.

The smart card reader drivers support the following OS:

- Windows 98SE
- Windows ME
- Windows 2000
- Windows 2003 Server
- Windows XP
- Windows VISTA
- Windows CE (ab 5.0)
- Windows 7
- Linux
- MacOS X

The driver-software is not part of the evaluation. The TOE ends at the USB interface of the host computer.

The connection between host and smart card reader bases on the functional range of the CCID standard. The USB interface is the physical and logical border between the TOE and the host. The objective is to use the smart card terminal among other things for the application “digital signature” in accordance with the German signature law (SigG).

The smart card reader as a class 2 reader is able to capture identification data (PIN) and to transmit it to a secure signature creation device (signature smart card) (SigG, §2, No. 10). Moreover, the TOE is used for the transmission of the hash value from the application to the signature card and for the return of the signature from the card to the application of signatures. Thus, the TOE represents a partial component for components of signature applications to be applied in accordance with SigG / SigV.

Therefore they are a subcomponent for the signature application component, which needs a security confirmation to be used for qualified electronic signature in accordance to SigG, §2, No. 3.

To use the TOE in accordance to SigG/SigV, applications (signature applications) as well as smart cards have to be used, which are evaluated and confirmed according to SigG/SigV.

The smart card terminal ST-2xxx fulfils the specific requirements according §15 paragraph 2 no.1a and paragraph 4 SigV.

Particularly the secure PIN entry, which is indicated to the user by LED states, is performed only under defined constraints. 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 7816-8): INS=0x24
- ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C
- UNBLOCK APPLICATION (EMV2004): INS=0x18

The SmartTerminal ST-2xxx is suitable both for office and private use. The TOE offers protection against attackers with a high attack potential. To this the user is enabled to check the intactness of the TOE with its sealing.

The SmartTerminal ST-2xxx offers the possibility of a secured firmware download for electronic signed firmware updates. Certified and confirmed as well as not certified firmware versions will be made available for download. Certified and confirmed versions will be explicitly labelled as such by its certification ID.

For the binary firmware file a hash value is generated based on the SHA-256 algorithm, which is encrypted with the asymmetrical RSA algorithm and a bit length of 2048 to build the signature. This functionality prevents the TOE from unauthorized manipulations.

The secure generation and administration of the necessary keys, which are used to create the secure signature is ensured by the vendors SCM Microsystems GmbH and ZF Electronics GmbH.

The vendor guarantees that each new version of the TOE gets a new version number and is therefore uniquely identifiable.

The installation package contains a software tool, which can be used to check the certified and confirmed firmware version of the smart card terminal ST-2xxx. Executing the software tool “`FWCheck.exe`” V 6.1 shows the firmware version of the connected smart card terminal ST-2xxx. Therefore the user can check if the certified and confirmed firmware 6.01 is used. This software tool is not part of the TOE.

The housing is sealed by means of a unforgeable secure security seal, which will be visibly destroyed during removal and thus only once usable.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.4.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

| TOE Security Function | Addressed issue |
|---|---|
| SF.PINCMD<br>(O.1, O.2, O.4) | Changing the terminal's state to secure PIN entry will be realised by an explicit CT-command according CCID. This CT-command contains the PIN-handling-arrangements and the chip card command, in which the PIN will be integrated at the specified position. The instruction byte will be used to check, if it is a PIN command, which has been explicitly expected.<br>The following list contains all allowed instruction bytes:<br>• VERIFY (ISO/IEC 7816-4): INS=0x20<br>• CHANGE REFERENCE DATA (ISO/IEC 7816-4): INS=0x24<br>• ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x28<br>• DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x26<br>• RESET RETRY COUNTER (ISO/IEC 7816-4): INS=0x2C<br>• UNBLOCK APPLICATION (EMV2004): INS=0x18<br>Personal identification data is buffered in RAM to send it together with the PIN command directly the chip card after entering. During the PIN entry the PIN-LED blinks orange until the PIN is complete or this activity has been aborted. Following events lead to an abort: Card removed, abort key pressed, time-out.<br>PIN entry progress is shown to the user with "*" for each digit. The fact that one of the numeric keys is pressed is reported to the host via the USB interface. The TOE itself uses the correct PIN.<br>Even a determined attacker with significant technical capabilities cannot bypass the security functions, as 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<br>(O.3) | The communication between PC-System and chip card bases on so called APDUs according CCID. An APDU received via the USB interface is buffered to send it to the chip card afterwards. The memory area for the PIN data will be cleaned 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 to ensure that not personal identification data or data fragments are still stored by the card terminal. The memory area contains both PIN and APDU. Furthermore the LED that shows the secure PIN entry will be turned off.<br>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 evasion would be only possible if a manipulated firmware would be loaded, which is however not possible due to SF.SECDOWN. |

| TOE Security Function | Addressed issue |
|---|---|
| SF.SECDOWN<br>(O.6) | 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.<br>The hash value over that firmware, which will be loaded, is determined based on the algorithm SHA-256 with a length by 256 bits.<br>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.<br>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.<br>As the probability of guessing or calculating the key is negligible, SF.SECDOWN is fulfilling the minimum strength of function “high”. |
| Sealing<br>(O.5) | The housing is sealed by means of a security seal, which will be destroyed during removal and thus can be used only once ans is protected against forgery.<br>Thus the user can recognize by the condition of the safety seal that no manipulations at the hardware were made. |

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 4.1.

The claimed TOE’s Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 5.2 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3 and 4.

This certification covers the following configurations of the TOE: The evaluated TOE is the security-sealed class 2 smart card reader ST-2xxx with the firmware version V6.01 in a fixed configuration and is labelled with Part No. ST-20xxUxZ-x/xx HWV03. Please note, that the driver software is not part of the SmartTerminal ST-2xxx CC evaluation. For details, please refer to chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

## 2 Identification of the TOE

The Target of Evaluation (TOE) is called:

**Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/SW | SmartTerminal ST-2xxx | Part No. ST-20xxUxZ-x/xx HWV03 with firmware version 6.01 | Firmware installed on Hardware |
| 2 | SW | FWcheck.exe | 06.01.10 | CDROM |
| 3 | DOC | Betriebsdokumentation “AGD” (german) | 6440417-04 | Printed Document |
| 4 | DOC | Bedienungsanleitung MKT + Terminal ST-2052U (german) | 6440533-03 | Printed Document |
| 5 | DOC | Instructions, SmartTerminal ST-2000U (english) | 6440411-03 | Printed Document |

Table 2: Deliverables of the TOE

The TOE is being delivered in several variants. Only those matching the Release for deliverable no. 1 in table 2 are covered by this certificate. In this case, “x” is to be understood as wild-card character. Details regarding the Part. No. can be found in the ST [6] in chapter 1.1.

The smart card readers are produced, tested, closed, labelled and sealed at the production site. The complete packages will be stocked in a high rack bracket before delivery to OEM customers. The user can verify the identity and authenticity of the smart card reader by the Part No. on the label, by the firmware version and by the intact security seal.

Physical identification of the security sealed TOE is achieved by using notes about the unique identification number from item 3 in table 2 to ensure that the device has not been tampered with.

Further the TOE identification can be done by checking the label data on the back of the TOE and by using the firmware check tool `FWcheck.exe`, which is part of the installation software, before using the reader.

# 3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Secure PIN entry, PIN protection and secure firmware update.

# 4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- non public environment
- suitable smartcards
- the user regularly checks security seal and it's serial number
- the user not being observed during PIN entry
- the user ensuring the secure PIN entry mode

- the user entering PIN only using the readers PIN pad
- the user checks the firmware using the provided tool on a regular basis
- the user only installs certified firmware on the reader

Details can be found in the Security Target [6] chapter 4.2.

# 5 Architectural Information

The TOE, the SmartTerminal ST-2xxx with the firmware version 6.01, comprises hard- and software and is delivered as a complete smart card reader (see table 3). Apart from the security sealing the hardware does not provide any security relevant features and can be separated as follows:

- microcontroller with internal volatile and non-volatile memory, USB-controller and smart card controller
- USB-interface including cable and connector
- display unit consisting of LEDs in different colours
- smart card interface

The firmware that provides the main security functions is composed of different subsystems. These subsystems and their functionality are listed in the next table.

| Subsystem | Description |
|---|---|
| USB SUBSYSTEM | This subsystem manages and implements all functions relating to the processing of the standard USB commands, and the host specific secure and non-secure commands. This subsystem helps to connect the host level commands through the USB bus with the secure download and the CCID subsystems. |
| CCID SUBSYSTEM | This subsystem shall process the CCID messages received from the USB subsystems. This subsystem dispatches the messages to SmartOS or Secure PIN management subsystems, based on the received message and updates the error/status/data returned by the other subsystems to the caller. Also this subsystem implements functions that manage the reader specifics for the host interface subsystems. |
| SMARTOS SUBSYSTEM | This subsystem implements functions that manage the smart card specifics for the host interface subsystems like USB Functions that provide methods for card power control, card reset and Submitting APDUs for processing all comprise this subsystem. Means to directly transmit or receive a stream of bytes, to support different cards are also included in this subsystem. This subsystem connects with the secure pin pad and CCID subsystems. |
| SECURE-PINPAD SUBSYSTEM | This subsystem implements SF.PINCMD and SF.CLMEM security functions as derived from the ST specification of this product. This subsystem shall process the Verify and Modify CCID PIN entry messages. It shall handle the user PIN entry, formatting of the PIN to the appropriate PIN format type selected and dispatches the APDU to the SmartOS subsystem. The response received from SmartOS is returned back to the CCID command-processing subsystem. |
| SECURE-DOWNLOAD SUBSYSTEM | This subsystem mainly implements the SF.SECDOWN security function as defined in the ST of this product. This subsystem shall implement functions that involve processing of USB DFU class requests and to successfully perform the DFU operation. When the DFU detach command is received, the USB subsystems abort any pending operation and hands over control to this subsystem to start the DFU process. Moreover, the purpose of this subsystem is to verify the functional firmware to be downloaded using a SHA-256 digest encrypted with the 2048-bit RSA Key as signature. |

Table 3: TOE Subsystems

# 6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7 IT Product Testing

## 7.1 Developer Tests

The developer's tests were conducted with the goal to confirm that the TOE meets the security functional requirements. The developer's strategy was to test the TOE against the specification of all security enforcing functions detailed in the functional specification (FSP) and in the high-level design (HLD). The manufacturer presented corresponding test objectives and specified suitable tests for each of the security functions

- SF.PINCMD
- SF.CLMEM
- SF.SECDOWN

The tests reported in the testing documentation completely covers the security functions of the TOE defined in the FSP and ST. The developer performed altogether 41 test cases on security function SF.PINCMD, one test case on security function SF.CLMEM and 9 test cases on security function SF.SECDOWN. Furthermore, the developer also performed approx. 75 test cases on non-secure function NSF1 SMARTCARD and NSF2 ZKA Implementation as documented within FSP.

With regard to the depth of testing, these tests ensure that the TSF have the effect as specified in HLD. The manufacturer conducted the TSF testing on the level of the subsystems mapping them to the related test cases and thus confirmed their correct functioning. Tests were conducted not only for all security functions but also for all subsystems and, moreover, all modules of the TOE. In doing so, the tests ensured that all external interfaces of the TOE and all internal interfaces between the subsystems were used. With regard to the depth of testing, these tests thus ensure that the TSF have the effect as specified.

The developer specified, conducted and documented suitable functional tests for each security functions. The test results obtained for all of the performed tests turned out to be as expected. No errors or other flaws occurred with regard to the security functionality, the interfaces defined in FSP and the TOE subsystems defined in HLD. Consequently, the test results demonstrate that the behaviour of the security functions are as specified.

## 7.2 Evaluator's Tests

The evaluator independent testing is summarized in the following:

### 7.2.1 Test Target

The TOE as the smart card reader family SmartTerminal ST-2xxx is the target of the independent testing. The TOE uses the Firmware Version V6.01.

The TOE configuration is described in the functional specification. All tests performed through the USB host Interface.

### 7.2.2 Test Subset

Due to the fact that the TOE only includes three security functions, tests concerning all of the security functions were carried out.

The evaluator's testing strategy was to test the functionality of the TOE as described in the Security Target [6]. The subset of tests was sampled so that the TOE security functions (TSF) with the external interfaces specified in the Functional Specification Document and subsystems from the Architectural Design Document were covered.

The test environment for the independent testing was equivalent to that used for the developer's tests. This includes a subset of the software tools used by the developer to perform the tests. All in all the evaluator conducted 107 tests within his independent testing. There were 84 tests performed on security function SF.PINCMD, 15 tests on SF.CLMEM and 8 tests on SF.SECDOWN.

Tests on SF.CLMEM were reused from the evaluation with the certification ID BSI-DSZ-CC-0592 and were not repeated during this evaluation. These tests were not repeated, due to the source code evaluation during the IMP evaluation (BSI-DSZ-CC-0592). Another reason is that these tests only check source code functionality in a way that is not possible to do with the real TOE and that the source code is identical to the evaluation with the certification ID BSI-DSZ-CC-0592.

### 7.2.3 Developer Tests

To check the validity of the developer tests the evaluator sampled a subset of these test, taking into consideration to cover all security functions and all external interfaces stimulating the TOE's behaviour. In addition, these developer tests taken from the developer’s test plan were repeated including the following amount of tests for each of the security functions.

During the independent testing, there were performed 5 tests on security function SF.PINCMD, 1 test on SF.CLMEM and 4 tests on SF.SECDOWN. All in all 10 developer tests were repeated. The test on SF.CLMEM was reused from the evaluation with the certification ID BSI-DSZ-CC-0592 and was not repeated during this evaluation. This test was not repeated, due to the source code evaluation during the IMP evaluation (BSI-DSZ-CC-0592). Another reason is that these tests only check source code functionality in a way that is not possible to do with the real TOE and that the source code is identical to the evaluation with the certification ID BSI-DSZ-CC-0592.

### 7.2.4 Results

The results of the independent evaluator tests including the repeated developer tests confirm the TOE functionality as described in ST, FSP and HLD. All the actual test results were consistent with the corresponding expected results and there resulted no hints to any errors.

## 7.3 Penetration Tests

The independent vulnerability analysis from the evaluation with the certification ID BSI-DSZ-CC-0592 has been reused, as the used firmware is identical. All tests, including those for the case have been repeated.

The Evaluator reports about the penetration test efforts in the following for the ETR, building on the independent vulnerability analysis.

Tested TOE configurations:

- The TOE was delivered with the name SmartTerminal ST-2xxx and provided to the examining place for the independent penetration test as an examining object inclusively by the manufacturer.
- The class 2 smart card reader SmartTerminal ST-2xxx, which has the firmware version 6.01 as defined in the security target [ST], is the TOE.

Base of the independent vulnerability search (the penetration tests are derived):

- Vulnerability search in manufacturer documents and test reports
- Vulnerability search in accordance with [CEM] or [AIS 34]

Verdict of the test activities:

- The Evaluator executed penetration tests, based on the independent vulnerability analysis of the Evaluator.
- The vulnerabilities aren't utilizable in the intended environment of the TOE.
- The TOE resists attackers with a high attack potential.

# 8 Evaluated Configuration

This certification covers the following configuration of the TOE:

The evaluated TOE is the security-sealed class 2 smart card reader ST-2xxx with the firmware version V6.01 in a fixed configuration and is labelled with Part No. ST-20xxUxZ-x/xx HWV03. Please note, that the driver software is not part of the SmartTerminal ST-2xxx CC evaluation.

# 9 Results of the Evaluation

## 9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 3 package as defined in the CC (see also part C of this report)
- The components ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0477-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the new firmware. It provides stronger algorithms for checking the integrity of other firmware to be installed.

The evaluation has confirmed:

| | |
|---|---|
| ● PP Conformance: | none |
| ● for the Functionality: | Common Criteria part 2 conformant |
| ● for the Assurance: | Common Criteria Part 3 conform<br>EAL 3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 |

- The following TOE Security Functions fulfil the claimed Strength of Function : high SF.PINCMD, SF.CLMEM, SF.SECDOWN

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

## 9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions:
  - SHA-256
- algorithms for the encryption and decryption:
  - RSA-2048

This holds for the following security functions:

- SF.SECDOWN

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). According to Federal Network Agency and the assessment of the BSI [15] the algorithms are suitable for ensuring a commensurate level of assurance for the signature of the firmware. The validity period of each algorithm is mentioned in the official catalogue [14] and summarized in chapter 10.

# 10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE shall be used. If non-certified updates or patches are available he should request the sponsor for providing a re-certification. In the meantime risk management process of the system using the TOE shall investigate and decide on the usage of not yet certified updates and patches or to take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

In addition, the following aspects need to be fulfilled when using the TOE:

With respect to “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen” ([14])

- the RSA 2048 algorithm will be appropriate until end of 2015 in context of qualified electronic signature according to German act on electronic signatures (SigG).
- the hash function SHA-256 will be appropriate until end of 2015 in context of qualified electronic signature according to German act on electronic signatures (SigG).

Furthermore, the secure operation of the SmartTerminal ST-2xxx requires implementation of and constant compliance with the following security measures:

- The integrated keypad of the SmartTerminal ST-2xxx allows you secure PIN-entry and is therefore suitable for signature-law-conformed applications in the home and office environment, including a trustworthy PC.
- Before using the SmartTerminal ST-2xxx, make sure that no security-relevant changes were made with the smart card reader by checking the intactness of the security seal.
- At the left and the right side, the SmartTerminal ST-2xxx is equipped with a falsification-safe seal. This allows you to recognize if someone opened the housing to perform any manipulations of the hardware. Please verify regularly if the seal is still intact before using the reader.
- Make sure that the SmartTerminal ST-2xxxis directly attached with the USB interface. There must be no other devices between the PC and the smart card reader with the exception of a USB hub, when needed.
- It is necessary that you install the SmartTerminal ST-2xxx in an area where access by unauthorized individuals is prevented and an unobserved PIN-entry is guaranteed.
- Verify the firmware version of the SmartTerminal ST-2xxx regularly. This allows you to ensure that the smart card reader is always operating with the certified firmware (V6.01). To check the firmware version, please use the "`FWcheck.exe`" utility provided with your smart card reader.

# 11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

# 12 Definitions

## 12.1 Acronyms

| | |
|---|---|
| **APDU** | Application Programming Data Unit |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CCID** | Device Class Specification for USB Chip/Smart Card Interface Devices ([11]) |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **EAL** | Evaluation Assurance Level |
| **IT** | Information Technology |

| | |
|---|---|
| **ITSEF** | Information Technology Security Evaluation Facility |
| **PC** | Personal Computer |
| **PC/SC** | Personal Computer/Smart Card |
| **PIN** | Personal Identification Number |
| **PP** | Protection Profile |
| **SigG** | Signaturgesetz, German Signature Law ([12]) |
| **SigV** | Signaturverordnung, German Signature Regulation ([13]) |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |
| **USB** | Universal Serial Bus |

## 12.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

**Extension** - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Object** - An entity within the TSC that contains or receives information and upon which subjects perform operations.

**Protection Profile** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

**Security Function** - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Strength of Function** - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

**SOF-basic** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

**SOF-medium** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

**SOF-high** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**Subject** - An entity within the TSC that causes operations to be performed.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**TSF Scope of Control** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

# 13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0660-2010, Version 1.10, 23. February 2010, Sicherheitsvorgaben EAL3+ Rezertifizierung SmartTerminal ST-2xxx, ZF Electronics GmbH

[7] Evaluation Technical Report, Version 7, 23 July 2010, Evaluation Technical Report (ETR), TÜV-Informationstechnik GmbH (confidential document)

[8] Configuration lists for the TOE (confidential documents):

- Configuration Item Record, Version 3.10, 28. August 2009, SCM Microsystems GmbH
- SAP-Stückliste ST-2000UCZ Material ST-2000UCZ, Verwendung: V, SmartCard-Reader Class2, Version 1.00, 7. January 2010, ZF Electronics GmbH
- Common-Criteria-Dokument Konfigurationsliste, Version 1.00, 18. January 2010, ZF Electronics GmbH

[9] Guidance documentation for the TOE, Version 6440417-04, December 2009, Betriebsdokumentation „AGD“ DE

[10] Guidance documentation for the TOE, Version 6440533-03, March 2009, Bedienungsanleitung MKT + Terminal ST-2052U

[11] Guidance documentation for the TOE, Version 6440411-03, May 2009, Instructions, SmartTerminal ST-2000U

[11] Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, 20. March 2001

[12] Signaturgesetz (SigG), Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - Sig)1) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)

[8] specifically

- AIS 32, Version 1, 2. July 2001, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 2, 24. October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 38, Version 2.0, 28. September 2007, Reuse of evaluation results

[13] 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)

[14] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 17. November 2008, veröffentlicht 27. Januar 2009 im Bundesanzeiger Nr. 13, Seite 346

[15] BSI - Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0, 20.06.2008

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

**Protection Profile criteria overview** (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

| **Assurance Class** | **Assurance Family** |
|---|---|
| Class APE: Protection Profile evaluation | TOE description (APE_DES) |
| | Security environment (APE_ENV) |
| | PP introduction (APE_INT) |
| | Security objectives (APE_OBJ) |
| | IT security requirements (APE_REQ) |
| | Explicitly stated IT security requirements (APE_SRE) |

Table 3 - Protection Profile families - CC extended requirements”

**Security Target criteria overview** (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

| **Assurance Class** | **Assurance Family** |
|---|---|
| Class ASE: Security Target evaluation | TOE description (ASE_DES) |
| | Security environment (ASE_ENV) |
| | ST introduction (ASE_INT) |
| | Security objectives (ASE_OBJ) |
| | PP claims (ASE_PPC) |
| | IT security requirements (ASE_REQ) |
| | Explicitly stated IT security requirements (ASE_SRE) |
| | TOE summary specification (ASE_TSS) |

Table 5 - Security Target families - CC extended requirements ”

**Assurance categorisation** (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

| **Assurance Class** | **Assurance Family** |
|---|---|
| ACM: Configuration management | CM automation (ACM_AUT) |
| | CM capabilities (ACM_CAP) |
| | CM scope (ACM_SCP) |
| ADO: Delivery and operation | Delivery (ADO_DEL) |
| | Installation, generation and start-up (ADO_IGS) |
| ADV: Development | Functional specification (ADV_FSP) |
| | High-level design (ADV_HLD) |
| | Implementation representation (ADV_IMP) |
| | TSF internals (ADV_INT) |
| | Low-level design (ADV_LLD) |
| | Representation correspondence (ADV_RCR) |
| | Security policy modeling (ADV_SPM) |
| AGD: Guidance documents | Administrator guidance (AGD_ADM) |
| | User guidance (AGD_USR) |
| ALC: Life cycle support | Development security (ALC_DVS) |
| | Flaw remediation (ALC_FLR) |
| | Life cycle definition (ALC_LCD) |
| | Tools and techniques (ALC_TAT) |
| ATE: Tests | Coverage (ATE_COV) |
| | Depth (ATE_DPT) |
| | Functional tests (ATE_FUN) |
| | Independent testing (ATE_IND) |
| AVA: Vulnerability assessment | Covert channel analysis (AVA_CCA) |
| | Misuse (AVA_MSU) |
| | Strength of TOE security functions (AVA_SOF) |
| | Vulnerability analysis (AVA_VLA) |

Table 1: Assurance family breakdown and mapping”

**Evaluation assurance levels** (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

**Evaluation assurance level (EAL) overview** (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

| **Assurance Class** | **Assurance Family** | **Assurance Components by Evaluation Assurance Level** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

Table 6: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

**Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

**Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed** (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested** (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested** (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

**Evaluation assurance level 7 (EAL7) - formally verified design and tested** (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

**Strength of TOE security functions (AVA_SOF)** (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

**Vulnerability analysis (AVA_VLA)** (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

# D Annexes

## List of annexes of this certification report

This page is intentionally left blank.

# Annex B of Certification Report BSI-DSZ-CC-0660-2010

## Evaluation results regarding development and production environment

The IT product Cherry SmartTerminal ST-2xxx; Firmwareversion: 6.01 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 6 August 2010, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (ACM_AUT.1, ACM_CAP.3, ACM_SCP.1),
- ADO – Delivery and operation (ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

ZF Electronics GmbH
spol. S r. o., Osvobozená 780, 43151 Klasterec, Czech Republic
(production site)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.