Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0511-2008

for

PalmSecure SDK Version 24 Premium

from

Fujitsu Limited

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0511-2008

biometric verification system

PalmSecure SDK Version 24 Premium

from	Fujitsu Limited
PP Conformance:	None
Functionality:	Product specific Security Target; Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 2

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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, 30 December 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all Evaluation Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

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

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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

2.2 International Recognition of CC - Certificates

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 February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. 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.

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 PalmSecure SDK Version 24 Premium has undergone the certification procedure at BSI.

The evaluation of the product PalmSecure SDK Version 24 Premium was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 27 November 2008. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Fujitsu Limited

The product was developed by: Fujitsu Limited

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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the

[6] Information Technology Security Evaluation Facility

assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 PalmSecure SDK Version 24 Premium has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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] Shiodome City Center, 5-2 Higashi-Shimbashi 1-chrome, Minato-ku, Tokyo, 105-7123, JAPAN

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 biometric verification system PalmSecure SDK Version 24 Premium.

The major mean of the PalmSecure SDK biometric verification system is to verify (accept or reject) the claimed identity of a human by using the structure of the veins in his palm as a unique characteristic of his body. The biometric system gets the Biometric Identification Record (BIR), associated with the user's identity from the database and captures the biometric characteristic of the user. If the Biometric Live Record (BLR) that is extracted from the captured characteristic and the BIR from the database are similar enough by a one-to-one comparison (which will be decided by using a threshold value), the claimed identity of the user is verified and the user will be accepted by the biometric system. Otherwise or if no BIR was found for the user, the user will be rejected from the biometric system.

The TOE consists of the PalmSecure Sensor (hardware part of the TOE) and the PalmSecure Library (software part of the TOE). The TOE is a software development kit which will be embedded into an overall application by an application developer using the PalmSecure Library. This overall application could be stand-alone or embedded in a network. However, the software part of the TOE, the PalmSecure Library, is located in one local environment, e.g. in a PC to which the hardware part of the TOE, the PalmSecure Sensor, is connected.

The Security Target [7] is the basis for this certification. It was developed based on the Protection Profile for Biometric Verification Mechanisms [11]. The Security Target [7] does not claim conformance to the Protection Profile for Biometric Verification Mechanisms [11].

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 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [7], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Function	Addressed issue
Identification and Authentication	Identification and Authentication of user
Residual Information deletion	Deletion of all memory area containing sensitive data after use
Replay detection	Detection of replayed capturing data

Table 1: TOE Security Functions

For more details please refer to the Security Target [7], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [7], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [7], chapter 3.

The TOE can have two different configurations: the Stand-alone solution or the Network-integrated solution. The TOE components are the same for both configurations. The software part of the TOE is a library which usage and functionality is independent from the current configuration. For details refer to chp. 8.

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 4, Para. 3, 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:

PalmSecure SDK Version 24 Premium

The following table outlines the TOE deliverables:

No	Type	Identifier		Release	Form of Delivery
1	SW	PalmSecure Library	Authentication Library	V24L10-S02	Downloadable from the Support Web Site
2	SW		Sensor driver	V11L02	
3	HW	PalmSecure Sensor	Sensor Hardware	Product number KD03231-B051, Revision 01A	Hardware
	HW		Sensor in mouse	Product number KD03231-B052, Revision 01A	
	HW		Sensor only or sensor in mouse	Product number KD03231-B05y, Revision 01A B05y : B053 – B059 The suffix “y” is designated and thus reserved for specific customers. The hardware of the sensor is the same.	
	FW		Sensor Firmware	V00L202	Stored in Sensor hardware
4	DOC	PalmSecure Guidance documentation for the application developer	Manual structure	U1PS-LA11-04ENZ3	Downloadable from the Support Web Site
5	DOC		System development guide	U2PS-LA21-08ENZ3	
6	DOC		PalmSecure sensor instruction manual	U3PS-LB11-08ENZ3	

No	Type	Identifier		Release	Form of Delivery
7	DOC	PalmSecure Guidance documentation for the application developer	Authentication accuracy data sheet	U3PS-LB21-06ENZ3	Downloadable from the Support Web Site
8	DOC		Hardware drawings	U3PS-LB31-07ENZ3	
9	DOC		Sample collection tool V01/ Authentication accuracy evaluation tool V01 operation guide	U3PS-LB41-07ENZ3	
10	DOC		Sample application V01 manual and Main process sequence	U4PS-LC11-06ENZ3	
11	DOC		Interface library sample for Visual Basic V01 manual and Main process sequence	U4PS-LC51-05ENZ3	
12	DOC		Interface library sample for Java V01 manual and Main process sequence	U4PS-LC61-05ENZ3	
13	DOC		Authentication library reference guide	U4PS-LC21-09ENZ3	
14	DOC		Sensor driver installation guide	U4PS-LC41-08ENZ3	
15	DOC		Sensor maintenance tool V01 operation guide	U5PS-LD11-04ENZ3	
16	DOC		Introduction tool V01 operation guide	U5PS-LD31-03ENZ3	
17	DOC		Firmware update tool V01 operation guide	U5PS-LD41-02ENZ3	
28	DOC		Security Guide	U6PS-LE11-01ENZ3	

Table 2: Deliverables of the TOE

The PalmSecure Sensor (the hardware part of the TOE: the Sensor itself and the Sensor firmware that is stored in the Sensor unit) is delivered from the developer's factory to the customer in a transport package. In addition a security seal is attached on the surface and the backside of the box.

The PalmSecure Library (the software part of the TOE: Authentication Library and Sensor Driver) is delivered by downloading from the SDK Support Website. Only authorized users can download the software. Access to the SDK Support Website is only possible after complete user registration for which the customer who has purchased Palm-Secure has to run trough the entire user registration process. User registration is available for one person for one product. To protect the files during download against tampering the Hyper Text Transfer Protocol Secure (HTTPS) is used. The components of the Authentication Library and the Sensor Driver are generated by decompressing the downloaded files.

The guidance documentation is delivered also by downloading from the SDK Support Website. The corresponding pdf-files are generated by decompressing the downloaded files.

The customer is able to verify that he has received the correct version of the PalmSecure Sensor by identifying the product number labelled on the bottom of the sensor and

comparing them to the ones listed in [9]. To determine and verify the version of the sensor's hardware and firmware, the “Sensor Maintenance Tool” can be used.

The components of the PalmSecure Library are checked using the file manager (e.g. Windows Explorer) to compare the file information (file name, file size, version number and last update date and time) with those of the file list in [9].

The guidance documents are checked comparing the revision number on each title page with that one of the guidance documentation list in [9].

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:

- Verify (accept or reject) the claimed identity of a human by using the structure of the veins in his palm as a unique characteristic of his body.

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:

- Support of security management by recording security relevant events as stated in OE.AUDIT_REACTION
- Access control as stated in OE.ROLES_AND_ACCESS
- The administrators are well trained and can be trusted as stated in OE.ADMINISTRATION
- Authentication of the administrator as stated in OE.AUTHADMIN
- Enrolment of user as stated in OE.ENROLMENT
- Availability of TOE operating equipment and adequate infrastructure as stated in OE.ENVIRONMENT
- Physical protection against unauthorized access to the TOE as stated in OE.PHYSICAL
- Availability of a fallback mechanism as stated in OE.FALLBACK

Details can be found in the Security Target [7], chapter 4.2.

5 Architectural Information

The TOE consists of a hardware part and a software part: The hardware part of the TOE is the PalmSecure Sensor which itself also contains firmware for its internal operation. The software part of the TOE is the PalmSecure Library which is used by an application running for example on a PC.

Hence the major characteristics of the TOE are:

Sensor subsystem

The sensor subsystem can be seen as a single security domain. It consists of the

sensor hardware and firmware and provides the Sensor-Interface which only purpose is capturing the palm vein data of the user.

Library subsystem

The library subsystem can be seen as a single security domain. It consists of the software (Authentication Library and Sensor Driver) and provides the Library-Interface. The Authentication Library is a software development kit which means a set of functions for design a PalmSecure based application system.

The following figure of the TOE shows its two parts. It is taken from [7]:

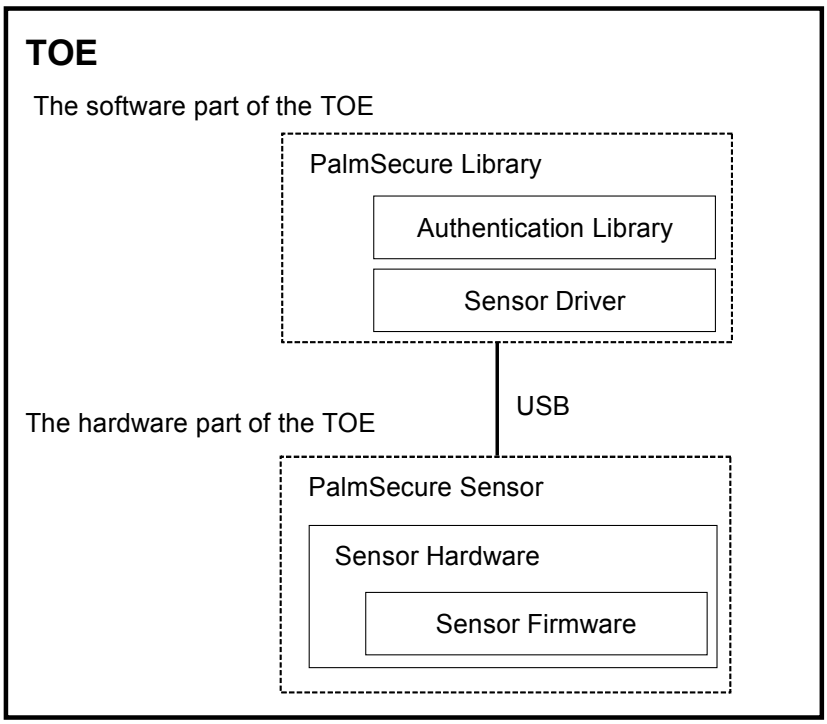

Figure 1: Software- and hardware-part of the TOE

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 Tests of the Developer

7.1.1 TOE test configuration / Interfaces

The Sensor-Interface and the Library-Interface of the TOE were tested in the Stand-alone configuration. The TOE was configured according to an adapted network solution for the FAR test because of its large extent.

Chapter 1.6 of [7] describes the required non-TOE hardware, software and firmware. The TOE environment and the related test equipment for the tests of the Sensor-Interface and the Library-Interface as well as for the FAR test were consistent with the described ones in [7]:

The tests of the Sensor-Interface were carried out during the software development and are independent from the possible configurations.

The tests of the Library-Interface were carried out by running the “Test Tool” on a standalone PC (Intel (R) Pentium (R) M 1.86 GHz, 782 MHz, 512 MB RAM, Microsoft Windows XP Professional Version 2002 Service Pack 2) with installed Authentication Library (PalmSecure SDK Version 24 Premium V24L10-S02). A Sensor unit (Product number KD03231-B051) was connected to the PC.

For the FAR test the following system configuration was used:

- One server PC (Fujitsu PRIMERGY (TX-200), Xeon (TM) 3.2 GHz, 2.0 GB Memory, 700 GB HDD Capacity, Microsoft Windows Server 2003 Standard Edition) which controls the collected data,
- Nine client PCs (HP (T5305), Pentium4 3.2 GHz, 512 MB Memory, 150 GB HDD Capacity, Microsoft Windows XP Professional Version 2002 Service Pack 2) with installed Authentication Library (PalmSecure SDK Version 24 Premium V24L10-S02) in accordance with the Stand-alone configuration.

7.1.2 Testing approach

The developer specified and implemented test cases for each defined TSFI. The test cases divided into those of the Sensor-Interface and of the Library-Interface. Thus all TSFIs are covered by several test cases.

The objectives of the tests of the Sensor-Interface were to show that all memory areas containing sensitive data are deleted, that the captured data is encrypted by the sensor and forwarded to the library, and that the transmission between sensor and library as well as between library and application is encrypted. The test activities by Fujitsu for testing of the Sensor-Interface included source code reviews and program analysis in debug mode.

For the tests of the Library-Interface the developer used the “Test Tool” for PalmSecure Version 24 Premium. This test tool consists of an executable program that calls one or more scenario files for each function of the library and writes evidence files. Fujitsu carried out positive (“Normal End Tests”) as well as negative (“Abnormal End Tests”) tests. Altogether there are more than 200 tests covered by such scenario-files.

To check the FAR whose value must not exceed 0.00008% (= 0.0000008) (see Annex A of [7]) Fujitsu collected more than 3500 samples and carried out the test for four different ethnic groups: Japanese people – this was the biggest one, Black people, White people and Japanese people with blood relations.

7.1.3 Test results

The results of the Sensor-Interface tests prove the correct implementation.

The results of the Library-Interface tests match with the expected ones.

The results of the FAR test evidences that the FAR of the PalmSecure SDK Version 24 Premium is not exceeded the value 0.00008%.

7.2 Independent Evaluator Tests

7.2.1 TOE test configuration / Interfaces

For testing the Sensor-Interface and the Library-Interface of the TOE the evaluators used the Stand-alone configuration. For the FAR test at the ITSEF and for testing the Sample Application the TOE was also configured as a Stand-alone solution. For the FAR test at Fujitsu an adapted network configuration was used.

The required non-TOE hardware, software and firmware is described in chapter 1.6 of [7]. The following configurations

A) Stand-alone PC with Pentium (R) 4CPU 320 GHz, 319 GHz, 512 MB RAM, Microsoft Windows XP Professional Version 2002 SP 2 and installed Authentication Library “PalmSecure SDK Version 24 Premium” (Version number V24L10-S02); Sensor unit (Product number KD03231-B051) connection

B) Stand-alone PC with Intel (R) Pentium (R) M 1.86 GHz, 782 MHz, 512 MB RAM, Microsoft Windows XP Professional Version 2002 SP 2 and installed Authentication Library “PalmSecure SDK Version 24 Premium” (Version number V24L10-S02); Sensor unit (Product number KD03231-B051) connection

C) Client-Server configuration:

- One server PC (Fujitsu PRIMERGY (TX-200), Xeon (TM) 3.2 GHz, 2.0 GB Memory, 700 GB HDD Capacity, Microsoft Windows Server 2003 Standard Edition),
- Nine client PCs (HP (T5305), Pentium4 3.2 GHz, 512 MB Memory, 150 GB HDD Capacity, Microsoft Windows XP Professional Version 2002 Service Pack 2) with installed Authentication Library “PalmSecure SDK Version 24 Premium” (Version number V24L10-S02).

were used. For the tests of the Sensor-Interface which were carried out at the developer’s site in the presence of the evaluators configuration (A) installed by the developer (the source code is compiled as ‘debug mode’ in order to set break points in the corresponding parts of it) was used. For the tests of the Library-Interface (which were carried out mostly at the evaluator’s site, but also at the developer’s site for the cases where a special sensor was needed which was only available at Fujitsu), for the tests of the Sample Application as well as for the evaluator’s FAR test (which were carried out at the evaluator’s site) configuration (B) installed by the evaluators was used. For the FAR test at Fujitsu configuration (C) installed by the developer was used.

7.2.2 Testing approach

Because the developer carried out the tests of the Sensor-Interface during the software development, it was not possible to repeat them by the evaluators. Thus the evaluators devised additional tests. These tests could be carried out only at the developer’s site, because these tests are only possible in ‘debug mode’. Hence break points could set in the corresponding parts of the source code. Furthermore, for a few tests an ICE (In Circuit Emulator) was connected to the micro processor of the PalmSecure Sensor.

The evaluators devised a subset of developer tests to verify the validity of the testing approach of the developer, particularly with regard to the tests of the Library-Interface.

For testing the Library-Interface the evaluators used the “Test Tool” for PalmSecure Version 24 Premium provided by the developer and installed by the evaluator on a Stand-alone PC of the evaluation facility. This test tool consists of an executable program that calls scenario files (ini-files) for each function of the library and writes evidence files. The evaluators repeated nearly all developer tests at the ITSEF excepting such tests which are related to functions or parameters which are out of scope of the evaluation (functions regarding enrolment and identification, parameters regarding threshold level which is to low, data format which is not used etc.).

The tests of the Library-Interface were carried out mostly at the evaluator’s site, but also at the developer’s site for the cases where a special sensor was needed and connected to the PC which was only available at Fujitsu.

For testing of the Library-Interface the evaluators chose and performed a set of developer tests.

The intention of testing the Sample Application is to examine the functionality of the PalmSecure Sensor and the PalmSecure Library when they are integrated in an overall application. Therefore the Sensor-Interface and the Library-Interface were additionally implicitly tested using the “Sample Application” from Fujitsu. It was shown that it is easy to use the sensor in a correct manner. Furthermore, the evaluators tried to achieve the acceptance of “manipulated” palm veins.

To examine the FAR denoted by the developer the FAR test was carried out with ca. 3500 samples of Fujitsu in the presence of the evaluators. Because of the large test extent (duration of three days), this test was carried out only once and has to be considered as developer and evaluator test at the same time. Furthermore, the evaluators carried out the FAR test with independent samples at the ITSEF. For this reason the ITSEF collected more than 350 independent samples (10% of all samples). For collecting the samples the ITSEF used the “Sample collection tool” from Fujitsu. For calculation of the FAR the “Authentication accuracy evaluation tool” was used. (Note: The ITSEF checked the source code of the “Sample collection tool” as well as of the “Authentication accuracy evaluation tool” to ensure that the FAR calculation is properly implemented.)

7.2.3 Test results

There is no deviation between the expected test results and the actual ones.

The actual results in fact match with the expected ones.

The results of the FAR test evidences that the FAR of the PalmSecure SDK Version 24 Premium is not exceeded the value 0.00008%.

7.3 Penetration Tests

The evaluators did not identify exploitable potential vulnerabilities during their evaluation activities. All identified potential vulnerabilities require Enhanced-Basic, Moderate or High attack potential and remain as residual vulnerabilities.

Moreover, some evaluator tests can be understood as penetration tests. The evaluators conduct manipulation attacks at the Sensor-Interface in connection with the “Sample Application”, in order to try to achieve the acceptance of “manipulated” palm veins. But since the biometric functionality is a part of the TOE, the corresponding test cases are described within the independent testing. All authentication attempts were rejected.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE can have two different configurations: the Stand-alone solution or the Network-integrated solution. The TOE components are the same for both configurations. The software part of the TOE is a library which usage and functionality is independent from the current configuration. Table 2 in chapter 2 lists all TOE components of PalmSecure SDK, Version 24 Premium with their exact references so as they are used for the evaluated configuration.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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.

The following guidance specific for the technology was used:

- Biometrics Evaluation Methodology Supplement [BEM], Version 1.0, August 2002

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target;
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

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 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 4, Para. 3, Clause 2). This holds for the TOE Security Functionality

- Identification and Authentication
- Replay detection

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.

11 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

BIR Biometric Identification Record

BLR Biometric Live Record

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

FAR False acceptance rate

HTTPS Hyper Text Transfer Protocol Secure

ICE In Circuit Emulator

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirements

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirements

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functions

TSFI TSF interface

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Biometric system - An automated system capable of capturing a biometric sample from a user, extracting biometric data from the sample, comparing the data with one or more reference templates, deciding on how well they match, and indicating whether or not an identification or verification of identity has been achieved.

Biometric Identification Record (BIR) - A BIR includes the reference template and other data associated with the user. This is the saved reference data record against that the comparison is accomplished.

Biometric Live Record (BLR) - This template includes the actual biometric data (actual biometric characteristic and user identity) to be verified with the biometric identity record.

Capture - The process of taking a biometric sample via a sensor from a user.

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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Replay attack - An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of an impostor attack.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

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

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

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

[6] Biometrics Evaluation Methodology Supplement, Version 1.0, August 2002

[7] Security Target BSI-DSZ-0511-2008, Version 1.0, 14. September 2008, Security Target for PalmSecure, Fujitsu

[8] Evaluation Technical Report, Version 1.1, 24.11.2008, SRC Security Research & Consulting GmbH, (confidential document)

[9] Security guide (PalmSecureTM Version 24 Premium), Fujitsu, First edition, September 2008

[10] Life-cycle support for PalmSecure, Fujitsu, Version 1.0, 17.09.2008

[11] Protection Profile - Biometric Verification Mechaninms Version 1.04, BSI-PP-0016-2005

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:

A) **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or

B) **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.

- describes the conformance to CC Part 3 (security assurance requirements) as either:

A) **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or

B) **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:

A) the SFRs of that PP or ST are identical to the SFRs in the package, or

B) the SARs of that PP or ST are identical to the SARs in the package.

- Package name Augmented - A PP or ST is an augmentation of a predefined package if:

A) the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.

B) the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

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

- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ 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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.