Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0016-2005

Protection Profile

for

Biometric Verification Mechanisms

Version 1.04

developed on behalf of the

Federal Ministry of the Interior, Germany

Certification Report

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Bundesamt für Sicherheit in der Informationstechnik

Certificate BSI-PP-0016-2005

Protection Profile

for

Biometric Verification Mechanisms Version 1.04

developed on behalf of the

Federal Ministry of the Interior, Germany

Common Criteria Arrangement

Assurance Package: EAL2, augmented with ADV_SPM.1

Bonn, August 30th, 2005

The Vice President of the Federal
Office for Information Security

Hange L.S.

The Protection Profile mentioned above was evaluated at an accredited and licenced/approved evaluation facility on the basis of the *Common Criteria for Information Technology Security Evaluation (CC), Version 2.1 (ISO/IEC 15408)* applying the *Common Methodology for Information Technology Security Evaluation (CEM), Part 1 Version 0.6, Part 2 Version 1.0* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

This certificate applies only to the specific version and release of the Protection Profile and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the Federal Office for Information Security. 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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Bundesamt für Sicherheit in der Informationstechnik (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of TOEs which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of a Protection Profile is carried out on the instigation of the author, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

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

[1] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (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
- BSI Certification - Description of the Procedure (BSI 7125)
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation, Version 2.1[5]
- Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0
- Biometrics Evaluation Methodology Supplement, Version 1.0, August 2002
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

[2] Act setting up the Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Bundesamtes für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung, BSIZertV) of 7 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 29 October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22 September 2000

2 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of Protection Profile certificates under certain conditions was agreed.

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005 and India in April 2005.

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 Protection Profile for Biometric Verification Mechanisms, Version 1.04 has undergone the certification procedure at the BSI.

The evaluation of the Protection Profile for Biometric Verification Mechanisms, Version 1.04 was conducted by CSC Ploenzke AG. The evaluation facility of CSC Ploenzke AG is an evaluation facility (ITSEF)[6] recognised by BSI.

Sponsor is the ‘Federal Office for Information Security (BSI)’, Germany on behalf of the Federal Ministry of the Interior, Germany.

The certification was concluded with

- the comparability check and
- the preparation of this Certification Report.

This work was completed by the BSI on August 30th, 2005.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-8.

The Protection Profile for Biometric Verification Mechanisms, Version 1.04 has been included in the BSI list of certified and registered Protection Profiles, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained via the BSI-Infoline +49 228 9582-111.

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

[7] BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

B Certification Results

Content of the Certification Results

1 PP Overview

The scope of this Protection Profile is to describe the functionality of biometric verification systems in terms of the CC and to define functional and assurance requirements for biometric verification systems.

Biometric products, which are conformant to this Protection Profile, provide a verification process to verify the claimed identity of a human being using a unique characteristic of his body.

This PP should cover the biometric verification process on a generic level and should be applicable to any biometric verification system. Therefore the descriptions of the requirements for the TOE are kept on a very general level so that the manufacturing of conformant products is possible for various IT environments. Where a relation to a certain biometric characteristic was necessary, fingerprint recognition is used in this PP. In these cases other technologies are addressed via application notes.

This PP describes a biometric system that works in a verification mode. Biometric identification is not addressed within this PP. Furthermore the enrolment process is out of scope of this PP and it is assumed that all authorized users have been enrolled. Last but not least a biometric verification system that is conformant with this PP has to verify the identity of a user for the purpose of controlling access to a portal.

Beside the biometric verification process every biometric system that is conformant to this PP includes a mechanism to identify and authenticate an administrator of the system with other means than biometrics and to enforce an access control for the objects of the TOE. This is especially important to limit the ability to change the threshold settings for the biometric verification process to an authorized administrator.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a TOE which is compliant to the Protection Profile for Biometric Verification Mechanisms, Version 1.04.

All functional requirements are drawn from Common Criteria, Version 2.1, Part 2.

Component	Component-Name
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.2	Full residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.3	Unforgeable authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of management function
FMT_SMR.1	Security roles
FPT_RPL.1	Replay detection

The functional requirements are adapted to biometrics by application notes.

3 Assurance Package

The security assurance requirements are based entirely on the assurance components defined in Part 3 of the Common Criteria. The assurance requirements comply with assurance level EAL2 (Evaluation Assurance Level 2) augmented with ADV_SPM.1.

4 Strength of Functions

The minimum strength of function level is SOF-basic.

For the biometric verification mechanism the SOF level is measured in terms of FAR (according to [3]). For SOF-basic a FAR of less than 1 in 100 is required.

5 Results of the Evaluation

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 [4] and all interpretations and guidelines of the scheme [5] as relevant for the TOE.

The verdict for the CC, Part 3 assurance component (according the class APE for the Protection Profile evaluation) is summarised in the following table.

CC Aspect	Result
CC Class APE	PASS
APE_DES.1	PASS
APE_ENV.1	PASS
APE_INT.1	PASS
APE_OBJ.1	PASS
APE_REQ.1	PASS
APE_SRE.1	PASS

The Protection Profile for Biometric Verification Mechanisms, Version 1.04 meets the requirements for Protection Profiles as specified in class APE of the CC.

6 Definitions

6.1 Acronyms

BEM	Biometrics Evaluation Methodology Supplement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
FAR	False Acceptance Rate
FRR	False Rejection Rate
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
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

6.2 Glossary

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

Biometric - A measurable physical characteristic or personal behavioural trait used to recognise the identity of an enrolee or verify a claimed identity.

Biometric feature - A representation from a biometric sample extracted by the extraction system

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. Note that in [CC] evaluation terms, a biometric system may be a product or part of a system.

Enrolment - During the enrolment process the system captures the biometric characteristic of a user and extracts the features it is working with.

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.

Identification - The objective of an identification process is quite similar to a verification process. But in contrast to verification process there is no claimed identity necessary.

Portal - The physical or logical point beyond which information or assets are protected by a biometric system.

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.

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.

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

Threshold - A parametric value used to convert a matching score to a decision. A threshold change will usually change both FAR and FRR - as FAR decreases, FRR increases.

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.

Verification – Process of accepting or refusing a claimed identity

7 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1 (ISO/IEC 15408)

[2] Common Methodology for Information Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0

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

[4] BSI Certification – Description of the Procedure (BSI 7125)

[5] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE

[6] German IT Security Certificates (BSI 7148, BSI 7149)

[7] Protection Profile for Biometric Verification Mechanisms, Version 1.04, BSI-PP-0016-2005

[8] Evaluation Technical Report, Version 0.8.1, 21.12.2004

This page is intentionally left blank.

C Annex: Protection Profile