BSI-PP-0024-2006

Protection Profile

Version 1.17

for a

Identity Manager

developed by

IBM Tivoli Security Product Development

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

Bundesamt
für Sicherheit in der
Informationstechnik

Certificate BSI-PP-0024-2006
Protection Profile
Version 1.17
for a
Identity Manager

Common Criteria Arrangement

developed by

IBM Tivoli Security Product Development

Assurance Package : EAL 3 augmented with
ALC_FLR.1

Bonn, January 27, 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

The Protection Profile mentioned above was evaluated at an accredited and licenced/approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.2 for conformance to the Common Criteria for IT Security Evaluation, 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.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185 - 189 – D-53175 Bonn – Postfach 20 03 63 – D-53133 Bonn
Telefon (0228) 9582-0 – Telefax (0228) 9582-455 – Infoline (0228) 9582-111

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (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 the Protection Profile is carried out on the instigation of the BSI.

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 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
- BSI Certification – Description of the Procedure [3]
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation, Version 2.2, [1]
- Common Methodology for IT Security Evaluation, Version 2.2 [2]

---

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 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

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 “Identity Manager Protection Profile, Version 1.17” has undergone the certification procedure at the BSI.

The evaluation of the “Identity Manager Protection Profile, Version 1.17” was conducted by atsec information security GmbH. The evaluation facility of atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by BSI.

Author is IBM.

The certification was concluded with

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

This work was completed by the BSI on January 27, 200604..

[5] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-10.

The “Identity Manager Protection Profile, Version 1.17” 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[6]. The Certification Report may also be obtained in electronic form at the internet address stated above.

B Certification Results

Content of he Certification Results

[6] 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

1 PP Overview

This „Identity Manager Protection Profile, Version 1.17“ is established by IBM as basis for the development of STs. The target of evaluation (TOE) is a product providing an identity management solution. This Protection Profile describes the TOE, its boundary, IT environment and IT security requirements.

Identity Management solutions provide the software and services needed for deploying policy-based provisioning solutions. They help companies automating the process of provisioning employees, contractors and business partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise environment.

The TOE provides the following Identity Management security functionality:

- entitlement decisions and export of user account information to management resources
- export and management of person and account data

The TOE provides the following security functionality to support the Identity Management functionality:

- identification and authentication of users
- authorization of user-initiated transactions
- auditing of transactions
- TSF protection

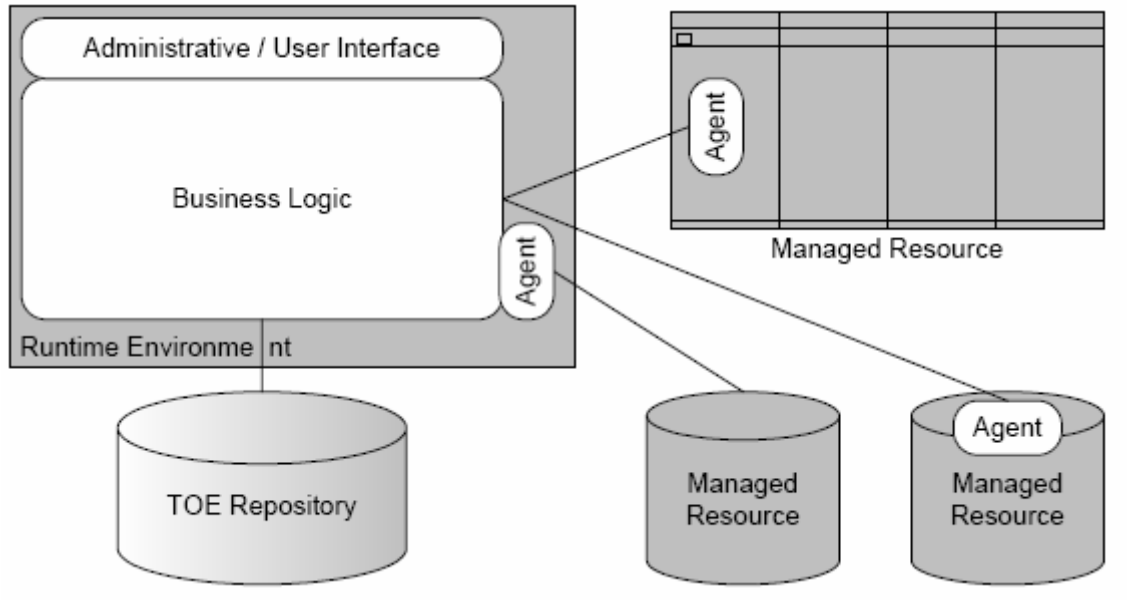

Figure 1: Structural view of TOE (white) and IT Environment (grey)

The TOE comprises a central element that implements its business logic and provides an interface to allow interaction with TOE users (e.g. management of entitlement rules). The central element of the TOE is likely to be implemented as an application that runs on a runtime environment provided by the IT environment.

The managed resources in the IT environment are interfaced by 'agents'. Agents transport account management requests generated by the TOE's business logic during provisioning to the managed resources that are expected to enforce these requests. For the purpose of this overview, IMPP envisions two different types of agents (without the intention to limit an actual TOE to the implementation of those types): agents that reside on the central runtime environment for the TOE and invoke account managements interfaces that are exported by managed resources, and agents that are installed on the managed resource itself (e.g. as a plug-in, service or daemon) and interface account management resources directly (e.g. the /etc/passwd file on a Linux system).

TSF data and user data is stored in a TOE Repository. Note that – since the storage of data is no core functionality of the TOE – IMPP does not stipulate whether the repository is implemented as part of the TOE or in the IT environment.

The PP defines the following Security Objectives for the TOE:

O.ACI	The TSF must ensure that only authorized users gain access to the TOE and the resources it protects. Access control shall be governed by access control information that may authorize access for single users or groups of users to single resources or groups of resources. Administrators shall not be restricted in accessing arbitrary resources.

O.AUDIT	The TSF must generate information about the status of security relevant transactions for recording. The TSF must present this information to authorized users.
O.FEED	The TSF must ensure that account and person data imported into the TOE are properly associated with the corresponding data already existent in the TOE data store.
O.I&A	The TSF must authenticate users and administrators which request access to the TOE and its resources.
O.PROVISION	The TSF must ensure that account generation on a managed resource is only initiated for persons that are entitled to possess an account on this managed resource.

The PP divided the Security Objectives definition for the environment of the TOE in two categories:

Security Objectives for the IT Environment:

OE.AUDIT	The runtime environment for the audit mechanism of the TOE must provide a reliable time source for audit record generation. Application Note: If the TOE itself provides a secure time source, the ST author shall merge this objective with O.AUDIT.
OE.COM_PROT	Communication of TOE external entities with the TOE as well as communication between physically distributed parts of the TOE must be protected to ensure the integrity and confidentiality of the communication. Application Note: In case the TOE implements functions for transaction security, the ST author may transform this objective into an objective for the TOE.
OE.ENFORCEMENT	The runtime environment for the TOE must provide a dedicated execution domain for the TOE to protect it from untrusted subjects.
OE.MANAGED	Each managed resource exchanging account data with the TOE must interpret this data in a consistent way and perform the account management actions requested by the TOE.
OE.REPOSITORY	The repository in the IT environment used by the TOE to store TSF or user data must protect such data against unauthorized access. Application Note: In case the TOE implements storage of TSF data and user data, the ST author may transform this objective into an objective for the TOE.

Non-IT Security Objectives for the Environment:

OE.ADMIN	Those responsible for the TOE shall ensure that the administrative personnel for the TOE and its underlying systems – as well as administrators for the repositories

	and data feed in the environment – are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator guidance. They must be well trained to securely administer all aspects of TOE installation, configuration and operation in accordance with its Security Target and initiate administrative actions from a secure environment using terminals and / or workstations they trust via secured connections to the TOE. They do not disclose their authentication credentials to others and securely transmit passwords they have generated for users to those users.
OE.AGENT	Those responsible for the TOE shall seek confidence that the runtime environment for an agent operates as specified and provides adequate protection measures against tampering with the agent and its interfaces.

OE.FEED	Those responsible for the TOE must ensure that the information provided by the IT environment that will be used for data import into the TOE allows proper association with the persons and their position in the organizational hierarchy as managed by the TOE.
OE.SERVER	Those responsible for the TOE must ensure that the TOE is protected against physical attack which might compromise IT security objectives. The underlying systems must be configured in a way that prevents unauthorized access to the TOE.
OE.USER	Those responsible for the TOE shall control the user community that can request access to resources protected by the TOE. This includes a configuration where the client systems allowed to submit requests to the TOE are controlled (e. g. a company internal network with a known and controlled user community protected against unauthorized access from external networks). Users must not disclose their authentication credentials to others**.**

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a TOE claiming compliance to the Identity Manager Protection Profile, Version 1.17.

All functional requirements are drawn from Common Criteria Part 2.

SFRs	Component-Name
FAU	**Security audit**
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Timing of authentication
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.2	Export of user data with security attributes
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.2	User authentication before any action
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FMT	**Security management**
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security rules

SFRs	Component-Name
FPT	**Protection of the TSF**
FPT_ITC.1	Inter-TSF trusted channel
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1	Non-bypassability of the TSF
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency

3 Assurance Package

The evaluation assurance level (EAL) 3 was chosen as a medium level of assurance reflecting the expected assurance requirements of commercial customers using the target of evaluation (TOE) for the protection of data with a low or medium level of sensitivity. The TOE is intended to provide a reasonable level of protection for this data comparable to the protection provided by most commercial-off-the-shelf operating system products. This is reflected as well in the definition of the TOE environment in chpt. 2 and the security objectives for the TOE in chpt. 4 of IMPP.

The assurance level EAL3 was augmented with ALC_FLR.1 to address the flaw remediation process that is part of the Mutual Recognition Arrangement. Since the evaluation methodology for ALC_FLR.1 has been harmonized, this was considered a useful augmentation for the assurance level chosen.

4 Strength of Functions

The PP claims for the functions provided by the TOE that are subject to probabilistic or permutational analysis a medium strength (SOF-medium) as a minimum. This allows resistance against attackers with a moderate attack potential.

5 Results of the Evaluation

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 [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components are 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 Identity Manager Protection Profile, Version 1.17 **meets the requirements for Protection Profiles as specified in class APE.**

6 Definitions

6.1 Acronyms

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

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

6.2 Glossary

Augmentation - The addition of one or more assurance component(s) from 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.

7 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.2

[2] Common Methodology for Information Security Evaluation, Version 2.2

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

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

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

[6] Protection Profile for Identity Manager, Version 1.17, January 12, 2006, IBM

[7] Evaluation Technical Report (ETR), Version 2.0, January 12, 2006

Annex: Protection Profile