Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0010-2004

for

Protection Profile

Waste Bin Identification Systems (WBIS-PP)
Version 1.04

developed by

Deutscher Städte- und Gemeindenbund

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-0010-2004

Protection Profile
Waste Bin Identification Systems
Version 1.04

developed by

Deutscher Städte- und Gemeindebund

Assurance Package : **EAL1**

Common Criteria Arrangement

Bonn, 27 May 2004

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 Bundesamt für Sicherheit in der Informationstechnik. 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 Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Bundesamt für Sicherheit in der Informationstechnik 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 183 – 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 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 [3]
- Procedure for the Issuance of a PP certificate by the BSI
- Common Criteria for Information Technology Security Evaluation [1], Version 2.1[5]
- Common Methodology for IT Security Evaluation [2], Part 1 Version 0.6, Part 2 Version 1.0

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.

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 ‘Waste Bin Identification Systems (WBIS-PP)’, Version 1.04 has undergone the certification procedure at the BSI.

The evaluation of the WBIS-PP, 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 ‘Deutscher Städte- und Gemeindebund’, Germany.

The certification was concluded with

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

This work was completed by the BSI on 27 May 2004.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-6.

The Protection Profile ‘Waste Bin Identification Systems (WBIS-PP)’, 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 sponsor[7]. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Deutscher Städte- und Gemeindebund, Marienstraße 6, 12207 Berlin

B Certification Results

Content of the Certification Results

1 PP Overview

This Protection Profile is the work of parties involved in manufacturing and operation of systems for waste disposal related industry.

The intent of this Protection Profile is to specify functional and assurance requirements for Waste Bin Identification Systems (WBIS) which are the target of evaluation (TOE). The Protection Profile defines the security requirements of WBIS for the transfer and storage of records of clearance data. The TOE may implement additional functions and security requirements, but these additional functions and security requirements are not subject to this Protection Profile.

WBIS in the sense of this document are systems, which allow to identify waste bins by an ID-tag (e.g. an electronic chip which is referred to as transponder) in order to determine how often a specific waste bin has been cleared. Note that this type of systems does not identify the waste directly but the waste bin, which contains the waste for disposal.

The purpose of this type of systems is to count, how often the waste bins have been cleared in order to allow an originator-related billing of waste fees. Frequently, such systems are combined with e.g. a weighing or volume measurement system in order to allow billing according to the frequency of clearance and the weight or volume of the waste disposed of. Other procedures can be thought of and can be integrated into this type of system in the future.

Many town councils in Germany have already implemented such systems from different manufacturers. Some manufacturers have received various ITSEC certificates for their products. However, the town councils as end-users need a certainty concerning the comparability of security certificates which can be required in invitations for tenders for such systems. Therefore BSI has been requested to ensure the comparability of competing security certificates by means of a Protection Profile. Aside from the initiative of the town councils as users for the creation of a Protection Profile, this Protection Profile can also be used for billing scenarios in the private domain and business areas.

WBIS comprise the electronic collection of data, the transfer and recording of clearance data (which serve as activity confirmation of the waste management enterprises) and the creation of notifications for waste fees by the responsible statutory corporations (cities and rural districts) or the issuing of invoices by the waste management enterprises. As a result of the vast amount of accumulated data it is not possible to manually check every clearance in detail which is to be invoiced. Therefore a high level of confidence is required for the technical reliability of such systems, in the respect that exactly those clearances which have actually been performed are related to the correct originator (i.e. the correct waste bin). As a result, it is necessary to protect the data relevant for the billing process (identification data and time stamps) against manipulation and loss within the system.

These data are created when a collection vehicle clears a waste bin. As a result, a record of clearance is formed based on the ID number of the bin.

After a collection vehicle has finished a clearance tour, the collected data are transmitted to the office of the maintenance and storage facility (either of the community or the private waste management enterprise) by means of possibly different media (data media, wire connection, wireless). In the office these data are stored in a central database. From there the data can be transmitted on a regular basis to authorities or regional computer centres for the billing process.

2 Security Functional Requirements

This section contains the functional requirements that must be satisfied by a WBIS-PP compliant TOE.

All functional requirements are drawn from Common Criteria, Version 2.1, Part 2 except for Security Functional Component FDP_ITT.5.

Component	Component-Name
FDP_DAU.1	Basic data authentication
FDP_ITT.5	Internal transfer integrity protection
FDP_SDI.1	Stored data integrity monitoring
FRU_FLT.1	Degraded fault tolerance

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 are assurance level EAL1 (Evaluation Assurance Level 1).

4 Strength of Functions

EAL1 does not include a component of the family AVA_SOF. Therefore a SOF-claim is not required in this PP.

5 Results of the Evaluation

The Protection Profile ‘Waste Bin Identification System (WBIS)‘, Version 1.04 meets the requirements for Protection Profiles as specified in class APE of the CC.

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
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WBIS	Waste Bin Identification Systems

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.

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.

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 2.1 (ISO/IEC 15408)

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

[3] BSI Certification – Description of the Procedure

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

[5] Protection Profile ‘Waste Bin Identification Systems (WBIS)‘, Version 1.04, BSI-PP-0010-2004

Annex: Protection Profile