Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0365-2006

for

ABox 1.0

from

T-Systems International GmbH
System Integration
Project Center Product Support & Services

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0365-2006

Softwareproduct

ABox 1.0

from

T-Systems International GmbH
System Integration
Project Center Product Support & Services

Common Criteria Arrangement
for components up to EAL4

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, Version 2.3*, *(ISO/IEC 154082005)* for conformance to the Common Criteria for IT Security Evaluation, Version 2.3 *(ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 14. August 2006

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

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.

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)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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 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 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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of 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 levels (EAL 1 – EAL 7).

2.2 CC - Certificates

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, 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 product ABox 1.0 has undergone the certification procedure at BSI.

The evaluation of the product ABox 1.0 was conducted by SRC Security Research & Consulting GmbH. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

T-Systems International GmbH
System Integration
Project Center Product Support & Services
Dachauer Strasse 651
80995 München

The certification is concluded with

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

This work was completed by the BSI on 14. August 2006.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18.

The product ABox 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] T-Systems International GmbH
System Integration
Project Center Product Support & Services
Dachauer Strasse 651
80995 München

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.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is a software, the so-called ABox 1.0 that provides security services, mainly:

- encryption and decryption of sensitive data;
- pseudonymisation of sensitive data and resolution of the pseudonyms;
- authorisation of users to read and write sensitive data on basis of a user group concept.

The TOE consists of two parts, the ABox Core and the ABox Admin Client (the shaded parts in Figure 1). The scope of delivery comprises the executables, libraries, configuration files and installation scripts for the ABox Core and ABox Admin Client, furthermore user and installation guidance (the user guidance covers also administration aspects). The ABox Core consists of the three indicated sub-systems, the ABox Admin Client constitutes a fourth subsystem.

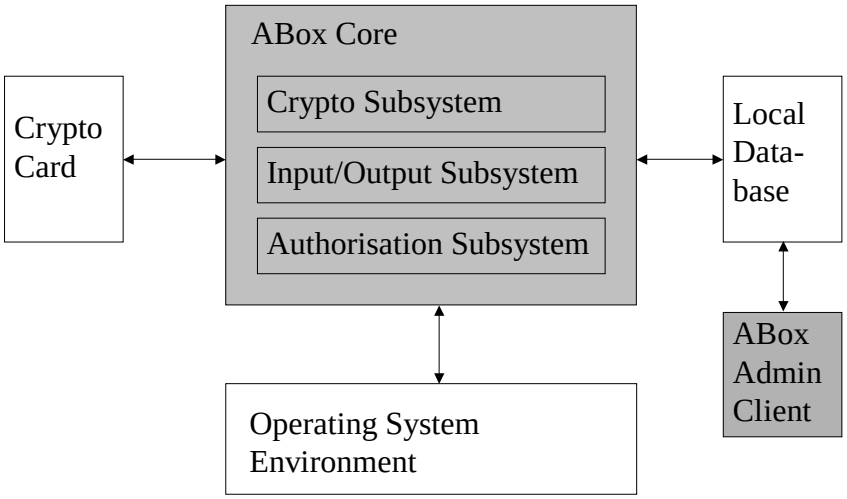

Figure 1 - Architecture of the "local ABox system"

The ABox Core is embedded into a local system (“local ABox system”) in which it is connected to an operating system environment (application software), to a database (“ABox database”) and optionally to a crypto card. TOE users interact with the TOE via the operating system environment. TOE management and configuration data are stored in the ABox database and are administered via an administrative interface, the ABox Admin Client.

The IT product ABox 1.0 was evaluated by SRC Security Research & Consulting GmbH. The evaluation was completed on 03. July 2006. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

[8] Information Technology Security Evaluation Facility

The sponsor, vendor and distributor is

T-Systems International GmbH
System Integration
Project Center Product Support & Services
Dachauer Strasse 651
80995 München

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL3 (Evaluation Assurance Level 3).

1.2 Functionality

The TOE Security Functional Requirements (SFR) are taken from CC part 2:

Requirement	Identifier
FCS_CKM.1	Cryptographic key generation
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_UCT.1	Basic data excahnge confidentiality
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

Table 1: TOE security functional requirements

1.3 Strength of Function

The TOE's strength of functions is claimed 'basic' (SOF-basic) for specific functions as indicated in the Security Target ([6], chapter 6.1).

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

1.4 Summary of Threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The assets to be protected by the TOE and its environment are as follows:

Name of asset	Description
sensitive user data	Confidential user data stored or processed in the system.
user authentication data	The user identifier and password entered by a user to authenticate himself to the system, and the reference values stored in the ABox database used for verification.
management data	Definition of user groups and their read/write members, the group specific data desensitisation method (pseudonymisation respectively which encryption algorithm with which key; software or hardware encryption).
encryption passwords	Passwords used for the key generation.
cryptographic keys	Keys used in the system for the encryption and decryption of sensitive user data.
pseudonym lists	Group specific lists stored in the ABox database indicating what pseudonyms are actually used in this group to reference sensitive user data and what contents each pseudonym stands for.
blacklists	Group specific lists of words that must not be contained in an input.
TOE software code	The programming code the TOE consists of.

Table 2: Assets to be protected by the TOE and its environment

The Security Target [6] considers the following subjects, which can interact with the TOE:

Name of subject	Description
ABox user	The ABox user is the legitimate user of the ABox Core.
supervisor	The supervisor defines users, user groups, their group owners and configuration data.
group owner	The group owner manages a particular user group, assigns and revokes users' write or read permissions for this group, may create user configurations, but may assign read or write permission only for the own group. Also he can designate a deputy.
deputy	The deputy continues the group owner's tasks (except for deputy designation) in his absence.
ABox database	The ABox database is connected to the TOE and stores the user authentication data, the cryptographic keys, the management data, and the pseudonym lists.
ABox WAN	The wide area network the ABox is embedded in, into which input stream is directed (after passage through the ABox Core) and from which output stream is received (which is directed through the ABox Core).
other person	All persons who interact with the TOE without being so authorised (as one of the preceding roles).

Table 3: Subjects that can interact with the TOE

The TOE and its environment shall comply to the following organisational security policies (which are security rules, procedures, practices, or guidelines imposed by an organisation upon its operations).

OSP.Desens: Data marked as sensitive shall leave the local ABox system only after being desensitised.

OSP.Conceal: Data marked as sensitive shall not be output (browser display, printer, …) to the user who has not the right to see it, in the case of pseudonymisation even not the belonging pseudonym (instead a constant message stating the non-availability of the data).

OSP.Administration**:** The configuration data of user groups and the assignment of users to user groups may be managed by supervisors, group owners and deputies as indicated in Table 3 about Subjects. It shall be possible that users with write permission for more than one user group may choose at the runtime which they want to exercise.

The TOE shall avert the threat as specified below:

T.Compromise: An attacker tries to acquire and disclose sensitive data.

As potential attackers all kinds of subjects as listed in Table 3 are considered, as far as they

- try to perform actions, which they are not allowed to by their access rights as defined in this ST and
- may have expertise, resources and motivation as expected from an attacker with low attack potential.

1.5 Special configuration requirements

Configuration setup

Before the ABox system components can be installed, the operation system environment has to be installed. This includes:

- LINUX Enterprise Server 9 for X86 with Service Pack 2 with module
  - Pwauth 2.2.8

  The operating system must be installed according to the EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server on IBM Hardware
- Apache Webserver 2.0.54 with the following module
  - Mod_auth_external 2.2.10
- Oracle Database Client 10.2 g for Linux
- Oracle Database Server 10.2 g for linux

- PHP-Runtime environment 5.05
- Utimaco CryptoServer 2000 (optional)

The ABox Core relies on a set of libraries which are provided by the Linux system or have to be installed during the system setup (see [14], sec. 3).

After installing the ABox the supervisors have to define the user groups and the group administrators (group owners and their deputies). Once a group administrator is defined, he will configure his user group. He will add and remove ABox users to or from his group and configure parameters like the encryption algorithm, MIME-Types, etc.

Each user must be a member of at least one group but can be member of more than one group. The user may have different rights in different groups. The data access to a target server is defined by the possible rights which may be read or write access.

ABox user configuration

A user may be authorised for several groups. In order to allow this, it must be recognised during the runtime which of the group definitions is valid, e.g. for writing. This will be done using a web dialog and allow the user to choose for what group definition he wishes to perform input/output operations. Initially, each user has a default user group assignment. The user can change his group assignment dynamically, within his authorised write groups, by invoking an ABox page in the browser.

In particular, the ABox Core provides a browser based dialog where the user has the possibility to change the active write group. The left column of the browser provides radio buttons where the user can actually set the active write group. The column in the middle indicates the assigned read groups (they can only be modified by an administrator). The right column just shows the ID and name of the group. The select-button stores the new user selection to the database.

1.6 Assumptions about the operating environment

The following assumptions hold for the usage environment:

A.Users: The users of the local ABox system will use the TOE according to the guidance and all other security instructions.

A.Administrators: The authorised administrators of the local ABox system will use the local ABox database according to the guidance and all other security instructions.

A.ABox_Access: The local ABox system is physically protected and access-controlled so that it may be accessed only by authorised users.

A.WAN: All storage media and transmission lines in the ABox WAN are protected against tapping of the transmitted data. The personnel having access to the data is trustworthy and will not compromise sensitive user data.

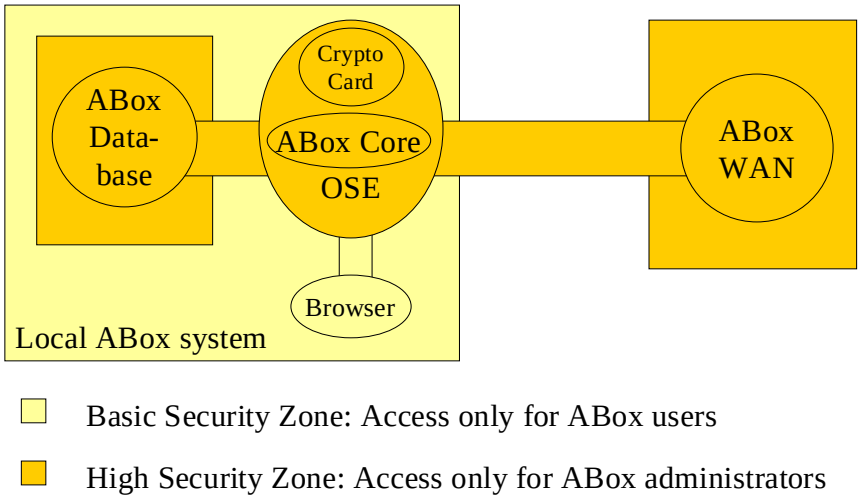

Figure 2 - Graphical representation of the access assumptions

1.7 Disclaimers

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:

ABox 1.0

The TOE consists of:

TOE component	Designation	Type	Transfer Form
TOE software	Provides the functionality of the TOE	SW	Electronic form
Installation Guide	Guidance for the installation of the TOE (Installation Guide for ABox 1.0, Version 1.1, T-Systems, 26.06.2006)	DOC	Document in paper / electronic form
Installation scripts	Scripts used for the installation of the TOE	SW	Electronic form
User Guidance	Guidance for the usage of the TOE by users and administrators (User Guidance for ABox 1.0, Version 1.3, T-Systems, 20.06.2006)	DOC	Document in paper / electronic form
Checksums	MD5 checksums to verify the integrity of the files	SW	Electronic form

Table 4: Deliverables of the TOE

3 Security Policy

The TOE shall comply to the following security policies:

- Data marked as sensitive shall leave the local ABox system only after being desensitised.
- Data marked as sensitive shall not be output (browser display, printer, …) to the user who has not the right to see it, in the case of pseudonymisation even not the belonging pseudonym (instead a constant message stating the non-availability of the data).

4 Assumptions and Clarification of Scope

4.1 Assumptions

A.Users - Trustworthiness of ABox users

The users of the local ABox system will use the TOE according to the guidance and all other security instructions.

A.Administrators - Trustworthiness of ABox administrators

The authorised administrators of the local ABox system will use the local ABox database according to the guidance and all other security instructions.

A.ABox_Access - Access to the local ABox system

The local ABox system is physically protected and access-controlled so that it may be accessed only by authorised users.

A.WAN - Security of the ABox WAN

All storage media and transmission lines in the ABox WAN are protected against tapping of the transmitted data. The personnel having access to the data is trustworthy and will not compromise sensitive user data.

4.2 Clarification of scope

none.

5 Architectural Information

The TOE is a software product and comprises four subsystems: The Input/Output filter, the Crypto Subsystem, the Authorisation Subsystem and the Administration Subsystem.

Subsystem Input/Output filter

The Input/Output Subsystem is the main subsystem of the TOE. There is only one main entry point to the subsystem. Over the defined apache module hook function the input and output HTTP requests respectively responses reach the TOE. Over this hook function the in-put/output filter subsystem process the HTTP streams using the same code base.

Crypto Subsystem

The Crypto Subsystem provides cryptographic services based on a software library or (optional) using a hardware module.

Authorisation Subsystem

The Authorisation Subsystem allows the user to change his/her active user (write) group within the active session. A script based dialog shows all groups the user is assigned to, and allows the user to select one and transmit the decision to the TOE. The active user (write) group is written to the database. It takes immediately effect for the next stream processing.

Administration Subsystem

This subsystem allows authorised users to administer the ABox configuration data. In this respect the ABox configuration data consist of groups and their parameters as well as user configuration data. The subsystem supports a role based access model. The three administrator roles supervisor, group owner and deputy are defined. It depends on the role of the user which workflow is accessible for him/her.

6 Documentation

The following documents are provided for a customer, who purchases the TOE:

- User Guidance for ABox 1.0, Version 1.3, T-Systems, 20.06.2006 [13]
- Installation Guide for ABox 1.0, Version 1.1, T-Systems, 26.06.2006 [14]

7 IT Product Testing

Tests of the Developer

The developer installed and tested the TOE on the platform as specified in chapter 1.5. The test settings contain two servers (one ABox server and one Oracle Database server) and dedicated test instances.

The following tools were specifically used for testing:

- the Internet Explorer Developer Toolbar
- the SAP Easy Access Tool 4.7
- the TBox, a specially developed tool for testing the ABox.

The developer tested the security mechanisms, the security functions, the subsystems and the external interfaces of the TOE.

Testing approach for coverage:

Most of the security properties indicated in the Functional Specification (FSP) were not tested separately, but in combinations. All TSF interface and all security properties of the FSP are mapped to tests.

Testing approach for depth:

Most of the security properties were tested in combinations. The TSF as defined in the high-level design (HLD) was completely mapped to the tests and the test documentation.

Tests of the Evaluator

These tests were conducted on 24.04.2006 and from 19.06.2006 to 20.06.2006 in Leinfelden-Echterdingen/Germany using the test environment of the developer. Bevore the evaluators started testing, they have checked the configuration of the test environment. Evaluator testing was carried out using the browser interface and the SAP easy access tool.

The evaluators assessed the developer's testing approach, coverage, depth and results. This included the following:

- the evaluators checked that the developer's testing approach covered the TOE's security mechanisms, security functions, subsystems and external interfaces;
- the evaluators repeated all of the developer's tests;
- the evaluators performed independently-devised functional tests to cover the security functions.

The evaluators' findings confirmed that:

- the developer's testing approach, depth, coverage and results were all adequate;
- the developer's tests covered the TOE's security mechanisms, security functions, subsystems and external interfaces;
- the actual results of the evaluator tests and the independently-devised functional tests were consistent with the expected test results.

The evaluators did not identify any obvious vulnerabilities during evaluation activities. Nevertheless the evaluators devised some supplementary test cases that could be considered as penetration tests.

8 Evaluated Configuration

The TOE is a software, the so-called ABox 1.0 together with guidance documentation. The TOE comprises two parts, the ABox Core and the ABox Admin Client. The ABox Core consists of the three indicated subsystems, the ABox Admin Client constitutes a fourth subsystem.

The ABox Core is embedded into a local system ("local ABox system") in which it is connected to an operating system environment (application software), to a database ("ABox database") and optionally to a crypto card. TOE users interact

with the TOE via the operating system environment. TOE management and configuration data are stored in the ABox database and are administered via an administrative interface, the ABox Admin Client.

The local ABox system is embedded into a larger system (“ABox WAN”) including a remote central database which can be accessed via a network (connected to the operating system environment) and including further local ABox systems.

9 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 (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL3.

The verdicts for the CC, Part 3 assurance components (according to EAL3 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS

Assurance classes and components		Verdict
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant
- The following TOE Security Functions fulfil the claimed Strength of Function:
  - TSF_Key_Generation
  - TSF_Crypt
  - TSF_Pseudonymisation

The results of the evaluation are only applicable to the ABox 1.0. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [13] + [14] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

none

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document. This document represents the complete Security Target used for evaluation.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
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

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

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

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

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

[6] Security Target for ABox 1.0, BSI-DSZ-0365-2006, Version V1.3, T-Systems, 21.06.2006)

[7] Evaluation Technical Report, Version 1.1, 30.06.2006, ABox 1.0, BSI-DSZ-0365-2006)

[8] Functional Specification for ABox 1.0, Version 1.2, T-Systems, 21.06.2006

[9] High-level Design for ABox 1.0, Version 1.1, T-Systems, 26.06.2006

[10] Test Documentation for ABox 1.0, Version 1.2, 12.05.2006

[11] Testcrypto Algorithmen for ABox 1.0, Version 1.1, 08.06.2006

[12] Test Coverage and test depth for ABox 1.0, Version 1.0, 26.06.2006

[13] User Guidance for ABox 1.0, Version 1.3, T-Systems, 20.06.2006

[14] Installation Guide for ABox 1.0, Version 1.1, T-Systems, 26.06.2006

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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