Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0807-2013

for

IBM DB2 Version 10.1 Enterprise Server Edition for Linux, UNIX and Windows (CC Configuration)

from

IBM Canada Ltd.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0807-2013

Database Management System

IBM DB2 Version 10.1 Enterprise Server Edition
for Linux, UNIX and Windows (CC Configuration)

from	IBM Canada Ltd.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 28 March 2013
For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department/

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

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

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

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 IBM DB2 Version 10.1 Enterprise Server Edition, for Linux, UNIX and Windows (CC Configuration) has undergone the certification procedure at BSI.

The evaluation of the product IBM DB2 Version 10.1 Enterprise Server Edition, for Linux, UNIX and Windows (CC Configuration) was conducted by atsec information security

GmbH. The evaluation was completed on 20 March 2013. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: IBM Canada Ltd..

The product was developed by: IBM Canada Ltd..

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product IBM DB2 Version 10.1 Enterprise Server Edition, for Linux, UNIX and Windows (CC Configuration) has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

[6] Information Technology Security Evaluation Facility

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

[7] IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario L3R 9Z7
Canada

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is IBM DB2 Version 10.1 Enterprise Server Edition for Linux, UNIX, and Windows (CC Configuration), a Database System offering a wide range of database related services.

The IBM DB2 for Linux, Unix and Windows Relational Database Management System (RDBMS) offers a wide range of database related services to multiple users or clients. As an RDBMS, the TOE supports the Structured Query Language (SQL) interface from the client to the database server.

Only the following operating environments systems are allowed in the evaluated configuration

- AIX 6.1 TL6 SP5
- Linux RHEL 5 update 6
- Linux SLES 10 with SP3
- Microsoft Windows Server 2008 R2 Enterprise Edition (64Bit)
- Solaris 10 update 9

The security functionality provided by IBM DB2 for Linux, Unix and Windows includes:

- Auditing of security relevant functions.
- Discretionary Access Control to objects using identities, privileges, authorities and access control lists associated with users, groups, roles and objects to determine if specific operations are allowed.
- Row and Column Access control, a more restrictive form of discretionary access control, where users need explicit access granted at the row level, the column level or both to access or modify data and higher level authorities does not apply.
- Label-Based Access Control to objects using security policies assigned to specific tables and security labels and exemptions assigned to specific users, groups and roles to determine if, in addition to DAC, access to applicable table rows or columns is allowed.
- Association of users and groups with database roles.
- Trusted contexts having the ability to use alternate identities without further authentication.
- Management of security functionality of the TOE as well as of users.
- Process separation to protect the TOE's resources.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	Addressed issue
Security Audit	The DB2 audit facility acts both at an instance level, recording all instance level activities, and at the database level for database specific activities. The audit log files, for instances and databases, are stored in file locations configured during installation and the audit configuration file (db2audit.cfg) is located in each instance's security subdirectory.
Access Control	Authorization is the process whereby DB2 obtains information about an authenticated DB2 user, indicating the database operations that the user may perform, and what data objects may be accessed. With each user request, there may be more than one authorization check, depending on the objects and operations involved.
Identification & Authentication	If a user attempts to access DB2 without a user ID and password while logged on to the DB2 host operating system (i.e., operational environment), DB2 will derive an authorization name ("authid") from the user ID of the user's host process. This is based on the assumption that the host has already identified and authenticated the user. When a user attempts to access DB2 remotely (i.e., while not logged onto the DB2 host operating system), they must provide a user identity and password. If the configured authentication server determines that the user identity exists and the password is valid, it will respond to DB2 with the authenticated user identity and any applicable group memberships. Otherwise, it will return a failed result that will cause DB2 to reject the request.
Security Management	All access control to objects subject to the Discretionary Access Control (DAC) security policy as well as to TSF data and functions are controlled using authorities and privileges. DB2 defines a number of authorities and privileges, which allow authorized users and administrators to perform specific functions or access specific resources. These authorities and privileges are assigned to objects using DB2 tables and configuration files (i.e., access control lists) that are similarly controlled with authorities and privileges. Members of the "user" role are most directly subject to the DAC policy and prevented from modifying the behaviour of the TSF. Privileges enable users to create, modify, or access database resources. Authority levels provide a method of grouping privileges and higher-level database manager maintenance and utility operations. Together, these act to control access to the database manager and its database objects.
TOE Protection	DB2 is designed to operate within a set of processes provided by the hosting operating system. DB2 does not support the ability to share its processes with non-TOE entities. Note that DB2 supports both "fenced" and "unfenced" routines. Fenced routines execute in their own process distinct from that of the DB2 server, while unfenced routines share the process with the DB2 server. Given that such routines are created by users and as such cannot be subject to evaluation, the evaluated

TOE Security Functions	Addressed issue
	configuration does not include any provisions for unfenced routines (i.e., they are not included in the evaluated configuration of the TOE). Furthermore, DB2 is designed in a manner that ensures that its interfaces do not offer unauthorized users any functions that might be used to corrupt, or otherwise inappropriately access, the TSF. As is the case with many application-only TOEs such as DB2, its protection mechanisms could be bypassed through the underlying environment should the assumptions and objectives for its environment not be fulfilled. Note that determination of fulfilment of those assumptions and objectives is not within the scope of the TOE.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1.

All TOE and environment security objectives have been derived from the statement of Organizational Security Policy or Secure Usage Assumptions. Therefore, there is no statement of explicit assets in the ST [6]. The TOE Security Problem is defined in terms of Assumptions and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.1 and 3.3.

For the configurations of the TOE covered by this certification please refer to chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM DB2 Version 10.1 Enterprise Server Edition, for Linux, UNIX and Windows (CC Configuration)

The following table outlines the TOE deliverables:

No	Type	Identifier	Version / Level	Form of Delivery
1.	SW	Platform: Windows Server 2008 R2 Enterprise Edition File: ccc_v10.1_ntx64.ese.zip Checksum: 26acf2a478347da28cc0a1037f 61f641cfdfb94825004e291d1544b7fb3e0a7d	DB2 V10.1.0.873	Electronic download

No	Type	Identifier	Version / Level	Form of Delivery
2.	SW	Platform: AIX 6.1 TL6 SP5 File: ccc_v10.1_aix64_ese.tar.gz Checksum: 45411807566235265f8de82919c90e525474fcf9e3162a43e5fcfd5e9ee82dc0	DB2 V10.1.0.873	Electronic download
3.	SW	Platform: Red Hat Enterprise Linux 5 Update 6 File: ccc_v10.1_linuxx64.ese.tar.gz Checksum: 8442440d79dc81952478898fc0fcd278cf86cce7a10d2f02973bbd3021fa25dc	DB2 V10.1.0.873	Electronic download
4.	SW	Platform: SuSE Linux Enterprise Server 10 SP3 File: ccc_v10.1_linuxx64.ese.tar.gz Checksum: 8442440d79dc81952478898fc0fcd278cf86cce7a10d2f02973bbd3021fa25dc	DB2 V10.1.0.873	Electronic download
5.	SW	Platform: Solaris 10 Update 9 File: ccc_v10.1_sun64.ese.tar.gz Checksum: a4e6bc6980c7c6fead0dba8da1646037db32699dcbb9c9266a153f6e79822340	DB2 V10.1.0.873	Electronic download
6.	DOC	Common Criteria Certification: Installing IBM DB2 10.1 for Linux, UNIX, and Windows, Enterprise Server Edition [8]	GC27-3899-00 November, 2012	Electronic download
7.	DOC	Common Criteria Certification: Administration and User Documentation - Volume 1 [9]	SC27-3897-00 November, 2012	Electronic download
8.	DOC	Common Criteria Certification: Administration and User Documentation - Volume 2 [10]	SC27-3898-00 November, 2012	Electronic download

Table 2: Deliverables of the TOE

The TOE software, IBM DB2 Version 10.1 Enterprise Server Edition for Linux, UNIX and Windows, is available from the following website which is published in [8], [9] and [10] which are made available as shown in the table 2 above: https://www.ibm.com/services/forms/preLogin.do?source=swg-IBMdb2esec3

Installation instructions as well as checksums to verify the TOE software are also included in the TOE documentation [8]. Customers are required to register with IBM and use the Download Director which utilizes secure hash security features.

The consumer can follow the instructions provided in section "Common Criteria certification of DB2 database products" of [9] and [10] which clearly spell out the firmware versions that need to be installed for the evaluated configuration. The guidance documents for the TOE are clearly labelled as being applicable to the TOE.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit,
- Access Control,

- Identification & Authentication,
- Security Management,
- TOE Protection.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled for the use of the TOE in its operational environment and by the TOE-Environment. The following topics are of relevance:

- Appropriate guidance documentation must be provided to enable administrators to install, manage, and operate the TOE in a manner that maintains IT security objectives.
- Administrators of the TOE and its operational Environment must not be careless, wilfully negligent or hostile, and must follow the instructions provided in the administrator guidance documentation.
- One or more competent individuals must be assigned to manage the TOE and the security of the information it contains.
- Authorized users must possess the appropriate authorization to access at least some of the information managed by the TOE and must act in a cooperative manner in a benign environment.
- Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security objectives.
- Those responsible for the TOE must ensure that those parts of the physical TOE and its associated operational environment critical to security policy are protected from attack, which might compromise IT security objectives.
- Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives and that credentials (e.g., clearances) are assigned appropriately, including ensuring that administrators are cleared to the highest security level processed by the TOE.
- Those responsible for the TOE must ensure that the components underlying the TOE fulfil the objectives for its operational environment described in this ST.
- The TOE’s operational environment must ensure that only authorized users gain access to the operational environment and its resources. The operational environment must support the TOE by ensuring that users are adequately authenticated on the TOE’s behalf.
- The TOE’s operational environment must be able to record the security relevant actions of users of the operational environment.

- The TOE's operational environment must provide cryptographic services suitable to allow the TOE to establish secure SSL connections.

- The TOE's operational environment must ensure that any information contained in a protected resource that may be assigned to the TOE is not released when the resource is recycled.

- The TOE's operational environment must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of operational environment security, including security relevant support for the TOE.

- The TOE's operational environment must be designed and implemented in a manner that ensures that it can protect the operational Environment of the TOE. The TOE's operational environment must provide a reliable time source and secure audit storage for the use of both the TOE and its operational Environment.

Details can be found in the Security Target [6], chapter 4.2.2.

5 Architectural Information

The TOE is a relational database management system (RDBMS) that supports the Structured Query Language (SQL) interface from a client that is connected to the database server. From the client, commands can be entered interactively or through an executing program to the database server to create databases, database tables, and to store and retrieve information from tables. The TOE can be installed on a number of possible operating environments. The TOE can be distributed across a number of logically (i.e., on the same underlying machine) or physically (i.e., on different underlying machines running the same operating system) separate partitions. From the user perspective, there is effectively no difference, while the distributed partitions work in concert to answer user queries. The TOE also supports Symmetric Multi Processing (SMP) architecture by distributing workload onto different processors in the same machine.

The TOE is comprised of the following main components:

- A Distributed Relational Database Architecture (DRDA) protocol handler allowing the TOE to act as a DRDA Application Server (AS). This allows one or more Application Requesters (AR) or clients to access a specific database instance or database and issue SQL or non-SQL requests. During initiation of communication between the client and the DRDA AS, a common security mechanism (described as the "Userid, Password" mechanism in the DRDA standard) is negotiated. If password validation fails, the connection with the client is terminated. If the password is authenticated, a session is established and the client may send SQL and non-SQL requests to the TOE for processing.

- A Structured Query Language (SQL) processing component which allows the TOE to analyse and process SQL requests from the client. The TOE supports the ANSI/ISO SQL2 standard for all types of SQL statements including:
  - Data Definition Language (DDL) statements that create, alter, drop, rename or transfer ownership of database objects.

  - Data Manipulation Language (DML) statements that are used to query or modify the data contained within the database objects.
  - GRANT and REVOKE statements that are used to control access to database authorities as well as privileges on database objects.
  - Transaction control statements that are used to manage the integrity of the database with respect to any modifications made by a client. These statements include the ROLLBACK and COMMIT statements.
  - Various other statements that are used to perform a number of actions on database objects or on the connection environment.
- A non-SQL processing component that allows the TOE to analyse and process client requests not concerned with SQL statements. These requests are used to invoke a number of utilities or application programming interfaces (APIs) that do not utilize SQL. Each API and utility has access privileges or authority requirements defined by the TOE. The non-SQL processing component enforces the discretionary access control policy for these requests by ensuring that the required privilege or authority is held by the requester.

The TOE includes an optional Database Partitioning Feature (DPF) allowing the database to be instantiated across multiple partitions on the same or separate machines for the purpose of scalability. When the TOE is instantiated on multiple systems they must all be running the same operating system. The overall security mechanisms of the TOE remain the same even though the processing may be spread across the partitions internally.

The TOE can use multiple processors if present and operational on the underlying machine for performance and scalability. While processing may be spread across different processors internally, the overall security mechanisms of the TOE remain the same.

The TOE includes a "trusted context" feature that defines a trust relationship based on an authorization name, a data stream encryption attribute (note that any encryption capability is provided by the TOE's operational environment) and an IP address. Any user associated with this definition of a trusted context object is considered trusted by the TOE and may be allowed to modify the "user" associated with the connection. This change of associated user may or may not require authentication of the user identity. This feature is intended for multi-tier environments where the middle tier, typically an application server, might already perform authentication of end users.

The TOE requires an authentication server to be configured. The TOE can be configured to utilize the authentication services of the underlying operating system, an externally available LDAP server, or an externally available KDC server. The TOE relies on the configured server for appropriate authentication services for users.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The TOE was installed and tested on each supported operating system in each of the following configurations:

- Stand-alone configuration - This test configuration is used for running test cases with the TOE installed on a single system or partition and the database existing on that single system or partition. This configuration was also used to test the symmetric multi-processing mode of operation of the TOE. Specific instructions for setting up this configuration were provided by the developer.

- Database Partitioning Feature (DPF) configuration - This test configuration was used for running test cases with the TOE installed on multiple systems and multiple partitions. Specifically, the TOE was installed into two separate partitions on two separate systems, providing a DPF configuration of four interconnected systems. Specific instructions for setting up this configuration were provided by the developer.

7.1 Developer Testing

Overview

The developer performed functional developer test within his test environment located in Markham, Ontario CA. All functional tests were performed on a TOE configuration consistent with the ST [6]. The test results of the developer functional tests had no deviations from the expected results.

Approach

The developer used an approach based on the TOE Security Functionality (TSF) as described in the Security Target [6]. For each Security Function, the developer identified and prepared test cases to verify the correct behaviour of the TOE. The test cases were performed utilizing the TOE Security Functional Interfaces (TSFI). All tests were run by the developer utilizing automated test tools and compliance of actual test results with expected test results noted in a log file.

Test Configuration

The developer tested the TOE with the following configurations consistent with those identified in the ST [6] and installed in accordance with installation guidance [8] and the CC User and Administrator Guidance ([9] and [10]).

- Stand-alone system testing
  - Windows Server 2008 R2 with SP3
  - SuSE SLES 10 with SP3 and RedHat 5.6 in separate partitions
  - AIX 6.1 TL6 SP5
  - Solaris 10 update 9
- Database Partitioning Feature (DPF) testing
  - Two logical nodes on each of the following systems comprising 4 nodes for each database:
    - 2 - Windows Server 2008 R2 with SP3 machines
    - 2 - SuSE SLES 10 with SP3 machines

- 2 - RedHat RHEL 5.6 machines
- 2 - AIX 6.1 TL6 SP5 machines
- 2 - Solaris 10 update 9 machines

In addition to the above configurations, testing was also performed with Symmetric Multi-Processing (SMP) enabled in each of the above configurations.

Test Result

All test results from all tested platforms and configurations show that the expected test results are identical to the actual test results.

Verdict

The evaluator has confirmed that the developer testing was performed in an operational environment conforming to the ST [6]. The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer.

The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases as demonstrated in the test coverage analysis. The evaluator found the testing of the TSF to be extensive and covering all of the TSFI as identified in the functional specification. The evaluator reviewed the test results provided by the developer and found them to be consistent with the test plan.

7.2 Evaluator Independent Testing

This section contains details about the testing performed by the evaluator in order to verify proper behaviour of the TOE interfaces.

Overview

The independent testing was done in two phases. The first phase was performed using test systems at the IBM facilities in Markham, Ontario. The evaluator witnessed the installation and configuration of the TOE per the instructions provided in [6], [8], [9] and [10]. The evaluator reran the entire test suite, as documented in the developers test plan, successfully.

In the second phase, the evaluator configured the TOE and the operational environment as stated in [6], [8], [9] and [10]. The evaluator executed the tests successfully.

Approach

The configuration for first phase was performed using the test systems and configuration provided by the developer (cp. Section “Test configuration” in previous sub-chapter). Regarding the configuration for the second phase the evaluator performed independent testing using the following configurations:

- Linux RedHat RHEL 5 update 6
- Linux Suse SLES 10 with SP 3

The systems were configured as two nodes of a Database Partitioning Feature (DPF) database.

Verdict

In both testing phases, the actual test results matched the expected test results and no deviations were observed.

7.3 Evaluator Penetration Testing

Overview

The penetration testing was performed using the evaluators testing environment at the atsec information security GmbH ITSEF in Austin, TX (cp. section “Approach” in previous subchapter). The final overall test result found no deviations between the expected and the actual test results. Additionally, no attack scenario with an attack potential less than or equal to Enhanced-Basic was successful.

Penetration Testing Approach

The approach taken by the evaluator was conformant with the assurance component chosen (AVA_VAN.3), examining the TOE to determine its resistance to an attack with an Enhanced-Basic attack potential. The evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. Additionally, the evaluator used publicly available scanners to assess the TOE for vulnerabilities. The evaluator assessed the potential vulnerabilities to determine which were and were not applicable to the TOE in its operational environment.

The evaluator developed attack scenarios for potential vulnerabilities that were applicable to the TOE in its operational environment to determine where these potential vulnerabilities could be exploited. After performing an analysis on the theoretical related attack potential, the evaluator conducted penetration tests for any of these scenarios where the attack potential was Enhanced-Basic or less. For each penetration test, the evaluator examined the results of the tests to determine if any of the penetration tests were successful in attacking the TOE with an attack potential of Enhanced-Basic or less.

Attack Scenarios Tested:

- AS-1: Buffer overflow in unfenced routines
- AS-2: Incorrect access permissions to non-default audit log, audit archive file and audit ASCII delimited audit file.

SFRs Penetration Tested:

TSS Penetration Tested	Related SFR(s)
DB2 is designed in a manner that ensures that its interfaces do not offer unauthorized users any functions that might be used to corrupt, or otherwise inappropriately access, the TSF.	n/a
Providing interfaces to the system administrator, applicable security administrator, and users granted execute access to the applicable audit routines for the review and archival of audit records.	FAU_SAR.1.1: system administrators, security administrators, or users granted privilege to execute audit routines are provided with the ability to read and archive audit information.
Ensuring that the user is a system administrator or security administrator (per their role) or alternately has been granted execute privilege to the applicable audit routines before allowing access to the audit records associated with their role or privileges.	FAU_SAR.2: all users shall be prohibited read access to the audit records except those that have been granted explicit read access.

Table 3: SFRs Penetration Tested

Verdict for sub-activity

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced-Basic was actually successful in the TOE's operational environment as defined in the ST [6] provided that all measures required by the developer are applied.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The Target of Evaluation includes the evaluated software versions of DB2 Enterprise Server Edition for Linux, Unix and Windows as specified in section "Common Criteria certification of DB2 database products" of [9] and [10].

The items listed in table 2 of this report represent the TOE.

As stated in [8], the following requirements and restrictions must be met to achieve the evaluated configuration:

Requirements

- The installation procedures documented in the following environment specific sections of [8] must be followed and configuration options selected during installation must not be modified:
  - *"Installing DB2 Enterprise 10.1 for a single-partition Common Criteria-compliant installation"*
  - *"Installing DB2 Enterprise 10.1 on Windows Server 2008 for a single-partition Common Criteria-compliant installation"*
  - *"Installing DB2 Enterprise 10.1 for a multi-partition Common Criteria-compliant installation"*
  - *"Installing DB2 Enterprise 10.1 on Windows Server 2008 for a multi-partition Common Criteria-compliant installation"*
- Databases must be created with the RESTRICTIVE operand specified.

- One of the following authentication mechanisms must be used[8]: SERVER_ENCRYPT, DATA_ENCRYPT, DATA_ENCRYPT_CMP, KERBEROS, or KRB_SERVER_ENCRYPT. These authentication mechanisms encrypt user credentials as they flow between clients and servers.
- When using the DB2 Database Partitioning Feature (DPF), the external security information that is used by the DB2 database manager for authentication and authorization must be configured consistently on each partition.

Restrictions

- The set of DB2 interfaces that may be used in the evaluated configuration are:
  - The DB2 installation program,
  - The command line processor,
  - DB2 commands,
  - DB2 application program interfaces (APIs),
  - SQL statements.

  Note: Other interfaces must not be used.
- The Workload Management feature must not be used.
- NOT FENCED user created routines are not supported.
- Named pipes are not supported as a communication protocol between remote clients and a database server.
- High availability database recovery (HADR) is not supported.
- The data encryption functions ENCRYPT, DECRYPT_BIN, DECRYPT_CHAR and GETHINT must not be used.
- User-written security plug-ins are not permitted.

9 Results of the Evaluation

9.1 CC specific results

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.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)

[8] Note: The user identity and password are provided to the DB2 host operating system, configured LDAP server, or configured KDC server (using Kerberos) for authentication.

- The components ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.1

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS Application Notes and Interpretations of the Scheme

AIX Advanced Interactive eXecutive

ANSI	American National Standards Institute
API	Application Programming Interfaces
AR	Application Requesters
AS	Application Server
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DAC	Discretionary Access Control
DDL	Data Definition Language
DML	Data Manipulation Language
DPF	Database Partitioning Feature
DRDA	Distributed Relational Database Architecture
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HADR	High Availability Database Recovery
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KDC	Key distribution center
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RDBMS	Relational Database Management System
RHEL	Red Hat Enterprise Linux
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR Security Functional Requirement

SLES SUSE Linux Enterprise Server

SMP Symmetric Multi Processing

SP Service Pack

SQL Structured Query Language

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

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

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

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

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

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9].

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

[6] Security Target BSI-DSZ-CC-0807-2013, Version 15, 20. September 2012, IBM DB2 Version 10.1 Enterprise Server Edition for Linux, UNIX, and Windows (CC Configuration), IBM Canada Ltd.

[7] Evaluation Technical Report, Version 1.2, 06. March 2013, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Guidance documentation for the TOE, Version GC27-3899-00, 14. November 2012, Common Criteria Certification: Installing IBM DB2 10.1 for Linux, UNIX, and Windows, Enterprise Server Edition

[9] Administration and User Documentation, Volume 1, Version SC27-3897-00, 14. November 2012, Common Criteria Certification: Administration and User Documentation - Volume 1

[10] Administration and User Documentation, Volume 2, Version SC27-3898-00, 14. November 2012, Common Criteria Certification: Administration and User Documentation - Volume 2

[9] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

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

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

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

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

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

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

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

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

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

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

Table 1: Evaluation assurance level summary”

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

“Objectives

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

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

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

“Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

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

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

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

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank