Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0622-2012

For

IBM DB2 Version 9.1
for z/OS Version 1 Release 10

from

IBM Corporation

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-0622-2012

Database Management System

IBM DB2 Version 9.1
for z/OS Version 1 Release 10

from IBM Corporation

Common Criteria Recognition Arrangement

PP Conformance:	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, 25 July 2007, Information Assurance Directorate, National Security Agency, Controlled Access Protection Profile, Version 1.d, NSA 1999-10-08
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

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, 20 July 2012

For the Federal Office for Information Security

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.

2.1 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.

---

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

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 9.1 for z/OS Version 1 Release 10 has undergone the certification procedure at BSI.

The evaluation of the product IBM DB2 Version 9.1 for z/OS Version 1 Release 10 was conducted by atsec information security GmbH. The evaluation was completed on 24 April 2012. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: IBM Corporation.

The product was developed by: IBM Corporation.

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,

[6] Information Technology Security Evaluation Facility

- the product is operated in the environment described, where 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 9.1 for z/OS Version 1 Release 10 has been included in the BSI list of the 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.

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 Corporation
555 Bailey Avenue
San Jose, CA 95141
USA

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 a combined TOE, consisting of:

- The “IBM z/OS Version 1 Release 10 (z/OS V1R10)” operating system, including the Resource Access Control Facility (RACF) which is used as the evaluated platform
- The “IBM DB2 Version 9.1 for z/OS” (DB2 9), which is built upon this platform

The DB2 v9.1 for z/OS Security Target [6] builds on the z/OS Security Target [8], which refers to the evaluated “IBM z/OS Version 1 Release 10” operating system.

DB2 9 is a relational database management system that operates as a subsystem of z/OS. DB2 is implemented by a set of address spaces plus a set of utilities.

The evaluation consist of z/OS and DB2, the TOE is a combination of both. Thus "TOE" always means DB2 and z/OS in this report. For z/OS, usually the term “z/OS platform” is used and for the application, “DB2.”

DB2 for z/OS is IBM’s flagship database management system, designed to efficiently and cost-effectively deliver information to enterprise-class e-business applications and leverage the capacity and processing power of IBM zSeries and z/OS.

Version 9.1 of DB2 introduces enhancements to performance, reliability/availability and security, breaking barriers in key areas of database deployment.

Users can use SQL statements to define databases and manage their content. Several “attach facilities” exist that can be used to submit SQL statements as well as database commands from user programs to DB2. DB2 will evaluate the user’s right to perform the requested actions before satisfying the request.

DB2 9 for z/OS provides security options for e-business with multilevel security and row-level security as well as high security, more granularity and more information for additional flexibility in applications and SQL, and encryption capabilities.

In addition, DB2 9 for z/OS improves access control by using database roles in a trusted context, which provides the flexibility for managing context-specific privileges and simplifies the processing of authorization. Improved filtering makes auditing more usable and the Secure Sockets Layer(SSL) data encryption on networks is more secure.

The TOE fulfills the requirements of the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2. [7] and the Controlled Access Protection Profile [7]. In the evaluated configuration. DB2 uses the access control and security management services provided by the Resource Access Control Facility (RACF) of z/OS for discretionary access controls and to implement multilevel security controls down to the granularity of individual rows in a database.

Additionally, the TOE provides access control functions for z/OS and DB2 using RACF as the central access control module. Access rights for both z/OS and DB2 objects are therefore managed using the same interface provided by RACF. Access controls defined by the SQL GRANT and REVOKE commands are not relevant and therefore ignored in the evaluated version of the TOE with access control to the DB2 objects provided by RACF.

The TOE also implements mandatory access control for both z/OS and DB2 objects. In DB2, mandatory access control is implemented by a dedicated column in each table that contains the sensitivity label of the row. This column is maintained by the TOE and can not be altered by a user unless he has the specific privilege to overwrite labels.

To operate a mainframe system which deploys the products constituting this TOE in either a CAPP or Labeled Security Mode of operation, the products must be installed in their evaluated version and configured in a secure manner as described in the directions delivered with the media and the accordant guides listed in the [8] and especially for DB2 9, “DB2 Version 9.1 for z/OS Requirements for the Common Criteria" [11].

The DB2 for z/OS security target [6] documents the security characteristics of the TOE described above in the Labeled Security and CAPP modes of operation.

The TOE is composed of one instance of z/OS V1R10 running on an abstract machine as the sole operating system exercising full control over it, and DB2 9 running on top of z/OS V1R10.

Multiple instances of the TOE may be connected in a basic sysplex or in a parallel sysplex, sharing their RACF database and acting like a single system. This functionality is provided by z/OS V1R10, and DB2 relies on the mechanisms provided by the underlying operating system.

The required runtime environment for the z/OS V1R10 platform is described in section “TOE description” of the z/OS Security Target [8]. This description is also valid for this combined TOE and is not restricted or expanded by DB2 9.

User identification and authentication and parts of access control to DB2 objects are provided by the Resource Access Control Facility (RACF), a z/OS Security Server component that is used by different services as the central instance for identification and authentication and for access control decisions. z/OS V1R10 and DB2 9 come with management functions that allow configuring the TSF and tailoring them to the customer’s needs.

Some elements that have been included in the TOE do not provide security functions. These elements run in authorized mode, so they could compromise the TOE if they do not behave properly. Because these elements are essential for the operation of many customer environments, the inclusion of these elements subjects them to scrutiny during the evaluation and ensures that they may be used by customers without affecting the TOE’s security status.

In its evaluated configuration, the TOE allows two modes of operation: Labeled Security mode and CAPP-mode. In both modes, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels, but all other configuration parameters are identical in the two modes.

Throughout the DB2 Security Target [6], any claims that are only valid for the Labeled Security mode are marked accordingly.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, 25 July 2007, Information Assurance Directorate, National Security Agency, Controlled Access Protection Profile, Version 1.d, NSA 1999-10-08 [7].

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.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] chapter 6. 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 Functionalities:

TOE Security Functionality	Addressed issue
Identification and authentication	DB2 relies on the identification and authentication performed by z/OS. When checking for the user's right to use authorities managed by DB2, the database management system uses the ID of the user verified by z/OS. Additionally, DB2 can establish a trusted connection with a user or system when a trusted context matches the characteristics of the connection, based on the user ID and connection trust attributes (e.g. IP address, domain name or SERVAUTH security zone name for a remote client, the job or task name for a local client). A trusted context allows the association of the trusted connection with a database role, a different user or a security label (in Labeled Security mode) for access control.
Object access control	In the evaluated configuration, DB2 uses RACF to check for and manage access control to DB2 objects. DB2 internal access controls based on the GRANT and REVOKE SQL statements will not be effective in the evaluated configuration. In the case of a trusted connection, access control also includes object ownership rules based on database roles. A database role can be assigned to the DB2 process by a trusted context. In Labeled Security mode, mandatory access control is in effect: DB2 then uses the labels defined in the RACF profiles related to DB2 objects as well as the DB2-managed labels of rows in tables. In any case, the label-based access checks for mandatory access control are performed using RACF. In the case of a trusted connection, the default security label defined for the related trusted context, if any, is assigned to the DB2 process.
Audit	The audit requirements are implemented using a mix of SMF records generated by RACF and the DB2 internal trace.
TSF management	In the evaluated configuration DB2 uses the functions provided by RACF to manage user profiles as well as the profiles related to DB2 objects. Access to authorities of DB2 objects is controlled by those profiles. Labels for rows in tables are assigned when they are created using the current label of the user that creates the row. The current label of the user is maintained by RACF.
TOE self protection	DB2 uses the protection mechanisms of z/OS with RACF to protect its address space, functions and objects from unauthorized access and manipulation.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7, and its references.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1 . Based on these assets the TOE Security Problem is defined in terms of Assumptions,

Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2, 3.3 and 3.4.

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 9.1 for z/OS Version 1 Release 10

The following tables outline the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	One of the following licensing options: ● DB2 Version 9.1 for z/OS (standard version) – product number 5635-DB2 ● DB2 Version 9.1 for z/OS (Value Unit Edition "VUE") -product number 5697-P12	9.1	Physical shipment (tapes)
2	SW	DB2 Utilities Suite for z/OS - product number 5655-N97	9.1	Physical shipment (tapes)
3	SW	● UK57609 (APAR PM10538) ● UK56520 (APAR PK90346) ● UK64090 (APAR PM28621) ● UK64250 (APAR PM28854) ● UK50217 (APAR PK75583) ● UK65907 (APAR PM33064)	N/A	Electronic download (via ShopzSeries)

No	Type	Identifier	Release	Form of Delivery
4	DOC	● ServerPac: Installing Your Order ● Requirements for the Common Criteria (SC19-2788-00) ● Memo to Customers of DB2 9 for z/OS Common Criteria Evaluated Base ● DB2 9 for z/OS (5635-DB2) standard licensing option: – DB2 for z/OS Codes (GC18-9843-05) – DB2 for z/OS Installation Guide (GC18-9846-07) – DB2 9 VUE Softcopy Publications CD (LK3T-7195-03) – DB2 for z/OS Licensed Program Specifications(GC18-9848-01) – DB2 for z/OS Messages (GC18-9849-05) – DB2 for z/OS Program Directory (GI10-8737-02) ● DB2 9 for z/OS (5697-P12) Value Unit Edition (VUE) licensing option: – DB2 for z/OS Installation Guide (GC18-9846-07) – Softcopy Publications CD (LK3T-7195-03) – DB2 9 for z/OS License Information (GC19-2414-02) – DB2 9 for z/OS Value Unit Edition Program Directory (GI10-8779-02) ● DB2 Utilities Suite for z/OS V9.1.0. (5655-N97): ● Licensed Information for DB2 Utilities Suite (GC19-1100-00) ● DB2 Utilities Suite for z/OS, V9R1 Program Directory(GI10-8647-00)	9.1	Physical shipment (hardcopies and CD-ROM)

Table 2: Deliverables of the TOE, DB 2 portion

No	Type	Identifier	Release	Form of Delivery
z/OS Version 1 Release 10 (V1R10) Common Criteria Evaluated Base Package:				
z/OS Version 1 Release 10 (z/OS V1R10, program number 5694-A01)				
1	SW	z/OS V1R10 Common Criteria Evaluated Base (IBM program number 5694-A01)	V1R10	Tape
2	DOC	z/OS V1R10 Program Directory	GI10-0670-10	Hardcopy
3	DOC	z/OS CD Collection Kit	SK3T-4269-21	CD-ROM
4	DOC	z/OS Hot Topics Newsletter	GA22-7501-15	Hardcopy
5	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
6	DOC	Memo to Customers of z/OS V1.10 Common Criteria Evaluated Base	n/a	Hardcopy

No	Type	Identifier	Release	Form of Delivery
7	DOC	z/OS V1R10.0 Planning for Multilevel Security and the Common Criteria	GA22-7509-09	Hardcopy
IBM Print Services Facility™ Version 4 Release 2 for z/OS (PSF V4.2.0, program number 5655-M32)				
8	SW	IBM Print Services Facility™ Version 4 Release 2 for z/OS (PSF V4.2.0, program number 5655-M32)	V4R2	Tape
9	DOC	PSF 4.2 CDROM Kit BOOK	SK3T-9927-02	CD-ROM
10	DOC	PSF 4.2 CDROM Kit PDF	SK3T-9928-02	CD-ROM
11	DOC	PSF Tiers-AFP/IPDS Printers	Z125-4564-18	Hardcopy
OGL/370 V1.1.0 (Program number 5688-191)				
12	SW	Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)	V1R1	Tape
13	DOC	Overlay Generation Language/370: User's Guide and Reference	S544370203	Hardcopy
14	DOC	OGL/370 V1R1.0: Getting Started	G544369100	Hardcopy
15	DOC	OGL/370 V1R1.0: LPS	G544369700	Hardcopy
16	DOC	OGL: Command Summary and Quick Reference	S544370301	Hardcopy
17	DOC	Program Directory OGL/370	GI10021201	Hardcopy
IBM Ported Tools for z/OS V1.1.3 (5655-M23)				
18	SW	IBM Ported Tools for z/OS V1.1.3 (Program number 5655-M23, optional)	V1.1.3	Tape
19	DOC	Program Directory IBM Ported Tools for z/OS V1.1.3	GI10-0769-03	Hardcopy
20	DOC	IBM Ported Tools for z/OS License Information	GA22-7986-05	Hardcopy
21	DOC	Supplementary Toolkit License Information	GA22-7986-06	Hardcopy
Additional Media				
22	SW	PTFs: UA44228, UA44851, UA44991, UA45841, UK38941, UK39926, UK41041 obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)	n/a	Electronic

Table 3: Deliverables of the TOE, z/OS portion

The DB2 portion of the TOE is delivered as a ServerPac (a preconfigured set of software modules) on a cartridge that is physically shipped to the customer and installed by the customer via CustomPac install dialogs, as well as applicable PTFs that are available for electronic download.

These additional PTFs must be electronically downloaded using ShopzSeries IBM website.

The delivery of the TOE is a chain of processes to produce and ship the TOE components called ServerPacs, a preconfigured set of software modules that can be installed by the customer. The process starts when the TOE has been built by the developers and delivered to the production facility in Boulder, CO, where they are collected, packaged, and finally delivered to the customer.

The evaluated version of z/OS can be orderd via an IBM sales representative or via the ShopzSeries web application (http://www.ibm.com/software/shopzseries). When filing an order via (secured) internet services, IBM requires customers to have an account with a

login name and password. Registration for such an account in turn requires a valid customer ID from IBM.

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:

- Identification and authentication
- Object access control
- Audit
- TSF management
- TOE self protection

For more information on these issues, see Security Target [6], chapter 1.

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 by the TOE-Environment. The following topics are of relevance:

- Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.
- Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical 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.
- The underlying abstract machine must provide a separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.
- When installed/available in the hardware the TOE is operating on, the cryptographic features provided by the processor or specific hardware coprocessors shall correctly perform the cryptographic operations the TOE requests them to perform.
- Those responsible for the TOE must ensure that users of the TOE are cleared for access to information depending on the classification of the information. They must also ensure that information is correctly classified to be protected by the security functions of the TOE.
- Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS.
- The underlying OS has been validated.

- Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

Details can be found in the Security Target [6], chapter 3.

5 Architectural Information

The Target of Evaluation (TOE) is the IBM DB2 Version 9.1 for z/OS on the IBM z/OS Version 1 Release 10 operating system, including the Resource Access Control Facility (RACF) as described in the DB2 v9.1 for z/OS Security Target ([6]).

The security description and configuration of the z/OS V1R10 operating system is provided in the z/OS Security Target [8] section 1.3 “TOE description”, and is considered in this evaluation. Only the DB2-specific functionality is described below.

DB2 portion of the TOE is a relational database management system that operates as a subsystem of z/OS. DB2 is implemented by a set of address spaces plus a set of utilities.

Users can access DB2 locally using "attachment facilities" or remotely via the Distributed Data Facility which uses the DRDA protocols defined in the Open Group Technical Standards DRDA-V1,DRDA-V2, and DRDA-V3.

Attachment facilities execute in the caller's address space and communicate with the DB2 address spaces to serve requests from the user. Attachment facilities included in the evaluated configuration include the TSO attachment facility via the DSN TSO command or the DB2I ISPF panels (which in turn use the DSN command to communicate with DB2).

Another attachment facility is the Call Attachment Facility (CAF), which allows programs executing under TSO or in the z/OS batch environment to communicate with DB2.

The Resource Recovery Services Attachment Facility (RRSAF) is a newer implementation of CAF with additional capabilities. RRS is a feature of z/OS that coordinates commit processing of recoverable resources in a z/OS system. DB2 supports use of these services for DB2 applications that use the RRS attachment facility provided with DB2. Use the RRS attachment to access resources such as SQL tables, DL/I databases, MQSeries messages, and recoverable VSAM files within a single transaction scope.

A requester using DRDA connects to an application server or database server. DRDA uses Distributed Data Management (DDM) and Formatted Data Object Content Architecture (FD:OCA) as part of the underlying architecture of DRDA. DDM is the communication language used for message interchange systems. FD:OCA is used to exchange user data among like or unlike systems. This allows external users to connect to DB2 and operate on DB2 databases.

The DB2 Utilities are a set of online and standalone programs providing database diagnostic and maintenance functions for administrators. The utilities do not use the standard attachment facilities and operate with the database files directly at the table space level.

The following figure shows the basic structure of DB2 and the attachment facilities supported in the evaluated configuration.

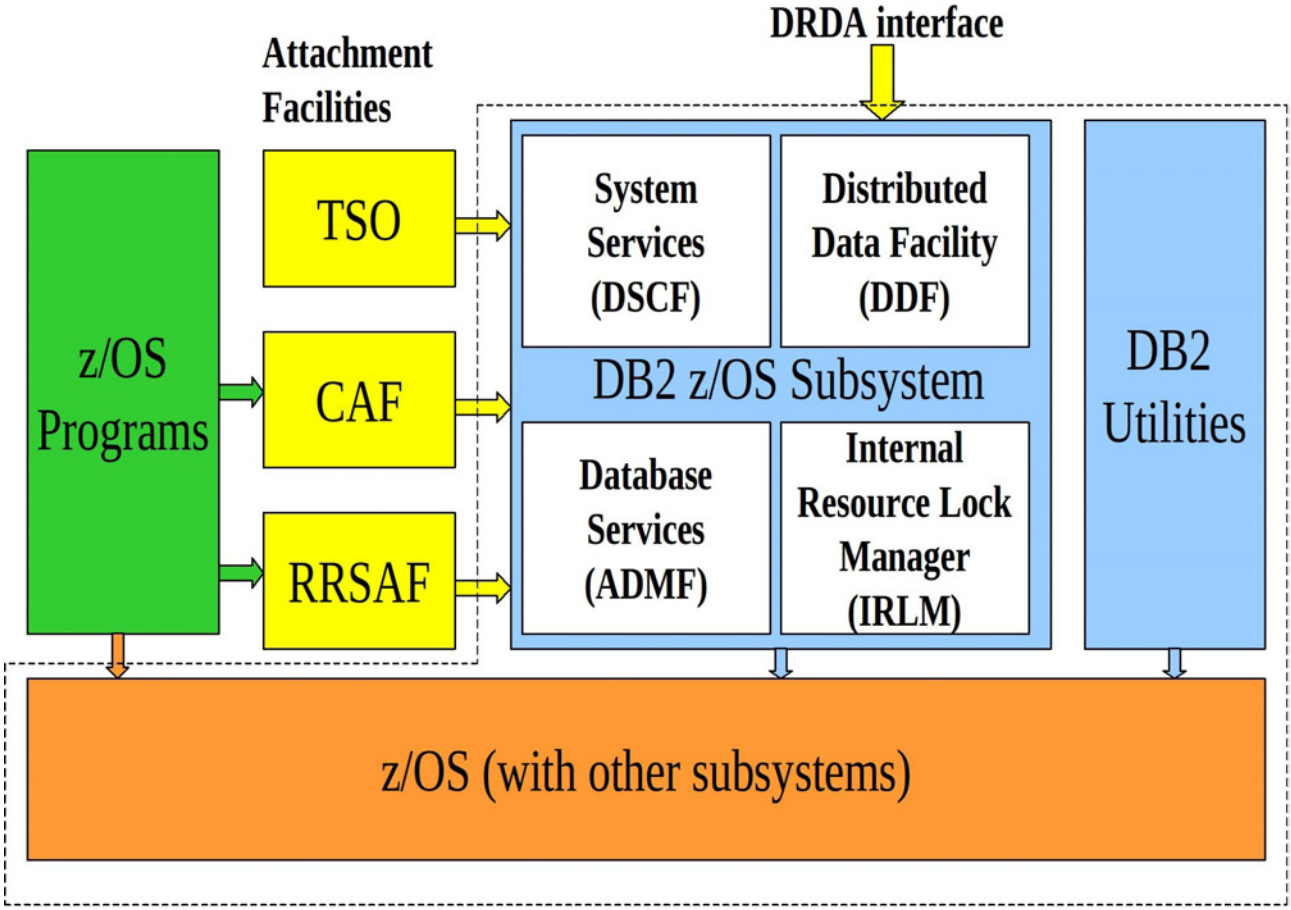

Figure 1:: Basic structure of DB2 for z/OS showing TOE structure with TOE boundary

The blue boxes in this figure represent the trusted parts of DB2, the yellow boxes represent those parts of the attachment facilities of DB2 executing in the user's address space or connections using the network interface. The brown box represents the z/OS system that has already been evaluated as the platform of this combined TOE. The green box represents (untrusted) user programs using services of z/OS and DB2.

The yellow arrows in the figure represent external interfaces of the trusted parts of DB2. The brown arrow represents the external interfaces of the trusted parts of z/OS (which have been assessed in the z/OS evaluation). The blue arrows represent the interface between the trusted part of DB2 and the trusted part of z/OS.

It should be noted that this figure shows the main parts of the TOE and its interfaces, not a flow of information. It should also be noted that the interfaces are not disjointed. The trusted parts of DB2, for example, will also use interfaces to the trusted parts of z/OS that are also used by other programs operating on top of z/OS.

Subsystem	Description
Relational Data Subsystem	
Relational Data Security Module	The module uses RACF to implement the security functions which is described at the start of the chapter. Subsequent sub-chapters describe how specific functions are implemented and how they interface with other modules or subsystems.
System Services Subsystem	
TSO Attachment	Verifies TSO attachment credentials by using RACF.
Call Attachment Facility	Verifies attachment credentials by using RACF.
RRSAF	Uses RACF to check whether the primary authorization ID of the allied address space is authorized to connect.
z/OS System Services	Identification and sign-on support for attachment facilities using RACF.
Authorization Security Interface	Authorization interface for other subsystems using RACF for access checks.
General Command Preprocessor Status:	Command parsing fronted to DB that performs the required authorization checks.
Audit Trace Security Interface	Audit log interface used by DB2 to generate the SMF log entries.
Instrumentation Facility Interface	Allows application to obtain trace information aboutDB2. It uses RDS which in turn uses RACF to verify the authorization for the instrumentation.
System Parameter Manager	DB2 system parameter interface available only for SYSADM or SYSOPR.
Service Controller	Interface between RDS and system services subcomponents.
Data Manager	The data manager handles the synchronized access to the DB using RDS if needed to enforce MLS.
Data Space Manager	Performs data set management for DB2 z/OS Access Method Services to modify VSAm data sets.
Buffer Manager	Performs storage buffer management and cleans out newly requested buffers, thereby enforcing object reuse requirements.
Stored Procedures Manager	Manages stored procedures and uses RDS for authentication.
Utilities Subsystem	
Utilities Subsystem Security Functions	Utilities work directly on VSAM data sets and are therefore directly authorized via RACF. When using multilevel security the table loading function validates seclabels.
Row Level Security	Provides a service to perform mandatory access control on the row level.
Distributed Data Services Subsystem	
DRDA Security Functions	Provides the DRDA interface and uses RACF to provide the related security functions.
Distributed Transaction Manager(DTM)	Uses DSN3AUTH to authenticate and ensure the user's authority to access DB2 as required by DRDA.

Table 4: TOE design

6 Documentation

The evaluated documentation as outlined in table 2 and table 3 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

7.1 Developer Testing

Testing Effort

The developer used a fully-automated test suite comprised of 66 test cases that split up into test case files where each test case file may test several functions and interface parameters. This test framework was used to test every ST claim, all interface functions, and subsystems, in both DAC and MAC context. Separate mapping files (for interfaces/subsystems and claims) were maintained. In addition, the developer used a summary sheet where the date of the successful execution of each test case was recorded. The test environment was comprised of several virtualized systems of DB2 on z/OS to test remote functionality. Most of the tests naturally focused on testing access privileges, which comprises the biggest portion of the TSF. In general, the testing effort allowed for very focused and fine-grained testing.

The test case description is embedded within the test files and refers explicitly to the test claims. The test environment was enhanced by scripts that check that the different test servers are still active during testing. Additional test scripts reverse the order of test cases to demonstrate that no interdependencies exist.

Approach

The developer's approach was to demonstrate that because all TCs ran successfully (which was supported by the automated result check) that all ST claims, interfaces, and subsystems are verified by the tests.

Configuration

The provided test system is a virtualized environment on z/VM. Several VMs allow for distributed testing. The test tool TCPUN is installed on these machines to drive the test suites. The test systems are statically configured with necessary RACF options from z/OS and the DB2 Common Criteria specific settings. This includes defining users in RACF. As part of the test scripts, options are set dynamically to allow for DAC and MAC contexts, and user privileges and authorities a reset dynamically as needed by each test case. The test environment was made available remotely. Test files were stored on the z/VM system and could be executed by the evaluator, either individually or as a group.

Depth

The tested behavior was covered down to the level of subsystems, and the evaluator could verify that most relevant execution paths were taken into account. Most test cases directly referred to the sections in the guidance and some cited paragraphs to smooth test development and verification in respect to specific TOE behavior. Each tested behavior was tested with different privileges if applicable, e.g., administrative users, users with explicit privileges for the task, or users without privileges (to test the negative case).

Results

The results of the developer showed a 100% successful test run.

7.2 Evaluator Testing Effort

Effort

The evaluator executed 2 of the 6 developer test suites where one of the test suites comprised the majority of all developer tests. The evaluator further devised 6 tests that are partially based on existing developer tests. A code review was performed to analyze the authentication mechanism available via a remote connection (DRDA).

Approach

The evaluator used the test tool TCPUN to execute the test cases and to determine whether any of the tests failed. The test tool produced a results file for each unsuccessful test case, and summary files on the results for several tests. The evaluator also used options of the tool to generate output files for test cases -- even the ones that were successful. This was used to verify the comparison logic of the tool that takes place when comparing the actual results with the provided verification file. All independent tests were executed on the test environment provided by the developer. Additional tests were devised to cover all attachment facilities and all privileges defined for the CAPP access control security function, and to determine that TOE setup options are enforced.

Configuration

The evaluator executed the developer test suites in both the Label Security and CAPP mode. The evaluator tests were performed in CAPP mode (no additional Label Security related tests were necessary).

Depth

Execution of the developer tests covered most interfaces and subsystems. The additional evaluator tests closed a gap for the attachment facilities testing (relevant for I&A functionality), and for testing all privileges (increasing the rigor of the already thorough testing of access control functions).

Results

All tests were run successfully. The code view revealed no weakness in the authentication logic.

7.3 Evaluator Penetration Testing

Penetration testing effort

The evaluator considered common sources for vulnerabilities of DB2 in general and narrowed the findings down to what is applicable to the z/OS version of the product. He also examined the vulnerabilities and defects tracked by the developer and whether they have been fixed. In each case, no exploitable vulnerabilities have been identified in these areas that would need additional penetration testing. The evaluator still devised tests related to the following:

- running vulnerability scanners on the TOE
- input validation on the remote TSFI
- session handling on the remote TSFI

- check of AC(1) modules

The vulnerability scanners were publicly available, while the input validation was performed by using custom C test code. The test code is based on the opendrda project, but was heavily revised during the testing activity, based on the new DRDA standard and information from the developer who observed the TOE behaviour via debug traces where the DRDA connection failed to be established.

Testing approach

The tests focused on using remote access to the TOE (using the DRDA interface), which enabled the evaluator to connect vulnerability scanners to the TOE to automatically search for vulnerabilities. The evaluator further focused the DRDA specification to perform more in-depth tests on specific DRDA aspects. This focused approach was favoured against an approach where a variety of functionality is not so deeply tested, because the developer already runs a very thorough suite of test cases on all aspects of the TSF, and because any remote vulnerabilities are usually much more critical to the TOE. The goal was to reveal any TOE behaviour that violates the security policy in terms of Identification and Authentication and to determine whether the TOE operation remains stable which would otherwise indicate incorrect verification of the input that might require additional investigation.

Test configuration

The test configuration comprised of the TOE residing in the developer test lab which was also used for independent testing. The test configuration was in accordance to the evaluated configuration. From the set of the different TOE setups provided by the developer, the test was run on a setup that supported the distributed data facility which provided the working remote DRDA interface. The evaluator used tools to connect to the TOE remotely via the DRDA interface. The vulnerability scanners were installed on a windows client while the fuzzy code was developed and executed on a Linux client (both residing or tunnelled into the test network).

Depth

The main goal was to perform in-depth tests on the DRDA data flow (exchanging individual protocol parameter values with invalid input, incorrect length parameters, and changing the order of protocol messages).

Results

The vulnerability scanners were not able to connect to the TOE. The fuzzy test did not reveal any violation of the TSF, and the TOE had stable operation across the testing phase, and returned proper error codes which indicated that all tested input variations were correctly handled.

The z/OS-specific penetration test derived during the evaluation of z/OS V1R6 was the building of a fuzzing-framework for SVC and PC calls.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is documented in DB2 Version 9.1 for z/OS Requirements for the Common Criteria [11]. It is based on one of the two shipping options: DB2 Version 9.1 for z/OS (standard version) - product number 5635-DB2 or DB2 Version 9.1 for z/OS

(Value Unit Edition "VUE") - product number 5697-P12, the underlying IBM z/OS Version 1 Release 10 and further components as listed in table 2 and 3.

The difference between the two shipping options of the DB2 portion relates to the product licensing, not to product functionality. The chosen licensing option will be visible as a string identifier in the record facility of z/OS, and in the ISPF panel during installation. Both TOE versions are completely representative because there is no functional difference between them which means the VUE-option does not contain additional functions, nor does it replace or remove functions of the standard edition. Therefore, although the actual testing only happened for an VUE-installation, its results apply to the non-VUE shipping version as well.

The software is to be used on the following hardware platforms:

The TOE is running within a logical partition provided by a certified version of PR/SM, on the z/Architecture as implemented by the following hardware platforms:

- IBM zSeries model z890, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM zSeries model z990, optionally with CryptoExpress2 card or PCIXCC and PCICA crypto cards
- IBM System z9 109, z9 BC, or z9 EC, optionally with CryptoExpress2 card.
- IBM System z10 Business Class, optionally with CryptoExpress2 card.
- IBM System z10 Enterprise Class, optionally with CryptoExpress2 card.

In addition, the TOE may run on a virtual machine provided by a certified version of z/VM.

This Evaluated Configuration Guide specifies a number of constraints, such as configuration values for various configuration files, specific steps to be taken during installation and information to administrators on how to manage the TOE.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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.

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)
- The components ALC_FLR.3 augmented for this TOE evaluation.
- All components claimed in the Security Target [6], chapter 2 and defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, 25 July 2007, Information Assurance Directorate, National Security Agency,
  Controlled Access Protection Profile, Version 1.d, NSA 1999-10-08 [7]
- 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.3

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 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 4, Para. 3, Clause 2). This holds for:

- The TOE Security Functions “RACF Passtickets”, “Authentication via Client Digital Certificates”, “Authentication via Kerberos” and “Communication Security” and
- for other usage of encryption and decryption within the TOE.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 and 3 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 policies 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.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

11 Security Target

For the purpose of publishing, the Security Target [6] and [8] 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

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

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionalities

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[8].

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

[6] Security Target BSI-DSZ-CC-0622-2012, Version 1.29, 2012-01-20, DB2 v9.1 for z/OS Security Target, IBM Corporation

[7] U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, 25 July 2007, Information Assurance Directorate, National Security Agency, Controlled Access Protection Profile, Version 1.d, NSA 1999-10-08

[8] Security Target BSI-DSZ-CC-0534, Version 5.11, 2009-03-16, Security Target for IBM z/OS Version 1 Release 10, IBM Corporation

[9] Evaluation Technical Report, Version 5, 2012-.05-10, Final Evaluation Technical Report, DB2 v9.1 for z/OS, atsec information security GmbH, (confidential document)

[10] Configuration list for the TOE (confidential document):

CMVC User Guidance: [CLGUIDANCE], 2011-04-13, File name: v9_plugins.pdf

CMVC Defect: [SECINT], 2009-11-17, File name: DB2 Security Integrity Vulnerabilities 2009.11.17.pdf

CMVC Source Code: [hdb9910], 2009-11-23, File name: hdb9910.pdf

CMVC DB2 Utilities Suite: [jdb991k], 2009-11-23, File name: alc/jdb991k.pdf

CMVC DB2 VUE (licensing option): [jdb991z], 2009-11-23, File name: jdb991z.pdf

CMVC object code (SMP/E tape loaded into SPA as TOE base): [OBJCODECI], 2009-07-31, File name: db2910_beta.files.txt

[8] Specifically

- AIS14, Version 7, 3. August 2010, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS19, Version 8, 19. Oktober 2010, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische ZufallszahlengeneratorenAIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

Teamroom CC evidence: [TROOMCI], 2012-01-30, File name: TeamRoomPlus_Configuration_List.pdf

COMLIB final Test Cases and Test Results: [TESTCASECI], 2011-06-17, File name: 110322.5b7.CCEAL4.BU1.zip

CMVC Test Plan: [TESTPLANCI], 2009-04-14, File name: v9 testplan.xls

(Preliminary) Test Results: [TESTRESCI], 2009-04-29, File name: ConfigList-V9-test-results.pdf

SPA source files (deltas, open APARs): [MINIFCI], 2009-07-31, File name: hdb106.pdf

SPA source files (committed PTFs fixed/tested/approved): [MINIJCI], 2009-07-31, File name: hdb110.pdf

SPA source files (original sources of original release, read only, never modified base code, metadata, control files, etc.): [MINILCI], 2009-07-31, File name: hdb112.pdf

RETAIN APAR list: [RETAINAPAR], 2011-04-18, File name: APARs_20110418.xls

RETAIN PTF list: [RETAINPTF], 2011-04-18, File name: PTFs_20110418.xls

CONFLIST z/OS R10 Element Configuration Lists, 2009-04-08, File name: cm.lists/cm.lists.r10.zip

[11] DB2 Version 9.1 for z/OS Requirements for the Common Criteria, Version SC19-2788-00, May 2011

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.