Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0753-2012

for

IBM RACF for z/OS, Version 1, Release 12

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-0753-2012

IBM RACF for z/OS
Version 1, Release 12

from	IBM Corporation
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_FLR.3

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

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, 23 February 2012

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

for components up
to EAL 4

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

This page is intentionally left blank

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.

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

[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

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.

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3, and AVA_VAN.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

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 RACF for z/OS, Version 1, Release 12 has undergone the certification procedure at BSI.

The evaluation of the product IBM RACF for z/OS, Version 1, Release 12 was conducted by atsec information security GmbH. The evaluation was completed on 8 February 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

[6] Information Technology Security Evaluation Facility

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report 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 RACF for z/OS, Version 1, Release 12 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
2455 South Road P328
Poughkeepsie NY 12601
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 the RACF (Resource Access Control Facility) component of the z/OS operating system. RACF is the component that is called within z/OS from any component that wants to perform user authentication, access control to protected resources and the management of user security attributes and access rights.

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 5 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] chapter 7.1. 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	Mode of Operation
Identification and Authentication of Users	All Modes
Discretionary Access Control	All Modes
Mandatory Access Control and Support for Security Labels	Labeled Security Mode
Auditing	All Modes
Security Management	All Modes

Table 1: TOE Security Functionalities

The TOE can be configured to two modes of operation, a standard mode and a Labeled Security Mode. For more details please refer to the Security Target [6] chapter 6.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2.1. 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.

This certification covers the following configurations of the TOE:

The Target of Evaluation is IBM RACF for z/OS, Version 1 Release 12. The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 represent the TOE. For further details refer to chapter 8.

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 RACF for z/OS Version 1, Release 12

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
RACF for z/OS V1R12 as integral part of *z/OS Version 1 Release 12 (z/OS V1.12, program number 5694-A01) Common Criteria Evaluated Base Package*				
1	SW	z/OS V1.12 Common Criteria Evaluated Base (IBM program number 5694-A01)	V1R12	Tape
2	DOC	z/OS V1.12 Program Directory	GI10-0670-12	Hardcopy
3	DOC	z/OS V1.12 DVD Collection Kit	SK3T-4271-25	CD-ROM
4	DOC	z/OS Hot Topics Newsletter	GA22-7501-19	Hardcopy
5	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
6	DOC	Memo to Customers of z/OS V1.12 Common Criteria Evaluated Base	n/a	Hardcopy
7	DOC	z/OS V1.12 Planning for Multilevel Security and the Common Criteria	GA22-7509-12	Hardcopy
IBM Print Services Facility™ Version 4 Release 3 for z/OS (PSF V4.3.0, program number 5655-M32)				
8	SW	IBM Print Services Facility™ Version 4 Release 3 for z/OS (PSF V4.3.0, program number 5655-M32)	V4R3	Tape
9	DOC	PSF V4.3 CDROM Kit BOOK	SK3T-9927-03	CD-ROM
10	DOC	PSF V4.3 CDROM Kit PDF	SK3T-9928-03	CD-ROM
11	DOC	PSF Tiers-AFP/IPDS Printers	Z125-4564-18	Hardcopy
12	DOC	PSF V4.3 Program Directory	GI11-4308-00	Hardcopy
OGL/370 V1.1.0 (program number 5688-191)				
13	SW	Overlay Generation Language Version 1 (OGLV1R1, program number 5688-191)	V1R1	Tape
14	DOC	OGL/370 V1.1.0: Getting Started	G544-3691-00	Hardcopy
15	DOC	OGL/370 V1.1.0: LPS	G544-3697-00	Hardcopy
16	DOC	OGL: Command Summary and Quick Reference	S544-3703-01	Hardcopy
17	DOC	Program Directory OGL/370	GI10-0212-01	Hardcopy
IBM Ported Tools for z/OS V1.2 (program number 5655-M23)				
18	SW	IBM Ported Tools for z/OS V1.2 (program number 5655-M23, optional)	V1.2	Tape
19	DOC	Program Directory IBM Ported Tools for z/OS V1.2.0	GI10-0769-05	Hardcopy
20	DOC	IBM Ported Tools for z/OS License Information	GA22-7986-08	Hardcopy
Additional Media				

No	Type	Identifier	Release	Form of Delivery
21	SW	PTFs (required): UK60305, UA56370, UA57861, UA55172, UA55781, UA56195, UA56629, UA57144, UA57354, UA55967, and UA57068	n/a	Electronically from ShopzSeries https://www.ibm.com/software/shopzseries

Table 2: Deliverables of the TOE

The evaluated version of RACF has to be ordered as part of z/OS V1R12 via an IBM sales representative or via the ShopzSeries web application (https://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.

The delivery of the tapes, DVDs, CDs and Documentation occurs in one package, which is manufactured specifically for this customer and shipped via courier services. Additional maintenance then needs to be downloaded by the customer via the ShopzSeries web site, following the instructions delivered with the package.

The media and documents delivered to the customer are labelled with the product, document and version numbers as indicated in the table above and can be checked by the users installing the system.

The TOE is an integral part of z/OS V1R12. The reference of z/OS V1R12 can be verified by the administrator during initial program load (`IPL`), when the system identification is displayed on the system console. The operator can also issue the operator command “`D IPLINFO`”, to display the z/OS version. The string "`z/OS 01.12.00`" should be displayed among other information.

Verification of the correct z/OS version as described above implies that the correct version of the TOE is installed.

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
- Discretionary Access Control
- in Labeled Security Mode: mandatory access control and Support for Security Labels
- Auditing
- Security Management

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 operational environment. The following topics are of relevance: Trained and trustworthy administrators, environmental support for protection of information, correct TOE setup, maintenance, prevention of physical attacks, recovery procedures, correct implementation of security protocols by the environment, only trusted programs to be executed with privileges, and cryptographic support from the underlying processing unit. Details can be found in the Security Target [6], chapters 4.2 and 6.

5 Architectural Information

The Target of Evaluation (TOE) is the RACF component of the z/OS operating system. RACF is the component that is called within z/OS from any component that wants to perform user authentication, access control to protected resources and the management of user security attributes and access rights.

RACF is designed as an authentication and access manager component that manages both user security attributes and access management attributes in its own database. Users are represented within RACF by user profiles and protected resources are represented by resource profiles. Users can be members of groups where each group is represented by a group profile.

Resource profiles are structured into classes, which represent the different types of resources. Within such a class an individual profile is represented by the name of the resource, which is unique within its class. Resource manager will then query RACF whenever they need to check a user's access rights to a resource. In this query they will specify the resource class, the name of the resource within the class, the type of access requested and the internal representation of the user that requests access. RACF is also called when a component within z/OS needs to authenticate a user. In this case the z/OS component will call RACF and will pass the identity of the user, the authentication credentials presented, the name of the component requesting user authentication and several other parameters to RACF. Based on this information RACF will authenticate the user and, if successful, create a control block representing the user with the security attributes assigned. This control block is later used when a component of z/OS calls RACF for checking access rights.

RACF also provides interfaces that allow the management of user profiles, digital certificates assigned to users, group profiles, resource profiles, access rights, security labels and general RACF attributes. RACF also provides an interface that z/OS components can call to generate a security related audit record.

Note: The RACF Remote Sharing Facility (RRSF) is not considered as a part of this evaluation and therefore must not be used in an evaluated system configuration.

5.1 Intended method of use

RACF is designed to be used by z/OS components to perform user authentication, validate a user's access to a resource, audit security critical events, and manage RACF profiles, access rights to resources and RACF security parameter. It also provides interfaces to extract RACF status information. This interface is a programming interface implemented by the RACROUTE macro. RACF will check if the calling application has the right to use the function called. In addition RACF exports a command interface that can be used by appropriately authorized users directly to perform management operations.

The Security Target [6] specifies two modes of operation: a "normal" mode where labeled security features are not configured as required in the Security Target and a "Labeled Security Mode" where labeled security is configured as described in the Security Target. In

"Labeled Security Mode" additional security functionality is active, which is marked with "Labeled Security Mode" in this document. Note that when functions of labeled security are configured differently than specified in the Security Target, the security functionality defined for the "normal" mode still works but additional restrictions may be imposed due to the way the functions for labeled security are configured.

These primary security features are supported by the domain separation and reference mediation properties of the other parts of the z/OS operating system, which ensure that the RACF functions are invoked when required and cannot be bypassed. RACF itself is protected by the architecture of the z/OS operating system from unauthorized tampering with the RACF functions and the RACF database.

RACF uses the z/OS mechanisms for establishing error recovery routines, which allows RACF to handle errors or exceptions detected by z/OS or the hardware and either recover from the error, perform any necessary clean-up operation and signal the error to the calling program, or (in the extreme case when RACF is not able to maintain its integrity e. g. when the RACF database is full or compromised) terminate RACF itself.

5.2 Identification and authentication

RACF provides support for the identification and authentication of users by the means of

- an alphanumeric RACF user ID and a system-encrypted password or password phrase.
- an alphanumeric RACF user ID and a Pass Ticket, which is a cryptographically-generated password substitute encompassing the user ID, the requested application name, and the current date/time.
- an x.509v3 digital certificate presented to a server application in the TOE environment that uses System SSL or TCP/IP Application Transparent TLS (AT-TLS) to provide TLS- or SSLv3- based client authentication, and then “mapped” (using TOE functions) by that server application or by AT-TLS to a RACF user ID.
- a Kerberos™ v5 ticket presented to a server application in the TOE environment that supports the Kerberos mechanism, and then mapped by that application through the GSS-API programming services. The TOE also provides functions (specifically the R_ticketServ, and R_GenSec services) that enable the application server to validate the Kerberos ticket, and thus the authentication of the principal. The application server then translates (or maps) the Kerberos principal (using the TOE provided function of R_userMap) to a RACF user ID.

The TOE security functions authenticate the claimed identity of the user by verifying the password/phrase (or other mechanism, as listed above) and returning the result to the trusted program that used the RACF functions for user identification and authentication. It is up to the trusted program to determine what to do when the user identification and authentication process fails. When a user is successfully identified and authenticated RACF creates control blocks containing the user's security attributes as managed by RACF. Those control blocks are used later when a resource manager calls RACF to determine the user's right to access resources or when the user calls RACF functions that require the user to hold specific RACF managed privileges.

The required password quality can be tailored to the policies of the installation using various parameters. When creating users, administrators are required to choose an initial password and optionally a password phrase that must usually be changed by the user during the initial logon that uses the password/phrase.

5.3 Discretionary access control

RACF implements the functions allowing resource managers within z/OS to control access to the resources they want to protect. Resources protected by RACF fall into two categories, based on the mechanisms used within RACF to describe them: Standard (e.g., MVS data sets, or general resources in classes defined by RACF or the system administrator), and UNIX (e.g., UNIX files,directories, and IPC objects instantiated by a UNIX file system). Discretionary access control (DAC) rules allow resource managers to differentiate access of users to resources based on different access types.

5.4 Mandatory access control and support for security labels

In addition to DAC, RACF provides mandatory access control (MAC) functions that are required for Labeled Security Mode, which impose additional access restrictions on information flow on security classification. Users and resources can have a security label specified in their profile. Security labels contain a hierarchical classification (security level), which specify the sensitivity (for example: public, internal use, or secret), and zero or more non-hierarchical security categories (for example: PROJECTA or PROJECTB).

The access control enforced by the TOE ensures that users can only read labeled information if their security labels dominate the label of the information, and that they can only write to labeled information containers if the label of the container dominates the subject's label, thus implementing the Bell-La Padula model of information flow control. The system can also be configured to allow write-down for certain authorized users.

MAC checks are performed before DAC checks.

5.5 Auditing

RACF provides an auditing capability that allows generating audit records for security-critical events. RACF provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. Audit records are generated by RACF and submitted to another component of z/OS (System Management Facilities (SMF)), which collects them into an audit trail.

RACF always generates audit records for such events as unauthorized attempts to access the system or changes to the status of the RACF database. The security administrator, auditors, and other users with appropriate authorization can configure which additional optional security events are to be logged. In addition to writing records to the audit trail, messages can be sent to the security console to immediately alert operators of detected policy violations. RACF provides SMF records for all RACF-protected resources (either "traditional" or z/OS UNIX-based).

For reporting, auditors can unload all or selected parts of the SMF data for further analysis in a human-readable formats and can then upload the data to a query or reporting package, such as DFSORT™ if desired.

5.6 Security management

RACF provides a set of commands and options to adequately manage the security functions of the TOE. Additionally, RACF provides the capability of managing users, groups of users, general resource profiles, and RACF SETROPTS options.

RACF recognizes several authorities that are able to perform the different management tasks related to the security of the TOE:

- General security options are managed by security administrators.
- In Labeled Security Mode: management of MAC attributes is performed by security administrators.
- Management of users and their security attributes is performed by security administrators. Management of groups (and to some extent users) can be delegated to group security administrators.
- Users can change their own passwords or password phrases, their default groups, and their user names (but not their user IDs).
- In Labeled Security Mode: users can choose their security labels at login, for some login methods. (Note: this also applies in normal mode if the administrator chooses to activate security label processing.)
- Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyse the audit trail.
- Security administrators can define what audit records are captured by the system.
- Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.

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 [6].

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 Test Configuration

The TOE may be running on machines within a logical partition provided by a certified version of IBM PR/SM. In addition, the TOE may run on a virtual machine provided by a certified version of IBM z/VM.

For the peripherals that can be used with the TOE, please refer to the Security Target [6], section 1.4.3.2.

IBM has tested the platforms (hardware and combinations of hardware with IBM PR/SM and/or IBM z/VM) for z/OS individually for their compliance to the z/Architecture using the Systems Assurance Kernel (SAK) suite of tests. These tests ensure that every platform provides the abstract machine interface that z/OS requires.

The test systems were running z/OS Version 1 Release 12 including the TOE in the evaluated configuration. Due to the massive amount of tests, testing was performed throughout the development of the TOE. To ensure proper testing of all security relevant behaviour of the TOE, the evaluators verified that all tests that might have been affected by any security-relevant change introduced late in the development cycle had been run on the evaluated configuration.

When assessing the test configuration, the evaluators determined that not all PTFs mandated by table 2 actually had been installed on the test systems used. For the missing PTFs, i.e. UA56370, UA55967, UA57068, the evaluators asked the developer for additional information about their security relevance. The developer provided details about the nature of the underlying problems as well as information on the respective fix. The evaluators examined the information provided and found it of no impact on security claims in the ST [6] as well as the general function of the system.

7.2 Developer Testing

Following a brief summary on the developer's environment:

- FVT for z/OS is largely performed on the VICOM test system. This is an enhanced z/VM system implementing the z/Architecture abstract machine interface. It allows testers to bring up individual, virtual test machines running z/OS with access to virtualized peripherals such as disks and network connections. For the purpose of the security function tests, this environment is fully equivalent to the machines running z/OS. This environment was also used by the evaluator for their independent testing
- IBM has provided a common test framework for tests that can be automated. COMSEC is an environment that can be operated in standard mode or Labeled Security mode. The BERD (Background Environment Random Driver) test driver submits the test cases as JES2 jobs. IBM's intention is to move more and more tests to this automated environment, which will ease the test effort required for the evaluations substantially. Starting with V1R9 a substantial number of tests has been ported to this environment. Additionally, most test teams ran their manual tests in the COMSEC test environment, which provides a complete test environment in the evaluated configuration of the TOE in the different modes of operation.
- The test systems were running z/OS version 1 release 12 in the evaluated configuration. The SDF team provided a pre-installed system image for VICOM and for the machines running the COMSEC tests, thus ensuring that the CCEB software version was used for all tests. The additional PTFs were applied to the VICOM and COMSEC systems as they became available, with any security-relevant tests for the PTFs being successfully re-run. For some APARs claimed by the ST, which have not been installed on the test systems, an analysis of their security impact revealed that they actually have no effect at all on the TOE functionality being tested.

The developer chose the following test approach:

- IBM's general test approach is defined in the process for Integrated Product Development (IPD) with developer tests, functional verification tests (FVT), and system verification tests (SVT). Per release, an overall effort of more than 100 person years is spent on FVT and SVT for the z/OS components. FVT and SVT is performed by independent test teams, with testers being independent from the developers. The different test teams have developed their own individual test and test documentation tools, but all implement the requirements set forth in the IPD documentation.
- For the purpose of the evaluation, FVT is of interest to the evaluator, since the single security functions claimed in the ST [6] are tested here. IBM decided to create a test bucket with the tests for the security functions, summarizing the tests in individual test plans, so that the evaluator had a chance to deal with the otherwise overwhelming complexity of the z/OS testing.
- IBM's test strategy for the evaluation had three cornerstones:

- The major internal security interface was the interface to RACF, which is tested exhaustively by the RACF test group
- Components requiring Identification and Authentication or Access Control services call RACF (with the exception of LDAP LDBM, which implements its own access control). For most of these services, it is sufficient to demonstrate that these interfaces call RACF, once the testing of the RACF interface (see above) has established confidence in the correct inner workings of RACF
- Due to the design of z/OS, a large number of internal interfaces is also visible externally, although the interfaces are not intended to be called by external, unprivileged subjects. For these interfaces, which are basically authorized programs, operator commands, certain callable services, SVC and PC routines, testing established only that these interfaces can not be called by unauthorized callers.

Apart from these tests, all components providing external interfaces for security functions were tested intensively. For the current version of z/OS this included additional tests for enhancements of the already existing TOE components RACF, CS390, USS, and LDAP introduced in the z/OS V1R12. All new test cases were determined to follow the approach of the already existing tests for the respective component.

These are the test results:

- The test results provided by the sponsor were generated on the configurations as described above. Although different test teams used different tools and test tracking databases, the evaluator verified that all provided results showed that tests had executed successfully and yielded the expected results.
- The testing provided was valid for both the standard mode and the Labeled Security mode of operation, with the exception of tests for multilevel security features, which were relevant to Labeled Security mode only. The test systems configured for Labeled Security mode are compliant to standard mode as well, so that tests run on these systems were always applicable to both modes of operation. For COMSEC, all applicable tests were run in dedicated Labeled Security mode and standard mode configurations.

Conclusion on developer's tests:

The evaluator verified that testing was performed on configurations conformant to the ST [6].

The evaluator was able to follow and fully understand the test approach based on the information provided by the developer. With this test environment, the developer was able to provide proof of the necessary coverage and test depth to the evaluator.

7.3 Evaluator Testing

The independent evaluator testing followed the CEM guidance to test every security function, without striving for exhaustive testing. For their own tests, the evaluator decided to focus on the most important security functions of the TOE in order to provide independent verification of their correct operation:

- Identification and authentication: The evaluator would only devise some basic, mostly implicit testing of the Identification and authentication functions in TSO/E, rlogin, ftp, su and JES, since these functions would be exercised extensively during the test activity by the testers. The testers tests focused on the Kerberos based authentication mechanisms.

- Discretionary access control: The evaluator focused on UNIX System Services ACLs, which also implicitly test UNIX permission bits. Other DAC tests involved
- USS IPC (all system calls for messages, semaphores and shared memory)
- DAC for different USS objects (device special files, IPC objects, directories)
- z/OS dataset access
- security-relevant USS system calls
- Mandatory Access Control: The evaluator re-ran their own tests on mandatory access control checks for data sets and Unix System Services files as their own regression tests. Testing of the write down override capability provided by FACILITY class profiles was also performed.
- Audit: Tests were used to check auditing of changes to the system clock.
- Security Management: The evaluator decided to devise no special tests here, since the setup of the test environment and the setup / cleanup of the tests would already include a major portion of the TSF found here.

For the set of developer tests to be re-run, the evaluator chose an approach supplementing their own tests and focusing on functionality changed since the previous evaluation.

The evaluator decided to focus on security functions claimed in the Security Target and not to run tests demonstrating that functions requiring authorization would fail when invoked unprivileged. This was in part due to the fact that the evaluator had experienced already sufficient issues with protection of security functions while bringing up the system in its evaluated configuration, following the guidance.

Apart from the tests re-run by the evaluator or during dedicated sessions set up for the evaluator to observe the testers running those tests, the evaluator gained confidence in the developer’s test efforts during their extended stay at the developer site, where they discussed with testers issues of testing or interpretations of the CC requirements, and were witnessing test executions while the test bucket was being created. The evaluator had already interviewed testers during site visits and examined the test databases with test cases and test results and test execution records.

All tests were run on the VICOM test system that had been set up by the evaluator according to the specifications found in the guidance, and on the COMSEC system set up by IBM and verified by the evaluator to be in the evaluated configuration.

During their testing, the evaluator could verify that the test functions behaved as expected.

Penetration tests have been conducted for the interfaces part of the attack surface where the analysis of the implementation representation could not completely validate that the function invoked via the interface by a caller not having all the required privileges would return with an error before doing anything potentially harmful. For those functions the evaluator tried to identify potentially security critical side-effects related to the way the function handles, validates and uses parameters or side-effects that potentially could result in denial-of-service. In addition the evaluator invoked some interfaces in an “unintended” way, especially some modules that are RACF commands, but which also can also be called directly as a job step in a batch job. In addition a specific penetration test has been conducted to verify a glitch in the behaviour of password based user authentication identified during the analysis of the implementation representation.

The penetration tests that attempted to misuse interfaces of RACF by invoking them deliberately in an environment where they are not supposed to be used all failed with error messages clearly indicating that RACF has detected the invalid environment and terminated the call. Invocations of interfaces with specifically crafted invalid parameter lists also all failed with error messages without the called function performing any security relevant action before terminating with an error.

The attempts to cause a potential denial of service by invoking functions that use locks for serialization also failed because those functions ended in such a short time that it was not even possible to validate if those lock have been used at all. Even if they had been used, the actual delay of other functions attempting to use the locks would have been too low to measure.

Concerning the behaviour of the password based authentication the tests confirmed the observation made by the evaluator during the analysis of the implementation representation, allowing a new user with an initial password consisting of uppercase only characters to authenticate correctly even if the password was entered with some characters entered as lowercase. The test also confirmed that this behaviour disappeared the first time a password for a user is defined that contains at least one lowercase character. The test also confirmed that the issue does not re-appear when a password consisting of uppercase characters only was set later for the user. The issue was addressed by adding a statement to the guidance advising the administrator to set the initial password of a new user such that it contains at least one lowercase character.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The Target of Evaluation is IBM RACF for z/OS, Version 1 Release 12. The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 represent the TOE.

This following configuration of the TOE is covered by this certification:

The z/OS V1R12 Common Criteria Evaluated Base package, and (if used) IBM Ported Tools for z/OS must be installed according to the directions delivered with the media and configured according to the instructions in [9]. Also all required PTFs as listed as item #21 in table 2 above must be installed.

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 5 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.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_FLR.3

Note that the guidance advises the administrator to set the initial password of a new user such that it contains at least one lowercase character.

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 9, Para. 4, Clause 2). This holds for: SHA256withRSAEncryption with key length 1024, 2048, 4096 as defined in PKCS#1 v1.5, November 1993, signatures using block type 1 for padding and (provided by the operational environment) SHA-256 as defined in NIST FIPS 180-2, August 2002 (as defined by the OIDSHA256withRSAEncryption) in the TOE Security functionality "Support for program signing and signature verification".

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 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.

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
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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
MAC	Mandatory Access Control
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.

Discretionary Access Control - An access control policy that allows authorized users and authorized administrators to control access to objects based on individual user identity or membership in a group (PROJECTA, for example).

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.

Mandatory Access Control - An access control policy that determines access based on the sensitivity (SECRET, for example) and category (PERSONNEL or MEDICAL, for example) of the information that is being accessed and the clearance of the user who is trying to gain access to that information.

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-0753-2012, Version 1.14, 7th February 2012, Security Target for IBM RACF for z/OS V1R12, IBM Corporation

[7] Evaluation Technical Report, 4, 8th February 2012, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Configuration list for the TOE, Version, 8th February 2012, z/OS R12 Element Configuration Lists (confidential document)

[9] Guidance documentation for the TOE, GA22-7509-12, November 2011, z/OS Planning for Multilevel Security and the Common Criteria

[8] specifically

- AIS 23, Version 2, 11 March 2009, Zusammentragen von Nachweisen der Entwickler
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim Release 3 = 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.