Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0752-2013

for

z/VM Version 6, Release 1

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-0752-2013

Operating System

z/VM Version 6, Release 1

from	IBM Corporation
PP Conformance:	Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010, OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010, OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria
Recognition
Arrangement

Common Criteria

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

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

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

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

Bonn, 20 February 2013

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

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....................7

1 Specifications of the Certification Procedure....................7
2 Recognition Agreements....................7
3 Performance of Evaluation and Certification....................8
4 Validity of the Certification Result....................8
5 Publication....................9

B Certification Results....................11

1 Executive Summary....................12
2 Identification of the TOE....................15
3 Security Policy....................16
4 Assumptions and Clarification of Scope....................16
5 Architectural Information....................16
6 Documentation....................18
7 IT Product Testing....................19
8 Evaluated Configuration....................23
9 Results of the Evaluation....................24
10 Obligations and Notes for the Usage of the TOE....................25
11 Security Target....................25
12 Definitions....................27
13 Bibliography....................29

C Excerpts from the Criteria....................31

CC Part1:....................31
CC Part 3:....................32

D Annexes....................41

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 z/VM Version 6, Release 1 has undergone the certification procedure at BSI.

The evaluation of the product z/VM Version 6, Release 1 was conducted by atsec information security GmbH. The evaluation was completed on 4 February 2013. 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,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

[6] Information Technology Security Evaluation Facility

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.

5 Publication

The product z/VM Version 6, Release 1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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 12601-5400, USA

This page is intentionally left blank.

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 z/VM Version 6 Release 1. z/VM is a highly secure, flexible, robust, scalable operating system implementing a virtual machine hypervisor for IBM System z® mainframe servers onto which to deploy mission-critical virtual servers. z/VM is designed to host other operating systems, each in its own virtual machine. Multiple virtual machines can run concurrently to perform a variety of functions requiring controlled, separated access to the information stored on the system. Apart from virtual servers, the TOE provides additional virtual machines for each logged in human user, separating the execution domain of virtual machine from others as defined in the virtual machine definitions stored in the system directory. In addition to the system directory, the RACF security server is employed to mediate access to resources and privileged functions.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [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 6.1. They are selected from Common Criteria Part 2 and from OSPP [7], where some SFRs have been defined as extended components. Thus the TOE is CC part 2 extended.

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

TOE Security Functions	Addressed issue
Identification and Authentication	The TOE provides identification and authentication of users by the means of an alphanumeric user ID and a system-encrypted password. The following parts of the TOE perform identification and authentication independently: ● Control Program (CP) ● RACF For supporting identification and authentication, the TOE employs RACF managing resource profiles and user profiles.
Discretionary Access Control (DAC)	For implementation of extended DAC rules, the TOE component RACF provides the capability and flexibility as required by the evaluation compared to the usage of the system. Basically, a user's authority to access a resource while operating in a RACF-protected system at any time is determined by a combination of these factors: ● User's identity and group membership ● User's attributes including group-level attributes ● User's group authorities

TOE Security Functions	Addressed issue
	● Security classification of the user and the resource profile ● Access authority specified in the resource profile
Mandatory Access Control (MAC) and Support for Security Labels	In addition to DAC, the TOE provides Mandatory Access Control (MAC), which imposes access restrictions to information based on security classification. Each user and each RACF controlled object can have a security classification specified in its profile. The security classification can be a security level and zero or more security categories. Security labels are maintained separately from privilege classes in RACF. The access control enforced by the TOE ensures that users may only read labeled information if their security label dominates the information's label, and that they may only write to labeled information containers if the container's label dominates the subject's.
Separation of virtual machines	Operating system failures that occur in virtual machines do not normally affect the TOE running on the real processor. If the error is isolated to a virtual machine, only that virtual machine fails and can be restarted without affecting any processes running in other virtual machines, in particular, mission-critical virtual servers are not affected by failures of virtual machines associated with the human users logged in. Supported by the underlying processor, the TOE restricts results of software failures (such as program checks) occurring in a virtual machine to this machine, thus not affecting other virtual machines or the CP. Failures of the Control Program that cannot be isolated to one of its virtual machines maintained result in its abnormal termination ("abend"). In the event of such an abend, the system will re-initialize itself, if possible. Special abend code numbers are used to identify the specific reason for the abend.
Auditing	The TOE provides an audit 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 the resource. The audit records generated by RACF are collected into files residing on disks that are protected from unauthorized modification or deletion by the DAC and (in Labeled Security Mode) MAC mechanism.
Object Reuse	The TOE provides a facility clearing protected objects and storage previously used by virtual machines or the TOE itself prior to reassignment to other virtual machines or the TOE. This ensures confidentiality of data maintained either by the TOE or by virtual machines. DASD devices and their derivatives (such as minidisks or temporary disks) are to be cleared manually by the administrator in accordance with the organizational policies. There is additional software support by the IBM Directory Maintenance Facility (DirMaint), which however is not part of this evaluation.
Security Management	The TOE provides a set of commands and options to adequately manage the security functions of the TOE. The TOE recognizes several roles that are able to perform the

TOE Security Functions	Addressed issue
	different management tasks related to the TOE's security: ● General security options are managed by security administrators. ● Management of MAC attributes is performed by security administrators in Labeled Security Mode. ● Management of users and their security attributes is performed by security administrators. Management of groups can be delegated to group security administrators. ● Management of virtual machine definitions is performed by security administrators. ● Users are allowed to change their own password, their default group, and their user name. ● Users may choose their security label from the range defined in their profile at login time in Labeled Security mode. ● Auditors manage the parameters of the audit system (e.g. list of audited events) and can analyse the audit trail.
TSF Protection	The TOE control program enforces integrity of its own domain. No virtual machine can access TOE resources without appropriate authorization. This prevents tampering with TOE resources by untrusted subjects. Supportive to this functionality are hardware implemented facilities, namely the Interpretive-Execution Facility (SIE instruction). Therefore, the hardware and firmware components providing the abstract machine for the TOE are required to be physically protected from unauthorized access.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] chapter 1.5.

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.

This certification covers the following configurations of the TOE:

The Target of Evaluation, IBM z/VM Version 6 Release 1, requires the following software components to be installed, enabled, and configured:

- CMS for operating RACF and TCP/IP
- Control Program (CP)
- RACF Security Server feature
- TCP/IP for z/VM
- PTF UM90240 (RSU4)
- PTF UM33246 (Super Cor PTF for 0910)
- PTF UK76856 (SSL APARs PM52716 and PM43382)

For further details refer to chapter 8 and section 1.5.4.4 of the ST [6].

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:

z/VM Version 6, Release 1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1.	SW	z/VM Version 6 Release 1, program number 5741-A07	V6R1	Tape/DVD
2.	DOC	Program Directory for z/VM V6R1 base	GI11-4319-00	Hardcopy
3.	DOC	Program Directory for RACF function level 610	GI11-4325-00	Hardcopy
4.	DOC	Guide for Automated Installation and Service	GC24-6197-00	Hardcopy
5.	DOC	December 2011 z/VM DVD Collection Kit	SK5T-7054-04	DVD
6.	DOC	z/VM V6R1 Secure Configuration Guide contained in #5 above	SC24-6230-02	Softcopy
7.	SW	RSU 4 (PTF UM90240) n/a Electronic Super Cor PTF for 0910 (PTF UM33246) SSL APARs PM52716 and PM43382 (PTF UK76856) to be obtained electronically from ShopzSeries https://www.ibm.com/software/shopzseries	n/a	Electronic

Table 2: Deliverables of the TOE

All hardcopy guidance documents and the publications DVD are packaged and securely shipped with the installation media via registered courier to the customer.

To install and configure the TOE such that it matches the evaluated configuration as described in the Security Target, the user has to follow the guidance provided in:

- z/VM V6R1.0 Secure Configuration Guide (SC24-6230-02) [10]

listed as item 6 above.

The z/VM V6R1.0 Secure Configuration Guide is part of the "December 2011 z/VM DVD Collection Kit" listed as item 5 above.

The Secure Configuration Guide contains references to other relevant guidance documentation contained in item 5, i.e. December 2011 z/VM DVD Collection Kit (SK5T-7054-04).

During the order process for the TOE, the customer needs to explicitly order the CC-certified version of z/VM Version 6 Release 1. This already ensures that the product delivered to the customer actually is the TOE containing all required components. The administrator after installation of the product according to the Secure Configuration Guide [10] also is able to verify the version of the TOE by querying the CPLEVEL and verifying the list of installed PTFs against the list of PTFs required as stated in the ST. Output of the CPLEVEL command[8]:

```
“….
q cplevel
z/VM Version 6 Release 1.0, service level 1003 (64-bit)
...”
```

3 Security Policy

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

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

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: competent and trustworthy administrators, trusted remote IT systems, correct configuration and setup of system, system maintenance, trusted physical environment, secure recovery mechanisms. Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

5.1 General Overview

The Target of Evaluation (TOE) is the z/VM virtual machine operating system with the software components as described in section 1.5.4 of the [6].

z/VM is an operating system designed to host other operating systems, each in its own virtual machine. Multiple virtual machines can run concurrently to perform a variety of functions requiring controlled, separated access to the information stored on the system. The TOE provides a virtual machine for each logged in user, separating the execution domain of each user from other users as defined in the virtual machine definitions stored in the system directory. In addition, the system directory contains access control information

[8] The only difference between the provided list and the results obtained are the time stamps and execution times of the commands issued.

for privileged functions, such as use of certain options of the processor's DIAGNOSE instruction. In addition to the system directory, the RACF security server is employed to mediate access to resources and privileged functions.

The TOE is seen as one instance of z/VM running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines. This abstract machine is provided by a logical partition (LPAR) of an IBM System z server.

The LPAR itself is not part of the TOE, but belongs to the TOE environment. It is to be noted that although a z/VM instance can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly within an LPAR. A z/VM instance running within a virtual machine is allowed, but this “second level” z/VM instance is not in an evaluated configuration, as some security functionality is implemented differently, in particular with respect to the usage of the processor's Start Interpretive Execution (SIE) instruction.

Multiple instances of the TOE may share the RACF database. This is done by sharing the DASD (direct access storage device) volume keeping the RACF database between the different z/VM instances. Although sharing of the RACF database between z/VM and z/OS is technically feasible, it is explicitly excluded from this evaluation.

The platforms selected for the evaluation consist of IBM products, which are available when the evaluation has been completed and will remain available for some period of time afterwards. Even if withdrawn from general marketing, the product may be obtained by special request to IBM.

The TOE security functions (TSF) are provided by the z/VM operating system kernel (called the Control Program – CP) and by an application called RACF that runs within a specially-privileged virtual machine. In addition to providing user authentication, access control, and audit services to CP, RACF can provide the same services to other authorized virtual machines. z/VM provides management functions that allow configuring the TSF and tailor them to the customer's needs.

Some elements have been included in the TOE which do not provide security functions, but run in authorized mode and could therefore, if misbehaved, compromise the TOE. Since these elements are substantial for the operation of many customer environments, they are included as trusted applications within the TOE.

In its evaluated configuration, the TOE allows two modes of operation: a standard mode meeting all requirements of the Operating System Protection Profile base [7] and its extended package for Virtualization, and a more restrictive mode called Labeled Security Mode, which additionally meets all requirements of the OSPP extended package for Labeled Security.

Labeled Security Mode enabled or disabled, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

5.2 Major structural components of the TOE

The TOE consists of three major components, i.e. the z/VM Control Program, the Security Manager RACF, and the TCP/IP component, with RACF and TCP/IP running within specific virtual machines maintained by CP.

The z/VM Control Program (CP) is primarily a real-machine resource manager. CP provides each user with an individual working environment known as a virtual machine. Each virtual machine is a functional equivalent of a real system, sharing the real processor instructions and its functionality, storage, console, and input/output (I/O) device resources. CP provides connectivity support that allows application programs running within virtual machines to exchange information with each other and to access resources residing on the same z/VM system or on different z/VM systems.

In order to create and maintain these rules (virtual machine definitions), additional management software is employed, that runs outside the CP, but is part of the TOE. Hence, each component of the management software runs within a virtual machine. The following list illustrates, which functionality runs within virtual machines:

- CMS: a single-user general-purpose operating system that is employed to run the RACF and TCP/IP applications. CMS does not provide any security functionality but implements a file system that can be used by applications running on top.
- RACF server: provides authentication, authorization, and audit services to CP and other authorized virtual machines that run applications on CMS. It runs within a virtual machine maintained by CP and communicates with CP through a tightly-controlled well-defined interface.
- TCP/IP server: provides traditional IP-based communications services. For SSL encrypted communication, it interacts with the SSL server, which is seen as a subcomponent of the TCP/IP component rather than an additional part of the TOE. Both the TCP/IP server and the SSL server are not part of CP, but each run within a respective virtual machine maintained by CP.

Embedded within the TCP/IP stack is the Telnet service that enables users to access their virtual machine consoles ("log on") from the IP network. In particular, this Telnet service receives console traffic from the network, removes the telnet or TN3270 protocol wrappers, and then forwards it to CP using a special form of the DIAGNOSE processor instruction. CP generates a virtual console session as a memory object. All outgoing information is sent from the CP back to the Telnet service, which encapsulates the information in the Telnet or TN3270E protocol and sends it back to the client. The TCP/IP server also provides SSL/TLS - by interacting with the SSL service virtual machine maintained by CP - allowing the establishment of cryptographically secured channels.

6 Documentation

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

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

7 IT Product Testing

7.1 Test Configuration

Developer as well as the independent evaluator testing was performed on the same configuration. The logical partition was provided by a certified version of PR/SM on a System z10 Enterprise Class server also referred to as System z10 High End.

The test system - for both the developer and the evaluator test sessions - had installed the TOE in its evaluated configuration as required by the [ST]. This was confirmed by the evaluator analysing developer evidence generated and running respective checks on his own.

Due to an evaluator finding when performing tests on the SSL server, an additional PTF needed to be generated and tested by the developer and the evaluator. Also for those additional tests, the evaluator was able to verify that the test system had installed the TOE in its evaluated configuration only containing the modification applied by the additional PTF.

7.2 Developer Testing

The following functional testing was performed by the developer:

TOE test configuration:

The tests were performed on a IBM internal system running within a logical partition of a System z10 High End server.

The test system had installed the z/VM Version 6 Release 1. An analysis of the instructions to determine the service level including expected output were performed by the evaluator to demonstrated that all required RSU and PTF as stated in section 1.5.4.1 of the ST were installed on the machine.

The TOE had been in its evaluated configuration when the developer tests were performed.

The limitation of tests performed to the test system identified above was accepted, because the system configuration was considered to be representative for all allowed configurations. The TOE relies on an underlying abstract machine that is compliant with the z/Architecture definition. Extensive testing was performed by the developer on all configurations (including the chosen one) to verify full z/Architecture compliance of the abstract machine provided to the TOE.

Testing approach:

The developer designed a specific CC related test suite that contains various test scenarios covering the security functions provided by the TOE.

The tests performed by the developer directly stimulate the following TSFI identified in the Functional Specification:

- CP commands
- RACF commands
- API
- RACF Report Writer
- TELNET Server

and observe the resulting behaviour.

The following TSFI are tested indirectly by the tests performed and the required test setup:

- System Directory
- TCP/IP configuration files and commands
- IUCV

All but two test cases are automated, i.e. after executing a script file, a significant amount of single tests are executed mediated by the CHUG test tool as well as the FACT test tool, the results of which are documented. Proper verification whether the actual test results match the expected results is already included in the respective test cases. The manual test cases related to the RACF Report Writer and the certificate based authentication implemented by the SSL Server contain sufficiently detailed information for the tester to decide on whether the actual test results obtained match the expected results.

The developer performed a significant amount of SAK testing verifying that the interface provided towards the virtual machines managed by the TOE is compliant with the z/Architecture definition. Those SAK tests, however, are to be considered negative tests, since the cannot actually prove compliance with z/Architecture but due to extensively issuing random processor instruction streams over a significant amount of time without ending up in any system errors, sufficient confidence of proper z/Architecture implementation is built up. The developer testing was performed to the depth of the TOE design at subsystem level, i.e. the developer test-depth analysis demonstrated that the TOE subsystems CP, RACF, and TCPIP have been subject to test cases exercising the TSFI and the TSF implemented by those components.

As result of an evaluator observation with respect to a deficiency limited to the TCPIP subsystem, the developer had to update the TCPIP subsystem and was required to repeat the TCPIP related tests in addition to the necessary functional testing of the changes applied. The developer testing, therefore, has been split up into two separate test session.

Testing results:

The test evidence provided by the developer and examined by the evaluator demonstrates that all but one test case were successful, i.e. the TOE behaviour observed during the tests matched the expected behaviour.

For one test case a deviation from the expected behaviour was identified, which resulted in opening a respective bugfix record. An analysis of the error performed by the developer resulted in the determination that the observed deviation does not present a security/integrity issue, i.e. no security mechanisms of the TOE were bypassed or disabled and no vulnerability is introduced.

7.3 Evaluator Testing Effort

The following independent testing was performed by the evaluator:

TOE test configuration:

The tests were performed on a IBM internal system running within a logical partition of a System z10 High End server. Note that this was the system the developer testing was also performed on.

The test system had installed the z/VM Version 6 Release 1, which was displayed after logon. Issuing the commands to determine the service level including expected output, the evaluator was able to verify that all required RSU and PTF as stated in section 1.5.4.1 of the ST were installed on the machine.

The TOE had been in its evaluated configuration when the evaluator tests were performed.

Subset size chosen; selection criteria for the security functions that compose the subset; security functions tested; developer tests performed:

The evaluator repeated a randomly chosen subset of the developer tests. For each of the test case groups "CP commands", "RACF commands", and "DIAGNOSE", coverage of at least 33% was achieved by the sampling strategy. The overall coverage achieved by the sample chosen was 39%.

No SAK test case was repeated.

In addition, the evaluator devised independent test cases to cover the TSFI that are not explicitly but only implicitly triggered by the developer tests repeated. The independent evaluator test cases directly triggered the TELNET Server, the TCP/IP configuration files and commands, the System Directory, and RACF and CP commands. The evaluator covered all TSFI except the API comprising the z/Architecture instructions and the RACF Report Writer by independent test cases, with those not explicitly listed above triggered indirectly.

Verdict for the activity:

The overall judgement on the results of evaluator testing during the evaluation is that all tests performed passed, i.e. the actual results achieved by the evaluator matched the expected results

By using developer tests as base for independent testing, the evaluator achieved the same test depth as the developer when repeating a subset of the developer tests. Therefore, the tests performed by the evaluator were at the level of the subsystems of the TOE design.

There were no failed tests that were caused by TOE behavior different from the expected behavior or violating requirements stated in ST.

7.4 Evaluator Penetration Testing

The evaluator consulted public domain information in order to identify vulnerabilities that would require performing penetration testing, but found no such vulnerabilities.

As for the penetration testing based on the evaluator's independent vulnerability analysis the evaluator devised three penetration test cases. Whereas one of the test cases was intended to identify additional interfaces potentially bearing weaknesses, the second and third test case were intended to explicitly probe for buffer overflow weaknesses . All tests were performed at the depth of the subsystems of the TOE design exercising the TCPIP subsystem of the TOE.

A port-scan was performed from within the same network segment the TOE was located in to eliminate interferences with other active network component. No open ports on the target machine other than the TELNET port, which was expected to be open for the purpose of establishing connections to the TOE as designed, thus matching the expected results.

Attempts to deliberately provoke buffer overflows during input of user credentials were performed. That test was performed using the standard clients to be used when accessing the TOE as well as from the command line. In particular, no specific setup reflecting other active network components was done. The tests revealed no weaknesses. The excessive inputs were rejected with error messages, thus matching the expected results.

In order to identify weaknesses in the implementation, a client using a modified openssl library was used for connecting with the TOE. The tests ran for a significant amount of time, no buffer overflows or other unexpected behaviour was observed.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The Target of Evaluation is z/VM Version 6 Release 1. The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 of this report represent the TOE.

TOE is one instance of z/VM running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over this abstract machine regardless which software runs inside of virtual machines. This abstract machine is provided by a logical partition (LPAR) of an IBM System z server.

A detailed list of supported IBM system z machine models is given in section 1.5.4.4 of the ST [6] which is the base for evaluation.

The LPAR itself is not part of the TOE, but belongs to the TOE environment. It is to be noted that although a z/VM instance technically can be run within a z/VM instance, the evaluated configuration is restricted to one z/VM instance running directly within an LPAR. A z/VM instance running within a virtual machine is allowed, but this “second level” z/VM instance is not in an evaluated configuration, as some security functionality is implemented differently, in particular with respect to the usage of the processor's Start Interpretive Execution (SIE) instruction.

Multiple instances of the TOE may share the RACF database. This is done by sharing the DASD (direct access storage device) volume keeping the RACF database between the different z/VM instances. Although sharing of the RACF database between z/VM and z/OS is technically feasible, it is explicitly excluded from this evaluation.

The evaluated configuration of the TOE is additionally defined by the configuration requirements to be met as stated in the Secure Configuration Guide e.g. table 2. The ST [6] in section 1.5.4.3 redirects readers to this document, which is part of the deliverables as listed in table 2.

8.1 Software Configuration

The TOE software components allow a broad range of configuration possibilities. However, to implement all security requirements, restrictions on the configuration must be made.

The Secure Configuration Guide [10] provides instructions and constraints for the evaluated configuration.

8.2 Hardware configurations

The following assumptions about the technical environment of the TOE are made. In the ST [6], the TOE is seen as one instance of z/VM running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine can be provided by one of the following: a logical partition provided by a certified version of PR/SM on an IBM System z processor:

- IBM System z10 Business Class
- IBM System z10 Enterprise Class
- zEnterprise 114
- zEnterprise 196

The abstract machine itself is not part of the TOE, rather, it belongs to the TOE environment. Nevertheless the correctness of separation and memory protection mechanisms implemented in the abstract machine is analyzed as part of the evaluation since those functions are crucial for the security of the TOE.

The following peripherals can be used with the TOE preserving the security functionality:

- all terminals supported by the TOE
- all storage devices supported by the TOE
- all network adapters supported by 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.

The Evaluation Methodology CEM [2] was used. For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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.

The evaluation has confirmed:

- PP Conformance:
  Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
  OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010,
  OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010 [10]
- for the Functionality:
  PP conformant
  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 9, Para. 4, Clause 2). This holds for: The TOE Security functionality according to the following table:

Algorithm	Key length	Intended purpose	Implementation standard
SHA-1	not applicable	integrity verification	U.S. NIST FIPS PUB 180-4
DSA	L=1024, N=160 bit	Authentication, Key Exchange	U.S. NIST FIPS PUB 186-3
RSA	2048 bit	Authentication, Key Exchange	U.S. NIST FIPS PUB 186-3
TDES in CBC mode	168 bit	encryption, decryption	U.S. NIST FIPS PUB 46-3, U.S. NIST PUB SP800-38A
AES in CBC mode	128 bit, 256 bit	encryption, decryption	U.S. NIST FIPS PUB 197, U.S. NIST PUB SP800-38A

10 Obligations and Notes for the Usage of the TOE

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

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

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

11 Security Target

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

This page is intentionally left blank.

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
CP	Control Program
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPL	Initial Program Load
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Mandatory Access Control
PP	Protection Profile
PR/SM	Processor Resource/Systems Manager™
RACF	Resource Access Control Facility
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Control Program (IBM) - The Control Program provides the kernel or nucleus of z/VM running in supervisor state outside the SIE instruction environment. It controls and manages the SIE instruction provided by the underlying processor providing a restricted computing environment for the virtual machines.

Discretionary Access Control (DAC) - 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.

Logical Processor (IBM) - A logical processor is a share of a real processor that is used by a logical partition (LPAR). Logical processors have the same behavior as real processors, but may "float" among the available real processors. The point-in-time mapping of a local processor to a real processor is managed by the PR/SM LPAR hypervisor which can overcommit the available CPU capacity, making LPARs wait for access to the CPU. This means that the total number of logical processors can exceed the number of real processors.

Mandatory Access Control (MAC) - An access control policy that determines access based on the sensitivity (SECRET, for example) or category (PERSONNEL or MEDICAL, for example) of the information being accessed and the access authority of the user attempting to access 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 Label (IBM) - A name that represents the combination of a hierarchical level of classification (IBM security level) and a set of non-hierarchical categories (security category). Security labels are used as the base for mandatory access control decisions. Security labels are sometimes referred to as SECLABELs.

Security Level (IBM) - A numerical value that represents the relative sensitivity of the information an object contains or that a user is permitted to access. A higher number represents a higher level of sensitivity. Security levels are sometimes referred to as SECLEVELs. The equivalent MLS term is classification.

Security Level (MLS policy in the Bell-LaPadula model) - The combination of a hierarchical classification (called security level in z/VM) and a set of nonhierarchical categories that represents the sensitivity of information is known as the security level. The equivalent term in other IBM documentation is security label.

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

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

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

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

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

13 Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-0752-2013, Version 1.1, 2013-01-18, IBM z/VM Version 6 Release 1 Security Target, IBM Corporation

[7] Operating System Protection Profile, Version 2.0, 01 June 2010, BSI-CC-PP-0067-2010,
OSPP Extended Package – Labeled Security, Version 2.0, 28 May 2010,
OSPP Extended Package – Virtualization, Version 2.0, 28 May 2010

[8] Evaluation Technical Report, Version 2, 2013-02-01, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[9] Configuration list for the TOE, 2012-03-21, Configlist for zVM CP, RACF, and TCPIP components (confidential document)

[10] Secure Configuration Guide IBM z/VM Version 6 Release 1, Version SC24-6230-02, Date 2012-03-21, IBM

[9] specifically

- AIS 20, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

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

Table 1: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.