Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0903-2015

for

z/VM Version 6, Release 3

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-0903-2015

Operating System

z/VM Version 6
Release 3

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
Valid Until:	29.03.2020

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement

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. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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, 30 March 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A. Certification

1. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For

---

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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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

"Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. This Domain is linked to a conformance claim to one of the related SOGIS Recommended Protection Profiles. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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.

As this certificate is a re-certification of a certificate issued according to CCRA-2000 this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

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 3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0752-2013. Specific results from the evaluation process BSI-DSZ-CC-0752-2013 were re-used.

The evaluation of the product z/VM Version 6, Release 3 was conducted by atsec information security GmbH. The evaluation was completed on 15 January 2015. 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.

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 order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited as outlined on the certificate.

The owner of the certificate is obliged

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report and the Security Target and user guidance documentation mentioned herein to any applicant of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

[6] Information Technology Security Evaluation Facility

3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the product's evaluated life cycle, e.g. related to development and production sites or processes, occur or the confidentiality of documentation and information related to the product or resulting from the evaluation and certification procedure is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the product or resulting from the evaluation and certification procedure that do not belong to the product deliverables according to the Certification Report part B chapter 2 to third parties, permission of the Certification Body at BSI has to be obtained.
4. to provide latest at of half of the certificate's validity period unsolicitedly and at his own expense current qualified evidence to the Certification Body at BSI that demonstrates that the requirements as outlined in the Security Target are up-to-date and remain valid in view of the respective status of technology. In general, this evidence is provided in the form of a re-assessment report according to the rules of the BSI Certification Scheme.

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 z/VM Version 6, Release 3 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
Dept G32, Bldg 256-3
Endicott NY
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 TOE is z/VM Version 6, Release 3 clustered as up to four cooperating instances of z/VM within a Single System Image (SSI).

z/VM is a scalable virtual machine hypervisor for IBM System z® mainframe servers onto which to deploy mission-critical virtual servers. A single System z server can host one z/VM instance per logical partition (LPAR), and each instance of z/VM can host tens to hundreds of virtual servers. Multiple instances of z/VM can be connected to form a networked system called a "collection". The communication aspects within z/VM used for these connections are also part of the evaluation. External communication links can be protected against loss of confidentiality and integrity by cryptographic protection mechanisms not part of the TOE.

z/VM offers multi-system clustering technology allowing between one and four z/VM instances in a SSI cluster. New instances of z/VM can be added to the cluster topology at runtime. Support for live guest relocation (LGR) allows the movement of Linux virtual servers without disruption to the operation. The z/VM systems are aware of each other and can take advantage of their combined resources. LGR enables clients to avoid loss of service due to planned outages by relocating guests from a system requiring maintenance to a system that remains active during the maintenance period.

Due to the functionality of performing identification and authentication of users, implementation of DAC and MAC, providing management facilities for all security-related functions and the fact that support functionality is hosted in different virtual machines, z/VM also resembles an operating system. Therefore, the Operating System Protection Profile ([7]) is used as a basis for the ST. z/VM meets all of the requirements of the Operating System Protection Profile base, as well as its extended packages for labeled security and virtualization.

z/VM provides identification and authentication of users using different authentication mechanisms, both discretionary and mandatory access control to a large number of different objects, separation of virtual machines, a configurable audit functionality, sophisticated security management functions, preparation of objects for reuse and functionality used internally to protect z/VM from interference and tampering by untrusted users or subjects.

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 6.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	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.
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 several factors.
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.
Separation of virtual machines	Operating system failures that occur in virtual machines cannot affect the TOE running on the real processor.
Auditing	The TOE provides an audit capability that allows generating audit records for security critical events.
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.
Security Management	The TOE provides a set of commands and options to adequately manage the security functions of the TOE.
TSF Protection	The TOE control program enforces integrity of its own domain. No virtual machine can access TOE resources without appropriate authorization.
SSI clustering	The SSI clustering mechanism integrates different z/VM systems into one cluster in order to share different resources. The SSI cluster communication ensures serialization of concurrent access to shared resources, if needed.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.5.3 and 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. 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 configurations of the TOE as outlined in chapter 8 of this report.

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

z/VM Version 6, Release 3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	z/VM Version 6 Release 3, program number 5741-A07	V6R3	Tape/DVD
2	DOC	Program Directory for z/VM V6R3 base	GI13-3401-00	Hard copy
3	DOC	Program Directory for RACF function level 630	GI13-3407-00	Hard copy
4	DOC	Guide for Automated Installation and Service	GC24-6246-02	Hard copy
5	DOC	z/VM 6.3 Certified Product Guidance sha256-Checksum: 71f38401dfeaf31605c35b62c508edd971c4ec6887f0e174f86e7c337d61dffb ZVM630-CC-Guidance.zip	n/a	Download
6	DOC	z/VM V6R3 Secure Configuration Guide sha256-Checksum: 6b4bef80a903fc522b67c403f07415b65a1f86e35f7ed18299217327af620e0a zVM 630 Secure Configuration Guide.pdf	SC24-6230-05	Download
7	SW	PTF UM34279 for APAR VM65474 containing RSU2 and other service to z/VM 6.3 provided by APAR VM65473 to be obtained electronically from ShopzSeries https://www.ibm.com/software/shopzseries	n/a	Electronic

Table 2: Deliverables of the TOE

All hard copy guidance documents 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 V6R3.0 Secure Configuration Guide (SC24-6230-05)

listed as item 6 above.

The Secure Configuration Guide contains references to other relevant guidance documentation contained in item 5, i.e. z/VM 6.3 Certified Product Guidance. Both the Secure Configuration Guide and the Certified Product Guidance are available from a secured IBM ResourceLink:

https://www.ibm.com/servers/resourcelink/lib03060.nsf/pages/zVM63SecureConfigurationGuide

2.1. Overview of Delivery Procedure

Customers with IBM customer ID may use the ShopzSeries web portal (www.ibm.com/software/shopzseries) to file an order of the TOE or may contact an IBM sales representative for support.

Orders for z/VM are processed by an Production Center. The z/VM image ordered is duplicated to an appropriate media set of the type ordered by the customer (i.e., tapes or DVD), which is then packed in a card-box and shrink wrapped. The final package is then delivered to the customer via a courier service together with a contents list.

The whole process starting at the preparation and labeling of the media until finally delivering the shrink wrapped package to the customer is under supervision of a control system making use of bar code identification for all parts of an order throughout the complete process. The bar code enables unambiguous association of the media and the additional documentation to a specific order number and, hence, to the customer who filed that respective order.

Once the package arrived at the customer's site, the customer is able to verify that the delivery matches their order by reviewing the contents list provided as part of the delivery and by cross checking the part numbers labeled on the delivered media.

2.2. Identification of the TOE by the User

During the order process for the TOE, the customer needs to explicitly order the CC-certified version of z/VM Version 6 Release 3. This already ensures that the product delivered to the customer actually is the TOE containing all required components. The administrator is also able to verify the version of the TOE by issuing the command

QUERY CPLEVEL

which will result in displaying the version string

z/VM Version 6 Release 3.0, service level 1302 (64bit)

In addition, the administrator is asked verify the list of installed PTFs against the list of PTFs required as stated in the ST. In oder to do so, the administrator may issue the commands

*VMFSIM QUERY 6VMCPR30 SVRAPPS * TDATA :PTF*

*VMFSIM QUERY 6VMRAC30 SVRAPPS * TDATA :PTF*

*VMFSIM QUERY 6VMTCP30 SVRAPPS * TDATA :PTF*

and should be able verify the presence of the following PTFs in the output received.

For CP:

UM33998 UM34002 UM34003 UM34004 UM34005 UM34010 UM34035 UM34036

UM34042 UM34044 UM34046 UM34055 UM34058 UM34062 UM34244 UM34278

For TCPIP:

UK95491 UK96279 UK98378 UQRSU01

For RACF, no PTFs should be reported.

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

- Mandatory access control and support for security labels in Labeled Security Mode
- Separation of virtual machines
- Audit
- Object reuse functionality
- Security management
- TSF protection
- SSI clustering

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 hypervisor product that is part of an SSI cluster formed by one or more z/VM instances with the software components.

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 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 an z/VM SSI cluster comprising of one through four individual z/VM systems. These individual z/VM systems each execute 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. These abstract machines are provided by logical partitions (LPAR) of IBM System z servers.

The LPARs themselves are not part of the TOE, but belong 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 such "second level" z/VM instances are not part of the evaluated configuration.

The z/VM Single System Image feature (SSI) enables up to four z/VM systems to be configured as members of an SSI cluster, sharing different resources.

Members of the SSI cluster can be on the same or separate hardware systems. SSI enables the members of the cluster to be managed as one system, which allows service to be applied to each member of the cluster, avoiding an outage to the entire cluster. SSI also introduces the concept of live guest relocation (LGR) where a running Linux guest operating system can be relocated from one member in an SSI cluster to another without the need to stop the running Linux guest.

All z/VM member instances of one SSI cluster share the RACF database, but they do not share the RACF audit disks. Each z/VM member instance must execute its own instance of RACF accessing the shared RACF database. The sharing of the RACF database is done by sharing the DASD (direct access storage device) volume keeping the RACF database between the different SSI z/VM member instances.

Different instances of the TOE may also share the RACF database. The sharing is implemented similarly to the sharing of the RACF database within the SSI cluster.

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.

In both modes, 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 up to four z/VM instances each defined by 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 TLS 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 TLS services allowing the establishment of a cryptographically secured channel to access a CP console.

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, i.e. on systems GDLMCCC and GDLPCCC each running within a logical partition. The logical partitions were provided by certified versions of PR/SM on an IBM System z10 Enterprise Class server and an IBM zEnterprise EC12 server, respectively.

The test systems - for both the developer and the evaluator test sessions - had installed the TOE in its evaluated configuration as required by the Secure Configuration Guide [10]. This was confirmed by the evaluator analysing developer evidence generated and running respective checks on his own.

7.2. Developer Testing

The following functional testing was performed by the developer:

TOE test configuration:

The tests were performed on system GDLMCCC as one of the configured SSI cluster members running within a logical partition of a System z10 High End server. Test related to the SSI feature also involved system GDLPCCC as a second cluster member configured and running within a logical partition of a IBM zEnterprise EC12 server.

The test systems each had installed the z/VM Version 6 Release 3 with SSI feature enabled. The evaluator verified that all required RSU and PTF as stated in section 1.5.4.1 of the ST [6] were installed on the machines.

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

The limitation of tests performed to the test systems 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 of the underlying hardware was performed by IBM on all processor 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 subset of TSFIs 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
- System Configuration
- 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. 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.

IBM usually performs 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 they 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. Note that for the current evaluation no SAK tests at the level of z/VM were deemed necessary by the developer as there have not been any changes to the z/Architecture since the previous evaluation. However, SAK tests have been actually performed at the level of the underlying PR/SM for the hardware platforms supported by z/VM and did not reveal any deviations as verified as part of the respective PR/SM evaluations performed.

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.

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 test cases related to one specific TSFI deviations from the expected behaviour were identified, which resulted in opening a respective bugfix record. A profound analysis of the error performed by the developer resulted in the determination that the observed deviations do not present a security/integrity issue, i.e. no security mechanisms of the TOE were bypassed or disabled and no vulnerability is introduced. The evaluator was able to verify that corrective actions to address the failure have been initiated already.

7.3. Evaluator Testing Effort

The evaluator repeated a randomly chosen subset of the developer tests for each of the test case groups "CP commands", "RACF commands", and "DIAGNOSE".

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 trigger 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 the following:

- all but a total of five developer tests re-performed passed, i.e. the actual results achieved by the evaluator matched the expected results. For each of the failing test cases, the developer provided a rationale on why the tests returned results that deviate from the expected output. While one test case failed due to an obvious but non-critical configuration issue, the others actually demonstrated correct behaviour of the command tested but reported failure due to errors in the test procedures that misinterpreted the output received. For those, corrective actions to properly update the test procedures have been already initiated.
- all test cases devised by the evaluator passed, i.e. the actual test results 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 behaviour different from the expected behaviour 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 a total of two penetration test cases. Whereas one of the test cases was intended to identify additional interfaces potentially bearing weaknesses, the second

test case was intended to explicitly probe for weaknesses of the TELNET server interface. All tests were performed at the depth of the subsystems of the TOE design exercising the TCPIP subsystem of the TOE.

8. Evaluated Configuration

The Target of Evaluation is z/VM Version 6 Release 3. The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 of this report represent the TOE.

The TOE is defined by an SSI cluster of up to four cooperating instances of the z/VM product each running on an abstract machine as the sole operating system on the level of the abstract machine and exercising full control over that abstract machine regardless which software runs inside of virtual machines. The abstract machines are provided by a logical partition (LPAR) of IBM System z servers. Sharing of the RACF database between z/VM and z/OS is technically feasible, it is explicitly excluded from this evaluation.

z/VM executes 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 with CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement Feature 3863 active
- IBM System z10 Enterprise Class with CPACF DES/TDES Enablement Feature 3863 active
- IBM zEnterprise 114 with CPACF DES/TDES Enablement Feature 3863 active
- IBM zEnterprise 196 with CPACF DES/TDES Enablement Feature 3863 active
- IBM zEnterprise EC12 with CPACF DES/TDES Enablement Feature 3863 active

The LPARs themselves are not part of the TOE, but belong 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 z/VM instances running directly within an LPAR. A z/VM instance running within a virtual machine is allowed, but such "second level" z/VM instances are not part of the evaluated configuration.

The evaluated configuration of the TOE is additionally defined by the configuration requirements to be met as stated in the Secure Configuration Guide [10]. 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.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5. 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0752-2013, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on:

- TOE functionality with respect to subsystem CP was enhanced by implementation of the Single System Image (SSI) feature including Life Guest Relocation (LGR) capability.
- TOE functionality with respect to subsystem TCPIP was modified to support TLS v1.2.
- TOE functionality with respect to subsystem RACF was modified to support a common security context within the SSI cluster by sharing the RACF database.

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 [7]
- 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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authenticity	RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-1	[RFC3447] (PKCS#1 v2.1) [FIPS180-4]	Modulus length: 2048,	No	Verification of certificate signatures provided for authentication Server

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
2		RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-256	(SHA)	3072, 4096	Yes	and Client certificates are used.
3		DSA signature verification using SHA-1	[FIPS186-3] (DSA) [FIPS-180-4] (SHA-1)	L= 1024 N= 160	No	
4	Authentication	RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-1	[RFC3447] (PKCS#1 v2.1)	Modulus length: 2048, 3072, 4096	No	Client signs message with private key bind to his certificate. Server verifies signature of the message.
5		RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-256			Yes	
6		RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-384			Yes	
7	Key agreement (key transport)	RSA encryption (client) and decryption (server) (RSAES-PKCS1-v1-5)	[RFC3447] (PKCS#1 v2.1)	Modulus length: 2048, 3072, 4096	Yes	Encrypted exchange of pre-master secret generated at client side
8	Key agreement	Diffie-Hellman	[RFC2631]	Groups with modulus size between 1024 bits and 2048bits (in multipls of 64 bits)	No	
9	Key derivation	HMAC with SHA-256 (TLSv1.2)	[RFC2104] (HMAC) [FIPS180-4] (SHA)	256	Yes	Symmetric keys and MAC keys for record layer
10		HMAC with SHA-1 (TLSv1.2)		160	Yes	
11		HMAC with SHA-1 and MD5 (TLSv1.1)			Yes	
12	Confidentiality	AES in CBC mode (AES_128_CBC, AES_256_CBC)	[FIPS197] (AES) [SP800-38A] (CBC)	|k| = 128, 256	Yes	Bulk data encryption / decryption (record layer)
13		Three-key TDES in CBC mode (3DES_EDE_CBC)	[FIPS46-3] (DES) [SP 800-67] (TDES/TDEA)	|k| = 168	Yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
			[SP 800-38A (CBC) [RFC4253] (SSH-2 using 3DES with CBC mode)			
14	Integrity and authenticity	HMAC with SHA-1 or SHA-256	[RFC2104] (HMAC) [FIPS180-4 (SHA)	160 (SHA-1) 256 (SHA-256)	Yes	Message authentication code (record layer)
15	Trusted Channel	TLSv1.2 [RFC5246]	[RFC5246] (TLSv1.2) additionally refer to lines 1-14 above	N/A	No	
16		TLSv1.1 [RFC4346]	[RFC4346] (TLSv1.1) additionally refer to lines 1-14 above		No	

Table 3: TOE cryptographic functionality

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 of 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
API	Application Programming Interface
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
CMS	Conversational Monitor System
CP	Control Program
cPP	Collaborative Protection Profile
DAC	Discretionary Access Control
DASD	Direct-access storage device
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
IUCV	Inter User Communication Vehicle
ITSEF	Information Technology Security Evaluation Facility
LGR	Live Guest Relocation
LPAR	Logical Partition
MAC	Mandatory Access Control
PP	Protection Profile
PR/SM	Processor Resource/System Manager
PTFs	Product temporary fix
RACF	IBM Resource Access Control Facility
RSU	Recommended Service Upgrade
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSI	Single System Image
SSL	Secure Sockets Layer

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.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (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-0903-2015, Version 1.2, Date 19 December 2014, IBM z/VM Version 6 Release 3 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 3, Date 19 December 2014, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[9] Configuration list for the TOE, Date 2014-04-14, Configation lists for zVM 6.3 CP, RACF, SSI, and TCP/IP components, Filename “[ConfCode] Configlist for zVM 6.3 CP RACF TCPIP SSI Components.zip”, (confidential documents)

[10] z/VM Version 6 Release 3 Secure Configuration Guide IBM,Version SC24-6230-05 Date 2014-05-27

[11] Program Directory for z/VM Version 6 Release 3, Version GI13-3401-00, Document Date: July 2013

[12] Program Directory for RACF Security Server for z/VM, function level 630, Version GI13-3407-00, Date July 2013

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

CC Part 1:

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
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

Assurance Class	Assurance Components
	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.

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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”

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.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.