Certification Report

BSI-DSZ-CC-1160-2021

for

PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems, Driver Level D41C with Bundle Level H13/S21b

from

IBM Corporation

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom   Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1160-2021 (*)

Server Applications: Virtualization

PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems
Driver Level D41C with Bundle Level H13/S21b

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

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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 and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the alexprovisions 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.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 21 April 2021
For the Federal Office for Information Security

Sandro Amendola   L.S.
Head of Division

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

---

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

[2]   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

[3]   BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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]

3. 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.

3.1. European Recognition of 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. For "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. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.3, ATE_DPT.3, ATE_FUN.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant

3.2. 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), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies

---

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

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. 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 PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems, Driver Level D41C with Bundle Level H13/S21b has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1133-2020. Specific results from the evaluation process BSI-DSZ-CC-1133-2020 were re-used.

The evaluation of the product PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems, Driver Level D41C with Bundle Level H13/S21b was conducted by atsec information security GmbH. The evaluation was completed on 13 April 2021. atsec information security GmbH is an evaluation facility (ITSEF)[5] 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.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this 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-assessment or 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 would require a re-assessment of the products resistance to state of the art attack methods, the

---

[5]   Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 21 April 2021 is valid until 20 April 2026. Validity can be re-newed by re-certification.

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, the Security Target and user guidance documentation mentioned herein to any customer 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,

3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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.

6. Publication

The product PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems, Driver Level D41C with Bundle Level H13/S21b 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

[6] IBM Corporation
2455 South Road, P329
Poughkeepsie NY 12601
USA

B. Certification Results

The following results represent a summary of

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

1.   Executive Summary

The Target of Evaluation (TOE) is PR/SM, Driver Level D41C with Bundle Level H13/S21b for IBM z15 T02 and IBM LinuxONE III LT2 Systems.

PR/SM is a hardware facility running on IBM z15 T02 and IBM LinuxONE III LT2 systems that enables the resources of a single physical machine to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition is a domain of execution, and is considered to be a subject capable of running a conventional system control program (SCP) such as z/OS™, z/VM™, z/VSE, z/TPF™, or Linux for System z. These operating systems run unmodified in a PR/SM partition.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
Identification and Authentication	The TOE supports identification and authentication of users by means of: • Unique identification via zone numbers assigned to each logical partition • Unique user IDs assigned to each user of the HMC/SE
Access Control and Information Flow Control	The TOE supports access control between users and resources by means of: • The TOE implements LPAR Security Controls which define a partition's access to IOCDSs, performance data, cryptographic hardware, the channel reconfiguration process, and the authority to reset or shutdown other partitions. • The TOE implements LPAR Security Controls which specify the partition's permissions to send BCPii commands to the SE part of the TOE and to specify which partition's configuration on the SE part of the TOE can receive and process BCPii commands. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission. • The TOE allows access to specific control units and devices on non-dedicated channels to be restricted. • The TOE insures that dedicated channels, storage and physical CPs are never shared. • The TOE will prevent the transfer of any message between a logical partition and any resource not explicitly allocated to it. • The TOE implements management access controls to define configurable role based authorized administrator access to the TOE's management functions.

TOE Security Functionality	Addressed issue
Auditing	The TOE supports auditing of relevant events by means of a security log with the following characteristics: • All security relevant events are recorded in the security log. This auditing mechanism cannot be bypassed. • The security log is protected from unauthorized deletions or modifications. • Applications in logical partitions cannot read the security log. • The security log can be offloaded for archival purposes.
Authorized Administration and Operation	The HMC/SE workplace is the window from where users start tasks for monitoring and operating the CPC (central processor complex). A user profile determines which tasks and controls users can use on the workplace. Not all tasks are available for each user. In addition to a set five predefined user roles supplied with the console the ability to define customized user roles is also provided. A user role is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (task roles) or it can be created to define the set of managed objects that are manageable for a user (managed resource roles). A customized user role is based on one of the predefined user roles from which objects or tasks are removed. Once user roles are defined or customized they can be used to create new users with their own permissions. A user can be created with one or more user roles. A detailed list of the console actions authorized for each predefined role is contained in a respective section "Tasks and default user IDs" in the HMC online help shipped pre-installed.
Object Reuse	The TOE supports object reuse by means of: • Clearing of all storage prior to allocation or re-allocation. • Resetting all information in physical processors before dispatching the processor to a new logical partition. • Resetting non-shared channel paths and attached I/O devices prior to allocation to a logical partition.
Reliability of Service	The TOE supports the control of the processor running time and wait completion processor parameters. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service.
TSF Protection	The TOE supports TSF protection by means of: • Self test whenever the TOE is loaded and started and periodically during the TOE's operation. • The PR/SM kernel is loaded into a protected area of central storage where it is inaccessible by any users, operating systems or applications. • An alternate (backup) SE operates to provide real time mirroring of relevant system data: IOCDSs, audit log, image profiles.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.5.2.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. 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 3.1, 3.2 and 3.3.

This certification covers the configurations of the TOE as outlined in chapter 8.

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

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

2.   Identification of the TOE

The Target of Evaluation (TOE) is called:

PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems,
Driver Level D41C with Bundle Level H13/S21b

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	LPAR Licensed Internal Code (LIC)	D41C Bundle H13/S21b / 2.15.0	n/a[7]
2	SW	HMC/SE Licensed Internal Code (LIC)		
3	DOC	Processor Resource/Systems Manager Planning Guide [9]	SB10-7175-01b	DVD
4	DOC	Hardware Management Console Operations Guide [8]	2.15.0	Pre-installed as integral part of the HMC online help system
5	DOC	Support Element Operations Guide [10]	2.15.0	Pre-installed as integral part of the SE online help system
6	DOC	Input/Output Configuration Program User's Guide for ICP IOCP [11]	SB10-7172-04	DVD
7	DOC	Stand-Alone Input/Output Configuration Program User's Guide [12]	SB10-7173-01	DVD
8	DOC	z15 Service Guide 8561 [13]	GC28-6998-00b	DVD
9	DOC	z15 Installation Manual for Physical Planning 8561 [14]	GC28-7002-00d	DVD
10	DOC	z15 Installation Manual 8561 [15]	GC28-6997-00f	DVD
11	DOC	z15 Service Guide 8562 [16]	GC28-7010-00	DVD
12	DOC	z15 Installation Manual for Physical Planning 8562 [17]	GC28-7011-00	DVD

[7] Note that the customer is not provided with any media that contains the installable LIC. All LIC is installed during manufacturing as part of the TOE delivery procedure. After physical hardware installation, specific checkout tests are performed at the customer's site by IBM personnel before the system is handed over.

No	Type	Identifier	Release	Form of Delivery
13	DOC	z15 Installation Manual 8562 [18]	GC28-7009-00	DVD

Table 2: Deliverables of the TOE

As integral part of an IBM z15 or LinuxONE III system, the TOE cannot be ordered stand-alone and is delivered together with hardware components not being part of the TOE but required for TOE operation. Those are:

- a model of the

  - IBM z15 or LinuxONE III machine type 8561

  - IBM z15 or LinuxONE III machine type 8562

  server family as listed in section 1.5.3 of the [6]

- a Support Element (SE) physically attached to the IBM z15 or LinuxONE III model above,

- an alternate Support Element for system data switchover in case the Primary SE fails operation, and

- an optional Hardware Management Console (HMC) for centralized administration of multiple SE.

The above table contains the items that comprise the different elements of the TOE, including software and guidance.

2.1. Overview of Delivery Procedure

The delivery procedure for the TOE is under full control of IBM. Once the ordered hardware the TOE is intended to run on, i.e. an IBM z15 T02 or LinuxONE III LT2 server, has been installed with Driver D41C at bundle level H13/S21b and is ready to be shipped, it is loaded into a climate-controlled truck, which is then locked. The customer is informed that the hardware is on its way.

Upon arrival at the customer's site, the truck is unlocked by IBM personnel and the hardware is unloaded. After physical installation of the hardware components, i.e. cabling and air conditioning, the TOE is tested by IBM service personnel.

Only after the hardware the TOE is pre-installed and has been successfully installed, the delivery and installation procedure as documented in respective installation manuals is considered to be complete by IBM and the TOE (and the underlying hardware) is handed over to the customer who is not involved in the whole process of preparing the machine (apart from providing the operational environment for physical installation) up to that moment.

As a final step, the IBM service personnel is expected to advise the customer to change the passwords for the predefined system users on the HMC/SE workplaces from their default values to customized, more secure passwords.

2.2. Identification of the TOE by the User

In order to identify the correct version of the TOE, the user may bring up the System Information Panel on the Support Element or an attached Hardware Management Console, which will show the version number, driver level, and bundle level and should read

"Version: 2.15.0 Driver level: 41 Bundle level: H13" or

"Version: 2.15.0 Driver level: 41 Bundle level: S21b" respectively.

Due to delivery and installation procedure under full IBM control and observed by the customer once the TOE arrived, customers are able to verify during physical installation that their order has been fulfilled correctly by IBM.

3.   Security Policy

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

- Identification and Authentication
- Access Control and Information Flow Control
- Auditing
- Authorized Administration and Operation
- Object Reuse
- Reliability of Service
- TSF Protection

4.   Assumptions and Clarification of Scope

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

- Security log data stored off of the TOE must be controlled for confidentiality and integrity according to the owner's needs.
- Personnel working as administrators or other privileged positions must be carefully selected and trained.
- The TOE must be protected during the setup phase.
- Physical access and remote access to the HMC and z System must be restricted only to authorized and approved users. In particular the HMC and the LAN connecting it to the SEs must be physically protected from access other than by authorized system administrators.
- The underlying hardware must provide separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.
- The underlying physical I/O LIC must provide separation mechanisms that can be used by the TOE to restrict access of one partition to authorized logical I/O resources.

Details can be found in the Security Target [6], chapter 4.2.

5.   Architectural Information

The TOE is the PR/SM Licensed Internal Code (LIC) kernel running on the z15 or LinuxONE III Systems. The kernel provides the capability to initialize the system in LPAR mode, which in the evaluated configuration is the only valid mode of operation. The TOE is implemented in LIC. The use of LIC prevents untrusted code from masquerading as part of the TOE and abusing TOE privileges. The TOE is composed of:

1. the LPAR LIC running on the Central Processing Complex (CPC) as a Hypervisor responsible for maintaining the isolation of logical partitions maintained and controlled by the TOE.

2. HMC LIC running on the Hardware Management Console (HMC) providing remote system administration functions to maintain the current configuration. The HMC is connected over internal network with one or more Support Elements.

3. SE LIC running on the Support Element (SE) physically located in the CPC cabinet and connected to the CPC. The SE also provides system administration functions to maintain the current configuration and can be used independently from an HMC connected to it.

PR/SM LIC provides the security administrator with the ability to define a completely secure system configuration. When the system is defined in such a manner, total separation of the logical partitions is achieved thereby preventing a partition from gaining any knowledge of another partition's operation.

Only functions related to logical partition isolation, physical resource allocation, access control and audit are the subject of the Security Target. Additional functions of PR/SM related to normal operations and maintenance of the system are not considered as security enforcing functions because the TOE will be configured to provide a configuration consistent with secure isolation such that these operations cannot be in conflict with the security policy of PR/SM.

The other functions are therefore not evaluated for correctness and no vulnerability analysis for those functions is performed.

The address space of the TSF is isolated from the address space of the partitions by hardware protection mechanisms (the "start interpretive execution" (SIE) instruction provided by the underlying processor as described below), and by the provision of separate hardware for the SE and I/O processors. The TSF LIC and data is therefore protected from modification or tampering.

The security administrator uses an I/O configuration utility (IOCP) to define an IOCDS of the I/O resources and their allocation to specific logical partitions. The IOCDS should be verified by the security administrator prior to activating the partitions. The TOE allows I/O resources to be dedicated to a single partition, relocatable among a defined set of partitions, or shared by a defined set of partitions. When an administrator wishes to activate a partition, the activation request is initiated from the HMC. LPAR will receive an external interrupt identified as coming from a BFYCALL command and issue the PCCALL instruction to obtain the description of the partition the administrator wishes to activate. LPAR will attempt to construct the partition and will inform the HMC of the success or failure of the command via the PCCALL instruction.

Several IOCDSs, defining different configurations, may be stored but only one is in effect at any time given. The configuration becomes effective as part of the activation sequence.

Standard hardware resources such as a central processor, including computation and control registers, timers, clocks and storage; and I/O resources are objects allocated to logical partitions. These objects are subject to a non-discretionary access control policy under which each logical partition is only permitted access to resources allocated to it. Logical partitions are logical objects that are built from existing physical objects. These logical objects fall into one of three classes:

   a) Logical processor facilities, which are supported by similar physical objects. Each such logical object is represented by an internal control block that contains current state information each time context is switched to a different logical partition.

   b) Logical storage, both central and storage class memory, is represented by the same amount of contiguous physical storage. PR/SM does not perform paging or move logical partitions once they have been placed in real storage. Physical storage can be de-allocated from one logical partition and reallocated to another. This feature can be disabled, and is subject to full object reuse control.

   c) Logical I/O resources (channels) are implemented by physical resources of the same type. Such resources can be configured so that they are not shared by partitions. A channel can be de-allocated from one logical partition and reallocated to another, under the control of the security administrator.

The z/Architecture® and ESA/390® architecture support two instruction states: problem and supervisor. Problem state instructions can be executed in either problem or supervisor state. Semi-privileged instructions can be executed in supervisor state, or in problem state subject to one or more additional authorizations. Privileged instructions can be executed only in supervisor state. The TOE exports a virtual machine including all architected instructions, and initiates the execution in supervisor state, so that all three classes of instruction can be executed within the logical partition. Thus each logical partition has both execution states available. PR/SM does not interfere with the logical partition's use of those states. A system control program (SCP) running in a logical partition can support z and ESA/390 architectural mode. The SCP can define whether it is running in z/Architecture mode or ESA/390 mode by a use of a SIGP instruction. Typically if the SCP understands z/Architecture mode it gets into z/Architecture mode immediately and remains in that mode.

The TOE supports and uses the "start interpretive execution" (SIE) instruction to create an interpretative execution environment in which the logical partitions execute. PR/SM begins execution in non-SIE mode. When a logical partition is to be activated, PR/SM establishes the parameters for each logical processor allocated to the partition in a control block called a "state description". PR/SM executes a SIE instruction, which dispatches the logical processor in SIE mode. The PR/SM hardware executes instructions in the logical processor in SIE mode until an exception condition occurs, which causes control to return to PR/SM in non-SIE mode. The exception conditions are events that cannot be handled in interpretative mode. PR/SM receives control in non-SIE mode. PR/SM maintains a state description for each logical processor of each logical partition so that each time a logical processor is dispatched, it is in the same context as when it last had control. Since this state description is updated by the hardware, it is impossible for one logical partition to acquire control with the wrong context (i.e. the context of another logical partition). The non-SIE/SIE distinction is a powerful privilege differentiation between PR/SM and the logical partitions.

The z15 or LinuxONE III Systems provide support for several features that are very helpful in many customer environments. However, these features are not recommended in a

secure environment. As a result, the TOE provides security related controls to disable such features assuring separation of the logical partition(s). The security related controls are outlined below:

Logical Partition Isolation

This control reserves reconfigurable unshared channel paths for the exclusive use of a logical partition. Channel paths assigned to an isolated logical partition are not available to other logical partitions and remain reserved for that LP when they are configured offline.

I/O Configuration Control Authority

This control can limit the ability of the logical partition to read or write any IOCDS in the configuration locally or remotely. Logical partitions with control authority for the I/O configuration data can read and write any non-write protected IOCDS in the configuration, and can change the I/O configuration dynamically.

BCPii Permissions

This control can limit the ability of the logical partition to send BCPii commands to other partition's configuration on the SE part of the TOE and whether a logical partition's configuration can receive and process BCPii commands from other partitions. This control can also limit from which specific logical partitions a partition can receive BCPii commands on the SE part of the TOE. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission.

Global Performance Data Control Authority

This control limits the ability of a logical partition to view central processor activity data for other logical partitions. Logical partitions with control authority for global performance data can view CP utilization data and Input/Output (IOP) busy data for all of the logical partitions in the configuration. A logical partition without control authority for the performance data can view only the CP utilization data for itself.

Cross-Partition Authority

This control can limit the capability of the logical partition to issue certain control program instructions that affect other logical partitions. Logical partitions with cross-partition authority can issue instructions to perform a system reset of another logical partition, deactivate any other logical partition, and provide support for the automatic reconfiguration facility.

In addition to the security controls mentioned above, the TOE also insures that central storage and storage class memory for each logical partition is isolated and cannot be shared with other logical partitions. The TOE rigidly enforces this "no sharing" rule during logical partition definition, logical partition activation, logical partition reconfiguration and during logical partition execution.

The TOE also "removes" central processors (CPs) from logical partitions by virtualizing physical CPs. Virtualized physical CPs are referred to as logical processors. Within the TOE, each logical CP is represented as a data structure that is associated with its specific logical partitions preventing the transfer of data between partitions.

Thus, when PR/SM is initialized for secure operation, one partition cannot gain access to the data within another partition nor modify any aspect of another partition.

With z/Architecture or ESA/390 architecture (which includes the functions of ESA/370 Architecture), these models have problem-program compatibility with S/360™, S/370™,

and 4300 processors. They can access virtual storage in multiple address spaces and data spaces. This extends addressability for system, sub-system, and application functions that use z/Architecture or ESA/390 architecture.

The Security Features are outlined in the following table.

TOE Security Functionality	Addressed issue
Identification and Authentication	The TOE supports identification and authentication of users by means of: • Unique identification via so-called "zone numbers" assigned to each logical partition • Unique user IDs assigned to each user of the HMC/SE For the logical partitions, there is no specific password. The logical partition is authenticated by its existence in the I/O Configuration Dataset (IOCDS) definition when activation occurs.The zone number is used to mediate access between the logical partition and the physical resources of the processor assigned to that logical partition. For the HMC/SE user, the required passwords are assigned by the security administrator. The use of the user ID and password allows the user of the HMC/SE to invoke the various functions that are defined as being allowed for that user ID.
Access Control and Information Flow Control	The TOE supports access control between users and resources by means of: • The TOE implements LPAR Security Controls which define a partition's access to IOCDSs, performance data, cryptographic hardware, the channel reconfiguration process, and the authority to reset or shutdown other partitions. • The TOE implements LPAR Security Controls which specify the partition's permissions to send BCPii commands to the SE part of the TOE and to specify which partition's configuration on the SE part of the TOE can receive and process BCPii commands. It should be noted that in the evaluated configuration no partition has either the send or receive BCPii permission. • The TOE allows access to specific control units and devices on non-dedicated channels to be restricted. • The TOE insures that dedicated channels, storage and physical CPs are never shared. • The TOE will prevent the transfer of any message between a logical partition and any resource not explicitly allocated to it. • The TOE implements management access controls to define configurable role based authorized administrator access to the management functions of the TOE.
Auditing	The TOE supports auditing of relevant events by means of a security log with the following characteristics: • All security relevant events are recorded in the security log. This auditing mechanism cannot be bypassed. • The security log is protected from unauthorized deletions or modifications. • Applications in logical partitions cannot read the security log. • The security log can be offloaded for archival purposes.
Authorized Administration and Operation	PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines, called "logical partitions". The HMC/SE workplace is the window from where users

TOE Security Functionality	Addressed issue
	start tasks for monitoring and operating the CPC (central processor complex). A user profile determines which tasks and controls users can use on the workplace. Not all tasks are available for each user.
	The following predefined default user IDs are established as part of base HMC/SE.
	OPERATOR (Operator) - A person with operator authority typically performs basic system startup and shutdown operations using predefine procedures.
	ADVANCED (Advanced Operator) - A person with advanced operator authority possesses operator authority plus the ability to perform some additional recovery and maintenance tasks.
	SYSPROG (Programmer) - A person with programmer authority has the ability to customize the system in order to determine its operation.
	ACSADMIN (Access Administrator) - A person with access administrator authority has the ability to create, modify, or delete user profiles on the HMC or for service mode on the support element. A user profile consists of user identification, a password, managed resource roles and task roles
	SERVICE (Service Representative) - A person with service representative authority has access to tasks related to the repair and maintenance of the system.
	In addition to the predefined user roles supplied with the console, the ability to define customized user roles is also provided. A user role is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (task roles) or it can be created to define the set of managed objects that are manageable for a user (managed resource roles). A customized user role is based on one of the predefined user roles from which objects or tasks are removed.
	Once user roles are defined or customized they can be used to create new users with their own permissions. A user can be created with one or more user roles.
	The following general definitions can be established:
	Administrator
	The Administrator is defined to be any user(s) with access to the HMC/SE workplace.
	Security Administrator
	Any administrator authorized to perform all of the following tasks:
	• Archive Security Logs
	• Change LPAR Controls
	• Change LPAR Group Controls
	• Change LPAR I/O Priority Queuing
	• Change LPAR Security
	• Customize/Delete Activation Profiles
	• Input/Output (I/O) Configuration
	• Logical Processor Add
	• Manage Users Wizard
	• Reassign Channel Path
	• System Details
	• User Management
	• View Security Logs
	A detailed list of the console actions authorized for each predefined role is

TOE Security Functionality	Addressed issue
	contained in a respective section "Tasks and default user IDs" of [8], which is integral part of the HMC online help.

Object Reuse	The TOE supports object reuse by means of:
	   • Clearing of all storage prior to allocation or re-allocation.
	   • Resetting all information in physical processors before dispatching the processor to a new logical partition.
	   • Resetting non-shared channel paths and attached I/O devices prior to allocation to a logical partition.

Reliability of Service	The TOE supports the control of the processor running time and wait completion processor parameters. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service

TSF Protection	The TOE supports TSF protection by means of:
	   • Self test whenever the TOE is loaded and started and periodically during operation of the TOE.
	   • The PR/SM kernel is loaded into a protected area of central storage where it is inaccessible by any users, operating systems or applications.
	   • An alternate (backup) SE operates to provide real time mirroring of relevant system data: IOCDSs, audit log, image profiles.

Table 3: Summary of security features

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 Configurations

With respect to the underlying hardware used, the test configuration is identical to the evaluated configuration of the TOE. However, some of the configuration requirements mandated by [9] do not fully apply to the test configuration as they refer to secure operation of the TOE at the customer's site. Moreover, in some cases overriding safeguards mandated for the TOE, like, for instance, security authorities settings for partitions, was required to actually allow to perform tests related to that safeguard, i.e. to verify that with an authority enabled, a logical partition in fact may perform actions but cannot do so with that authority removed.

The evaluator assessed the configuration deviations identified during his analysis of developer test cases and test approach and concluded that the configuration tested by the developer was consistent with the evaluated configuration of the TOE.

7.2. Developer Testing

For security specific testing the evaluator identified the following developer testing effort:

- The security test suite runs for any major driver change.
- A random subset of the security test suite FTP06 must be included in the driver regression testing, which however is out of scope for this evaluation

The combination of the above ensures that changes to the driver, including interim changes not covered by complete FTP06 execution, do not affect the security functions of the TOE.

There is significant more effort spent by the developer in addition to the security specific testing:

- New features that are implemented in the TOE have to follow the strict development procedures. This includes, that in parallel to the design, test cases need to be written. This is done by creating test variation lists, i.e. checking what variations of inputs, configurations etc. need to be tested, and writing test cases. The whole process is shadowed by review cycles ensuring a broad agreement, and coverage of all necessary test scenarios. If the design documentation points out that other parts of the system may be affected by the new feature, test cases are written to verify that there is no negative impact. Tests must complete successfully before the new feature is approved.
- If errors are reported, the TOE gets fixed by the developer. After fixing the bug and informal testing by the developer, the newly built driver is tested to verify that the bug is fixed. Normal regression tests ensure that the TOE as a whole is still functional.
- New drivers are tested using the System Assurance Kernel (SAK), which is also included in the FTP06 test suite. SAK is used for rigorous and continuous testing of the TOE. SAK provides a pseudo-random stream of instructions from a customizable set of instructions that are issued to a logical partition thus simulating a running application. The tool would reveal unexpected system behaviour during the intense test runs on the TOE, e.g. if some processor instructions are not properly simulated by the TOE. Running SAK successfully for a long period without crash and without detecting unexpected behaviour, gives a rather good confidence that the TOE is working correctly.

As determined by the evaluator, there are no specific configuration requirements for the TOE to be tested in its evaluated configuration apart from running the tests on one of the hardware platforms listed in the ST using the appropriate version of the TOE and configuring the separation conditions as explicitly required by assumption A.Sep_Strength and Appendix B of [9].

Additional requirements and assumptions from the ST may be neglected for testing since they have been considered to have no impact on the testing itself nor do they impact the security functionality of the TOE.

The evaluator concluded that the configuration chosen for developer testing was in accordance with the evaluated configuration as defined by the ST [6].

The tests performed by the developer were at the level of the modules of the TOE design.

The actual test results obtained by the developer during the developer testing performed in October 2020 matched the expected test results laid down in the test documentation. Also, the SAK testing performed did not return any deviation from the z/Architecture definition.

7.3.   Evaluator Testing Effort

The following testing was performed by the evaluator:

a) **TOE test configurations:**

The tests were performed on the following systems:

- IBM z15 server model T01 (machine type 8561) at microcode driver level D41C with bundle level H13/S21b.

- IBM z15 server model T02 (machine type 8562) at microcode driver level D41C with bundle level H13/S21b.

This configuration was consistent with the platform configuration given in the ST.

The correct driver level was confirmed by the evaluator using the System Information Panel on the Support Element and the Console Information Panel on the HMC while being logged on in SERVICE mode. The respective panels stated driver levels as "41" with bundle levels "S21b" and "H13", respectively, which matches the TOE version stated in the ST.

The general machine configuration was modified on a test-specific basis (e.g. by defining specific IOCDS) to adapt the machine configuration to the test purpose. As a result of this setup, the TOE at any time was in its evaluated configuration when performing the evaluator tests.

b) **Subset size chosen; selection criteria for the interfaces that compose the subset; interfaces tested; developer tests performed:**

The evaluator performed a subset of the developer test suite, deliberately skipping AK testing, which has already been confirmed to be effective by multiple evaluations. The sampled subset chosen was considered appropriate in size and coverage.

The following security functions as stated in the ST were subject to testing:

1. Identification and Authentication

2. Access Control and Information Flow Control

3. Audit and Accountability

4. Authorized Administration

5. Authorized Operations

6. Object Reuse

7. Reliability of Service

8. Self Test

As a result of testing the above mentioned security functions, the following interfaces (TSFI) have been included in the evaluator testing:

1. GUI as part of testing of all security functions

2. z/Architecture as part of tests related to security function Authorized Operations

3. SCLP as part of tests related to all tested security functions except Self Test

4. CHSC as part of tests related to security functions Authorized Operations and Object Reuse

5. IOCP as part of tests related to security function Access Control and Information Flow Control

6. SIE as part of all tests that involve running LPARs[8]

The subset chosen by the evaluator covers all interfaces to the TOE security functions.

In addition to repetition of developer tests, the evaluator applied variations to the test steps and input data and observed the deviating results of the TOE.

c) **Verdict for the activity:**

The overall judgment on the results of testing during the evaluation is that all security tests passed, i.e. the actual results achieved by the evaluator either exactly matched the expected results, or, in case of test variations, matched the expectation of the evaluator.

By using developer tests as base for independent testing, the evaluator achieved the same test depth as the developer when performing the developer tests. Therefore, the tests performed by the evaluator in October 2020 were at the level of the modules 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 [6].

7.4. Evaluator Penetration Testing

The evaluator did neither devise nor conduct additional penetration testing apart from his source code analysis performed with respect to an identified potential vulnerability. That analysis at level of the LPAR LIC source code was based on an assumed misuse of SCLP in order to gain unauthorized access to storage areas actually allocated to partitions other than the partition issuing the SCLP. Examination of the implementation revealed that no such penetration is feasible.

8.   Evaluated Configuration

This certification covers the following configurations of the TOE:

The Target of Evaluation is IBM PR/SM for IBM z15 T02 and IBM LinuxONE III LT2 Systems at driver level D41C with bundle level H13/S21b. The TOE is firmware only and is accompanied by guidance documentation. The items listed in table 2 of this report represent the TOE.

The TOE can be run on a number of hardware models all belonging to the IBM z15 or LinuxONE III server family. The various machine models as stated in section 1.5.3 of [6] are not part of the TOE but provide the underlying abstract machine for TOE operation.

---

[8] Note that SIE is a TSFI not accessible from the outside but invoked whenever a logical partition is operative.

The supported machine models differ with respect to the number and type of use of available central processors. However, those differences have no impact on the validity of the evaluation activities performed.

The evaluated configuration of the TOE is defined by the mandatory configuration requirements to be met as stated in section "Trusted Configuration" in Appendix B of [9]. The [6] directly 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) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5 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-1133-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was laid on verification that security functionality of the TOE has not been impacted by introduction of a new hardware platform and other functional changes applied.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
                          Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
                          EAL 5 augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5

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

9.2.   Results of cryptographic assessment

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

10.   Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of

Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

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. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. 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
CHSC	Channel Subsystem Call
CPC	Central Processor Complex
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMC	Hardware Management Console
IOCDS	Input/Output Configuration Dataset
IOCP	Input/Output Configuration Program
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LIC	Licensed Internal Code
LPAR	Logical Partition
PP	Protection Profile
PR/SM	Processor Resource/Systems Manager™

SAR	Security Assurance Requirement
SE	Support Element
SIE	Start Interpretive Execution
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

I/O Configuration Data Set - This is a system file that defines the available logical partitions, and the allocation of the available the I/O devices to the defined logical partitions.

Informal - Expressed in natural language.

Logical Partition - A virtual machine which runs on the host system. It has a unique identifier (the zone number) and name. A logical partition can be both an object and a user of the system. A logical partition has attributes determining whether the logical partition is authorized for various actions. Other attributes define the amount of logical processor and storage resources to be allocated to the partition, and the scheduling parameters for the partition's processors. The possible logical partitions are defined in the current configuration object. Only activated logical partitions may use the system.

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

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM),
Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-
Produkte) and Scheme documentation on requirements for the Evaluation Facility,
approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also
on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1160-2021, Version 20.2a, 2021-04-06, PR/SM for IBM
z15 T02 and IBM LinuxOne III LT2 Security Target, IBM Corporation

[7] Evaluation Technical Report, Version 5, 2021-04-06, Final Evaluation Technical
Report, atsec information security GmbH (confidential document)

[8] z15 System Hardware Management Console Operations Guide, Version 2.15.0,
2020-05-01, IBM Corporation

[9] IBM Z Processor Resource/Systems Manager Planning Guide, Version SB10-7175-
01b, 2021-01-29, IBM Corporation

[10] z15 System Support Element Operations Guide, Version 2.15.0, 2020-05-01, IBM
Corporation

[11] IBM Z - Input/Output Configuration Program User's Guide for ICP IOCP, Version
SB10-7172-04, 2020-04-14, IBM Corporation

[12] IBM Z Stand-Alone Input/Output Configuration Program User's Guide, Version
SB10-7173-01, 2019-09-13, IBM Corporation

[13] IBM Z 8561 Service Guide, Version GC28-6998-00b, 2020-01-17, IBM Corporation

[14] IBM Z 8561 Installation Manual for Physical Planning, Version GC28-7002-00d,
2020-03-30, IBM Corporation

[15] IBM Z 8561 Installation Manual All Models, Version GC28-6997-00f, 2020-05-14,
IBM Corporation

[16] IBM Z 8562 Service Guide, Version GC28-7010-00, 2020-04-16, IBM Corporation

---

[9]specifically

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

- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 &
CCv3.1) and EAL 6 (CCv3.1)

- AIS 38, Version 2, Reuse of evaluation results

[17]   IBM Z 8562 Installation Manual for Physical Planning, GC28-7011-00, 2020-04-14, IBM Corporation

[18]   IBM Z 8562 Installation Manual All Models, GC28-7009-00, 2020-05-13, IBM Corporation

C.   **Annexes**

List of annexes of this certification report   31 / 31

Annex A: Security Target provided within a separate document.

Note: End of report