Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 6/19
(Certification No.)

Prodotto: **IBM z/OS Version 2 Release 3**
(Product)

Sviluppato da: **IBM Corporation**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 31 luglio 2019

Common Criteria

Fino a EAL2 *(Up to EAL2)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM z/OS Version 2 Release 3

OCSI/CERT/ATS/01/2018/RC

Version 1.0

31 July 2019

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	31/07/2019

2 Table of contents

3 Acronyms

AES	Advanced Encryption Standard
APAR	Authorized Program Analysis Report
API	Application Programming Interface
BCP	Base Control Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPACF	Central Processor Assist for Cryptographic Function
cPP	collaborative Protection Profile
DAC	Discretionary Access Control
DASD	Direct Access Storage Device
DES	Data Encryption Standard
DFSMS	Data Facility Storage Management Subsystem
DPCM	Decreto del Presidente del Consiglio dei Ministri
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IPL	Initial Program Load
IUCV	Inter User Communication Vehicle
IT	Information Technology
JES2	Job Entry System 2
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza

MAC	Mandatory Access Control
NIS	Nota Informativa dello Schema
NJE	Network Job Entry
OCSI	Organismo di Certificazione della Sicurezza Informatica
PKI	Public Key Infrastructure
PP	Protection Profile
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMF	System Management Facilities
SHA	Secure Hash Algorithm
SRB	Service Request Block
SSL	Secure Sockets Layer
SSH	Secure SHell
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO	Time Sharing Option
USS	UNIX System Services

4 References

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[ETR] Final Evaluation Technical Report “IBM z/OS Version 2 Release 3”, OCSI-CERT-ATS-01-2018_ETR_190614_v3, Version 3, atsec information security GmbH, 14 June 2019

[ETR-TEST] Evaluation Technical Report - Assurance Class ATE, Version: 3, Date: 2019-04-18

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 01 June 2010

[OSPP-LS] OSPP Extended Package – Labeled Security, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[OSPP-EIA] OSPP Extended Package – Extended Identification and Authentication, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[MLSGUIDE] z/OS Version 2 Release 3 - Planning for Multilevel Security and the Common Criteria, Version: GA32-0891-30, Date: 2019-05-15

[RFC4217] “Securing FTP with TLS”, October 2005

[ST] IBM z/OS Version 2 Release 3 Security Target, Version 12.10, IBM Corporation, 25 February 2019

[ZARCH] “z/Architecture Principles of Operation”, Version: SA22-7832-11, Date: September 2017

5 Recognition of the certificate

5.1 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA]) was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “IBM z/OS Version 2 Release 3”, developed by International Business Machines Corp. (IBM).

z/OS Version 2 Release 3 (also referred to in the following as z/OS V2R3 or z/OS) is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "IBM z/OS Version 2 Release 3" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	IBM z/OS Version 2 Release 3
Security Target	IBM z/OS Version 2 Release 3 Security Target, Version 12.10 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	Operating System Protection Profile v2.0 [OSPP] with [OSPP-LS] and [OSPP-EIA] Extended Packages (EP).
Evaluation starting date	13 February 2018
Evaluation ending date	17 June 2019

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are met.

7.3 Evaluated product

This paragraph summarizes the main functional and security features of the TOE; for a detailed description, refer to the Security Target [ST].

The Target of Evaluation (TOE) is z/OS Version 2 Release 3 with the following elements:

- z/OS Version 2 Release 3 (V2R3)
- IBM Print Services Facility^{TM} Version 4 Release 5 for z/OS

- Overlay Generation Language Version 1 Release 1

z/OS is a general-purpose, multi-user, multi-tasking operating system for enterprise computing systems. Multiple users can use z/OS simultaneously to perform a variety of functions that require controlled, shared access to the information stored on the system.

z/OS can be configured for two modes of operation, a Standard Mode and a Labeled Security Mode.

The Security Target [ST] on which the evaluation activity was based is conformant to the certified Protection Profile "Operating System Protection Profile (OSPP)" [OSPP] and its extended packages for Labeled Security ([OSPP-LS]) and Extended Identification and Authentication ([OSPP-EIA]).

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria ([CC]). z/OS meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [ST], section 7.1. These are selected from Common Criteria Part 2 and from OSPP, where some SFRs have been defined as extended components. Thus, z/OS is CC part 2 extended. There are also requirements relevant for the operational environment of the TOE which are outlined following an SFR-like notation in the Security Target ([ST], chapter 6).

The TOE security functions are described more in detail in section 7.3.2.3.

For more details concerning the software version defining the TOE, the abstract machine the TOE runs on and the user guidance documentation delivered with the TOE please refer to the remainder of this report.

7.3.1 TOE Architecture

7.3.1.1 TOE general overview

The TOE is one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine, the most of which not being part of the TOE, can be provided by one of the options in section 9.3.2.

Multiple instances of z/OS may be connected in two ways, i.e. in a basic sysplex or in a parallel sysplex with the instances sharing their RACF database. The individual instances of z/OS can be run alone or within a network as a set of cooperating hosts, operating under and implementing the same set of security policies. For more details, refer to the Security Target [ST].

The abstract machine defined by the z/Architecture is not part of the TOE but belongs to the TOE operational environment. Nevertheless, the correctness of separation and memory protection mechanisms implemented in the abstract machine is analyzed as part of the evaluation, since those functions are crucial for the security of the TOE. The cryptographic instructions implementing the AES, Triple-DES, SHA-1 and SHA-2 algorithms provided by the CPACF feature of the processor have been also analyzed in the evaluation to correctly support the TSF.

Transmission Control Protocol/Internet Protocol (TCP/IP) network services, connections and communication that occur outside of a sysplex are restricted to one security label; that is, each system regards its peers as single-label hosts. Other network communication is disallowed, with the exception of the Job Entry System 2 (JES2) Network Job Entry (NJE) protocol.

Most of the TOE security functions (TSF) are provided by the z/OS operating system Base Control Program (BCP) and the Resource Access Control Facility (RACF), a z/OS component that is used by different services as the central instance for identification and authentication and for access control decisions. z/OS comes with management functions that allow configuring of the TOE security functions to tailor them to the customer's needs.

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

In its evaluated configuration, z/OS Version 2 Release 3 allows two modes of operation: a standard mode meeting all requirements of the Operating System Protection Profile base [OSPP] and its extended package for Extended Identification and Authentication [OSPP-EIA], and a more restrictive mode called Labeled Security Mode, which additionally meets all requirements of the OSPP extended package for Labeled Security [OSPP-LS]. 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.

CPACF functionality is provided by processor instructions of the underlying abstract machine, which are treated as part of the TSF. Cryptographic functionality provided by specific cryptographic coprocessors on CryptoExpress cards is not part of the TOE.

Cryptographic functions implemented by the CEX3, CEX4, CEX5 or CEX6 coprocessors are still part of the TOE operational environment and therefore have not been evaluated to the degree required by the target assurance level in this evaluation. In order to use only the cryptographic functions provided by the TOE a user needs to configure the TOE such that either no cryptographic coprocessor is installed or that the use of those functions is disabled.

A user who wants to use cryptographic functions provided by a coprocessor should be aware that, although those functions have been tested during the evaluation for functional correctness, no further analysis of the design and implementation of those cryptographic functions implemented on the coprocessors has been performed in this evaluation. Especially, no analysis for potentially exploitable side channels of the implementation of the cryptographic functions of the coprocessors has been performed.

7.3.1.2 Major software components of the TOE

z/OS Version 2 Release 3 includes the following main subsystems:

- **Base Control Program (BCP)**: BCP is the core subsystem of z/OS responsible for (real and virtual) storage management, management of address spaces, tasks and SRBs, scheduling, handling of interrupts and exceptions, synchronization and other basic services.

- **System Management Facilities (SMF)**: SMF collects and records system and job-related information that the installation can use for: billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, maintaining system security.

- **Data Facility Storage Management Subsystem (DFSMS)**: System-managed storage is the IBM automated approach to managing storage resources. It uses software programs to manage data security, placement, migration, backup, recall, recovery, and deletion so that current data is available when needed, space is made available for creating new data and for extending current data, and obsolete data is removed from storage.

- **Resource Access Control Facility (RACF)**: RACF is the central component within z/OS responsible for the identification and authentication of users, for access control, and for the generation of security event related audit records (which RACF sends to SMF to get those audit records included in the SMF audit).

- **Integrated Cryptographic Service Facility (ICSF)**: ICSF is the main provider of basic cryptographic services within z/OS and for the functions specified in the SFRs. It is utilized for the basic cryptographic services for certificate/key generation for certificates used for user authentication as well as certificates used in the establishment of trusted channels.

- **Communications Server**: The Communications Server component of z/OS is responsible for the implementation of the TCP/IP stack and the higher level protocols (except for SSH). As security functionality the Communications Server provides: access control on the objects, trusted channels, IP filtering capabilities.

- **Directory Services**: The z/OS Lightweight Directory Access Protocol (LDAP) server, part of IBM Tivoli Directory Server for z/OS (IBM), is based on a client/server model that provides client access to an LDAP server. An LDAP directory provides an easy way to maintain directory information in a central location for storage, update, retrieval, and exchange.

- **Public Key Infrastructure (PKI)**: The z/OS Cryptographic Services allow z/OS to establish a PKI infrastructure and serve as a certificate authority for internal and external users, issuing and administering digital certificates in accordance with organization's policies.

- **Job Entry Subsystem 2 (JES2)**: z/OS uses a job entry subsystem (JES) to receive jobs into the operating system, schedule them for processing by z/OS, and to control their output processing. JES2 is descended from HASP (Houston automatic spooling priority). HASP is defined as a computer program that provides supplementary job management, data management, and task management functions such as scheduling, control of job flow, and spooling.

- **Time Sharing Option (TSO/E)**: TSO/E is the primary user interface to the z/OS system. TSO/E provides numerous commands for both end users and system programmers that allow them to interact with TSO/E and the z/OS system.
- **UNIX System Services (USS)**: The z/OS support for z/OS UNIX enables two open systems interfaces on the z/OS operating system: an application program interface (API), which is XPG4 UNIX 1995 conforming and an interactive z/OS shell interface.
- **OpenSSH:** Secure Shell (SSH) is a network protocol which provides an alternative for insecure remote login and command execution facilities, such as telnet, rlogin and rsh. SSH encrypts traffic in both directions, preventing traffic sniffing and password theft. The SSH that is provided for z/OS is a port of OpenSSH 6.4p1, available from www.openssh.org.

7.3.2 TOE security features

7.3.2.1 Security policy

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

- Identification and Authentication,
- Access Control,
- Communication Security,
- Security Management,
- Auditing,
- Object Reuse,
- TSF Protection,
- Confidentiality Protection of Data Sets.

7.3.2.2 Operational environment security objectives

The assumptions for the correct operation of the TOE defined in the Security Target [ST] and some aspects of Threats and Organisational Security Policies are not covered by the TOE. These aspects lead to specific security objectives to be fulfilled by the TOE operational environment. The following objectives for the operational environment have to be assured:

- Those responsible for the TOE are competent and trustworthy.
- Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner.
- Those responsible for the TOE must establish and implement procedures to ensure that the system is distributed, installed and configured in a secure manner.
- Authorized users of the TOE must ensure that the comprehensive diagnostics facilities are invoked at every scheduled preventative maintenance period.
- Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack.
- Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure system recovery from failure or other discontinuity.
- The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

For a complete description of the security objectives for the TOE operational environment, please refer to section 4.2 of the z/OS V2R3 Security Target [ST].

7.3.2.3 Security functions

The TOE Security Functional Requirements are implemented by the TOE Security Functions, summarized in Table 1. For more details on the security functionality provided by the TOE please refer to the Security Target [ST].

TOE Security Function	**implementation**
Identification and authentication	Alphanumeric RACF user ID and system-encrypted password or password phrase.
	Alphanumeric RACF user ID and PassTicket encompassing the user ID, the requested application name, and the current date/time.
	X.509v3 digital certificate with TLS-based client authentication mapped to a RACF user ID.
	Kerberos^{TM} v5 ticket mapped through the TOE-provided GSS-API programming services or alternate functions mapped to a RACF user ID.
	LDAP LDBM bind DN or LDAP ICTX or SDBM bind DN together with a RACF password or password phrase mapped to RACF user ID and the password/phrase.
	Digital certificates presented to LDAP over TLS mapped to a RACF user ID.
Access Control	Discretionary Access Control (DAC): z/OS supports access controls that are capable of

TOE Security Function	implementation
	enforcing access limitations on individual users and data objects. Discretionary access control (DAC) allows individual users to specify how such resources as direct access storage devices (DASDs), tape data sets and tape volumes are to be shared.
	Mandatory Access Control (MAC): mandatory access control (MAC) functions are required for Labeled Security Mode, which impose additional access restrictions on information flow on security classification. Users and resources can have a security label specified in their profile. The access control ensures that users can only read labeled information if their security labels dominate the information's label, and that they can only write to labeled information containers if the container's label dominates the subject's, thus implementing the Bell-LaPadula model of information flow control. Security label checking will also occur in standard operation mode, if the administrator has configured security labels and if resources and users have labels assigned to them.
Communication security	z/OS provides means of secure communication between systems sharing the same security policy. z/OS TCP/IP provides the means for associating labels with all IP addresses in the network and for defining Virtual IP addresses (VIPAs) with specific labels on a multilevel system. z/OS TCP/IP considers the user's label when choosing a source address for communications. z/OS UNIX System Services also provides the means to run up to eight instances of the z/OS TCP/IP stack which can each be restricted to a single label. Either of these approaches can be used to ensure that most communications between multilevel systems do not use a multilevel address on both ends and thereby avoid the need for explicit labeling. TCP/IP-based communication can be further controlled by the access control function for TCP/IP connections, which allows controlling of the connection establishment based on access to the TCP/IP stack in general, individual network address and individual ports on a per-application or per-user basis. Additional means implemented in z/OS for securing the communication are • TLS v1.1 and v1.2 optionally with x.509-based client authentication • IPSec with IKE key exchange method • Kerberos^{TM} version 5 networking protocols • OpenSSH, an SSH v2 implementation including ssh, scp and sftp
Security management	z/OS provides a set of commands and options to adequately manage its security functions, the capability of managing users, groups of users, general resource profiles, and RACF SETROPTS options via the z/OS LDAP server. z/OS also provides a Java class that allows Java programs to issue commands to manage users and groups. Both the LDAP and the Java class ultimately create a RACF command and pass it to RACF using a programming interface, and then RACF runs the command using the identity associated with the LDAP session or the Java program. z/OS recognizes several authorities that are able to perform the different management tasks related to the its security. Security administrators are in charge of managing general security options, MAC attributes, management, users and their security attributes and can delegate group security administrators or users to manage groups. Security administrators can define what audit records are captured by the system and auditors manage the parameters of the audit system and can analyze the audit trail. Users can change their own passwords or password phrases, their default groups, and their user names (but not their user IDs) and choose their security labels at login, for some login methods. Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.
Auditing	The RACF component of z/OS provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. Audit records are collected by the System Management Facilities (SMF) into an audit trail, which is protected from unauthorized modification or deletion by the DAC and (in Labeled Security Mode) MAC mechanisms. In addition to writing records to the audit trail,

TOE Security Function	implementation
	messages can be sent to the security console to immediately alert operators of detected policy violations. RACF provides SMF records for all RACF-protected resources (either “traditional” or z/OS UNIX-based) as well as for LDAP-based resources. Remote applications can use an LDAP interface to request that RACF generate an SMF audit record. For reporting, auditors can unload all or selected parts of the SMF data for further analysis in a human-readable formats and can then upload the data to a query or reporting package, such as DFSORT^{TM} if desired. The system can be configured to halt on exhaustion of audit trail space to prevent audit data loss. Operators are warned when audit trail space consumption reaches a predefined threshold.
Object reuse	Reuse of protected objects and of storage is handled by various hardware and software controls, and by administrative practices. All memory content of non-shared page frames is cleared before making it accessible to other address spaces or data spaces. DASD data sets can be purged during deletion with the RACF ERASE option and tape volumes can be erased on return to the scratch pool. All resources allocated to UNIX objects are cleared before reuse. Other data pools are under strict TOE control and cannot be accessed directly by normal users.
TSF protection	TSF protection is based on several protection mechanisms that are supported by the underlying abstract machine z/OS is executed upon. In addition to the protection mechanism of the underlying abstract machine, z/OS also uses software mechanisms like the authorized program facility (APF), specific privileges for programs in the UNIX system services environment to protect the TSF.
Confidentiality Protection of Data Sets	With z/OS confidentiality protection of data sets, users can encrypt data at rest without requiring application changes. z/OS data set encryption through RACF commands and SMS policies allows the administrator to identify the data sets or groups of data sets that require encryption. The administrator can specify an encryption key label, which refers to an encryption key. Both the key label and encryption key must exist in the ICSF key repository (CKDS). With data set encryption, the administrator is able to protect viewing the data in the clear. This is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

Table 1 – TOE Security Functions

7.3.3 Cryptographic functions

The Cryptographic Functions are enlisted in Table 2:

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
CPACF						
1	Cryptographic Primitive (CPACF)	TDES in CFB, OFB, and CBC-CS modes	FIPS 46-3 (TDES), NIST Special Publication 800-38A, 2001 Edition (CFB and OFB modes of operation), Addendum to NIST SP 800-38A, October 2010 (CBC-CS mode of operation), NIST Special Publication 800-38D (GCM mode of operation) Note: the CBC-CS mode is implemented in accordance with [NIST-CBC-CS_PROP]. This mode is not used by the TSF for any security function claimed in the ST.	|k|=168	No	CPACF instructions
2	Cryptographic Primitive CPACF)	AES in CFB, OFB, and CBC-CS modes	FIPS 197 (AES), NIST Special Publication 800-38A, 2001 Edition (CFB and OFB modes of operation), Addendum to NIST SP 800-38A, October 2010 (CBC-CS mode of operation), NIST Special Publication 800-38D (GCM mode of operation)	|k|=128, 192, 256	yes	CPACF instructions
3	Cryptographic Primitive (CPACF)	SHA-1	FIPS 180-4	none	No	CPACF instructions
4	Cryptographic Primitive (CPACF)	SHA-{224, 256, 384, 512}	FIPS 180-4	none	yes	CPACF instructions
ICSF / CLIC						
5	Cryptographic Primitive	RSA signature generation	[PKCS#1 v2.1] (RSA)	Moduluslength= 2048, 4096	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
6	Cryptographic Primitive	RSA signature generation	[PKCS#1 v2.1] (RSA)	Moduluslength= 1024	No	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
7	Cryptographic Primitive	RSA key generation		Moduluslength= 2048, 4096	yes	ICSF CSFPGKP/CSFPGKP6 function
8	Cryptographic Primitive	RSA key generation		Moduluslength= 1024	No	ICSF CSFPGKP/CSFPGKP6 function
9	Cryptographic Primitive, Authentication	RSA signature verification, used by RACF for certificate based user authentication (which calls ICSF)	[PKCS#1 v2.1] (RSA)	Moduluslength= 2048, 4096	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function) (primitive also used for certificate based user authentication)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
10	Cryptographic Primitive, Authentication	RSA signature verification, used by RACF for certificate based user authentication (which calls ICSF)	[PKCS#1 v2.1] (RSA)	Moduluslength= 1024	No	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function) (primitive also used for certificate based user authentication)
11	Cryptographic Primitive	DSA signature generation	[FIPS 180-4] (DSA)	Plength= 1024, Qlength= 160	No	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
12	Cryptographic Primitive	DSA signature verification	[FIPS 180-4] (DSA)	Plength= 1024, Qlength= 160	No	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
13	Cryptographic Primitive	ECDSA signature generation	[FIPS 180-4] (ECDSA)	Key sizes corresponding to the used NIST elliptic curves secp{224, 256, 384, 521}r1 (SEC2)	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
14	Cryptographic Primitive	ECDSA signature verification	[FIPS 180-4] (ECDSA)	Key sizes corresponding to the used NIST elliptic curves secp{224, 256, 384, 521}r1 (SEC2)	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
15	Cryptographic Primitive	ECDSA signature generation	[ISO 14888-3] (ECDSA) (RFC 5639) BrainPool curves	Key sizes corresponding to the used elliptic curves brainpoolP{224, 256, 320, 384, 512}r1	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
16	Cryptographic Primitive	ECDSA signature verification	[ISO 14888-3] (ECDSA) (RFC 5639) BrainPool curves	Key sizes corresponding to the used elliptic curves brainpoolP{224, 256, 320, 384, 512}r1	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
17	Key agreement	ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{224, 256, 384, 521}r1 (SEC2) and brainpoolP{224, 256, 320, 384, 512}r1 (RFC 5639)	yes	ICSF PKCS#11 CSFPDVK/CSFPDVK6 function
System SSL						
18	Cryptographic Primitive	DSA signature generation	[FIPS 180-4] (DSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	L=1024, N=160	No	System SSL function gsk_sign_data
19	Cryptographic Primitive	DSA signature verification	[FIPS 180-4] (DSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	L=1024, N=160	No	System SSL function gsk_verify_data
20	Trusted Channel	TLS V1.1	[RFC4346] (V1.1)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
21	Trusted Channel	TLS V1.2	[RFC5246] (V1.2)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
Communications Server 390 (CS390)						
22	Trusted Channel	IPSec	[RFC4301] through [RFC4305], [RFC4308], and [RFC4835]	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
OpenSSH						

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
23	Authentication	RSA (SSH)	[RFC4253] (SSH)	Moduluslength= 2048, 4096	Yes	Implemented in the OpenSSL library
24	Authentication	DSA (SSH)	[RFC4253] (SSH)	L=1024, N=160	No	Implemented in the OpenSSL library
25	Key agreement	DH (SSH)	[RFC4253] (SSH)	Plength 1024	No	Implemented in the OpenSSL library
26	Key agreement	ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{224, 256, 384, 521}r1 (SEC2) and brainpoolP{224, 256, 320, 384, 512}r1 (RFC 5639)	yes	ICSF PKCS#11 CSFPDVK/CSF PDVK6 function
27	Key agreement	DH (SSH)	[RFC4253] (SSH)	Plength 1024	No	Implemented in the OpenSSL library
28	Trusted Channel	SSH V2	[RFC4250] (lists the RFCs defining SSH V2)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	

Table 2 – Cryptographic functions

7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for secure usage of the TOE is delivered to the customer together with the product. The guidance documentation ([MLSGUIDE]) contains all the information for installation, configuration and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims strict conformance to [OSPP] Protection Profile and [OSPP-LS] and [OSPP-EIA] Extended Packages.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] including all requirements in EAL4 package augmented by ALC_FLR.3.

All Security Functional Requirements (SFRs) have been selected or derived by extension from CC Part 2 [CC2]. In particular, the Security Target claims strict conformance to the [OSPP] PP and [OSPP-LS] and [OSPP-EIA] Extended Packages. As for [OSPP] three extended components are included:

- FCS_RNG.1: Random number generation,
- FDP_RIP.3: Full residual information protection of subjects, and

- FIA_USB.2: Enhanced user-subject binding.

As for [OSPP-EIA] two extended components are included:

- FIA_UAU.8: Authentication policy decisions, and
- FIA_UID.3: Identification policy decisions.

Users should refer to the Security Target [ST] for a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that it constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body (OCSI) has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security GmbH.

The evaluation was completed on 17 June 2019 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 19 June 2019. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist. It remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR], issued by the LVS atsec information security GmbH, and the documents required for the certification, and considering the evaluation activities which was carried out, the Certification Body (OCSI) concluded that TOE “IBM z/OS Version 2 Release 3” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 3 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_FLR.3.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass

Assurance classes and components		**Verdict**
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	Pass
Tests	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 3 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (“Statement of Certification”).

Potential customers of the product “IBM z/OS Version 2 Release 3” are suggested to properly understand the specific purpose of the certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in section 4.2 of the Security Target [ST]. Potential customers are advised to check that they meet the identified requirements and to pay attention to the recommendations contained in this Report.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A - Guidelines for secure usage of the TOE includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([MLSGUIDE]).

It is assumed that the TOE operates securely if the assumptions about the operational environment described in par. 4.2 of the document [TDS] are satisfied. In particular, it is assumed that the admnistrators of the TOE are adequately trained to the correct usage of the TOE and chosen among the trusted personnel of the organizaition. The TOE is not realized to counter threats from unexperienced, non-trusted or negligent adminstrators.

It should also be noted that the security of the TOE's operations is conditional on the correct functioning of the hardware platforms on which the TOE is installed and of all the reliable external IT systems on which the TOE is based to support the implementation of its security policy. The operational environment specifications are described in the document [ST].

9 Annex A - Guidelines for secure usage of the TOE

This Annex provides considerations particularly relevant to the potential customers of the TOE.

9.1 TOE delivery

The evaluated version of z/OS can be ordered via an IBM sales representative or via the ShopzSeries web application (http://www.ibm.com/software/shopzseries). When filing an order via (secured) internet services, IBM requires customers to have an account with a login name and password. Registration for such an account in turn requires a valid customer ID from IBM.

No	Type	Identifier	Release	Form of Delivery
z/OS Version 2 Release 3 (z/OS V2.3, program number1 5650-ZOS)[1] Common Criteria Evaluated Base Package				
1	SW	z/OS V2.3 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R3	Tape
2	DOC	z/OS V2.3 Program Directory	GI11-9848-02	Hardcopy
3	DOC	z/OS V2.3 Documentation Collection Hashsums for download (ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/c27843007-CC_Eval.zip) SHA224: 84851b31fbf1bb4056944796b6f766c9d7ba1d36b4c26cf62d989c12 SHA256: 53d4a0ba82a3b67d031f3876fbceb88186b7d1ff2fe6af4ca6e8f7a7a422546d SHA384: d8d8b6c595d13ecb7a19f056395f62ea155a848c8f07a51d63ce812a7c485e73a9b83d26fee16cf67d6c452aaa794ef2 SHA512: 6c7207620867fc2d9ff80e72e31115a568c9606cf3b866a962739a297b32ab9206e4ead0bc2ebbb244f98c10b0cf906973b91		
4	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
5	DOC	Memo to Customers of z/OS V2.3 Common Criteria Evaluated Base	n/a	Hardcopy
6	DOC	z/OS V2.3 Planning for Multilevel Security and the Common Criteria; Document Number GA32-0891-30 SHA256 hashsum of the document:: 48cee926a44883fd7cb93b49e995b7f19f5da309b48a24aaef917a9738001b8f		
IBM Print Services Facility^{TM} Version 4 Release 5 for z/OS (PSF V4.5.0, program number 5655-M32)				
7	SW	IBM Print Services Facility^{TM} Version 4 Release 5 for z/OS (PSF V4.5.0, program number 5655-M32)	V4R5	Tape
8	DOC	Program Directory PSF V4.5 Base	GI13-3005-00	Hardcopy
OGL/370 V1.1.0 (program number 5688-191)				
9	SW	Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)	V1R1	Tape
10	DOC	OGL/370 V1.1.0: Getting Started	G544-3691-00	Hardcopy

[1] The "program number" (or "product number") is IBM's technical identification of the product "z/OS". It is used for order and license purposes and does not uniquely identify the TOE. The string z/OS Version 2 Release 3 uniquely identifies the TOE.

No	Type	Identifier	Release	Form of Delivery
11	DOC	OGL/370 V1.1.0: LPS	G544-3697-00	Hardcopy
12	DOC	OGL: Command Summary and Quick Reference	S544-3703-01	Hardcopy
13	DOC	Program Directory OGL/370	GI10-0212-01	Hardcopy
Additional Media				
14	SW	PTFs for the following APARs (required): • OA52110 (PTF UA93049), • OA52192 (PTF UA93490), • OA52722 (PTF UA93924), • OA52830 (PTF UA92871), • OA52834 (PTF UA94035), • OA52932 (PTF UA93783), • OA53036 (PTF UA93779), • OA53223 (PTF UA94801), • OA53626 (PTF UA95087), • OA53643 (PTF UA94136), • OA53716 (PTF UA95334), • OA53755 (PTF UA94051), • OA53759 (PTF UA96307), • OA53764 (PTF UA94053), • OA53775 (PTF UA93986), • OA53792 (PTF UA94309), • OA53799 (PTF UA93869), • OA53809 (PTF UA94644), • OA53813 (PTF UA95903), • OA53818 (PTF UA95262), • OA53856 (PTF UA94198), • OA53930 (PTF UA95160), • OA53934 (PTF UA94422), • OA53946 (PTF UA94612), • OA53961 (PTF UA95898), • OA53962 (PTF UA95899), • OA54024 (PTF UA93979), • OA54059 (PTF UA94332), • OA55396 (PTF UA97378), • OA55435 (PTF UA96829), • OA55444 (PTF UA96532), • OA55483 (PTF UA96530), • OA55692 (PTF UA96528), • OA56409 (PTF UA97819), • OA56418 (PTF UA97888), • PH04246 (PTF UI59826), • PI82795 (PTF UI48034), • PI86170 (DOC), • PI87297 (PTF UI50688), • PI87424 (PTF UI50691), • PI87427 (PTF UI50685), • PI87482 (PTF UI53437), • PI87585 (PTF UI52347), • PI87635 (PTF UI50686), • PI87646 (PTF UI50680), • PI87652 (PTF UI50681), • PI89400 (PTF UI52529), These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)	n/a	Electronic

Table 4 – TOE deliverables

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

The download of the TOE guidance (see item#3 in Table 4 above) is described in [MLSGUIDE], i.e. the customer downloads a guidance package from an IBM FTP Server and then verifies the package against the hashsums provided in [MLSGUIDE].

Table 4 contains the items that comprise the different elements of the TOE, including software and guidance.

9.2 Identification of the TOE

The media delivered to the customer are labeled with the product, document and version numbers as indicated in Table 4 and can be checked by the users installing the system.

The TOE reference can be verified by the administrator during initial program load (IPL), when the system identification is displayed on the system console. The operator can also issue the operator command D IPLINFO, to display the z/OS version. The string "z/OS 02.03.00" should be displayed among other information.

9.3 Installation, initialization and secure usage of the TOE

9.3.1 Software installation and configuration

The complete list of SW components to be installed is reported in Table 4. The same software elements are used in the Labeled Security Mode and Standard Mode of operation, except as otherwise noted. The mode of operation is defined by the configuration of the labeling-related options in RACF. Details are described in z/OS Planning for Multilevel Security and the Common Criteria ([MLSGUIDE]).

Installations may choose not to use any of the elements delivered within the ServerPac, but they are required to install, configure, and use at least the RACF and ICSF components of the z/OS Security Server element.

In addition, any software outside the TOE may be added without affecting the security characteristics of the system, if it cannot run:

- in supervisor state
- as APF-authorized
- with keys 0 through 7
- with UID(0)
- with authority to FACILITY resources BPX.DAEMON, BPX.SERVER, or BPX.SUPERUSER
- with authority to UNIXPRIV resources

This explicitly excludes:

- replacement of any element in the ServerPac providing security functions relevant to this evaluation by other third-party products;
- installing system exits that run authorized (supervisor state, system key, or APF-authorized), with the exception of the ICHPWX11 sample and its associated IRRPHREX routine;
- installing IBM Tivoli Directory Server plug-ins that have not been evaluated;
- using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

Note: *The evaluated software configuration is not invalidated by installing and operating other appropriately-certified components that possibly run authorized. However, the evaluation of those components must show that the component and the security policies implemented by the component do not undermine the security policies of the TOE.*

The IBM Tivoli Directory Server for z/OS component may be used as the LDAP server, but:

- For client authentication via digital certificates the administrator must configure the LDAP server to map the certificate to a RACF user ID and to fail the bind if the certificate does not map to a RACF user ID. The allowable LDAP configuration provides three options for forming an LDBM subject:
    - LDAP may use the original DN from the certificate; or
    - LDAP may replace the original DN with an SDBM-format DN based on the RACF user ID; or
    - LDAP may add the SDBM-format DN to the LDAP subject, giving a subject with two DNs, either of which will work in LDAP ACLs.
- Client authentication using the Kerberos mechanism has not been evaluated for LDAP and cannot be used in the evaluated configuration.
- Authentication via passwords stored in LDAP cannot be used. Authentication must occur using RACF passwords or password phrases. Note that if an LDBM bind DN is specified when binding to the server, the password/phrase specified must be for the RACF user ID associated with that bind DN by the LDAP administrator;
- In Labeled Security Mode, only the ICTX or LDBM configurations can be used. In standard mode the LDBM, CDBM, and SDBM back-ends and the ICTX plug-in may be used. Other LDAP back-end configurations and plug-ins have not been evaluated and must not be used.
- (Labeled Security Mode only) Each running instance of the LDAP server must run with a single, non-SYSMULTI, non-SYSNONE, security label. Multiple server instances may run at the same time, with the same or different security labels.

In labeled security mode, each running instance of the HTTP server must run with a security label that is neither SYSMULTI nor SYSNONE.

The SSH daemon sshd may be used, but if used:

- must be configured to use protocol version 2 and either TDES or one of the AES-based cipher suites,
- must be configured in privilege separation mode, and
- must be configured to allow only password-based (including password phrase) authentication of users or public-key based authentication of users with the public keys stored in RACF keyrings. Rhost-based and public-key based user authentication with the keys stored elsewhere may not be used in the evaluated configuration. In Labeled Security Mode sshd should be configured with the SYSMULTI security label.

The Network Authentication Service component of the Integrated Security Services component, if used, and applications exploiting it, must satisfy the following constraints:

- The Network Authentication Service must use the SAF (RACF) registry. The NDBM registry is not a valid configuration for this evaluation.
- Cross Realm Trust relationships with foreign Kerberos realms are allowed, but the foreign KDC must be capable of supporting the same cipher as does the z/OS KDC.
- In order to ensure strong cryptographic protection of Kerberos tickets, Triple DES or AES should be utilized by the z/OS KDC and any KDC participating in a cross-realm trust relationship with the z/OS KDC. DES should only be used in network environments where the threat of cryptographic attacks against the tickets and Kerberos-protected sessions is deemed low enough to justify the use of these weaker encryption protocols.
- Applications supporting Kerberos may use a combination of application specific protocols and the GSS-API functions or the equivalent native platform callable services (the SAF R_TicketServ and R_GenSec callable services) to authenticate clients, and in client-server authentication. Only the Kerberos mechanism may be used by applications that utilize GSS-API or the equivalent native platform functions. The GSS-API and R_GenSec services also enable the encryption of sensitive application messages passed via application specific protocols. These services enable the secure communication between client and server applications. The GSS-API services include the message integrity and privacy functions that validate the authenticity and secure the communications between clients and servers.

The Network File System (NFS) Server may be used, but must be configured with the SAF or SAFEXPORT option, to ensure that all file and directory access (except possibly directory mounting) has appropriate RACF security checks made.

TLS:

- TLS (Transport Layer Security) processing, if used, must use TLS V1.1 or TLS V1.2 protocols. TLS (Transport Layer Security), if used, must use one of the cipher suites listed in the FCS_COP.1(NET) SFR of the ST.

- Any application performing client authentication using client digital certificates over TLS must be configured to use RACF profiles in the RACDCERT or DIGTRING classes or PKCS#11 tokens in ICSF to store the keyrings that contain the application private key and the allowed Certificate Authority (CA) certificates that may be used to provide the client certificates that the application will support. The use of gskkyman for this purpose is not part of the evaluated configuration.

Communications Server:

- The z/OS FTP server and client, and the z/OS TN3270 server, support both manually-configured TLS, or AT-TLS. This evaluation has considered only AT-TLS configurations, and as a result manual configuration of those components to use TLS is not allowed for evaluated configurations.

- The z/OS FTP server and client can support either the protocols from the draft standard for securing FTP with TLS, or the protocols from the formal RFC 4217 level of Security FTP with TLS [RFC4217]. This evaluation has considered only the formal RFC 4217 level of support, and as a result that option must be used in the evaluated configuration.

- The following applications must not be used in Labeled Security configurations, as noted in the Communications Server IP Configuration Guide: HOMETEST command, IUCV, LPD, LPQ command, LPR command, LPRM command, LPRSET command, NCPROUTE, NPF, Portmapper, SMTP, SNMP NetView client, TELNET client command, TESTSITE command, TNF, VMCF, z/OS UNIX Network SLAPM2 subagent, z/OS UNIX OMPROUTE SNMP subagent, z/OS UNIX popper, z/OS UNIX RSVP agent, z/OS UNIX SNMP client command, z/OS UNIX SNMP server and agent, z/OS UNIX Trap Forwarder Daemon.

- IPSec (IP Security) processing, if used, must use the ciphers listed in the FCS_COP.1(NET) SFR.

RACF:

- Do not use the RACF remote sharing facility (RRSF) in remote mode. If you use RRSF in local mode, ensure that command direction cannot be used by taking one of the following actions:

    - Ensure that the RRFSFDATA class is not active.

    - Define the profile DIRECT.* in the RRSFDATA class with UACC(NONE) and no users in the access list.

  Do not use multifactor authentication. You can disable the use of multifactor authentication by making the MFADEF class inactive.

Any client that is delivered with the product that executes with the user's privileges must be used with care, since the TSF can not protect those clients from potentially hostile programs. Passwords/phrases a user enters into those client programs that those clients use to pass to the corresponding server to authenticate the user may potentially be spoofed by hostile programs running in the user's address space. This includes client programs for telnet, TN3270, ftp, r-commands, ssh, all LDAP utilities and Kerberos administration utilities that require the user to enter his password/phrase. When using those client programs the user should take care that no untrusted potentially hostile program has been called during his session.

The following elements and element components cannot be used in an evaluated system, either because they violate the security policies stated in this Security Target or because they have been removed from the evaluated configuration due to time and resource constraints of the evaluation. As they are part of the base system, either they must be not configured for use or they must be deactivated, as described in Chapter 7 of [MLSGUIDE]:

- All Bulk Data Transfer (BDT) elements: BDT, BDT File-to-File, and BDT Systems Network Architecture (SNA) NJE
- The DFS^{TM} Server Message Block (SMB) components of the Distributed File Service element
- Infoprint Server
- JES3
- IBM Ported Tools for z/OS HTTP Server V7.0

In addition, the following cannot be used in the certified configuration:

- The Advanced Program-to-Program Communication/Multiple Virtual Storage (APPC/MVS) component of the BCP
- The DFSMS Object Access Method for content management type applications
- The RACF remote sharing facility in remote mode.
- JES2 NJE communication via TCP/IP. JES2 NJE must use SNA or BSC in the certified configuration.
- JES2 Execution Batch Monitor (XBM) facility
- Most functions of Enterprise Identity Mapping (EIM). For details, see the manual [MLSGUIDE]

9.3.2 Hardware installation and configuration

The TOE is one instance of z/OS running on an abstract machine as the sole operating system and exercising full control over this abstract machine. This abstract machine, which is not being part of the TOE, can be provided by one of the following:

- a logical partition provided by a certified version of PR/SM running on:

  - IBM zEnterprise zEC12/BC12 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express3 or Crypto Express4S card, and with or without the zEnterprise BladeCenter Extension (zBX).
  - IBM z13/z13s with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express4, Crypto Express4S or Crypto Express5S cards, with or without the zEnterprise BladeCenter Extension (zBX)[2].
  - IBM z14 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express5S or Crypto Express6S cards.
- a certified version of IBM z/VM executing in a logical partition provided by PR/SM on one of the above-listed System z^{TM} processors.

[2] If the configuration includes a zEnterprise BladeCenter Extension (zBX), the operating systems running in the zBX are not part of the TOE. They are external systems, connected to z/OS only via the built-in TCP/IP networking facilities included in the zEnterprise System and zBX.

10 Annex B – Evaluated configuration

The Target of Evaluation is IBM z/OS Version 2 Release 3. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 4 represent the TOE.

The z/OS V2R3 Common Criteria Evaluated Base package must be installed and congigured according to the directions in section 9.3.1 as for the SW parts and directions in section 9.3.2 as for the HW parts.

11 Annex C –Test activities

This Annex describes the effort of both Developer and LVS in testing activities. For the assurance level EAL4, augmented with ALC_FLR.3, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Security Target requires the software packages comprising the TOE to be run on an abstract machine implementing the z/Architecture machine interface as defined in the "z/Architecture Principles of Operation" [ZARCH]. The hardware platforms implementing this abstract machine are:

- IBM zEnterprise zEC12/BC12 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express3 or Crypto Express4S card, and with or without the zEnterprise BladeCenter Extension (zBX).
- IBM z13/z13s with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express4, Crypto Express4S or Crypto Express5S cards, with or without the zEnterprise BladeCenter Extension (zBX).
- IBM z14 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express5S or Crypto Express6S cards.

Note that the above mentioned CryptoExpress cards are not part of z/OS and therefore the implementation of the cryptographic functions provided by those cards has not been analyzed. Testing has been performed using those cards to ensure that the cryptographic functions provided by those cards work in principle. No vulnerability analysis or side channel analysis for those cryptographic functions has been performed. The claims made in the Security Target concerning the cryptographic functions therefore apply to those functions implemented in software or by the CPACF feature.

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

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

The test systems have run z/OS Version 2 Release 3 in the evaluated configuration. Due to the massive amount of tests, testing was performed throughout the development of the TOE. To ensure proper testing of all security relevant behavior of the TOE, the evaluators verified that all tests that might have been affected by any security-relevant change introduced late in the development cycle had been run on the evaluated configuration.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

IBM tests the platforms for z/OS individually for their compliance to the z/Architecture using the Systems Assurance Kernel (SAK) suite of tests. These tests ensure that every platform provides the abstract machine interface that z/OS requires to be run. SAK testing is important not only to the z/OS evaluation, but to other evaluations (PR/SM, z/VM) as well.

FVT for z/OS is largely performed on the VICOM test system. This is an enhanced z/VM system implementing the z/Architecture abstract machine interface. It allows testers to bring up individual, virtual test machines running z/OS with access to virtualized peripherals such as disks and network connections. For the purpose of the security function tests, this environment is fully equivalent to the machines running z/OS. This environment was also used by the evaluators for their independent testing.

IBM has provided a common test framework for tests that can be automated. COMSEC is an environment that can be operated in standard mode or Labeled Security mode. The BERD (Background Environment Random Driver) test driver submits the testcases as JES2 jobs. IBM's intention is to move more and more tests to this automated environment, which will ease the test effort required for the evaluations substantially. Starting with V1R9 a substantial number of tests has been ported to this environment. Additionally, most test teams ran their manual tests in the COMSEC test environment, which provides a complete test environment in the evaluated configuration of the TOE in the different modes of operation.

The test systems have run z/OS Version 2 Release 3 in the evaluated configuration. The SDF team provided a pre-installed system image for VICOM and for the machines running the COMSEC tests, thus ensuring that the CCEB software version was used for all tests. The additional PTFs were applied to the VICOM and COMSEC systems as they became available, with any security-relevant tests for the PTFs being successfully re-run.

IBM's general test approach is defined in the process for Integrated Product Development (IPD) with developer tests, functional verification tests (FVT), and system verification tests (SVT). For each release, an overall effort of more than 100 person years is spent on FVT and SVT for the z/OS components. FVT and SVT is performed by independent test teams, with testers being independent from the developers. The different test teams have developed their own individual test and test documentation tools, but all implement the requirements set forth in the IPD documentation.

For the purpose of the evaluation, FVT is of interest to the evaluators, since the single security functions claimed in the [ST] are tested in this context. IBM decided to create a test bucket with the tests for the security functions, summarizing the tests in individual test plans, so that the evaluators had a chance to deal with the otherwise overwhelming complexity of the z/OS testing.

IBM's test strategy for the evaluation had three cornerstones:

- The major internal security interface was the interface to RACF, which is tested exhaustively by the RACF test group.

- Components requiring Identification and Authentication or Access Control services called RACF (with the exception of LDAP LDBM, which implements its own access control). For most of these services, it has been sufficient to demonstrate that these interfaces called RACF, once the testing of the RACF interface (see above) had established confidence in the correct inner workings of RACF.

- Due to the design of z/OS, a large number of internal interfaces is also visible externally, although the interfaces are not intended to be called by external, unprivileged subjects. For these interfaces, which are basically authorized programs, operator commands, certain callable services, SVC and PC routines, testing established only that these interfaces cannot be called by unauthorized callers.

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

For components providing cryptographic functions, testing was performed with and without hardware cryptographic support in order to test the correct usage of the hardware cryptographic functions, if present, and the correct implementation of the software within the TOE.

11.2.2 Test coverage

The developer provided a mapping between the TSF of the [ST], the TSFI in the functional specification and the tests performed. The evaluator checked this mapping and examined the test cases to verify whether the tests covered the functions and their interfaces. Although exhaustive testing is not required, the sponsor provided evidence that significant detail of the security functions have been tested.

The evaluators determined that developer tests provided the required coverage: Testing covered all TSF identified in the Security Target on all interfaces identified in the functional specification.

Test depth was verified against the TOE subsystems and the security enforcing modules:

- For most security functions relevant to this evaluation, subsystems invoke RACF functions to take security-relevant decisions, access control, identification and authentication, security management and the generation of security-relevant audit records are mostly handled by RACF.

- All other security-relevant functions are implemented within the subsystems themselves, thus keeping security functions isolated within them.

- For cryptographic functions, hardware support provided by the IT environment of the TOE is accessed through the ICSF component.

- For the self-protection, BCP and the underlying abstract machine work together to provide memory protection and different authorization mechanisms such as APF or AKM.

The evaluators verified that all security-relevant details of the TOE design at the level of subsystems have been taken into account for testing. In particular, testing of the RACF subsystem interfaces has been performed directly at these interfaces as well as over the subsystems invoking RACF.

11.2.3 Test results

Although different test teams used different tools and test tracking databases, the evaluators verified that all provided results showed that tests had executed successfully and yielded the expected results.

The testing results provided were valid for both the standard mode and the Labeled Security mode of operation, with the exception of tests for multilevel security features, which were relevant to Labeled Security mode only. The test systems configured for Labeled Security mode are compliant to standard mode as well, so that tests run on these systems were always applicable to both modes of operation. For COMSEC, all applicable tests were run in dedicated Labeled Security mode and standard mode configurations.

The evaluators verified that testing was performed on configurations conformant to the ST, with the exception of a number of patches, which has been accepted by the evaluators after having examined the potential impact of the patches.

The evaluators were able to follow and fully understand the test approach based on the information provided by the developer.

With this test environment, the developer was able to provide proof of the necessary coverage and test depth to the evaluators. In fact, IBM provided only a portion of their overall testing to the evaluators, to help them manage the complexity of the system.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The independent evaluator testing followed the CEM guidance to test every security function, without repeating in a exhaustive way all tests of the developer.

In addition to having re-run a sample of the developer's tests and observed the testing by IBM testers during dedicated sessions, the evaluators gained evidence of the developer's commitment during their long stay at the development site. In this context, the evaluators discussed problems or interpretations of the CC requirements with the testers and witnessed the tests being performed during the creation of the test bucket. The evaluators had already interviewed the testers during the site visits and examined the databases with the test cases and the related results and execution records.

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

One exception to this were additional patches, which the developer recommends for the TOE, even though they were not part of the CC test installation. However, as discussed in [ETR-TEST], the evaluator provided an explanation on why this was accepted.

11.3.2 Test coverage

For their own tests, the evaluators decided to focus on the most important security functions of the TOE in order to provide independent verification of their correct operation:

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

- Discretionary access control: The evaluators focused on UNIX System Services ACLs, which also implicitly test UNIX permission bits. Other DAC tests involved
  - USS IPC (all system calls for messages, semaphores and shared memory)
  - DAC for different USS objects (device special files, IPC objects, directories)
  - z/OS dataset access
  - security-relevant USS system calls

- Mandatory Access Control: The evaluators re-ran their own tests on mandatory access control checks for data sets and Unix System Services files as their own regression tests. Testing of the writedown override capability provided by FACILITY class profiles was also performed.

- Communication security: The evaluators chose to ensure that secure communications channels (SSL, Kerberos and Intrusion Detections functions) did not contain hidden platform specific implementation errors by testing interoperability with non-zSeries systems. Application-transparent TLS (AT-TLS) was also tested with a non-z/OS platform, checking different policy settings.

- Audit: Tests were used to check auditing of changes to the system clock.

- Security Management: The evaluators decided to devise no special tests here, since the setup of the test environment and the setup/cleanup of the tests would already include a major portion of the TSF found.

- TOE Self Protection: The only function suitably testable is object re-use. The evaluators have decided to focus on the issue of memory pages probably containing left-over information. All other self-protection features were properties that could not be easily "challenged" by evaluator tests.

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

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

11.3.3 Test results

All test cases devised by the Evaluators passed, i.e. the actual test results matched the expected results.

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

11.4 Vulnerability analysis and penetration tests

11.4.1 Testing approach

As for vulnerability assessment the changes introduced in V2R3 with respect to the previous version oft he TOE did not yield major potential for penetration testing.

The evaluator penetration testing covered areas not already touched by previous evaluations.

11.4.2 Test coverage

The evaluator verified initially the presence of the flaw indicated in the CVE-2018-15473. However, the flaw in itself was not considered problematic, as it did not subvert any claims or SFRs.

Table 5 reports penetration tests which have been executed.

USS Syscalls	*Effort*: The penetration testing examined the available system calls, supplying random arguments. No specific security function was subject to testing here. However, the system calls represent the full set of functions available to USS subjects. *Configuration*: The TOE was in its evaluated configuration. *Depth*: Any problem that would occur during testing, would potentially subvert the security functions behind that system call. The USS subsystem, as well as RACF are subject to testing here.
USS Stability	*Effort*: The penetration testing examined the USS subsystem's kernel with regard to resilience against random instruction streams. No specific security function was subject to testing here. *Configuration*: The TOE was in its evaluated configuration. *Depth*: The USS kernel the full set of functions available to USS subjects. Thus, any problem that would occur during testing, could potentially subvert the security functions the USS kernel controls. The USS subsystem, as well as RACF are subject to testing here.
TN3270 Control Character processing in program output	*Effort*: This is a classic penetration test, where irregular program output is not sanitized and the controlling terminal could be subverted. *Configuration*: The TOE was in its evaluated configuration. *Depth*: Any additional input from that terminal could then be used to subvert the

	system, thereby affecting all TSF. The system's console is one of the most privileged entry points into the system.

Table 5 – Penetration testing

11.4.3 Test results

The TOE withstood the penetration testing efforts in all tests.

11.4.4 Residual vulnerabilities

The evaluators have also performed their vulnerability analysis based on the information provided in the ST, the design documentation, the implementation representation and the user guidance. The evaluator did not find any new vulnerability introduced by the new or modified functionality introduced with z/OS V2R3 that could be exploited in the operational environment. No vulnerability was reported in the public sources for vulnerabilities that the evaluator checked (CVE and the z/OS-specific RACF mailing list).

The evaluator analyzed in detail the additional security functionality that was newly introduced in z/OS V2R3 or that has changed in z/OS V2R3 to identify potential vulnerabilities introduced by the design and implementation of those functions. The evaluator did not identify such a vulnerability exploitable in the intended operational environment of the TOE when the guidance for configuring and operating the TOE is observed by the trusted administrative personnel.

The following summarizes the findings of the evaluator from the previous evaluation, which also apply to z/OS V2R3:

- Checking the design and the guidance documentation, the evaluator detected that the TOE is vulnerable to Trojan horse attacks, viruses, worms and similar attacks in a similar way as other operating systems. The TOE does not include functionality that would actively prohibit this. Successfully developing and launching such an attack requires knowledge of the TOE and an attack potential beyond the one identified in the Security Target. Therefore, those vulnerabilities are considered to be not exploitable in the intended environment of the TOE. One also needs to consider that the extensive auditing capabilities of the TOE allow identifying such an attack thereby reducing the probability that such an attack is not detected early.

- Checking the design documentation, the evaluator discovered that the mandatory access control function of the TOE is not implemented to avoid covert channels. Llike in most other multi-level secure operating systems, label-based security is added on top of an operating system that was not designed with information flow control in mind. As a result, the evaluator could see as part of his analysis of the TOE design and guidance documents that the TOE has a considerable number of covert channels (like all other multi-level secure operating systems where labeled security has been added), mainly related to system control blocks and other data held in storage common to all address spaces. Exploiting such a covert channel requires a Trojan horse program, which have been rated as requiring knowledge of the TOE and an attack potential beyond the one identified in the Security Target. Covert channels are therefore considered to be a residual vulnerability not exploitable in the intended environment of the TOE. Since the assurance packages considered in this evaluation do not require a covert channel analysis, the evaluator did neither perform any analysis to get a list of covert channels nor an analysis to determine their bandwidth.

The residual vulnerabilities in Table 6 are present in the TOE. For each vulnerability the assessment of the attach potential is provided.

CVE-2018-0734	"The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p)." Assessment As indicated above, a timing side channel. This vulnerability is considered by OpenSSL to be of low severity, as it is difficult to exploit and no known exploits are present. This vulnerability is about recovering credentials of the OpenSSH host, therefore the SFRs that would be affected this are: FTP_ITC.1. As a side effect of this flaw, the contents of the host private key contained in a protected file would also be disseminated, which would subvert FDP_ACC.1(PSO) and FDP_ACF.1(TSO). However, as only the host key could be recovered mounting an attack impersonating the host would require additional network level subversions, such as taking over the host's ip address. The evaluator considered the CEM, appendix B 4.2 for calculating the attack potential here. *Elapsed Time*: The version of the OpenSSL library being used is not advertised, so the attacker needs some time to figure out the exact version that is being used in the TOE. Additionally, the attack programs need to be developed: Between one and two months. 5 points. *Expertise*: As no publicly available exploit is known, and the issue involves reconstructing private keys out of timing information, expert knowledge is needed.6 points. *Knowledge of the TOE*: Public knowledge of the TOE is sufficient. 0 points. *Window of Opportunity*: As the attack can only be mounted and more importantly developed with access to the TOE. A moderate window of opportunity is needed here. 4 points. *Equipment*: No exploit is known, therefore specialized slightly bespoke equipment is needed: 5 points *Summary*: 19 points, which would require an attack potential of "moderate".
CVE-2018-0735	"The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p)." Assessment As indicated above, a timing side channel. This vulnerability is considered by OpenSSL to be of low severity, as it is difficult to exploit and no known exploits are present. This vulnerability is about recovering credentials of the OpenSSH host, therefore the SFRs that would be affected this are: FTP_ITC.1. As a side effect of this flaw, the contents of the host private key contained in a protected file would also be disseminated, which would subvert FDP_ACC.1(PSO) and FDP_ACF.1(TSO). However, as only the host key could be recovered mounting an attack impersonating the host would require additional network level subversions, such as taking over the host's ip address. The evaluator considered the CEM, appendix B 4.2 for calculating the attack potential here. *Elapsed Time*: The version of the OpenSSL library being used is not advertised, so the attacker needs some time to figure out the exact version that is being used in the TOE. Additionally, the attack programs need to be developed: Between one and two months. 5 points. *Expertise*: As no publicly available exploit is known, and the issue involves reconstructing private keys out of timing information, expert knowledge is needed.6 points. *Knowledge of the TOE*: Public knowledge of the TOE is sufficient. 0 points. *Window of Opportunity*: As the attack can only be mounted and more importantly developed with access to the TOE. A moderate window of opportunity is needed here. 4 points. *Equipment*: No exploit is known, therefore specialized slightly bespoke equipment is needed: 5 points

	Summary: 19 points, which would require an attack potential of "moderate".

Table 6 – Residual vulnerabilities