Swedish Certification Body for IT Security

Certification Report

Canonical Ubuntu LTS 16.04.4

Issue: 1.0, 2018-jul-04

Authorisation: Jerry Johansson, Lead Certifier, CSEC

Table of Contents

1 Executive Summary 3

2 Identification 5

3 Security Policy 6

3.1 Auditing 6
3.2 Cryptography 6
3.3 Packet filter 6
3.4 Identification and Authentication 6
3.5 Discretionary Access Control 7
3.6 Authoritative Access Control 7
3.7 Virtual Machine Environments 7
3.8 Security Management 7

4 Assumptions and Clarifications of Scope 8

4.1 Usage Assumptions 8
4.2 Environmental Assumptions 8
4.3 Organizational Security Policies 9
4.4 Clarification of Scope 9

5 Architectural Information 10

6 Documentation 11

7 IT Product Testing 12

7.1 Developer Testing 12
7.2 Evaluator Testing 12
7.3 Evaluator Penetration Testing 13

8 Evaluated Configuration 14

9 Results of the Evaluation 15

10 Evaluator Comments and Recommendations 16

11 Certifier Comments and Recommendations 17

12 Glossary 18

13 Bibliography 19

Appendix A - QMS Consistency 20

1 Executive Summary

The Target of Evaluation, TOE, is a Linux-based general-purpose operating system. The TOE also includes a virtualization environment based on the Linux KVM technology, where Ubuntu implements the host system for the virtual machine environment and management of the virtual machines. The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved peer systems operating within the same management domain.

The TOE has been evaluated on the following hardware platforms:

x86 64bit Intel Xeon processors:

- Supermicro SYS-5018R-WR

IBM System z based on z/Architecture processors:

- IBM z13

IBM System P based on OpenPOWER processors:

- IBM Power System S822L (PowerNV 8247-22L)
- IBM Power System S822LC (PowerNV 8001-22C)
- IBM Power System S822LC (PowerNV 8335-GTB)

The TOE is delivered via download in the form of a ISO image. A SHA-256 checksum is calculated and signed, by several trusted entities within Canonical Group Limited, using a GPG signing key. Both of these values are made publicly available from one location and are to be used for verification of the TOE.

As the TOE is a general purpose operating system, there are many possible configurations and modifications that can be made in the Linux kernel. The evaluation only covers a subset of all possible operational modes of Ubuntu, these are defined in chapter 8 Evaluated configuration.

The ST do not make conformance claims to any protection profiles. The ST does however derive its security functional requirements from Operating System Protection Profile v2.0 with the extended package for virtualization.

There are ten assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the ten threats and comply with the three organisational security policy (OSP) in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, and to some extent in the approved foreign location in Austin, Texas, USA, and was completed on the 27th of June 2018.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 2, augmented by ALC_FLR.3 Flaw reporting procedures.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 2 + ALC_FLR.3.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2016011
Name and version of the certified IT product	Ubuntu LTS 16.04.4 with KVM and QEMU 2.5
Security Target	Security Target for Ubuntu 16.04 LTS, version 1.0
Assurance level	EAL 2 + ALC_FLR.3
Sponsor	Canonical Group Limited
Developer	Canonical Group Limited
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2018-07-04

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptography
- Packet Filter
- Identification and Authentication
- Discretionary Access Control
- Authoritative Access Control
- Virtual Machine Environments
- Security Management

3.1 Auditing

The Lightweight Audit Framework (LAF) is designed to be an audit system making Linux compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows configuring the events to be actually audited from the set of all events that are possible to be audited.

3.2 Cryptography

The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided, using OpenSSH where password-based and public-key-based authentication are allowed. In addition, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt. Space(with the help of a Password-Based Key-Derivation Function version 2).

3.3 Packet filter

The TOE provides a stateless and stateful packet filter for regular IP-based communication. OSI Layer 3 (IP) and OSI layer 4 (TCP, UDP, ICMP) network protocols can be controlled using this packet filter. To allow virtual machines to communicate with the environment, the TOE provides a bridging functionality. The packet filtering functionality offered by the TOE is hooked into the TCP/IP stack of the kernel at different locations. Based on these locations, different filtering capabilities are applicable.

3.4 Identification and Authentication

User identification and authentication in the TOE includes all forms of interactive log-in (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the su or sudo command. These all rely on explicit authentication information provided interactively by a user. The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported. Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

3.5 Discretionary Access Control

DAC allows owners of named objects to control the access permissions to these objects. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms. In addition to the standard Unix-type permission bits for file system objects as well as IPC objects, the TOE implements POSIX access control lists.

3.6 Authoritative Access Control

The TOE supports authoritative or mandatory access control based on the following concept:

- To separate virtual machines and their resources at runtime AppArmor rules defined by AppArmor policies are used. The virtual machine resources are labeled to belong to one particular virtual machine by that policy. In addition a virtual machine is awarded a unique label by that policy. The TOE ensures that virtual machines can only access resources bearing the same label.

3.7 Virtual Machine Environments

The TOE implements the host system for virtual machines. It acts as a hypervisor which provides an environment to allow other operating systems execute concurrently.

3.8 Security Management

The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes four assumptions on the usage of the TOE.

A.AUTHUSER - Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.DETECT - Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.

A.MANAGE - The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.TRAINEDUSER - Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

4.2 Environmental Assumptions

Six assumptions on the environment are made in the Security Target.

A.PHYSICAL - It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.PEER.MGT - All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.

A.PEER.FUNC - All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.

A.IT.FUNC - The trusted IT systems executing the TOE are assumed to correctly implement the functionality required by the TSF to enforce the security functions.

A.KEYS - It is assumed that digital certificates, certificate revocation lists (CRLs) used for certificate validation, private and public keys, as well as passwords used for:

-SSH client authentication,

-SSH server authentication,

-Password protecting the disk encryption schema

generated externally or by the TOE, meeting the corresponding standards and providing sufficient security strength through the use of appropriate key lengths and message digest algorithms. It is also assumed that Administrators verify the integrity and authenticity of digital certificates and key material before importing them into the TOE, and verifying that certificates are signed using strong hash algorithms.

A.CONNECT - All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.3 Organizational Security Policies

The Security Target [ST] places three organizational Security Policies on the usage of - the TOE.

P.ACCOUNTABILITY - The users of the TOE shall be held accountable for their security-relevant actions within the TOE.

P.USER - Authority shall only be given to users who are trusted to perform the actions correctly. P.PROTECT_SSH_KEY When using SSH with public-key-based authentication, organizational procedures must exist that ensure users protect their private SSH key component against its use by any other user.

P.CP.ANCHOR - Users shall control the confidentiality protection anchor for their confidentiality-protected user data, and reset/replace/modify it if desired.

4.4 Clarification of Scope

The Security Target [ST] contains ten threats, which have been considered during the evaluation.

T.ACCESS.TSFDATA - A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.

T.ACCESS.USERDATA - A threat agent might gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy.

T.ACCESS.TSFFUNC - A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.

T.ACCESS.COMM - A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.

T.RESTRICT.NETTRAFFIC - A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.

T.IA.MASQUERADE - A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.IA.USER - A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.

T.ACCESS.COMPENV - A threat agent might utilize or modify the runtime environment of other compartments in an unauthorized manner.

T.INFOFLOW.COMP - A threat agent might get access to information without authorization by the information flow control policy.

T.COMM.COMP - A threat agent might access the data communicated between compartments or between a compartment and an external entity to read or modify the transferred data.

T.ACCESS.CP.USERDATA - A threat agent might gain access to user data at rest which is confidentiality protected without possessing the authorization of the owner, either at runtime of the TOE or when the TSF are inactive.

5 Architectural Information

Ubuntu is a highly-configurable Linux-based multi-user multi-tasking operating system. Ubuntu may provide services to several users at the same time. After successful login, the users have access to a general computing environment, allowing the start-up of user applications, issuing user commands at shell level, creating and accessing files. The TOE provides adequate mechanisms to separate the users and protect their data. Privileged commands are restricted to administrative users. The TOE Security Functions (TSF) consist of functions of Ubuntu that run in kernel mode plus a set of trusted processes.

Administrative tools are implemented as standard Linux applications. System administration tools include the standard command line tools. To access the Ubuntu host system for managing virtual machines, the TOE provides management access to the libvirtd virtual machine management daemon via OpenSSH.

The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved peer systems operating within the same management domain. The TOE includes standard networking applications, including applications allowing access of the TOE via cryptographically protected communication channels, such as SSH.

Discretionary access rights (e.g. read, write, execute) can be assigned to data objects with respect to subjects identified with their UID, GID and supplemental GIDs. Once a subject is granted access to an object, the content of that object may be used freely to influence other objects accessible to this subject.

Ubuntu provides virtualization environment based on the Linux KVM technology. Ubuntu implements the host system for the virtual machine environment and manages the virtual machines. In addition, Ubuntu provides management interfaces to administer the virtual machine environment as well as full auditing of user and administrator operations. The KVM technology separates the runtime environment of virtual machines from each other. The Linux kernel operates as the hypervisor to the virtual machines but provides a normal computing environment to administrators of the virtual machines. Therefore, the Linux kernel supports the concurrent execution of virtual machines and regular applications . Ubuntu uses the processor virtualization support to ensure that the virtual machines execute close to the native speed of the hardware.

AppArmor is also part of the evaluated Linux kernel. AppArmor policies restricts virtual machines to a set of defined resources assigned to the respective virtual machine. Any other resource, including general operating system resources or resources from other users are inaccessible based on the AppArmor restrictions.

6 Documentation

The TOE and its documentation are supplied on ISO images distributed via the Ubuntu web site. The TOE further includes a package holding the additional user and administrator documentation:

- ISO Image Ubuntu 16.04.4, ubuntu-16.04.4-server-<architecture>.iso
- ubuntu-commoncriteria-1.0-0ubuntu0.16.04.deb Debian package from Canonical.

The following documents are included in the TOE:

- Evaluated Configuration Guide, version 0.9, 2018-05-18
- Manual pages for all applications, configuration files and system calls (as part of the TOE)
- The package contains the configuration script (Configure-Ubuntu-16.04-Common-Criteria.sh)
- The tarball with software related to the evaluated configuration (Ubuntu-16.04-Common-Criteria.tar.gz)

7 IT Product Testing

The evaluator has verified that the developer testing was performed on hardware conformant to the ST. The evaluator was able to follow and fully understand the developer testing approach by using the provided test documentation.

The evaluator analyzed the developers test coverage and depth by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the identified TSFI as well as the identified subsystem/internal interfaces.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the expected test results according to the test plan.

7.1 Developer Testing

The developer ran all the tests on one of each general CPU type listed in the ST. The selection of the CPUs was based on the fact that the differences between the machines are related to the provided hardware environment that has no impact on the security of the TOE. The test systems were configured to conform to the ST and the instructions in the Evaluated Configuration Guidance.

The test suite used incorporates a common framework for the automated tests in which individual test cases adhere to a common structure for setup, execution and cleanup of the tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behavior with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS, OK or FAIL. The testing were mainly conducted in the form of automated tests. In addition, several tests although originating from the automated test suite, were executed manually.

The testing was conducted on all the identified TSFI identified from the functional specification:

- System Calls
- Trusted programs (and the corresponding network protocol SSH v2.)
- KVM IOCTLs and hypervisor calls
- TSF database files (security critical configuration files)
- AppArmor interfaces including its configuration and control files
- DBUS Programs
- socket protocols (e.g. netlink)
- general network protocols applicable to information flow control
- Miscellaneous interfaces that don't fit into the categories above, either because there are no external interfaces, or the security functionality is not directly visible at the interface.

All test results from all tested environments show that the expected test results were identical to the actual test results. All the tests were executed successfully.

7.2 Evaluator Testing

The evaluator testing effort consisted the execution of the developer tests as well as execution of the tests created by the evaluator. The tests were performed remotely at different developer's sites depending on the desired test system. The evaluator performed tests on all hardware architectures types supported by the TOE, by using the same selection of CPUs as the developer. The evaluator ran all the automated developer tests, and also devised additional tests. When devising the additional test the following reasons were taken into consideration:

- A variation of an audit-test case to verify the result checking in the test framework works as expected.
- A variation of an audit-test case to verify the file system object DAC tests on different file systems (the developer tests normally only use one file system type), to ensure that DAC is enforced as expected (with a few known exception as some file systems do not support some file object types).
- Some basic privilege checks for some management commands that can only be performed by root but which has not been tested by the developer.
- Functionality provided through the netlink interface and which requires certain commands to be only to be executed by root and which is not covered by developer testing.
- Additional SSH cipher tests to extend the test scope of the developer.

The evaluator created several test cases for testing a few functional aspects where the developer test cases were considered by the evaluator to be not broad enough. During the evaluator's review of the test cases provided by the developer, the evaluator gained confidence in the developer testing effort and the depth of test coverage in the developer supplied test cases. All evaluator-written tests passed successfully.

7.3 Evaluator Penetration Testing

The evaluator performed searches of public vulnerability databases as well as penetration testing. The evaluator chose a mix of publicly available PoCs and fuzzing of complex application level interfaces, in order to identify flaws within the TOE.

Additional testing were further scheduled for the following parts of the TOE:

- Meltdown and Spectre
- "DBus fuzzing"
- "syscall thrashing"

Application level tests ran on an x86_64 platform, system call level tests ran on the actual platforms. During the vulnerability testing the evaluator found residual vulnerabilities. These residual vulnerabilities were found to be outside of the scope of this evaluation as they would require an attack potential of "Enhanced-Basic" or higher.

The residual vulnerabilities are: CVE-2018-9056, CVE-2018-3639, CVE-2017-16808, CVE-2017-0861, CVE-2017-15129, CVE-2017-17805, CVE-2017-17806, and CVE-2017-18075.

8 Evaluated Configuration

The evaluated configuration is defined as follows:

- The CC evaluated package set must be selected at install time in accordance with the description provided in the Evaluated Configuration Guide and installed accordingly.
- The TOE supports the use of IPv4 and IPv6, both are also supported in the evaluated configuration. IPv6 conforms to the following RFCs:
- RFC 2460 specifying the basic IPv6 protocol
- IPv6 source address selection as documented in RFC 3484
- Linux implements several new socket options (IPV6_RECVPKTINFO, IPV6_PKTINFO, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_RECVDSTOPTS, IPV6_DSTOPTS, IPV6_RTHDRDSTOPTS, IPV6_RECVRTHDR, IPV6_RTHDR, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_{RECV,}TCLASS) and ancillary data in order to support advanced IPv6 applications including ping, traceroute, routing daemons and others. The following section introduces Internet Protocol Version 6 (IPv6). For additional information about referenced socket options and advanced IPv6 applications, see RFC 3542
- Transition from IPv4 to IPv6: dual stack, and configured tunneling according to RFC 4213.
- The default configuration for identification and authentication are the defined password-based PAM modules as well as public-key based authentication for OpenSSH. Support for other authentication options, e.g. smart card authentication, is not included in the evaluation configuration.
- If the system console is used, it must be subject to the same physical protection as the TOE.

Deviations from the configurations and settings specified with the Evaluated Configuration Guide are not permitted. The TOE comprises a single system (and optional peripherals) running the TOE software listed. Cluster configurations are not permitted in the evaluated configuration. The evaluated configuration does not allow to dynamically load and unload device drivers as kernel modules.

If other systems are connected to a network they need to be configured and managed by the same authority using an appropriate security policy that does not conflict with the security policy of the TOE. All links between this network and untrusted networks (e. g. the Internet) need to be protected by appropriate measures such as carefully configured firewall systems that prohibit attacks from the untrusted networks. Those protections are part of the TOE environment.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Systematic Flaw Remediation	ALC_FLR.3	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Certifier Comments and Recommendations

As the threat landscape is shifting at a high pace, the current security level can swiftly change, as new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. The certifier notes that for many scenarios a reasonable policy would be to keep products up to date with the latest version of the firmware/software. However, the benefit of installing firmware/software updates must be balanced with the potential risks that such changes might have unexpected effect on the behavior of the evaluated security functionality. Ubuntu LTS is intended to be updated over time as indicated by the augmentataion by ALC_FLR. The Developer's intents to maintain and update the TOE in order to keep it relevant over time.

The evaluator have consistently used CC and CEM version 3.1 revision 4 during the evaluation, but the certifier has verified that the evaluation complies with CC and CEM version 3.1 revision 5 which is the latest version.

12 Glossary

AppArmor	Application Armor, Linux kernel Security Module
CPU	Central Processing Unit
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DBUS	Desktop Bus (a software bus)
ECG	Evaluated Configuration Guidance
GID	Group Identifier
GPG	GNU Privacy Guard
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IOCTL	Input/Output Control
LAF	Lightweight Audit Framework
LTS	Long-term Support
OpenSSH	Open Secure Shell
OSI	The Open Systems Interconnection model
PAM	Password-based Modules
PoC	Proof of Concept
RFC	Request for Comments
SHA	Secure Hashing Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
UID	User Identifier

13 Bibliography

ST Security Target for Ubuntu 16.04 LTS, Canonical Group Limited, 2018-06-27, document version 1.0

ECG Evaluated Configuration Guide, Canonical Group Limited, 2018-05-18, document version 0.9

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2018-04-24, document version 29.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2017-04-04, document version 7.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2016-11-01:

QMS 1.20	valid from 2016-10-20
QMS 1.20.1	valid from 2017-01-12
QMS 1.20.2	valid from 2017-02-27
QMS 1.20.3	valid from 2017-04-24
QMS 1.20.4	valid from 2017-05-11
QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.21.3”.

The certifier concluded that, from QMS 1.20 to the current QMS 1.21.3, there are no changes with impact on the result of the certification.