Ärendetyp: 6 Diarienummer: 19FMV3919-37:1

Dokument ID 7DFAYPHQVZ4V-1834444990-2491

CSEC

Swedish Certification Body for IT Security

Certification Report - DriveLock Agent

Issue: 1.0, 2021-apr-07

Authorisation: Ulf Noring, Lead Certifier , CSEC

SWEDAC ACKREDITERING

Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is the software DriveLock Agent 2019.2 (Device and Application Control) SP 1 and accompanying guidance documentation.

The TOE is an application and device control software-only TOE for use on workstation PCs running a Windows 10 (64bit) operating system. Its main functions are:

● Blocking unwanted devices from use, therefore preventing unwanted data import or export and potential system compromise by malicious devices.

● Blocking unwanted applications from executing, preventing system degradation and other undesirable effects that could be caused by these applications.

● Auditing events that trigger the security functions mentioned above.

The DriveLock Agent 2019.2 application also supports file and drive encryption, but that functionality has not been evaluated, only the functionality mentioned above. Please refer to chapter 2.4.2 of the [ST] for more details.

The certified version of the TOE is available to registered customers only, after purchasing a license. Registered customers have access to non-public information in the DriveLock Support Portal

(accessible at https://my.drivelock.support/wm/kb.html). Knowledgebase article KBA00341 contains information on and links to the TOE and its documentation.

The TOE is provided as a downloadable ISO image. The knowledgebase article mentioned above also contains a SHA2 hash value of the ISO file which can be used to verify the integrity of the ISO file. In addition, the article lists the SHA2 hashes of the principal installation archives inside the ISO file.

The ST does not claim conformance to any Protection Profile.

There are six assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the six threats and comply with the organisational security policy (OSP) in the ST. The assumptions, threats and 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. The evaluation was completed on 2021-03-17. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

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 the Common Methodology for evaluation assurance level EAL 3 augmented by ALC_FLR.3.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB.

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

As specified in the security target of this evaluation, the invocation of cryptographic primitives has been included in the TOE, while the implementation of these primitives has been located in the TOE environment. Therefore the invocation of cryptographic primitives has been in the scope of this evaluation, while correctness of implementation of cryptographic primitives has been excluded from the TOE. Correctness of implementation is done through third party certification NIST Cryptographic Algorithm Validation Program (CAVP) certificates # C785, # C796, # C797, # C798 mentioned in chapter 6.2.2 Cryptographic Algorithm Validation of the Windows 10 Security Target [WIN10ST], which the DriveLock Agent Security Target refers to.

Users of this product are advised to consider their acceptance of this third party affirmation regarding the correctness of implementation of the cryptographic primitives.

2 Identification

Certification Identification	
Certification ID	CSEC2019015
Name and version of the certified IT product	DriveLock Agent 2019.2 (Device and Application Control) SP 1
Security Target Identification	DriveLock Agent 2019.2 (Device and Application Control) Security Target, Joachim Schneider, 2021-03-17, document version 1.32
EAL	EAL 3 + ALC_FLR.3
Sponsor	DriveLock SE
Developer	DriveLock SE
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	1.22.3
Scheme Notes Release	17.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2021-04-07

3 Security Policy

The TOE provides the following security functionality:

- Device Control
- Application Control
- Audit Generation
- TOE Management

3.1 Device Control

Device Control enables the TOE administrator to control which devices can be used on a workstation by which user. The rules are defined by deploying a policy that essentially uses a white-list approach. To enforce these rules the TOE contains a kernel-mode component (driver) that is aware of a device being connected before that device becomes operational. Whenever a device is connected to the system, the operating system processes a sequence of PnP (Plug-and-Play) events to install and activate the device. Device Control intercepts some of these events and evaluates if the device should become accessible, based on the policy data and the current Windows user. If the result of this evaluation is that the device shall not be permitted, Device Control prevents completion of the required PnP activities, forcing the device activation to fail. As a result, the device remains unable to interact with the system and thus inaccessible to system and users. If the device is permitted, the installation and activation of the device by the Windows PnP manager proceeds normally and the device becomes available to the system and thus to the user.

3.2 Application Control

Application Control enables the operator to control which executables are permitted to run on a workstation and what permitted executables are allowed to access. A white-list based policy defines the permitted executables. The criterion to permit an executable image is a match of the cryptographic hash calculated over the executable contents to an entry in a hash database. Multiple whitelist rules can be defined; additional parameters control the applicability of a specific whitelist rule, e.g. the currently logged-on Windows user.

To enforce the operator-defined policy the TOE contains a kernel-mode component that monitors any requests to create a new process or load an executable file (e.g. a DLL). Whenever such an event occurs the TOE evaluates if the executable image about to be loaded is permitted by its policy or not. If the executable is not permitted, the request is aborted by the TOE, preventing the executable from running.

If an executable is permitted to run, the TOE administrator can additionally control the access of the resulting process to files or registry keys. Processes can be explicitly allowed or denied access to such resources. The TOE kernel mode components intercept access attempts and block them if they are not permissible according to the defined policy. Note that access is permitted unless a rule exists that forbids it. Explicitly allowing access is only required if access to a resource is generally not allowed by a rule, and an exception is required for a specific process, overriding the general rule. Selectable rule priorities are used to unambiguously define such situations.

3.3 Audit Generation

The TOE generates audit records of various events related to its security functions (see 7.1.2 in [ST] for details). An operator-defined audit policy controls which events are recorded and where they are sent. This audit trail is buffered locally using the event log facilities provided by the operating system. In addition, events can be sent to other destinations, like the DriveLock Enterprise Service, SMTP, or SNMP addresses. Thetable below details the most relevant audit events in relation to the security functions of this summary.

Function	Event(s)
Device Control	Device arrival and reaction of the TSF (blocked or allowed) Device removal Device access reconfiguration due to Windows user change
Application Control	Attempts to execute and reaction of the TSF (blocked or allowed) Attempts to access files or registry keys and reaction of the TSF (blocked or allowed) Problems accessing TSF data (hash database) or policy data
Audit Generation	Agent service start-up and shutdown
TOE Management	Problems accessing the Enterprise Service Missing TSF data (policies) Problems with connection security (TLS, certificates, etc.) Problems with received TSF data update packages

Review of the audit data recorded is possible in the DriveLock Control Center (not part of the TOE), where a variety of filtering options is available.

3.4 TOE Management

The administration of the TOE takes place on a central server (DriveLock Enterprise Service), using the Management Console. All management data is maintained by the server in a database. All these components are not part of the TOE.

The TOE receives its configuration and policy data over a network connection to an intranet web service running on the server. This connection is a secure channel that ensures confidentiality and authenticity. The secure channel is provided by the TOE environment. To protect the integrity of the local TSF data all policy data received via this channel must be digitally signed with a specific key, otherwise the data is rejected. This key is deployed as part of the initial configuration of the TOE by the TOE administrator. The cryptographic functions for signature verification are provided by the TOE environment. The TOE also verifies that the received policy data is newer than the data it is intended to replace. This ensures that an attacker cannot reuse outdated but validly signed policy updates to undo later policy changes.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

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

A.POLICY

Policy definition and maintenance:

It is assumed that the TOE administrator defines and deploys suitable policies for Device Control, Application Control, and Audit, carefully following the available guidance for the TOE. It is also assumed that the administrator keeps the policies current and that policy rules are configured to apply to the intended users and computers.

A.TRUSTEDADMIN

Trustworthy administrators:

It is assumed that the administrators of the TOE are trustworthy and sufficiently familiar with the TOE to minimize the risk inadvertent misconfiguration, and do not intentionally subvert the TOE’s operation.

4.2 Environmental Assumptions

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

A.EVENTLOG

Operating system event log:

It is assumed that the operating system event log is properly configured to receive and retain the TOE-generated audit records until they can be analyzed by the TOE administrator(s).

A.OSLOGON

Operating system logon:

It is assumed that user identification and authentication is performed by the operating system and that the TOE can query the current Windows user to determine access rights and associate user identities with its audit records where applicable.

A.RELIABLETIME

Reliable time source:

It is assumed that the TOE and its environment have access to the correct time by using the operating system functions intended for this purpose.

A.SECURECONN

Secure connection to the administrative backend:

It is assumed that a secure network connection is available to the TOE to connect to its server.

4.3 Clarification of Scope

The Security Target contains six threats, which have been considered during the evaluation.

T.DATAEXPORT

A user AG.USER exports local data AS.LOCALDATA from the workstation to a removable device which is unknown and/or not allowed. Alternatively, a permitted process AG.LEGITPROCESS accesses local data it is not allowed to access.

T.DATAIMPORT

A user AG.USER imports data from a removable device which is unknown or not allowed to connect to the workstation, modifying the data AS.LOCALDATA stored on the workstation.

T.DEGRADESYS

An illicit process AG.ILLICITPROCESS degrades the AS.RESOURCES, such as performance (e.g. real-time capability) or resources (e.g. storage capacity) of the workstation by using these for its own purposes.

T.CORRUPTSYS

An illicit process AG.ILLICITPROCESS manipulates or sabotages the execution of the legitimate processes AS.LEGITPROCESS on the workstation, compromising system integrity AS.INTEGRITY. Alternatively, an illicit process AG.ILLICITPROCESS denies legitimate users AG.USER access to the workstation (AS.RESOURCES) or its data (AS.LOCALDATA). Finally, a permitted process AG.LEGITPROCESS modifies files or settings it is not allowed to access.

T.CORRUPTTSFD

A malicious user AG.USER or process AG.ILLICITPROCESS modifies the TSF data (AS.TSFDATA) to manipulate or degrade the security functions of the TOE. Alternatively, a malicious user AG.USER impersonates the server and supplies unauthorized updates to the TSF data.

T.HOSTILEDEVICE

An attacker AG.OUTSIDER connects (or induces an unknowing AG.USER to do so) a manipulated device to the system to gain control (e.g. a USB cable secretly posing as a keyboard), compromising system integrity (AS.INTEGRITY) or accessing workstation data (AS.LOCALDATA).

The Security Target contains one Organisational Security Policy (OSP), which has been considered during the evaluation.

OSP.AUDIT

Events relevant to the management and enforcement of the TOE security policies shall be recorded as specified by the operator.

5 Architectural Information

The TOE is a software application for Windows 10 and consists of user-mode and kernel-mode components.

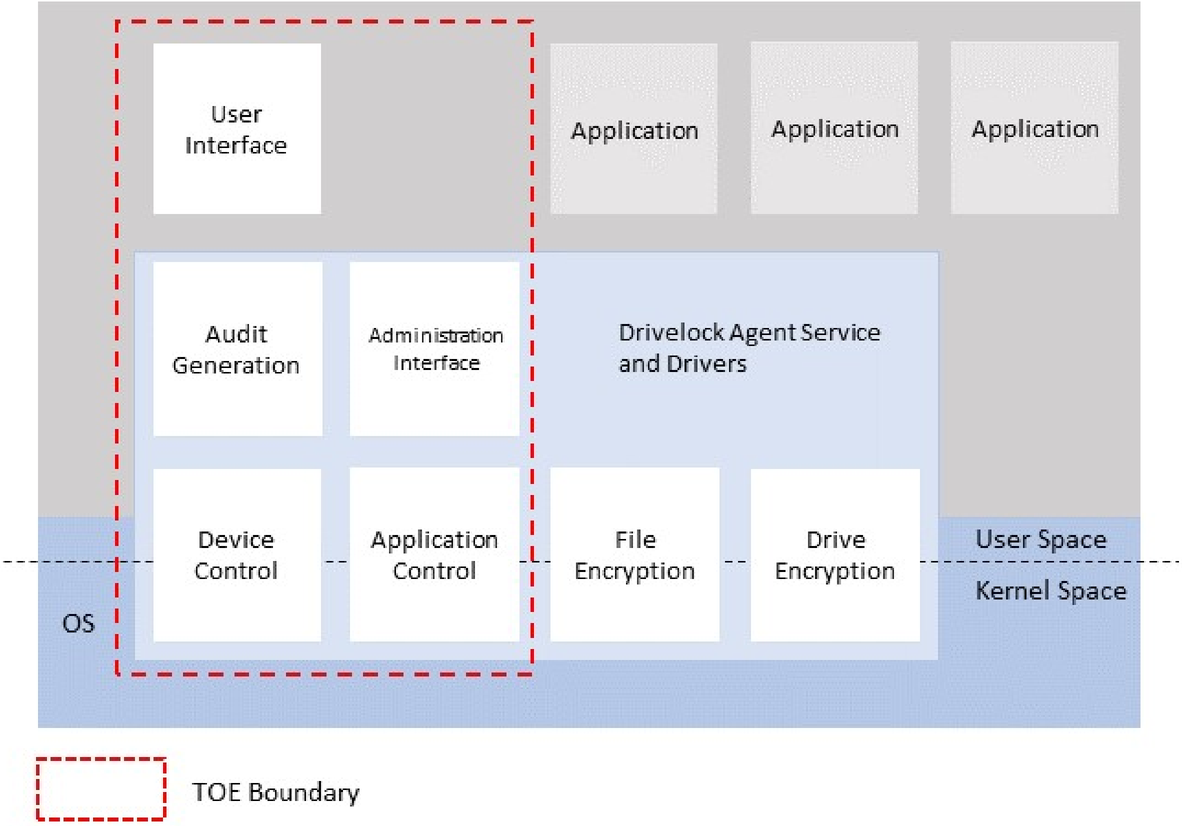
The kernel-mode components (drivers) implement most of the TOE security function interaction with the operating system. They are implemented as filter drivers and inserted in various operating system driver stacks. From there, the TOE drivers can influence the outcome of various operating system calls or events, e.g. prevent activation of a device or prevent the creation of a process.

The user-mode components reside in a user-mode service. They implement the interaction with the user and the backend, such as the administration interface over which the TOE receives its policy and configuration data, or the mechanism forwarding the audit trail entries to the destination(s) configured for these entries. The user-mode service also passes policy and configuration data to the drivers. For specific functions the policy enforcement by the driver(s) is supported by a user mode component as well, e.g. where a policy decision would be very difficult to make in kernel-mode code.

As seen below, the primary security functions of the TOE are implemented as combinations of a kernel mode driver and a matching user mode component:

• Device Control: This component enforces device filtering, i.e. control over access to devices and ports.

• Application Control: This component controls execution of executable files, and access to system resources by running processes.



The TOE also contains additional components that run in user mode only:

- Audit Generation: This component collects and routes all audit events logged by the other components.
- Administration Interface: This component implements a bidirectional interface with a DriveLock Enterprise Service. It retrieves configuration updates from and sends audit data to the server.
- User Interface: This component runs as a separate application and mainly provides status information to the current user. Its other functionality, e.g. management of encrypted drives and containers, is not part of this evaluation.

6 Documentation

The following documentation comprise the TOE guidance:

INSTALL_GUIDE	DriveLock Installation Guide 2019.2
ADMIN_GUIDE	DriveLock Administration Guide 2019.2
CC_GUIDE	DriveLock 2019.2, Manual Supplement for Certification Compliant Operation
CONTROL_CENTER	DriveLock Control Center User Guide 2019.2
EVENTS	DriveLock Events, List of DriveLock Events 2019.2 SP1
USER_GUIDE	DriveLock 2019.2
REL_NOTES	DriveLock Release Notes 2019.2 SP1

7 IT Product Testing

7.1 Developer Testing

The developer employed a manual test approach which covers all the security relevant subsystems of the TOE. The developer provided test evidence that indicates that all tests in the test plan have been successfully executed with a "Passed" result.

7.2 Evaluator Testing

The developer performed manual testing of the TOE. The evaluators developed additional manual tests. In total, 9 out of 20 developer tests were executed by the evaluators. The selected tests were not only repeated, but also augmented by the evaluator to widen the test scope and to validate the effectiveness of these tests. The evaluator also devised three manual tests focusing on edge case functionality such as legacy device access control. All evaluator test cases and sample developer tests were completed successfully.

7.3 Penetration Testing

The evaluator examined the TOE using a combination of attack scenarios that cover the following:

- Application Control
- Security Architecture
- General Networking Configuration

During the penetration testing the following TOE subsystems were subject to testing:

- Application Control
- TOE Management

The approach was a combination of fuzzing, architectural timing, load and close examination. The TOE withstood all penetration efforts.

8 Evaluated Configuration

The TOE is a Windows 10 64-bit software application. For the evaluated configuration the method Centrally Stored Policy must be used. In addition, the centrally stored policies need to be signed before they are deployed, i.e. the server connection must be set up using a configuration certificate All other deployment methods available were not evaluated and cannot be used.

Configuration signing uses certificates. The certificates are a security critical component for this mechanism and should generally fulfill at least the following requirements:

Algorithm: RSA
Key Length: 4096 bits
Integrity Hash: SHA256
Validity: ≤ 4 years

To guard against the use of outdated versions of the SSL and TLS protocols, the DES-server shall be configured to use only TLS 1.2. This is achieved by setting the string value securityProtocols under HKLM/SOFTWARE/CenterTools/DES to the value Tls12.

● Agent Hardening settings:

❍ Agent Service Permissions: Other permissions than Query Service Information shall only be allowed for TOE administrators

❍ Run Agent in Non-stoppable mode

❍ Start DriveLock Agent in safe mode

❍ Agent Remote Control Settings: Enable HTTPS

❍ Agent Remote Control Settings: Enforce HTTPS

❍ Password to uninstall DriveLock is suitable complex and strong

❍ Disable Offline Unlock requests

● Audit of the following events needs to be configured: 105, 108, 456, 639, 522, 523, 294, 130, 129, 473, 474, 600, 221, 222

For the configuration of the Enterprise Service Connection the following aspects need to be considered for a certification compliant installation:

❍ Permissions: These must be set to allow only TOE administrators to change the Enterprise Service configuration.

❍ Updates: Automatic updates must be disabled. An Agent update would replace the certified software version with a newer version, which is likely not certified.

❍ Network settings: The Use SSL for connections from agent to the server optionmust be checked (enabled) to secure the connections. Note that SSL is used as a generic term here, designating both the SSL and TLS protocols.

● Drive locking must be enabled (and appropriate whitelist rules defined) for at least these drive types:

❍ Floppy disk drives

❍ CD-ROM/DVD drives

❍ USB connected drives

❍ Firewire (IEEE-1394) bus connected drives

❍ SD bus connected drives

❍ Other removable drives

❍ Fixed disks, because e.g. an external drive connected to an eSATA port may be detected as a fixed disk

● Locking must be enabled (and rules defined) for these ports and devices:

❍ Serial and parallel ports

❍ Bluetooth transmitters

❍ Infrared interfaces

❍ PCMCIA controllers

❍ Human Interface Devices (to thwart Bad USB and related attacks)

❍ Mobile phones (as they usually provide data export and import to/from their storage)

❍ Modems

❍ Media Player devices

❍ SD Host Controllers

❍ Tape Drives

❍ PCMCIA and flash memory devices

● If the system event log is used to store the audit events generated by the TOE, the event log size on the workstation must be configured large enough for the selected review period.

● The workstation must be configured to require user authentication before any access to the system. This is required to correctly identify the current user for rule evaluation and association of audit events with users. If manual user logon is not feasible due to operational concerns, unauthorized access to the workstation must be prevented by other means.

● The workstation time and date need to be set correctly. This is required for proper timestamps on audit records, and for certificate and policy update verification. The easiest ways to achieve this is to have the workstation synchronize its clock with a domain controller or an internet time source, which both NIST and Microsoft provide.

● The workstation needs a secure connection via TLS to the DriveLock Enterprise Server. The TLS configuration defaults (cipher suites and priorities) of Windows 10 are suitable for this purpose; they should only be changed with good reason by experienced security experts. However, to ensure that the workstation does not permit connections using outdated versions of the secure connection protocols, SSL 3.0, TLS 1.0, and TLS 1.1 need to be disabled.

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 evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

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

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional specification	ADV_FSP.3	PASS
TOE design	ADV_TDS.2	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.3	PASS
CM scope	ALC_CMS.3	PASS
Delivery	ALC_DEL.1	PASS
Development security	ALC_DSV.1	PASS
Flaw remediation	ALC_FLR.3	PASS
Life-cycle definition	ALC_LCD.1	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.2	PASS
Depth	ATE_DPT.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

None.

11 Glossary

CC	Common Critera
CSEC	The Swedish Certification Body for IT Security
DES	DriveLock Enterprise Service
DLL	Dynamic-Link Library
EAL	Evaluated Assurance Level
eSATA	External Serial AT Attachment
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
NTP	Network Time Protocol
OS	Operating System
PCMCIA	Personal Computer Memory Card International Association
PnP	Plug and Play
PP	Protection Profile
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

12 Bibliography

12.1 General

CC Combination of CCp1, CCp2, CCp3, and CEM (see below)

CCp1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3 Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

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

ST DriveLock Agent 2019.2 (Device and Application Control) Security Target, Joachim Schneider, 2021-03-17, document version 1.32

SP-002 SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2019-01-16, document version 8.0

12.2 Documentation

INSTALL_GUIDE DriveLock Installation Guide 2019.2, DriveLock SE, 2020-06-29

ADMIN_GUIDE DriveLock Administration Guide 2019.2, DriveLock SE, 2020-06-29

CC_GUIDE DriveLock 2019.2, Manual Supplement for Certification Compliant Operation, DriveLock SE, 2021-03-17, document version 1.52

CONTROL_CENTER DriveLock Control Center User Guide 2019.2, DriveLock SE, 2020-03-21

EVENTS DriveLock Events, List of DriveLock Events 2019.2 SP1, DriveLock SE, 2020-03-25

USER_GUIDE DriveLock 2019.2, DriveLock SE, 2020-03-21

REL_NOTES DriveLock Release Notes 2019.2 SP1, DriveLock SE, 2020-03-21

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.24.1	2020-12-03	None
1.24	2020-11-19	None
1.23.2	2020-05-11	None
1.23.1	2020-03-06	None
1.23	2019-10-14	Exception given for this certification to still use SP-188 version 8.0 as changes introduced in QMS 1.23 meant only EAL 4 and above could place cryptographic implementations in the environment.
1.22.3	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL3.
SN-18	3.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	3.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-28	1.0	Updated procedures application, evaluation and certification	Evaluator reports should be received in two batches.