Swedish Certification Body for IT Security

Certification Report- LogPoint 5.2.5

Issue: 1.0, 2015-aug-28

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The TOE is a Security Information and Event Management (SIEM) system. It is part of an enterprise network and collects and analyses log information from devices on this network.

The TOE receives this log information (referred to as events) and then it is normalized, indexed and stored according to well-defined policies. Alert rules are used to automatically identify and inform users of suspicious activity on the network indicated by analyzing the log information. In addition the TOE provides an extensive forensic capability to enable an authorized user to search for vulnerabilities on the network.

The TOE is a software-only TOE. The TOE can be operated on a single machine or as multiple TOEs in a distributed configuration, i.e.:

- Single LogPoint appliance
- Multiple LogPoint appliances working together in a distributed configuration

The TOE acquires event data in a number of distinct ways. Network based devices send events to the TOE. The TOE collects events from a number of different devices using collectors listening on specific network ports. Some of these operate in real-time, such as the Syslog, SNMP Trap, and Netflow collectors. Others are batch oriented, such as the FTP Collector.

Other devices require LogPoint to actively retrieve event information. For such devices, a dedicated fetcher polls the device for information at scheduled intervals. LogPoint supports the following collectors and fetchers:

COLLECTORS	FETCHERS
Syslog Collector	FTP Fetcher
SNMP Trap Collector	SCP Fetcher
FTP Collector	WMI Fetcher
Net Flow Collector	SNMP Fetcher
Snare Collector	OPSEC Fetcher
FileSystem Collector	Adhoc OPSEC Fetcher

Figure 1: Collectors and fetchers supported by the TOE

The TOE uses OpenVPN incorporating TLS v1.2 to secure the inter-TSF channels used. However, neither OpenVPN nor the cryptographic primitives are part of the TOE, but considered the TOE environment.

Incase of OpenVPN, the client and the server are mutually authenticated using X.509 certificates. The DHE_RSA_AES256_SHA256 is the only supported TLS cipher suite for OpenVPN communication.

RSA 2048 bit private key is generated during the installation of the LogPoint and is not changed during the lifetime of the LogPoint Instance. A 2048 bit Diffie Hellman key is also generated during the same time using OpenSSL tool.

The evaluation has been performed by atsec information system AB in their premises in Danderyd, Sweden. 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 EAL3, augmented by ALC_FLR.1 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 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 3 + ALC_FLR.1.

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.

2 Identification

Certification Identification	
Certification ID	CSEC2014005
Name and version of the certified IT product	LogPoint 5.2.5
Security Target Identification	LogPoint A/S LogPointTM 5.2.5 Common Criteria EAL3+ Security Target, LogPoint A/S, 2015-04-16, document version 030
EAL	EAL3 + ALC_FLR.1
Sponsor	LogPoint A/S
Developer	LogPoint A/S
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2015-08-28

3 Security Policy

The security functional requirements implemented by the TOE are grouped under the following Security Function Classes:

- SIEM
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

3.1 SIEM

Broadly the SIEM security features of LogPoint™ can be described as:

- Data collection
- Data normalization
- Data storage
- Data indexing
- Data enrichment or Lookup
- Search
- Dashboard
- Alert
- Correlation
- Incident
- Report

Each of them is described in more detail in the Security Target [ST].

3.2 Security Audit

The TOE performs auditing of authentication attempts and administrative actions, and stores these audit data. The TOE audit logs include all of the following: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. These audit logs can be reviewed by an authorized user (including sorting audit output). Audit records are protected against unauthorized deletion and modification.

3.3 User Data Protection

The TOE uses access control to protect the TOE user data. The TOE user data that is protected is the event data. However, the access control policy also applies to the audit data (TSF data). Identity based access control in the form of user identification and authentication is used to provide access control. The access control policy is described below.

3.4 Multiple Access Control SFP

The TOE enforces an access control mechanism. TOE access control decisions are made based on the permission information available for a given subject and a given object.

An authorized LogPoint administrator can define the specific services for all TOE users. An authorized user account administrator can define the specific services all TOE users in the user groups Operator and Admin.

3.5 Identification and Authentication

The TOE requires that the TOE authenticate all TOE users prior to being granted access to the TOE functionality. The TOE can perform the identification and authentication of users, but may also be configured to use an LDAP server (TOE environment) for user authentication.

3.6 Security Management

The TOE provides authorized administrators with the capabilities to configure, monitor and manage the TOE to fulfill the security objectives. Security management principles relate to management of access control policies as well as management of events and incidents. Authorized administrators configure the TOE with the Console via a webbased connection.

There are a number of different roles associated with the TOE. These roles are realized through user groups. A user assumes a specific role by being a member of a specific user group. By default there are two built-in user groups: LogPoint Administrator and User Account Administrator. In order to conform to this Security Target, two additional user groups must be created, based on two built-in permission groups, Admin and Operator. The Admin user group must be created based on the Admin permission group and the Operator user group must be created based on the Operator permission group.

The four TOE user groups (roles) and their associated permissions are as follows:

- LogPoint Administrator
  - Can perform system related tasks
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- User Account Administrator
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Admin
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Operator
  - Read-only Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)

TOE users are distinct from the users of the Operating System; such as the TOE users are not users in the Operating System.

3.7 Trusted Channels

Whenever the TOE connects to a separate remote TOE for the purpose of transferring event data, the OpenVPN in the Operational Environment establishes a virtual private network (VPN) for the purpose. This ensures the confidentiality and integrity of TSF Data when it leaves the TOE boundary. The VPN is implemented using OpenVPN and this is not part of the TOE.

A HTTP connection is also used between TOE and a separate remote TOE to transfer the UUID/Identifier of the client to the server. An UUID is a unique value for each LogPoint installation and created/calculated during the installation of the LogPoint and remain unchanged during the lifetime of the LogPoint. An HTTP connection, which is established inside the VPN tunnel, is used to provide same static tunnel IP address to the OpenVPN client each time it connects to the OpenVPN server.

In regards to OpenVPN configuration and events on client side, as the configuration details (Private IP for VPN tunnel, IP address of Open Door server reachable from DLP and the password) from the VPN server is saved in the Distributed LogPoint, this starts operating as an OpenVPN client. In case of HTTP communication, a python module named “Request” acts as HTTP client and initiate HTTP connection to get static tunnel IP address for the OpenVPN session.

Similarly, in regards to OpenVPN configuration and events on the server side, when open door is enabled in the LogPoint, it behaves as an OpenVPN server, listening on UDP port 1194 for OpenVPN connection request from the client. In case of HTTP communication, gunicorn, a python application server, acts as HTTP server and listens on TCP port 18000 for HTTP request. No additional setting needs to be configured for Logpoint to make it listen to the TCP port 18000.

TLSv1.2 is the TLS protocol and DHE_RSA_AES256_SHA256 is the cipher suite explicitly defined for TLS handshake protocol on both OpenVPN client and server. In addition AES256 with CBC (Cipher Block Chaining) with SHA256 are explicitly defined as data channel protocol used for OpenVPN.

After the end of TLSv1.2 handshake protocol both OpenVPN client and server possesses a shared master secret, which is used to encrypt the bulk data i.e. actual LogPoint event data.

OpenSSL command line tool is used to create a private key, a Diffie-Hellman key and a X.509 certificate. OpenSSL uses “libcrypto”, which is a general-purpose cryptographic library, and “libssl”, which is a SSL specific cryptographic library.

The cryptographic library “libcrypto v1.0.0” and “libssl v1.0.0”, relied upon by the OpenSSL, which is relied upon by OpenVPN, which ultimately relied upon, by the TOE has been tested by the developers of “LogPoint A/S”. The implementation of “libcrypto v1.0.0” and “libssl v.1.0.0” is outside the TOE scope, and its internals are not covered by the evaluation.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

Two usage assumptions have been defined in the Security Target [ST]:

MANAGEMENT It is assumed that LogPoint administrators are trained, qualified, non-hostile and follow all guidance.

A.USERS It is assumed that authorized users have the authorization to access at least some of the information managed by the TOE and that they act in a cooperating manner.

4.2 Environmental Assumptions

Nine environment assumptions have been defined in the Security Target [ST]:

A.LOCATE It is assumed that the TOE is physically secure, i.e. no unauthorized persons have physical access to the TOE and its underlying system.

A.FIREWALL The IT environment shall provide a firewall or other suitable means to protect the TOE from untrusted networks.

A.INTEROPERATIVE The TOE shall be used in a way that it is interoperable with the network it monitors.

A.TIME The IT environment shall provide reliable timestamps to the TOE.

A.ENRICHMENT The IT environment shall provide appropriate data enrichment sources.

A.KEYS It is assumed that private RSA keys used for the VPN nodes and the VPN tunnel are of high quality and not disclosed.

A.LDAP The IT environment shall provide a trusted and reliable LDAP server for user authentication. LDAP server is an optional component.

A.NET The network that the authorized administrator uses to access the LogPoint Console is trusted.

A.SMTP The IT environment shall provide a trusted and reliable SMTP server for email exchange. The IT Environment shall provide a secure connection from the TOE to the SMTP server

4.3 Organizational Security Policies

Five Organizational Security Policies have been defined in the Security Target [ST]:

P.MANAGE The TOE shall provide the means to configure and manage the TOE security functions.

P.SIEM_COLLECT All events from devices are collected and stored.

P.SIEM_ANALYZE All events from devices are monitored and reported upon.

P.SIEM_MANAGE Events correlated and classified as incidents are managed to resolution.

P.SIEM_PURPOSE Event data collected and/or generated by the TOE is used for authorized purposes only.

4.4 Clarification of Scope

Six threats have been defined in the Security Target [ST]:

T.INSIDER An authorized user may intentionally or unintentionally remove or destroy TOE user data, disclose TOE user data or halt the TOE without being detected.

T.UNAUTH An unauthorized user may gain access to the TOE security functions, TSF data or user data that is under the control of the TOE so that it is being disclosed, compromised or destroyed.

T.ACCESS An authorized user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted.

T.OVERFLOW An unauthorized entity may halt the execution of the TOE or cause malfunction of the TOE by creating an influx of user data that the TOE cannot handle.

T.FAIL_TO_DETECT The TOE may analyze event data received from each device and fail to recognize vulnerabilities or inappropriate activity by an unauthorized user.

T.FAIL_TO_REACT The TOE may fail to react to identified or suspected vulnerabilities or malicious attack on the enterprise network by an unauthorized user.

5 Architectural Information

The TOE consists of a set of software applications that collectively make up the TOE.

The hardware platform on which the TOE is installed is dedicated to functioning as the TOE with no secondary function. The TOE can also be installed on a virtual machine with the same restriction that the machine only functions as the TOE.

For a TOE installation that consists of more than one appliance operating as a distributed system, each appliance has the same hardware and software requirements as described below.

The TOE runs on any Linux-based operating system. However, for the purpose of evaluation, the following hardware and software configuration is used:

Item	Identification	Description
Operating System	Ubuntu 12.04.3 LTS	
Hardware	Intel-compatible quad core CPU, 2GHz minimum Memory: 8GB or more recommended Disk Space 100GB (RAID-1 protected) recommended Network adapter: 1GB network adapter	
Software	Mongo DB v1.8.3	an open-source document database, and leading NoSQL database
	Nginx v1.1.19	an HTTP and reverse proxy server, as well as a mail proxy server
	Gunicorn v18.0	a Python WSGI HTTP Server for UNIX
	Openvpn v2.3.4	OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections
	Openssl v1.0.1f	OpenSSL is an open-source implementation of the SSL and TLS protocols

Table 1: Hardware and Software

All of the required software, including the TOE, Operating system and other software is provided as an ISO image file/patch that is delivered electronically to the customer.

To access the TOE web interface, an authorized user requires a network-attached computer with a compatible browser installed (Google Chrome, Mozilla Firefox 10.x or later, Microsoft Internet Explorer 7 or later, Apple Safari).

If LDAP is used for user authentication then a suitable LDAP server needs to be installed. OpenLDAP is included in Ubuntu's default repositories under the package "slapd". Appropriate measures shall be employed to ensure the security of user credentials delivered from the TOE to the LDAP server.

6 Documentation

the following guidance documentation is part of the TOE:

- LogPoint™ 5.2.5 Release Notes [RELEASE]
- LogPoint™ 5.2.5 Installation Manual [INSTMAN]
- LogPoint™ 5.2.5 Administrator Manual [ADMMAN]
- LogPoint™ 5.2.5 User Manual [USRMAN]
- LogPoint™ 5.2.5 Security Guide [CCGUIDE]

7 IT Product Testing

7.1 Developer Testing

7.1.1 Testing Effort

The developer uses manual tests, within a partially virtualized environment. The test network consists of multiple TOEs as well as various test servers (e.g., LDAP).

The test cases are clearly documented, stating:

- the required environment configuration
- the purpose of the test
- test instructions (steps)
- expected results
- observed outcome
- test analysis (pass/fail)

7.1.2 Approach

The testing approach of the developer is to test all TOE interfaces, as well as all TOE subsystems.

All claimed TOE security functions are covered by test cases.

7.1.3 Configuration

The TOE is deployed in a distributed configuration, i.e., multiple TOE devices are present in the test environment. Depending on the test case, a single device or the distributed configuration is used.

Several test log sources (devices) are present in the environment. They are used to exercise various collectors/fetchers during specific test cases, e.g., for FTP, syslog or OPSEC.

7.1.4 Depth

The developer has tested all interfaces, fetchers and collectors. Specific test cases were provided for each kind of protocol, e.g., syslog or OPSEC.

7.1.5 Results

The developer has provided the results of all test cases. All tests were successfull.

7.2 Evaluator Testing Effort

7.2.1 Testing Effort

The evaluator added additional test cases to verify the user access right testing and negative testing of the authentication.

The test cases were clearly documented, stating the

- Starting Configuration
- Purpose
- Procedure
- Expected Results
- Actual Results

- Pass/Fail
- Clean Up

7.2.2 Approach

The evaluator performed additional testing to cover all SFRs as stated in the Security Target. In addition, negative testing was performed to verify the proper function of the authentication mechanisms.

7.2.3 Configuration

The testing environment of the developer was used for the evaluator testing. I.e., the same resources as for the developer had been available.

7.2.4 Depth

The evaluator performed test cases specific for the selected protocol / functionality, and observed the results that were logged by the TOE.

7.2.5 Results

All test cases completed successfully, i.e., no errors were observed.

7.3 Evaluator Penetration Testing

7.3.1 Effort

The evaluator performed manual tests against multiple TOE interfaces. The test documentation clearly states the

- Test description
- Tested vulnerability
- Additional pre-test actions
- Additional post-test actions
- Test actions
- Expected results
- Observed results

7.3.2 Approach

Based on the TOE design and evaluation scope, the evaluator identified the TOE's log file parsers as the exposed attack surface. The focus of the tests was therefore to cause unintended behavior of the TOE by providing malicious log content.

7.3.3 Configuration

The evaluator installed the TOE in a single-appliance configuration. Due to the nature of the exposed attack surface, testing the distributed configuration would not generate any security benefit. The evaluator used additonal client machines to provide the malicious content to the TOE.

7.3.4 Depth

The evaluator identified the log parsers that are in use by the TOE and performed attacks against each of them. Each parser was provided with input specific to its protocol/technology.

7.3.5 Results

All tests completed successfully. I.e., no negative behaviour was observed.

8 Evaluated Configuration

The evaluated configurations of LogPoint v5.2.5 should be deployed in either of the following operational environments:

- Single LogPoint appliance
- Multiple LogPoint appliances working together in a distributed configuration

The operational environment includes all of the source machines and other network devices such as firewalls that provide event data to the LogPoint v5.2.5. The TOE user is required to create an Operational Environment that ensures the level of security needed to protect the data stored on the LogPoint system.

The following functionalities are not supported in the evaluated configuration.

- Do not enable LogPoint Lite.
- Do not enable support connection at the time of installation.
- The li-admin should not be used for the operation in evaluated configuration after the installation procedure is completed.
- Disable SSH connection for li-admin and support user using the command “disable-sshusers” from the terminal.
- Do not configure Alert notification setups such as SSH, SNMP and HTTP. Only Email alert notification is supported in the CC evaluated configuration.
- Built in collectors and fetchers are part of evaluated configuration. Any other collectors and fetchers other than in the table Collectors and Fetchers should not be configured/installed.
- Do not change the default-predefined limit of 90% for Disk Usage Notification.

The TOE consists of the following software components:

1. LogPoint v5.2.0 application, which is available as a DVD ISO image.
2. LogPoint v5.2.3 Patch
3. LogPoint v5.2.4 Patch
4. LogPoint v5.2.5 Patch
5. SecurityUpdate v2.0 Security Patch
6. SecurityUpdate v3.0 Security Patch
7. SecurityUpdate v4.0 Security Patch
8. SecurityUpdate v5.0 Security Patch

For the purposes of defining the TOE configuration, two specific scenarios are presented:

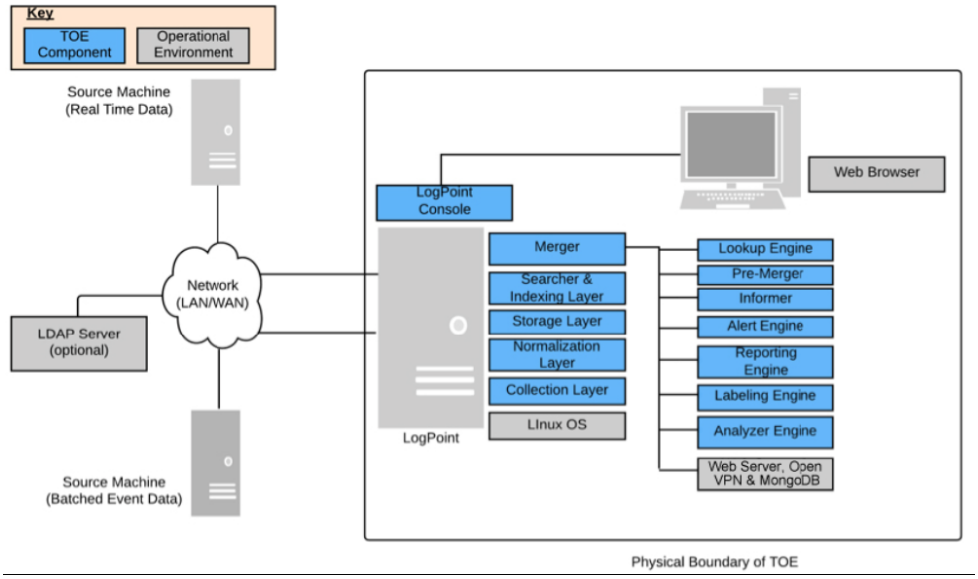

Figure 2: Single Appliance LogPoint Deployment

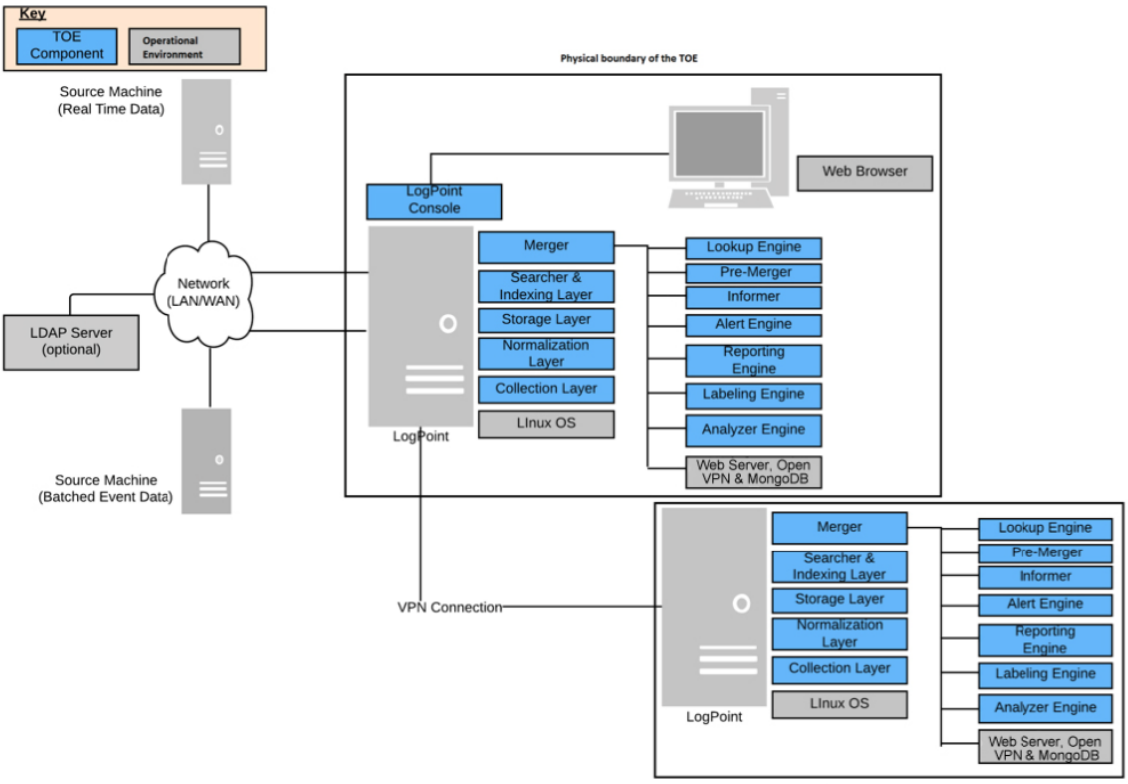

Figure 3: Multiple Appliance LogPoint Deployment

Whenever the TOE connects to a separate remote TOE (Multiple Appliance LogPoint Deployment) for the purpose of transferring event data, the OpenVPN in the Operational Environment establishes a virtual private network (VPN) for the purpose. This ensures the confidentiality and integrity of TSF Data when it leaves the TOE boundary. The VPN is implemented using OpenVPN and this is not part of the TOE.

9 Results of the Evaluation

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
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
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Authrisation controls	ALC_CMC.3	Pass
Implementation representation CM coverage	ALC_CMS.3	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Flaw reporting procedure	ALC_FLR.1	Pass
Development	ADV	Pass
Security Architecure description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.3	Pass
Architecual design	ADV_TDS.2	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: Basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Vulnerability analysis	AVA_VAN.2	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

Augmentation	The addition of one or more requirement(s) to a package.
Authentication data	Information used to verify the claimed identity of a user.
Authorised user	A user who may, in accordance with the SFRs, perform an operation.
Class	A grouping of CC families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Element	An indivisible statement of security need.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Family	A grouping of components that share a similar goal but may differ in emphasis or rigour.
Guidance documentation	Documentation that describes the delivery, preparation, operation, management and/or use of the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Operation (on an object)	A specific type of action performed by a subject on an object.
Operational environment	The environment in which the TOE is operated.

Organisational Security Policy (OSP)	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
PP evaluation	Assessment of a PP against defined criteria.
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Function Policy (SFP)	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
Semiformal	Expressed in a restricted syntax language with defined semantics.
ST evaluation	Assessment of an ST against defined criteria.
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE evaluation	Assessment of a TOE against defined criteria.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functionality (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.
Transfers outside of the TOE	TSF mediated communication of data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted path	A means by which a user and a TSF can communicate

	with necessary confidence.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
TSF Interface (TSFI)	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
User	See external entity
User data	Data created by and for the user, that does not affect the operation of the TSF.

12 Bibliography

[CCp1]	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001
[CCp2]	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002
[CCp3]	Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004
[SP-002]	Evaluation and Certification, SP-002, Issue: 22.0, 2014-12-12, 14FMV9859-38:1, FMV/CSEC
[ST]	LogPoint A/S LogPointTM 5.2.5 Common Criteria EAL3+ Security Target, LogPoint A/S, 2015-04-16, document version 030
[ADMMAN]	Welcome to LogPoint Administrator Manual Release 5.2.5, Manual Release 5.2.5, 2015-07-17
[CCGUIDE]	Security Guide - Supplement for Common Criteria - Operational User Guidance and Preparative Procedures,Version 008, 2015-07-13
[INSTMAN]	LogPoint Welcome to Installation Manual Release 5.2.5, 2015-02-20
[RELEASE]	Release Notes LogPoint v5.2.5, 2015-07-20
[USRMAN]	Welcome to LogPoint User Manual Release 5.2.5, 2015-05-06

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 2014-05-14:

QMS 1.16.1 valid from 2014-03-27

QMS 1.16.2 valid from 2014-07-07

QMS 1.17 valid from 2014-11-20

QMS 1.17.1 valid from 2014-12-02

QMS 1.17.2 valid from 2015-01-13

QMS 1.17.3 valid from 2015-01-29

QMS 1.18 valid from 2015-06-18

QMS 1.18.1 valid from 2015-08-21

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 QMS 1.18.1”.

The certifier concluded that, from QMS 1.16.1 to the current QMS 1.18.1, there are no changes with impact on the result of the certification.