Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Symantec Messaging Gateway

Certification Report
2016/101

21 October 2016
Version 1.0

Amendment Record

Version	Date	Description
0.1	13 October 2016	Internal
1.0	21 October 2016	External release

Executive Summary

This report describes the findings of the IT security evaluation of Symantec Messaging Gateway v10.6.1-4 against Common Criteria.

The Target of Evaluation (TOE) is Symantec Messaging Gateway (SMG). Symantec Messaging Gateway offers enterprises a comprehensive gateway-based message-security solution. Symantec Messaging Gateway delivers inbound and outbound messaging security, real-time anti-spam and antivirus protection, advanced content filtering, and data loss prevention in a single platform.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security audit**: The TOE generates spam reports and virus reports to provide the Administrator with insight on the filtering activity. Additionally, the TOE supports the provision of log data from each system component and supports the ability to notify an Administrator when a specific event is triggered.
- **User data protection**: The spam detection, virus detection, monitoring, and managing capabilities of the TOE ensure that the information received by the customer network is free of potential risks.
- **Identification and authentication**: The TOE supports identity-based identification and authentication of an Operator. Operators authenticate via a Web-based HTTPS GUI connected to the Control Centre, and operators can assume a role of Administrator or Limited Administrator.
- **Security management**: The TOE provides administrators with the capabilities to configure, monitor, and manage the TOE to fulfil the Security Objectives. Security Management principles relate to Security Audit, SMTP Information Flow Control, and Component Services. Administrators configure the TOE via web-based connection.
- **Trusted path/channels**: The TOE requires remote users to initiate a trusted communication path using HTTPS/TLSv1.2 for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all Symantec Messaging Gateway administrative communication. HTTPS/TLSv1.2 ensures the administrative session communication pathway is secured from disclosure and modification.

This report concludes that the product has complied with the Evaluation Assurance Level (EAL) 2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 14 September 2016.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction 1
1.1 Overview 1
1.2 Purpose 1
1.3 Identification 1
Chapter 2 – Target of Evaluation 3
2.1 Overview 3
2.2 Description of the TOE 3
2.3 TOE Functionality 3
2.4 TOE Architecture 4
2.5 Clarification of Scope 6
2.5.1 Evaluated Functionality 6
2.5.2 Non-evaluated Functionality and Services 6
2.6 Security 7
2.6.1 Security Policy 7
2.7 Usage 7
2.7.1 Evaluated Configuration 7
2.7.2 Secure Delivery 7
2.7.2.1 Assurance of Proper Physical Delivery 7
2.7.2.2 Masquerade Prevention 7
2.7.2.3 Assurance of Electronic Delivery 8
2.7.3 Installation of the TOE 8
2.8 Version Verification 8
2.9 Documentation and Guidance 8
2.10 Secure Usage 9
Chapter 3 – Evaluation 10
3.1 Overview 10
3.2 Evaluation Procedures 10
3.3 Testing 10
3.3.1 Testing Coverage 10
3.3.2 Test phases 10
3.4 Penetration Testing 10
Chapter 4 – Certification 12
4.1 Overview 12
4.2 Assurance 12
4.3 Certification Result 12
4.4 Recommendations 13
Annex A – References and Abbreviations 14

A.1 References 14
A.2 Abbreviations 15

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Symantec Messaging Gateway (SMG) against the requirements of the Common Criteria (CC), Evaluation Assurance Level (EAL) 2

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Symantec Messaging Gateway (SMG).

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Symantec Messaging Gateway (SMG)
Software Version	10.6.1-4
Hardware Platforms	Symantec 8340, 8360, or 8380 hardware appliance or as a virtual appliance on hardware specifications listed in the ST and running ESXI version 5.0 or later
Security Target	Symantec Messaging Gateway 10.6 Security Target Version 1.6, 11 October 2016
Evaluation Technical Report	Evaluation Technical Report Symantec Messaging Gateway, v1.0 dated 13 October 2016 Document reference EFS –T044 ETR

Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, September 2012, Version 3.1.Rev 4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev 4
Conformance	EAL 2
Sponsor	IP Australia 47 Bowes Street Phillip ACT 2606 Australia
Developer	Symantec Corporation 350 Ellis Street Mountain View, CA 94043 http://www.symantec.com
Evaluation Facility	BAE Systems Applied Intelligence Level 1, 14 Childers Street, Canberra, ACT, 2601 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is Symantec Messaging Gateway (SMG). Symantec Messaging Gateway offers enterprises a comprehensive gateway-based message-security solution. Symantec Messaging Gateway delivers inbound and outbound messaging security, real-time anti-spam and antivirus protection, advanced content filtering, and data loss prevention in a single platform.

The logical scope of the TOE is SMG version 10.6.1-4 running on a Symantec 8340, 8360, or 8380 hardware appliance. The TOE is also capable of running as virtual appliance on any machine that meets the required hardware specifications listed in the ST and running ESXI version 5.0 or later.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security audit**: The TOE generates spam reports and virus reports to provide the Administrator with insight on the filtering activity. Additionally, the TOE supports the provision of log data from each system component and supports the ability to notify an Administrator when a specific event is triggered.
- **User data protection**: The spam detection, virus detection, monitoring, and managing capabilities of the TOE ensure that the information received by the customer network is free of potential risks.
- **Identification and authentication**: The TOE supports identity-based identification and authentication of an Operator. Operators authenticate via a Web-based HTTPS GUI connected to the Control Centre, and operators can assume a role of Administrator or Limited Administrator.
- **Security management**: The TOE provides administrators with the capabilities to configure, monitor, and manage the TOE to fulfil the Security Objectives. Security Management principles relate to Security Audit, SMTP Information Flow Control, and Component Services. Administrators configure the TOE via web-based connection.
- **Trusted path/channels**: The TOE requires remote users to initiate a trusted communication path using HTTPS/TLSv1.2 for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all Symantec Messaging Gateway administrative communication. HTTPS/TLSv1.2 ensures the administrative session communication pathway is secured from disclosure and modification.

2.4 TOE Architecture

The Symantec Messaging Gateway Series appliances and Symantec Messaging Gateway Virtual Edition are composed of two components that can be combined on appliances or deployed with multiple appliances depending on network needs.

Consumers may deploy any appliance model as a combined control centre / scanner, dedicated scanner, or dedicated control centre.

Component	Description
Control Center	A Control Centre lets you configure and manage Symantec Messaging Gateway from a Web-based interface. From a single Web-based console, administrators can easily manage multiple Messaging Gateway appliances to view trends, attack statistics, and noncompliance incidents. Lightweight Directory Access Protocol (LDAP) credentials can be used to authenticate administrative access and configure groups and policies. One Control Center must be configured for your site. One Control Centre controls one or more Scanners.
Scanner	Scanners can perform all of the following tasks: • Process the inbound messages and outbound messages and route messages for delivery. • Download virus definitions, spam signatures, and other security updates from Symantec Security Response. • Run filters, render verdicts, and apply actions to messages in accordance with the appropriate policies and settings. You can configure one or more Scanners.
Control Center and Scanner	Performs both functions. This configuration is suitable for smaller installations.

Table 2 - TOE Components

The TOE's evaluated configuration requires one or more instances of a Scanner and one instance of a Control Centre. The TOE is integrated into a network, and all SMTP flowing into the network must pass through the services provided by the TOE.

The TOE can be implemented in a distributed manner, where one appliance running as a Control Centre communicates with multiple appliances running as Scanners.

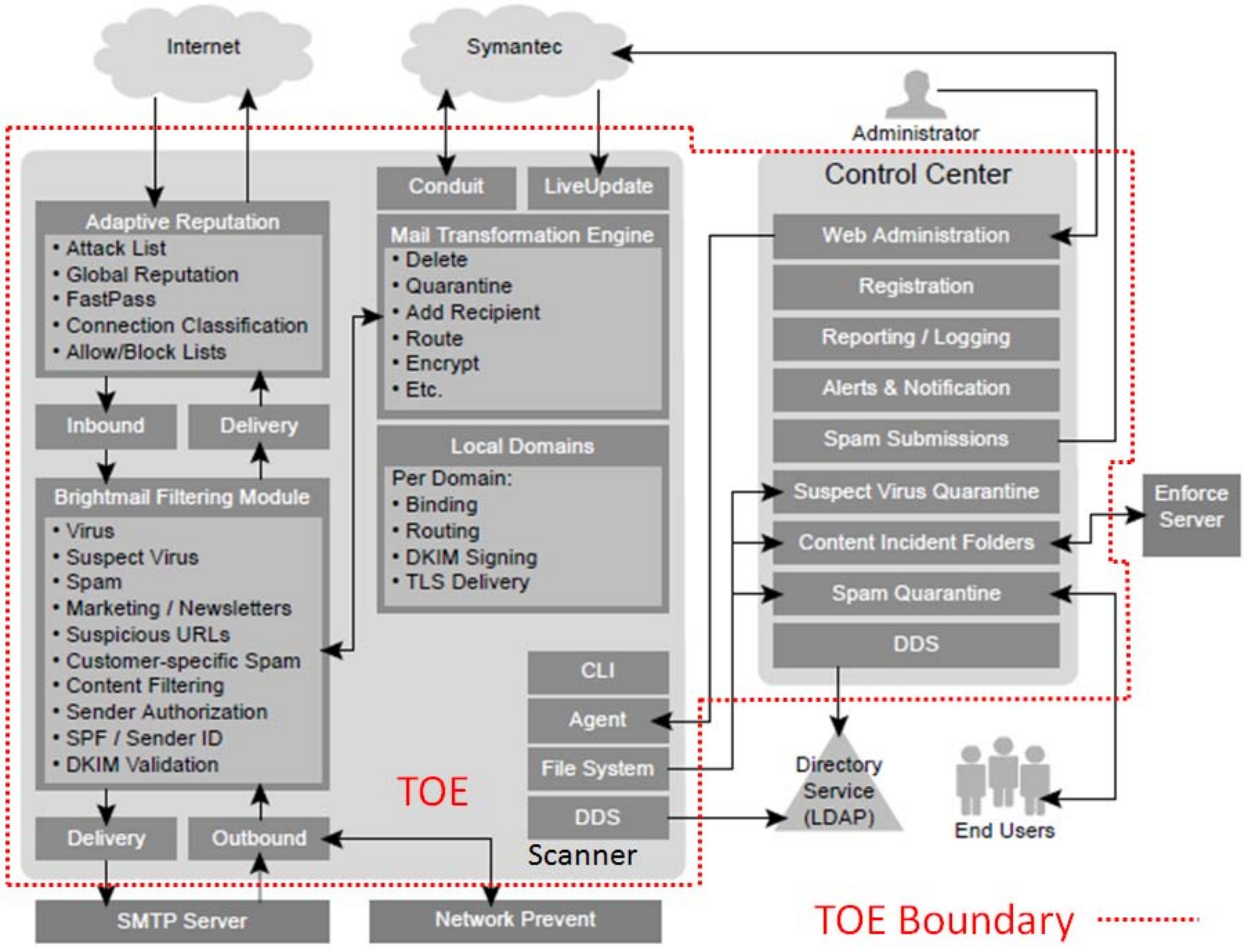

Figure 1: TOE Architecture

Figure 1 above shows how Symantec Messaging Gateway processes an email message. This diagram assumes that the message passes through the Brightmail Filtering Module to the Mail Transformation Engine without being rejected.
The path an email message takes is as follows:

1. At the gateway, global reputation determines if the sending IP is a Good Sender or a Bad Sender. It accepts or rejects the connection based on the distinction.
2. Connection Classification classifies the sending IP into one of 10 classes based on local reputation. It either accepts or defers the connection based on class membership.
3. Before the MTA accepts the message, it checks the domain address and email address. The MTA determines if it belongs to the Local Good Sender Domains or Local Bad Sender Domains group. If it does, it applies the configured action to the message. If appropriate, the MTA moves the message to its inbound queue.
4. The Brightmail Filtering Module consults the directory data service to expand the message's distribution list and determines policy group membership.
5. The Brightmail Filtering Module determines each recipient's filtering policies.
6. Antivirus filters determine whether the message is infected.

7. Spam filters determine whether the message is spam or suspected spam.
8. Unwanted mail filters (including marketing newsletters, redirect URLs, and customer-specific spam) determine whether the message is unwanted.
9. Content filtering policy filters scan the message and attachments for restricted content.
10. The Mail Transformation Engine performs actions according to filtering results and configurable policies and applies them to each recipient's message based on policy group membership.
11. Messages may be held in quarantine for review based on policy configuration. Messages in content incident folders can be remediate through the console.
12. Messages are then inserted into the delivery queue for delivery by the MTA.

Note: Symantec Messaging Gateway does not filter any messages that do not flow through the SMTP gateway. For example, it does not filter the messages that are sent between mailboxes on the same Microsoft Exchange Server or within an Exchange organization.
The administrator connects via HTTPS to the Control Centre through a Web browser to configure and manage the TOE. New administrators can be added based on attributes and group memberships that are found in LDAP directory structures. Administrative policies can be configured and assigned to specific LDAP-based groups. The TOE relies upon a NTP server in the operational environment to provide accurate timestamps.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies. The evaluated configuration is based on the default installation of the TOE with configuration implemented as per the Symantec Messaging Gateway guidance documentation (Ref 2). The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

Functionalities evaluated are as described in Section 2.3 TOE Functionality above.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 4) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

There are no components that are considered outside of the scope of the TOE.

2.6 Security

2.6.1 Security Policy

The following Organisational Security Policies apply to the TOE as specified in the ST:

POLICY	DESCRIPTION
P.INCOMING	All incoming network traffic via SMTP protocols shall be able to be monitored for malicious/undesired email.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the Symantec Messaging Gateway. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Symantec Messaging Gateway guidance documentation (Ref 2).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE.

2.7.2.1 Assurance of Proper Physical Delivery

There are a number of mechanisms provided in the below process for a customer to ensure that they have received a product that has not been tampered with.

- Outside packaging: If the outside shipping box and tape have not been broken, and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with

- Inside packaging: If the plastic bag or seal on the plastic bag are damaged or removed, the device may have been tampered with

- Delivery times: if delivery times coincide with the tracking information from the carrier, it can be assumed that the package was not tampered. It is assumed that the trusted carriers (FedEx and UPS) provide reasonable measures to protect the products from tampering during shipping.

2.7.2.2 Masquerade Prevention

There are a number of mechanisms provided in the below process for a customer to ensure that they are receiving a product sent by Symantec that has not been masqueraded by another company or entity.

Customers must request the shipment of a Symantec product. Orders are never shipped without being requested.

When a product is shipped, an Advanced Shipment Notification is sent to the email address provided by the customer when the order is taken. This email includes the following information:

- Purchase Order Number
- Symantec Order Number to be used to track the shipment
- Carrier tracking number to be used to track the shipment
- List of Items shipped including serial numbers
- Address and contacts of the customer who ordered the product and who the product will be shipped to.

If a customer wants to verify that a box they have received was sent by Symantec they can do the following:

- Compare the carrier tracking number or the Symantec order number listed in the Symantec shipment notification with the tracking number on the package received.

2.7.2.3 Assurance of Electronic Delivery

To ensure that a customer receives a product that has not been tampered with during the download process, Symantec provides a SHA-1 hash value of the ISO image, which can be verified by the end user.

Administrators should verify the hash value on the downloaded product before installing.

2.7.3 Installation of the TOE

The guidance documentation (Ref 2) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The steps to verify that the TOE version is the same as the one identified in the Security Target are as follows:

- In the Control Centre, click Administration > Hosts > Version
- On the Updates tab, click the Host drop-down list and select a host
- Examine the provided information to verify the installed version of the TOE.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased: Symantec Messaging Gateway guidance documentation (Ref 2). All Common Criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

ASSUMPTION	DESCRIPTION
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Administrators of the TOE are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.LOCATE	The processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.
A.CONFIG	The TOE is configured to handle all SMTP traffic flow.
A.TIMESOURCE	The TOE has a trusted source for system time.

The above are assumptions as listed in the ST.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Refs 5 and 6).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 3).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 7) were also upheld. The evaluation was based on the default installation and configuration of the TOE taken from Symantec Messaging Gateway guidance documentation (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

The Evaluators have examined the provided developer test documentation and found that it shows the correspondence between the tests present in the test documentation and the TSFIs identified within the functional specification. Furthermore, the Evaluator repeated a subset of developer's tests as well as performing functional and vulnerability tests developed by the Evaluator.

3.3.2 Test phases

Testing is determined in the assurance requirements in the CEM. The evaluation was conducted during the period between the 29th of June 2016 and the 14th of September 2016.

3.4 Penetration Testing

The evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with EAL 2.

Agencies can have confidence that the scope of an evaluation against an EAL 2 covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the Certifiers and of the Evaluation Technical Report (Ref 8) the Australasian Certification Authority **certifies** the evaluation of the Symantec Messaging Gateway product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied Intelligence **has determined** that Symantec Messaging Gateway upholds the claims made in the Security Target (Ref 1) and **has met** the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

The analysis is supported by testing as outlined in the CEM assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 4) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

Annex A – References and Abbreviations

A.1 References

1. Symantec Messaging Gateway Version 10.6 Security Target, v1.6 dated 11 October 2016

2. Guidance documentation:

   - Symantec Messaging Gateway 10.6 Administration Guide
   - Symantec™ Messaging Gateway 10.6 Getting Started Guide
   - Symantec™ Messaging Gateway 10.6 Installation Guide

3. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4

4. 2016 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4

6. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

7. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014

8. Evaluation Technical Report - Symantec Messaging Gateway, v1.0 dated 13 October 2016

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
ISM	Information Security Manual
MTA	Mail Transformation Engine
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interfaces
TSP	TOE Security Policy