National Cyber Security Centre

0122

Common Criteria Certification Report

No. CRP302

Egress Email and File Protection

Version 4.8

running on Microsoft Windows

Issue 1.1

August 2018

NCSC Certification Body
IA Service Management, NCSC
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme (the Scheme) and has met the specified Common Criteria (CC) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	Egress Software Technologies Limited	Developer	Egress Software Technologies Limited
Product Name, Version	Egress Email and File Protection, Version 4.8		
Platform / Integrated Circuit	None		
Description	Egress Email and File Protection provides a desktop email encryption service, designed to secure and control information.		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(s) or (c)PP Conformance	None		
EAL	EAL2		
CLEF	CGI IT UK Limited		
CC Certificate	P302	Date Certified	8 August 2017

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the NCSC Certification Body, which is managed by NCSC on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation [TOE] in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with CCRA supporting documents, CC Parts 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

The NCSC Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the above product at the stated version, to the Sponsor as summarised on Page 2 ‘Certification Statement’ of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements. *This Issue 1.1 (August 2018) of the Certification Report reflects the re-branding of the product name since Issue 1.0 (August 2017) of the Certification Report.*

2. Prospective consumers of the above product at the stated version should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to the CC EAL2 assurance level on 26 July 2017:

   Egress Email and File Protection, Version 4.8, running on Microsoft Windows

4. The Developer was Egress Software Technologies Limited.

5. The product provides a combination of policy-based gateway and desktop email encryption software designed to secure and control information. It keeps the data owner in control of shared information, allowing revoking of access to emails and attached files in real-time, even after delivery.

6. The evaluated configuration of the product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III ‘Evaluated Configuration’ of this report.

7. An overview of the TOE and its product architecture is provided in Chapter IV, TOE Architecture, of this report. Configuration requirements are specified in [ST] Section 2.

Security Target

8. [ST] fully specifies the TOE’s Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) that refine the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

9. The assurance requirements are taken from CC Part 3 [CC3].

10. The OSPs that must be met are specified in [ST] Section 4.2.

11. The environmental objectives and assumptions related to the operating environment are detailed in Chapter III (in ‘Environmental Requirements’) of this report.

Evaluation Conduct

12. The evaluation used CCRA supporting documents (as appropriate), international interpretations (as appropriate) and relevant UK interpretations.

13. The NCSC Certification Body monitored the evaluation, which was performed by the CGI IT UK Limited Commercial Evaluation Facility (CLEF), and witnessed a sample of Evaluator tests. The evaluation addressed the requirements specified in [ST]. The results of that work, completed in July 2017, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

14. The TOE should be used in accordance with the environmental assumptions specified in [ST]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

15. The TOE should be used in accordance with its supporting guidance documentation included in the evaluated configuration.

Conclusions

16. The conclusions of the NCSC Certification Body are summarised on Page 2 ‘Certification Statement’ of this report.

Recommendations

17. Chapter II ‘TOE Security Guidance’ of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

18. The TOE relies on the underlying platform (i.e. Microsoft Windows operating system) for encryption algorithms. System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that they have appropriate confidence in the encryption mechanisms of the underlying platform, particularly any patches or updates.

Disclaimers

19. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). This is

specified in Chapter III 'Evaluated Configuration' of this report. The [ETR] on which this Certification Report is based relates only to the specific items tested.

20. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the NCSC Certification Body's view on that date (see paragraph 60).

21. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V 'TOE Testing' of this report) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

22. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate authorising Scheme.

23. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

24. The opinions and interpretations stated under 'Recommendations' above and in Chapter II 'TOE Security Guidance' of this report are based on the experience of the NCSC Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

25. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

26. The Egress Switch Client (ESC) is downloaded from the www.egress.com website using a secure connection. On receipt of the TOE, the consumer should check that the evaluated version has been supplied, and should check that the security of the TOE has not been compromised during delivery. Specific advice on installation is provided in the document below:

    - ‘Egress Switch Installation and Uninstallation’ [IU].

27. The Egress Switch Gateway (ESG), Egress Switch Infrastructure (ESI) and External Connection Point (ECP) are usually supplied, installed and set up by Egress engineers. The installation can be repeated using the documents below:

    - ‘Egress Switch Gateway Installation Guide’ [ESG-IG];
    - ‘Egress Server Infrastructure Installation Guide’ [ESI-IG].

Guidance Documents

28. Specific advice on secure configuration is provided in the documents below:

    - ‘Evaluated Configuration Guide’ [ECG];
    - ‘Egress Server Infrastructure Installation Guide’ [ESI-IG].

29. The User Guide and Administration Guide documentation is as follows:

    - ‘Egress Switch Desktop Client 4.6 User Guide’ [DCUG];
    - ‘Egress Switch Administration Panel User Guide’ [APUG].

30. To maintain secure operation, the consumer should follow the guidance in [DCUG] and [APUG].

III. EVALUATED CONFIGURATION

TOE Identification

31. The TOE is *Egress Email and File Protection, Version 4.8*, which consists of:
    a) Egress Switch Client (ESC), identified as 4.80.22412;
    b) Egress Switch Gateway (ESG), identified as 4.70.225290.0;
    c) Egress Server Infrastructure (ESI), identified as 4.60.22404.0.

TOE Documentation

32. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in ‘Guidance Documents') of this report.

TOE Scope

33. The TOE scope is defined in [ST] Section 2.4.2. Functionality that is outside the TOE scope is defined in [ST] Section 2.3.

34. The product provides a number of encryption based methods for protecting data transfers, but only the secure email functionality is included within the TOE scope.

TOE Configuration

35. The evaluated configuration of the TOE is defined in [ST] Section 2.4.3. Configuration advice is provided in the Evaluated Configuration Guide [ECG].

36. The TOE consists of three logical software components, identified as:
    a) Egress Switch Client (ESC), which is client based;
    b) Egress Switch Gateway (ESG), which is server based;
    c) Egress Server Infrastructure (ESI), which is server based.

37. The ESI consists of four sub-components, identified as:
    a) External Connection Point (ECP);
    b) Internal Connection Point (ICP);
    c) Authentication Server (AuS);
    d) Database Server (DBS).

38. These components and sub-components are depicted in the figures below, which show the scope of the TOE and two (or more) instances of the TOE communicating over an insecure network. Note that:
    a) it is possible for the TOE to operate with or without the ESC component being installed on (some or all) of the email client machines;
    b) the ICP includes a means of configuring and managing the TOE;

c) all users and most administrators of the TOE need to have their own TOE account (which is separate from any account(s) they also have in the Operational Environment (OE)).

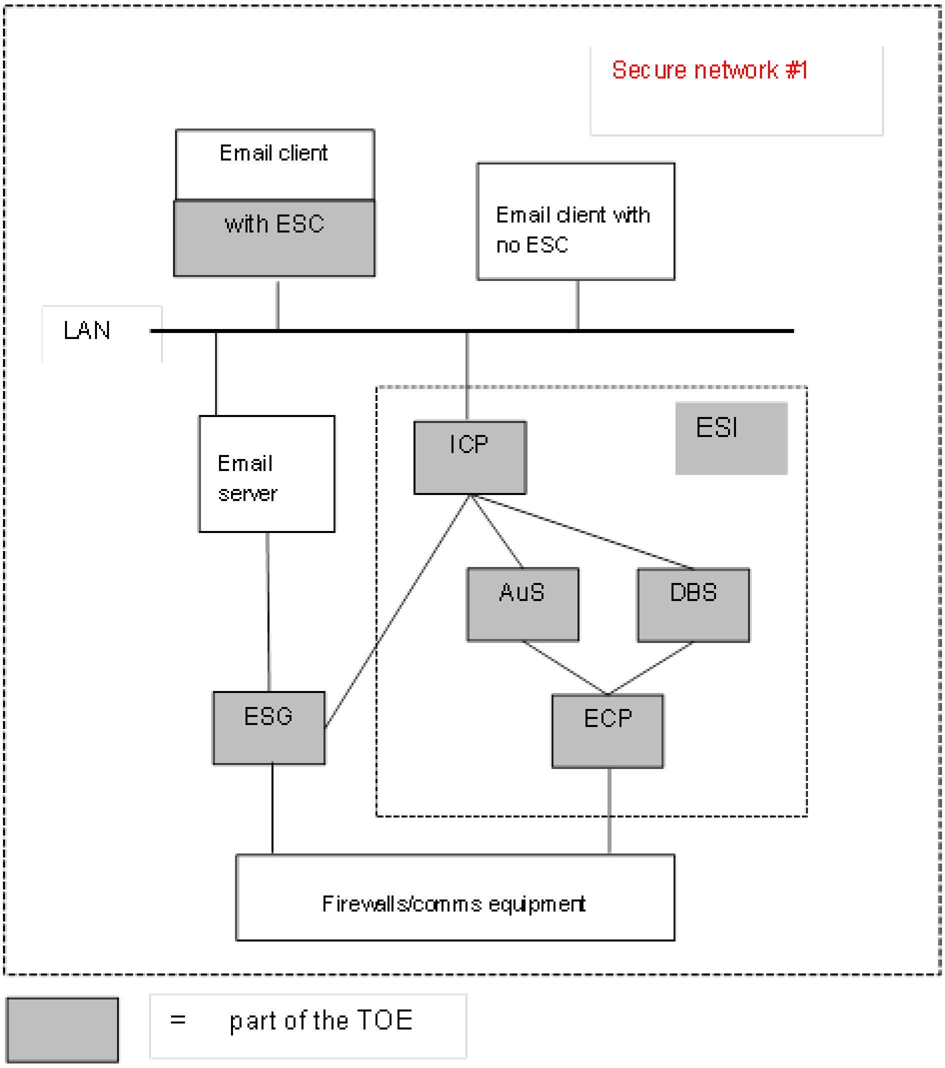
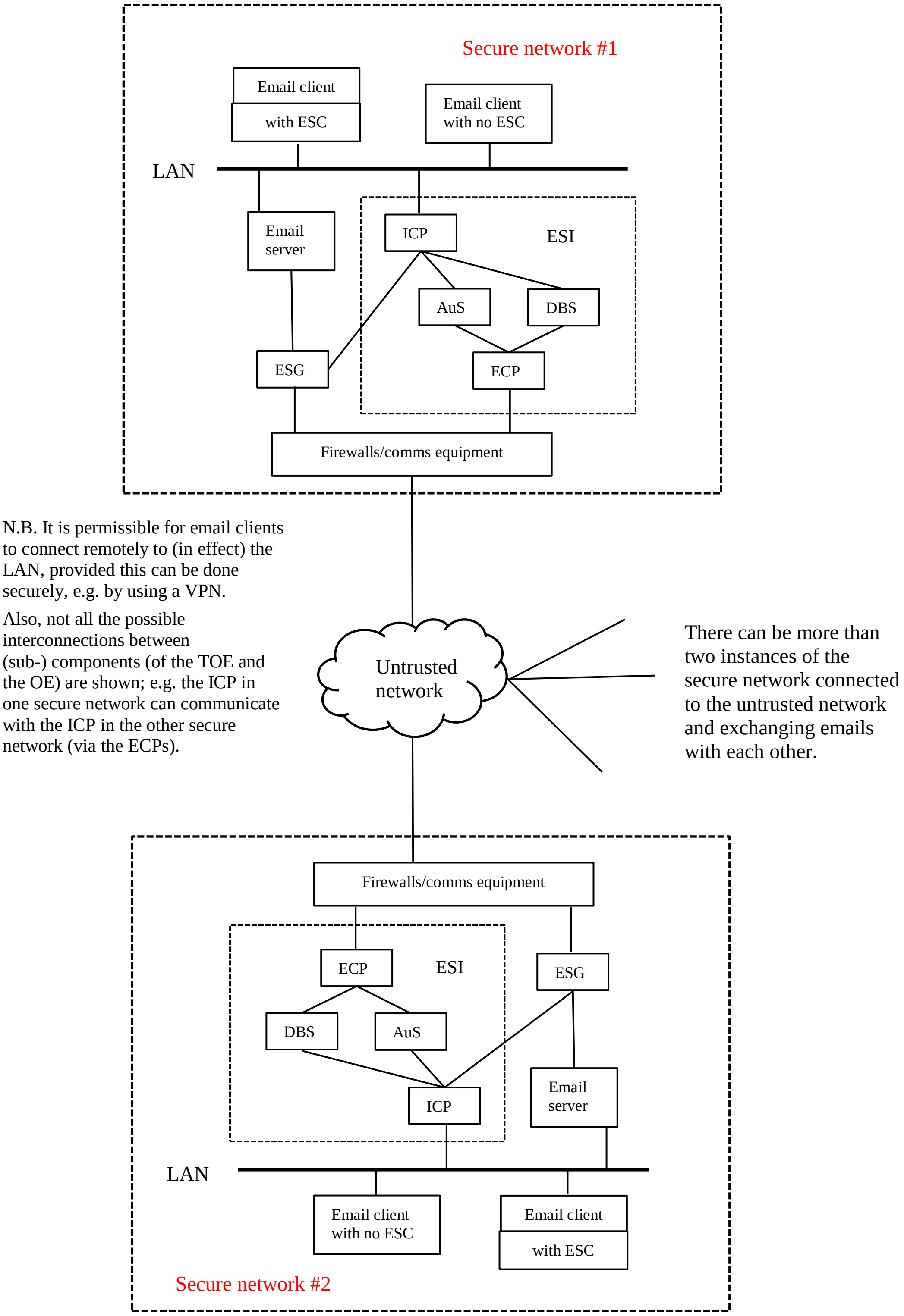


Figure 1 - Scope of the TOE



N.B. It is permissible for email clients to connect remotely to (in effect) the LAN, provided this can be done securely, e.g. by using a VPN.

Also, not all the possible interconnections between (sub-) components (of the TOE and the OE) are shown; e.g. the ICP in one secure network can communicate with the ICP in the other secure network (via the ECPs).

There can be more than two instances of the secure network connected to the untrusted network and exchanging emails with each other.

Figure 2 - Typical Setup

Environmental Requirements

39. The environmental objectives for the TOE are stated in [ST] Section 5.2

40. The environmental assumptions for the TOE are stated in [ST] Section 4.3.

41. The platforms on which the TOE runs are detailed in [ST] Section 2.4.3.

42. The environmental IT configuration is shown in the table below:

Component	Platform/Product
TOE ESG	Microsoft Windows Server 2008 R2 (64 bit), or Microsoft Windows Server 2012 R2 (64 bit) or Microsoft Windows Server 2016 (64 bit)
TOE ESC	Microsoft Windows 7 (32/64 bit), or Microsoft Windows 8.1 (32/64 bit), or Microsoft Windows 10 (32/64 bit) (all including Microsoft Outlook)
TOE ECP	As the TOE ESG
TOE ICP	As the TOE ESG
TOE AuS	As the TOE ESG
TOE DBS	As the TOE ESG (plus Microsoft SQL Server 2008 R2 or 2012)
OE email server	As the TOE ESG, including Microsoft Exchange Server
OE user PC with no ESC	As the TOE ESC
OE LDAP server	As the TOE ESG (plus Microsoft AD LDS)

Test Configurations

43. The Evaluators used the following configuration for their testing:

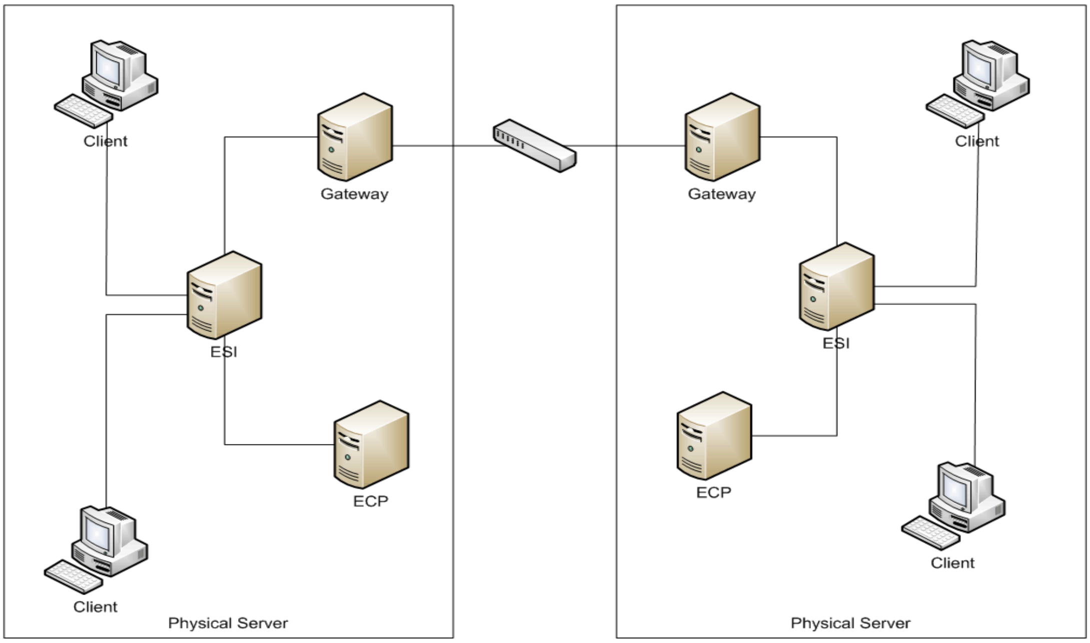


Figure 3 - Test Configuration

44. The operating systems were Windows Server 2008 R2 and Windows Server 2016 for the servers, and Windows 10 for the clients.

45. The SQL database version was 2012.

46. Each network was virtualised using Hyper-V Version 6.3.9600.16.384, running on:

    a) a PC configured with Intel Xeon E3-1270 v3 @ 3.5Ghz 3.49GHz processor with 16 Gigabytes RAM and 930 Gigabytes hard drive; and

    b) a PC configured with Intel Xeon E3-1270 v3 @ 3.5Ghz 3.49GHz processor with 16 Gigabytes RAM and 232 Gigabytes hard drive.

47. The switch was a Netgear GS208.

48. Each virtual machine was installed with a relevant version of Windows. Each machine was configured as shown below:

Machine	RAM (Gigabytes)	Disk Space (Gigabytes)
ESI1	2.0	59
WS2012ECP	2.0	59
Gateway-1	4	115
W10	1.95	59
W10C	2	49.4
ESI-2	2.0	59.6
ECP-2	2.0	49.4
Gateway	2.0	29.4
W10	1.95	59.5
W10D	1.95	59.5

49. During the Evaluators' testing, the version of Windows was updated from Server 2008 to Server 2012, so some tests were repeated, with identical results. Also, the version of the TOE was updated, so some tests were repeated, with identical results. The evaluators concluded that the operating system, provided that it continues to include the necessary encryption suites, does not affect the correct operation of the TOE.

50. The Developers used a similar configuration for their testing.

IV. TOE ARCHITECTURE

Introduction

51. This Chapter gives an overview of the product and the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III, Evaluated Configuration, of this report.

TOE Description and Architecture

52. The TOE is described in [ST] Section 2.4

TOE Design Subsystems

53. The TOE comprises the following security components:

Component	Function
Egress Switch Gateway (ESG)	The ESG is located at the boundary of a secure network, and it processes incoming and outgoing emails destined for, or coming from, the network's "vanilla" email server. Processing is dictated by the TOE's *policies* which the ESG obtains from the DBS. If a *corporate policy* dictates that an outgoing email must be encrypted, then the ESG encrypts it with a one-time AES key (unless that has already been done by an ESC component) and releases it (as part of a *package* with a unique id) for onward transmission over an insecure network. The ESG also creates a *packreg* object (containing the key and other details of the email/*package*), and stores ("registers") this in the DBS. The *packreg* may be linked to a *onemail policy* (and possibly *corporate policies* as well) which specifies any additional authentication requirements that must be met before the email's decryption key can be released. When the ESG receives an encrypted email (from another instance of the TOE) contained in a *package*, then - for recipient(s) that have ESC available - it can simply pass the email on to them via the "vanilla" email server. For other recipient(s), the ESG attempts to decrypt the email[2].
Egress Switch Client (ESC)	The ESC is installed in a *user*'s client machine, enabling that user to encrypt an outgoing email (before it is sent to the "vanilla" email server) and to decrypt an (encrypted) incoming email retrieved from the "vanilla" email server. Encryption and decryption are done in a similar manner as by the ESG. The only difference is that obtaining the decryption key for an email that was sent from within the same secure network does not involve another TOE instance.)

[2] If decryption fails for some reason, e.g. the decryption key cannot be retrieved, then the ESG's behaviour proceeds as per the relevant *policy* (which may be, for example, to forward the encrypted email to the recipient(s) with a message saying that decryption failed).

Component	Function
External Connection Point (ECP)	The ECP is located at the boundary of a secure network, and handles incoming (HTTPS) requests from another TOE instance - made on behalf of recipient(s) of an encrypted email - for a decryption key. The ECP authenticates the sender's X.509 certificate - (checking that it has not been revoked) - then passes the request on to the ICP. If the ICP decides the request is valid it provides a copy of the key, which the ECP then forwards on to the requesting TOE instance. The ECP also forwards (HTTPS) requests for a decryption key to another TOE instance on behalf of the ESG (or an ESC).
Internal Connection Point (ICP)	The ICP is located within a secure network, and handles requests for a decryption key. It also includes a facility for configuring and managing the TOE (which may be accessed from a browser via a web interface if the ICP host machine is appropriately configured). However, if a user attempts to access it, the management facility requires that user to first supply valid TOE account details (username and password).
Authentication Server (AuS)	The AuS authenticates TOE account usernames and passwords. (For example, when a user attempts to access the TOE management facility, the ICP requests the AuS to authenticate the user-supplied username and password.)
Database Server (DBS)	The DBS stores TSF and user data, particularly *policies* and *packregs*, and the TOE's audit records. This collection of data is referred to as the "TOE database".

TOE Dependencies

54. The TOE dependencies, provided by the Windows operating system, are:

- SQL Server to manage the database;
- Windows encryption algorithms to correctly perform the selected encryption/decryption.

TOE Security Functionality Interface

55. The TSFI is:

- the interface between the Egress Switch Client and Microsoft Outlook;
- the interface to the Windows encryption algorithms;
- the interface to the SQL database.

V. TOE TESTING

Developer Testing

56. The Developer's security tests covered:
    - all SFRs;
    - all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
    - all TOE Security Functionality;
    - the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interfaces') of this report;

57. The Developer's security tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. The Evaluators repeated a sample of the Developer's security tests.

Evaluator Testing

58. The Evaluators devised and ran 27 independent security functional tests, different from those performed by the Developer. No anomalies were found.

59. The Evaluators also devised and ran 11 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

60. The Evaluators completed their penetration tests on 4 May 2017.

Vulnerability Analysis

61. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

62. The platforms relevant to the TOE are detailed in Chapter III 'Evaluated Configuration' of this report.

VI. REFERENCES

[APUG]	Egress Switch Administration Panel User Guide, Egress, November 2015
[CC]	Common Criteria for Information Technology Security Evaluation (comprising Parts 1 [CC1], 2 [CC2] and 3 [CC3]).
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1 - Introduction and General Model, Common Criteria Maintenance Board, CCMB-2012-09-001, Version 3.1 R4, September 2012
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2 - Security Functional Components, Common Criteria Maintenance Board, CCMB-2012-09-002, Version 3.1 R4, September 2012
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3 - Security Assurance Components, Common Criteria Maintenance Board, CCMB-2012-09-003, Version 3.1 R4, September 2012
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, 2 July 2014
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2012-09-004, Version 3.1 R4, September 2012
[DCUG]	Egress Switch Desktop Client - User Guide v4.8, Egress, July 2017
[ECG]	Evaluated Configuration Guide, Egress, February 2017
[ESG-IG]	Egress Switch Gateway Installation Guide, Egress, Version 4.0
[ESI-IG]	Egress Server Infrastructure Installation Guide, Egress, Version 4.0
[ETR]	Evaluation Technical Report, CGI CLEF, LFL/T280 ETR, Issue 1.2, 24 July 2017
[IU]	Egress Switch Installation and Uninstallation, Egress, August 2013

[MRA]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee, Senior Officials Group – Information Systems Security (SOGIS), Version 3.0, 8 January 2010.
[ST]	Security Target, Egress, 56133.LFL/T280-cons.ST.1, Issue 1.5, 24 July 2017
[UKSP00]	Abbreviations and References, UK IT Security Evaluation and Certification Scheme, UKSP 00, Issue 1.8, August 2013.
[UKSP01]	Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 6.6, August 2014.
[UKSP02P1]	CLEF Requirements - Startup and Operations, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part I, Issue 4.6, August 2016.
[UKSP02P2]	CLEF Requirements - Conduct of an Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part II, Issue 3.1, August 2013.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML); standard CC abbreviations (e.g. TOE, TSF) in [CC1] and [UKSP00]; and abbreviations (e.g. CLEF, CR) in [UKSP00].

AD LDS	Active Directory - Lightweight Directory Service
AuS	Authentication Server
CESG	UK’s National Technical Authority for Information Assurance (CESG has been subsumed into the NCSC)
DBS	Database Server
ECP	External Connection Point
ESC	Egress Switch Client
ESG	Egress Switch Gateway
ESI	Egress Server Infrastructure
ICP	Internal Connection Point
NCSC	UK’s National Cyber Security Centre
OE	Operational Environment

(This page is intentionally blank.)

VIII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG Certified Product

Common Criteria

P302

This is to certify that

Egress Software Technologies Ltd.

Egress Email and File Protection

Version 4.8

Running on Microsoft Windows

has been evaluated under the terms of the

Common Criteria Scheme

Common Criteria

UKAS PRODUCT CERTIFICATION

INFORMATION TECHNOLOGY SECURITY SOGIS IT SECURITY CERTIFIED MUTUAL RECOGNITION AGREEMENT

AUTHORISED BY
DIRECTOR GENERAL
FOR GOVERNMENT
AND INDUSTRY CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
CGI IT UK Ltd

DATE AWARDED
8 August 2017

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.

The NCSC Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to *ISO/IEC17065:2012* to provide product conformity certification as follows:

- Category: Type Testing Product Certification of IT Products and Systems.
- Standards: Common Criteria for Information Technology Security Evaluation (CC) EAL1 – EAL7.

Details are provided on the UKAS Website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA)

The IT Product identified in this certificate has been evaluated at an accredited and licensed/approved Evaluation Facility or at an Evaluation Facility established under the laws, statutory instruments, or other official administrative procedures of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification/Validation Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification/Validation Report. The Evaluation has been conducted in accordance with the provisions of the Common Criteria Scheme and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NCSC or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the NCSC or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement.

Senior Officials Group – Information Systems Security (SOGIS) Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The NCSC Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgements or for loss sustained as a result of reliance upon those judgements by a third party.

All judgements contained in this certificate, and in the associated Certification Report, are covered by the Agreement.

In conformance with the requirements of *ISO/IEC17065:2012*, the *CCRA* and the *SOGIS MRA*, the Common Criteria website (www.commoncriteriaportal.org) provides additional information as follows:

- Type of product (i.e. product category); and
- Details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).

All IT product names and company names used in this certificate are for identification purposes only and may not be trademarks of their respective owners.

Evaluation is not a guarantee of freedom from security vulnerabilities. This certificate reflects the view of CESG at the time of evaluation. It is the responsibility of users (both prospective and existing) to check whether any security vulnerabilities have been discovered since the date shown on this certificate.