



Schedule 1 – Egress Service Definition

Table of Contents

| | | |
|-------|---|----|
| 1 | INTRODUCTION..... | 4 |
| 1.1 | Executive Summary..... | 4 |
| 2 | SERVICE OVERVIEW | 5 |
| 2.1 | Secure Communication with 3 rd Parties..... | 5 |
| 2.2 | Introduction to Egress Switch | 5 |
| 2.2.1 | Flexible Low Cost Infrastructure | 5 |
| 2.2.2 | Desktop & Gateway Email Encryption | 6 |
| 2.2.3 | Secure Large File Transfer..... | 6 |
| 2.2.4 | Secure Removable Media | 6 |
| 2.2.5 | Powerful Policy Enforcement..... | 6 |
| 3 | SECURITY ACCREDITATION | 8 |
| 3.1 | Product Assurance | 8 |
| 3.2 | Data Centre Accreditation | 8 |
| 3.2.1 | Security Standards | 8 |
| 4 | SERVICE MANAGEMENT | 10 |
| 4.1 | On-boarding Process..... | 10 |
| 4.2 | Off-boarding Process | 10 |
| 4.2.1 | Notification of Requirements for Termination Services | 10 |
| 4.2.2 | Integrated Transition Planning..... | 10 |
| 4.2.3 | Production of Exit Plans | 11 |
| 4.2.4 | Content of the Exit Plan | 11 |
| 4.2.5 | The Exit Plan will contain, as a minimum:..... | 11 |
| 4.2.6 | In addition, the Exit Plan shall:..... | 12 |
| 4.3 | Back-up & Disaster Recovery Process..... | 12 |
| 5 | SERVICE CONSTRAINTS | 13 |
| 5.1 | Maintenance Schedule | 13 |
| 5.2 | Service & Severity Levels..... | 14 |
| 5.3 | APPENDIX TO PART A | 15 |
| 5.3.1 | Compensation Scheme | 15 |
| 5.3.2 | Availability..... | 15 |
| 5.3.3 | Service Credits..... | 16 |
| 6 | PROFESSIONAL SERVICES..... | 17 |
| 6.1 | Administrator Training..... | 17 |
| 6.2 | Account Customisation | 17 |
| 7 | SOFTWARE EVALUATION | 18 |
| 7.1 | How to Trial Egress Switch..... | 18 |

| | | |
|-------|--|----|
| 7.2 | Features of the Business Trial | 18 |
| 7.3 | Technical Requirements & Service Dependencies..... | 18 |
| 8 | CONSUMER RESPONSIBILITIES | 19 |
| 9 | CHARGING & INVOICING..... | 20 |
| 9.1 | Part A – Charging..... | 20 |
| 9.1.1 | Milestone Payments | 20 |
| 9.1.2 | Service Charges | 20 |
| 9.2 | Part B – Invoicing | 20 |
| 9.2.1 | Supplier Invoices | 20 |
| 9.2.2 | Payment Terms | 21 |
| 10 | TERMINATION TERMS..... | 22 |

1 INTRODUCTION

1.1 Executive Summary

The purpose of this document is to provide a high-level description of the Egress Software Technologies security service's technical and operational model.

The intended audience of this document are public and private sector organisations that require the ability to share confidential information with third parties that are unable to access or utilise Government Secure Networks.

2 SERVICE OVERVIEW

2.1 Secure Communication with 3rd Parties

Service users and customers have a reasonable expectation that their sensitive personal information will be shared securely and efficiently between Government organizations and third parties. However, it is commonly accepted that there is currently no pan Government solution for communication of confidential data outside of Government networks.

Current local solutions are either designed to meet specific service needs, installed as local implementations, or simply not practical for day to day use (e.g. Winzip).

Existing national investment is targeted at improving secure communications within different parts of the public sector, for example Central Government to Local Government or within the NHS. However, there already exists a daily need to communicate with a large number of voluntary, community sector, and private sector partners and providers which are not currently supported by these initiatives.

Egress Software fully acknowledges the role of GCMail, NHSmail, CJSM, and other secure Government networks like GSI and PNN in addressing many of the issues with regards internal communication between local and central Government, health, and criminal justice organizations. Designed to compliment these projects, Egress offer security services that addresses a key gap identified across local and central Government where there is no coherent or widely recognized way of communicating sensitive personal/business information with partners and service providers in the third sector, private sector, or even small Government agencies.

Useful links:

Improving Support for Collaboration (“Secure communications with 3rd Parties”)
<http://tinyurl.com/bljaxy>

Secure Communications with Third Parties Project
<https://govx.socitm.gov.uk/spaces/sc3p/>

2.2 Introduction to Egress Switch

2.2.1 Flexible Low Cost Infrastructure

Leveraging patented key management and a choice of on-premise or hosted infrastructure, Egress Switch enables organisations and individuals to rapidly deploy email & file encryption throughout their business, without the need for end user training.

2.2.2 Desktop & Gateway Email Encryption

Sending messages and attachments by email remains the most popular business tool for sharing information. For this reason, confidential data is increasingly sent to unauthorised recipients accidentally resulting in costly fines and damaged reputations.

Egress Switch provides a unique and transparent way to encrypt email that is simple to use and fast to deploy using integrated desktop, gateway, and mobile applications. MS Outlook and Lotus Notes add-ins enable users to send and receive information in the usual manner. The Egress Switch policy engine removes unnecessary decisions, and administrators can configure policies such as enforced encryption based on email address, size, content & type of data. Alternatively, users can be given freedom of choice when sending information externally.

2.2.3 Secure Large File Transfer

Today's businesses often need to exchange large volumes of information that is too big to be sent by email. Egress Switch integrates transparently with all internet server protocols (FTP(s), HTTP(s), MS SharePoint) to enable users to upload large files to the internet or to local secure servers.

Confidential files are encrypted locally then uploaded via a secure channel to administrator defined server addresses. Recipients are then notified of the secure file location to download. Files downloaded from the secure server still have the added benefit of 'follow the data' encryption and can be managed in real-time like any other Switch file delivery mechanism. Cloud storage is also provided for organisations that want to avoid the cost and infrastructure required for hosting and managing the uploaded information.

2.2.4 Secure Removable Media

Physical media such as CD/DVD and USB flash drives are popular and cost effective options for exchanging large amounts of information. Egress Switch enables organisations to share information on any type of removable media. The Egress Switch client includes an integrated burning application for securely authoring CDs, DVDs and Blue Ray media. Unlike traditional security products Egress Switch can provide real-time access control and auditing of physical media.

2.2.5 Powerful Policy Enforcement

At the heart of the Egress Switch infrastructure is a powerful and flexible policy engine. The policy engine is centrally managed allowing

administrators to enforce decisions over how data should be sent, what security policies are required, and how data access is audited.

Useful links:

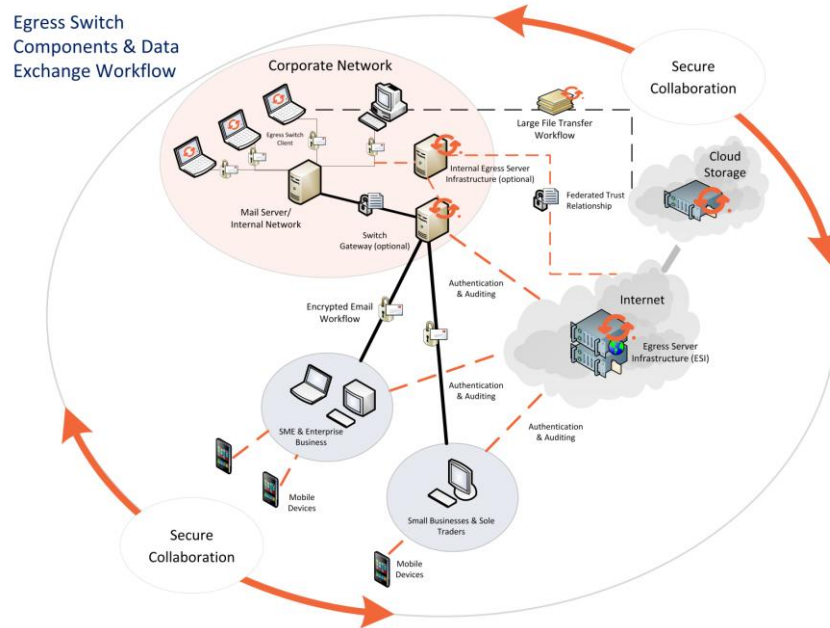
Egress Switch Datasheet

http://www.egress.com/assets/files/Egress_Switch_Data_Sheet_v2.4.pdf

Switch Fusion Datasheet

http://www.egress.com/assets/files/Egress_Switch_Fusion.pdf

Egress Architecture



3 SECURITY ACCREDITATION

3.1 Product Assurance

3.1.1 CESG Claims Tested Mark (CCTM)

The CESG Claims Tested Mark (CCTM) scheme provides a government quality mark for the public and private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by vendors.

Certification details:

Product Name: Egress Switch
Vendor Name: Egress Software Technologies
Models/Version: 2.3
CCTM Awarded Date: 10th June 2011
CCTM Valid Until Date: 9th June 2012
CCTM Certificate Number: 2011/06/0099

Please refer to Schedule 3.1 (“CCTM-CERT-2011-06-99”).

Useful links:

Marketing Statement

http://www.cesg.gov.uk/products_services/iacs/cctm1/cctm-55.shtml

IA Claims Document

http://www.cesg.gov.uk/products_services/iacs/cctm1/pdf/cctm_doc_icd_egress.pdf

Test Report Summary

http://www.cesg.gov.uk/products_services/iacs/cctm1/pdf/cctm_doc_trs_egress.pdf

3.2 Data Centre Accreditation

3.2.1 Security Standards

To underline our commitment to security Egress Software Technologies only work alongside Partners that consistently demonstrate industry best practise.

3.2.1.1 Controlled Access

Access to building, data floors, and individual areas is via individually programmed access cards leveraging the latest in biometric and visual identification to ensure secure, single-person entry.

3.2.1.2 Accreditations

- I. ISO 27001:2005
- II. ISO 9001:2008
- III. ISO 14001:2004
- IV. PAS 2060:2010

Note:

For more detailed information please refer to Schedule 3.2 (“UK Fast-Data-Centre-Outsourcing”)

4 SERVICE MANAGEMENT

4.1 On-boarding Process

Please refer to Schedule 4.1 ("Project Implementation Plan Example.zip")

4.2 Off-boarding Process

4.2.1 Notification of Requirements for Termination Services

The Customer shall require the provision of Termination Services by notifying the Supplier in writing ("**Termination Assistance Notice**") such notice to be provided at least six months prior to the date of termination or expiry of this Contract or any part of this Contract or as soon as reasonably practicable (but in any event, not later than three months) following the service by either Party of any notice to terminate. The Termination Assistance Notice shall specify the:

- 4.2.1.1 date from which Termination Services are required which shall be no earlier than 12 months prior to expiry of this Contract or from the service by either Party of any notice to terminate, as the case may be;
- 4.2.1.2 nature of the Termination Services required; and
- 4.2.1.3 period(s) during which it is anticipated that Termination Services will be required, recognising that the Termination Services may comprise a number of different elements each of which may involve a different delivery period, but in no event shall any such element continue longer than 6 months from the date that the Supplier ceases to provide the Services unless subsequently modified pursuant to paragraph 5.9.

4.2.2 Integrated Transition Planning

- 4.2.2.1 As soon as reasonably practicable following the Supplier's or the Customer's receipt of a Termination Assistance Notice, the Supplier, the Customer and the Replacement Supplier will work together in good faith, to assist the Customer in the development of its Integrated Transition Plan based on the Exit Plan and the implementation plan agreed between the Customer and the

Replacement Supplier in respect of the transfer of services to the Replacement Supplier;

4.2.2.2 As soon as possible following the appointment of any Replacement Supplier, the Customer, the Supplier and such Replacement Supplier will review the Exit Plan and agree any required changes to be made to the Exit Plan, having regard to the methods, processes and strategy to be used by the Replacement Supplier for transfer of responsibility of the Services without impacting on the way in which the Supplier provides the Services during the Term unless agreed between the Parties.

4.2.3 Production of Exit Plans

The Supplier shall produce a full version of the Exit Plan within twelve months after the Effective Date and shall review and (if appropriate) update the Exit Plan to reflect changes in the Service:

4.2.3.1 every twelve (12) month thereafter; and

4.2.3.2 within 30 days after service of notice of termination by either Party,

In each case setting out the Suppliers proposed methodology for achieving an orderly transition of Services from the Supplier to the Customer and/or its Replacement Supplier on the expiry or termination of this Contract and which complies with the requirements set out in paragraphs 4.2.4 and 4.2.5.

4.2.4 Content of the Exit Plan

4.2.4.1 Within 30 days after the submission of the Exit Plan, the Parties will use their respective reasonable endeavours to agree the contents of the Exit Plan. If the parties are unable to agree the contents of the Exit Plan then such dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.2.5 The Exit Plan will contain, as a minimum:

4.2.5.1 separate mechanisms for dealing with Ordinary Exit and Emergency Exit, the provisions relating to Emergency Exit being prepared on the assumption that the Supplier may be unable to provide the full level of assistance which is required by the provisions relating to Ordinary Exit, and in the case of Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Customer shall

require to enable the Customer or its subcontracts to provide the Services;

4.2.5.2 the description of both the transfer and cessation processes, including an illustrative timetable, applicable in the case of an Ordinary Exit and an Emergency Exit.

4.2.6 In addition, the Exit Plan shall:

4.2.6.1 document how the Services could transfer to the Replacement Supplier and/or the Customer, including details of the proposed arrangements for transferring documentation, data, contracts and the segregation of the Customer's technology components from any technology components operated by the Supplier or its Sub-contractor (where applicable);

4.2.6.2 specify the scope of the Termination Services that may be required for the benefit of the Customer any charges that would be payable for the provision of such Termination Services and detail how such services would be provided (if required), during the Termination Assistance Period;

4.2.6.3 address each of the issues set out in this schedule to facilitate the transition of the Services from the Supplier to the Replacement Supplier and/or the Customer with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period;

4.2.6.4 provide a timetable and implementation plan, including details of the Supplier's expected levels of resources, and identify critical issues and risks in providing the Termination Services.

4.3 Back-up & Disaster Recovery Process

4.3.1 Egress Software Technologies Ltd has invested extensively to create a resilient and robust managed service architecture. Egress Software offer a unique managed service that is highly scalable and utilises the benefits of dedicated ISO 9001 server data-centres combined with the flexibility of cloud services.

The Egress service is distributed across multiple data centres located in different geographical locations providing 100% uptime. This ensures the Switch service is available 24/7 without any service interruption or loss of data. In addition, bare metal backups of all servers are performed daily to ensure any server can be restored in minutes in the event of failure.

5 SERVICE CONSTRAINTS

PART A

5.1 Maintenance Schedule

- 5.1.1 The Supplier shall create and maintain a rolling maintenance schedule with regard to the Services to be agreed with the Customer. The Maintenance Schedule shall be discussed annually in advance and updated by the Project Board in accordance with the procedures set out in Schedule 5.1 (“Governance”).
- 5.1.2 When the Supplier wishes to carry out any maintenance to the Services (other than Emergency Maintenance), it shall ensure that;
 - 5.1.2.1 the timing of the planned maintenance is in accordance with the requirements of the Maintenance Schedule or is an otherwise agreed in writing with the Customer’s Representative at least 10 Working Days in advance;
 - 5.1.2.2 in carried out during Non-Core Hours;
 - 5.1.2.3 once agreed with the Customer’s Representative the planned maintenance (which shall be known as ‘Permitted Maintenance’) is forthwith entered onto the Maintenance Schedule; and
 - 5.1.2.4 the permitted Maintenance is subsequently carried out in accordance with the Maintenance Schedule
 - 5.1.2.5 The Supplier will be allowed to book a maximum of 24 hours Service Downtown for Permitted Maintenance in any one calendar month which shall take place between the hours and on the day specified in the Maintenance Schedule unless otherwise agreed in writing with the Customer. For the avoidance of doubt Permitted Maintenance shall not exceed 24 hours per calendar month. However a maximum 11 periods of downtime per annum with be allowed under this Agreement. This must be agreed annually in advance between the Supplier and the Customer.
 - 5.1.2.6 Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with paragraph 5.1.2.5 will be subtracted from the total number of hours in the relevant Service Period when calculating Availability, in accordance with the Appendix to this Part A.
 - 5.1.2.7 Service Points shall accrue as set out in the Appendix to this Part A if any Service Downtime occurs as a result of Emergency Maintenance

undertaken by the Supplier or where maintenance undertaken by the Supplier exceeds 24 hours in any Calendar Month.

5.1.2.8 The Supplier shall carry out any necessary maintenance where it reasonably suspects that the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such time as to avoid (or where this is not possible so as to minimise disruption to the Services).

5.1.2.9 The Supplier will provide wherever possible five days notice information the Customer which weekends will be affected by planned maintenance, however if a requirement becomes urgent then this may not be possible.

PART B

5.2 Service & Severity Levels

Please refer to Schedule 5.2 (“Egress Client and User Services Agreement”).

5.3 APPENDIX TO PART A

5.3.1 Compensation Scheme

The following compensation scheme will be utilised, when the system availability has been measured over a calendar month:

| System Availability | Compensation to the Customer (based upon a % of the monthly charge for that Managed Service Fees which can be credited or used for other services) |
|---------------------|--|
| 99% – 100% | 0% |
| 98% - 98.99% | 5% |
| 97% - 97.99% | 10% |
| 96% - 96.99% | 15% |
| 95% - 95.99% | 20% |
| 94% - 94.99% | 25% |
| 87% - 93.99% | 30% plus 1% per additional 0.1% decrement |

5.3.2 Availability

5.3.2.1 The Operational Service shall be Available (and “Available” shall be interpreted accordingly) when End Users are able to access and utilise all of the Operational Services during the Core Hours.

5.3.2.2 Availability is calculated from Critical calls (“Category 1 fault”) against the production environment for the Application Software. If the production environment was unavailable during the calendar month, the time it was unavailable is calculated to give the downtime for that month.

$$\text{Service Availability \%} = \frac{(\text{MP} - \text{SD}) \times 100}{\text{MP}}$$

Where:

MP = Total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = Total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service period

- 5.3.2.3 Downtime resulting from the following will not be included in the calculation above includes:
 - 5.3.2.3.1 Overrun of batch schedules where the batch run is overloaded;
 - 5.3.2.3.2 Overrun of overnight processing due to the Application Software;
- 5.3.2.4 Emergency or scheduled Maintenance as agreed with the Customer Scheduled Maintenance weekend (no more than 11 per annum), which Egress will publish and agree with the Customer at the beginning of each calendar year;
- 5.3.2.5 A hardware failure at the Customer site;
- 5.3.2.6 Internet Network failure, excluding MPLS;
- 5.3.2.7 Application Software Problems;
- 5.3.2.8 Intentional or accidental damage to hardware/software or communications links at the Customer Site by non-Supplier personnel.

5.3.3 Service Credits

- 5.3.3.1 Any Service Credits paid to the Customer under this Service Agreement for credits against Availability and Service performance index will be discussed with the Customer, and the Supplier shall arrange for a credit to be raised for this amount, or arrange for the provisions of service, whichever is agreed between the parties. The Service Credit Payments will be to a maximum of the one hundred percent (100%) of the total monthly Managed Service charges due to the Supplier within a calendar month relating to the Service Component affected. These are based on the Supplier receiving a minimum of 50 Category 1 fault calls within any one calendar month. For the avoidance of doubt the Supplier will not be liable for payment of compensation relating to System Availability and Service performance index for the same incident.

6 PROFESSIONAL SERVICES

6.1 Administrator Training

6.1.1 Available on request

6.2 Account Customisation

6.2.1 Available on request

7 SOFTWARE EVALUATION

7.1 How to Trial Egress Switch

A FREE 14 day trial of Egress Switch allows you to evaluate some of the advanced features Switch has to offer.

To get your trial started complete the Request form (below) and an Egress representative will be in touch with you to help get things set up.

<http://www.egress.com/free-trial/>

7.2 Features of the Business Trial

- Centralised management of users and billing
- Fully configurable user interface and recipient experience
- Access to the Egress hosted cloud storage for sharing large files
- Customisable policy notes and legal disclaimers
- Policy controls that can enforce encryption based on data type, content, location, recipient, classification, size of data, or meta data
- Access to workflow utilities to help streamline business process

7.3 Technical Requirements & Service Dependencies

- Microsoft Windows 2003, XP, Vista, or 7 (32/64 bit)
- Apple Mac OS X 10.6 or later
- Microsoft .NET framework 2.0 SP1+ Runtime libraries
- MS Outlook 2003/2007/2010 (not required)
- Internet Connection

8 CONSUMER RESPONSIBILITIES

Please refer to Schedule 5.2 (“Egress Client and User Services Agreement”).

9 CHARGING & INVOICING

9.1 Part A – Charging

The purpose of this Part A of the schedule is to set out the provisions relating to the Charges applicable to the Services.

9.1.1 Milestone Payments

Not used.

9.1.2 Service Charges

The customer will pay the Service Charges to the Supplier for all Operational Services annually to the end of the Term.

Annual Subscription

| Quantity | Product Code | Per User Cost (£) |
|--------------|--------------|-------------------|
| 1 - 1000 | ESA1000 | 30.00 |
| 1001 - 2500 | ESA2500 | 28.50 |
| 2501 - 5000 | ESA5000 | 27.00 |
| 5001 - 7500 | ESA7500 | 25.50 |
| 7501 - 10000 | ESA10000 | 24.00 |
| Contact us | Contact us | Contact us |

Note:

- I. The user cost listed above includes Standard Support & Product Maintenance (Premium Support is also available at an additional charge).
- II. Site Licenses are available on request.
- III. Multiple Year Contracts are available on request.
- IV. Any Service Charges will be payable annually in advance.

9.2 Part B – Invoicing

This Part B of the schedule sets out the method by which the Supplier shall raise invoices to the Customer for payment, together with the requirements which apply to such invoices, and the payment terms thereof.

9.2.1 Supplier Invoices

9.2.1.1 The Supplier shall ensure that each document contains the following information:

- I. The data of the invoice;
- II. A unique invoice number;
- III. The year or other period(s) to which the relevant Charge(s) relate;
- IV. Details of the correct Contract reference;
- V. The reference number of the purchase order issued by the Customer to which it relates (if any);
- VI. The total Charges gross and net of any applicable deductions and, separately, the amount of any disbursements properly chargeable to the Customer under the terms of the Contract, and, separately, any VAT on other sales tax payable in respect of the same;
- VII. A contact name and telephone number of a responsible person in the Supplier's financial department and in the event of administrative queries;
- VIII. The banking details for payment to the Supplier via electronic transfer of funds (ie name and address of bank, sort code, account name and number) and;
- IX. The Supplier VAT and Company Registration numbers;

Note:

All Supplier invoices shall be expressed in sterling

9.2.2 Payment Terms

The Customer shall make payment to the Supplier within thirty (30) days of receipt of a valid invoice by the Customer at its nominated address for invoices.

10 TERMINATION TERMS

Please refer to Schedule 5.2 (“Egress Client and User Services Agreement”).