



CCTM IA CLAIMS DOCUMENT (ICD)

Echoworx

Managed Secure Email and Managed Secure Documents v6
Managed Secure Email and Managed Secure Documents: Secure Mail (v6); Secure DOX (v6); Period of assessment: 01/01/09 – 12/15/09;

VENDOR DETAILS	TEST LABORATORY DETAILS
Echoworx	SiVenture
4101 Yonge Street Suite 708 Toronto, Ontario Canada M2P 1N6	Unit 6 Cordwallis Park Clivemont Road Maidenhead, Berkshire SL6 7BU
Telephone Number: +1 416 226 8600	Telephone Number: +44 (0) 1628 6513 66
Email: aligiannis@echoworx.com	Email: simon.milford@siventure.com
Website: http://www.echoworx.com	Website: http://www.siventure.com

CERTIFICATE DETAILS	
CCTM Certificate Number	2010/02/0068
CCTM Awarded on	5 th February 2010
CCTM Award Expires on	4 th February 2011
ICD Issue Date	5 th February 2010

TABLE OF CONTENTS

1	INTRODUCTION.....	3
1.1	Background.....	3
1.2	Objectives.....	3
1.3	Purpose of Document.....	3
1.4	Structure.....	4
2	SERVICE DESCRIPTION.....	5
2.1	Service Identification.....	5
2.2	Service Overview.....	6
2.3	Usage assumptions.....	11
3	CCTM CLAIMS FOR THE IS SERVICE.....	13
3.1	Claims Statements.....	13
3.2	Existing assurance certificates.....	14
ANNEX A	GLOSSARY OF TERMS.....	15
A.1	Acronyms.....	15
A.2	Glossary.....	16
ANNEX B	MARKETING STATEMENT.....	17

1 INTRODUCTION

1.1 Background

This document outlines the IA claims made by Echoworx in regard to the suitability of the Managed Secure Email and Managed Secure Documents portfolio of services for use in the UK Public Sector for sending and receiving secure email (including attachments) and protection of files and folders.

The Portfolio comprises the following services:

- Secure Mail - a plug-in that handles the complexity of encrypting, decrypting, digitally-signing and authenticating S/MIME email messages.
- Secure DOX - offers enterprises a secure, collaborative environment for sharing encrypted files and folders.

This ICD only focuses on Secure Mail, & Secure DOX. The S/MIME encryption keys used by both products are generated by the Echoworx Secure Services (ESS) platform. ESS provides a fully-managed public key infrastructure (PKI), with automated key and certificate management, digital ID recovery and managed key escrow.

The Portfolio has been originally developed and marketed by Echoworx Corporation (4101 Yonge Street, Suite 708, Toronto, Ontario M2P 1N6 Canada).

1.2 Objectives

1.2.1 The objectives of this ICD are to provide:

- identification within the Managed Secure Email and Managed Secure Documents Portfolio of the services Secure Mail and Secure DOX;
- a service overview, detailing the functionality and security architecture of the Secure Mail and Secure DOX services;
- identification of the assets to be protected and the threats to these assets;
- a description of the expected operational environment, organisational security policies and environmental security requirements;
- the security claims for the Secure Mail and Secure DOX services.

1.3 Purpose of Document

1.3.1 This document is the ICD for Managed Secure Email and Managed Secure Documents Portfolio of services

1.3.2 This ICD is the baseline document for the CCTM Claims Test of Managed Secure Email and Managed Secure Documents Portfolio of services.

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material.
- Section 2 contains the description of functionality of the services Secure Mail and Secure DOX; and all the information related to the security of these services Secure Mail and Secure DOX.
- Section 3 details the security functionality claims that are being made.

2 SERVICE DESCRIPTION

2.1 Service Identification

Service Name: Managed Secure Email and Managed Secure Documents

Versions: There is no overall version number for the Managed Secure Email and Managed Secure Documents, the individual components to be evaluated under this ICD are at the following versions:

Secure Mail v6;

Secure DOX v6;

The following table identifies the platforms to be used for testing and for which the CCT Mark will apply:

Software component	Version / service pack
Secure Mail	
Operating system	Microsoft Windows XP Professional with Service Pack 3, 32 bit Microsoft Windows Vista Ultimate, 32 or 64 bit Microsoft Windows 7 32, or 64 bit
Email client	Microsoft Outlook 2002 or above Microsoft Windows Live Mail Microsoft Outlook Express 6.0 or above
Web browser	Internet Explorer 6.0 on Windows XP Internet Explorer 7.0 on Windows Vista (32-bit) Internet Explorer 7.0 on Windows Vista (64-bit) Internet Explorer 8.0 on Windows 7 (32-bit) Internet Explorer 8.0 on Windows 7 (64-bit)
Secure DOX	
Operating system	Microsoft Windows XP Professional with Service Pack 3 Microsoft Windows Vista SP1, 32 bit
Web browser	Internet Explorer 6.0 and 7.0 on Windows XP Internet Explorer 8.0 on Windows Vista (32-bit)

Period of Assessment: Jan 01, 2009 to Dec 15, 2009.

2.2 Service Overview

The service portfolio comprises five distinct services for: facilitating the exchange of secure email; supplying encrypted documents via the web; providing the facility for users to encrypt files and folders.

This ICD has been written for the evaluation of two of the services:

- Secure Mail;
- Secure DOX;

2.2.1 Secure Mail

Secure Mail uses industry trusted standards and provides simple, cost effective, end-to-end email encryption as a managed service that resides within the messaging environment. Subscribers digitally sign, encrypt and decrypt messages using desktop and mobile email clients such as Microsoft Outlook and Outlook Express/Windows Live Mail. Run from a centrally managed encryption platform, Secure Mail is simple to deploy and requires minimal administration.

2.2.2 Secure DOX

Secure DOX is a data encryption application that allows businesses to easily and cost effectively protect sensitive information stored on local drives, removable drives (e.g. USB keys) and shared network drives.

Whether it's enabling workgroups to securely share documents on an internal file server or protecting sensitive information stored on a laptop, Secure DOX can help establish a data privacy best practice, minimize the risk of a costly data breach and enable compliance with government laws, industry regulations and partners that mandate the encryption of sensitive data.

2.2.3 Security architecture

2.2.3.1 Overview

The Echoworx Secure Services (ESS) platform provides elements of the security architecture used by the services under test (see 1.1 Background for more details regarding the ESS).

The platform provides Global Directory, Administration, Reporting, Provisioning, Branding, and Key and Trust

Services to the Portfolio services. These services enable the following features:

- subscribers to be registered and administered
- certificates to be signed in trust and managed on behalf of the subscribers
- enterprise-specific branding to be applied to those elements of the services viewed by subscribers and recipients
- public credentials to be served to requesting Portfolio services for purposes of encryption
- key escrow to enable managed recovery of nominated subscriber cipher keys
- reporting of enterprises and subscriptions.

The figure below illustrates the ESS platform services and illustrates the hardware components on which the services run. The hardware in the Echoworx hosting environment is configured for resilience (dual servers, load-balanced, with resilient network connectivity).



2.2.3.2 Public Key Infrastructure

The managed PKI provides trusted certificates with a trusted certification path to Echoworx Root CA Certificate, which is WebTrust Certified (<https://cert.webtrust.org/ViewSeal?id=548>) and audited by Deloitte to assure integrity of the Echoworx CA root certificate. There are established key and certificate life

cycle management controls, maintained and monitored on an ongoing basis through operations policies and procedures, and regular auditing.

Echoworx is a Microsoft Root CA Program Member (<http://support.microsoft.com/kb/931125>), ensuring that the Echoworx CA Root Certificate is distributed with Windows Operating Systems and Windows Critical Updates.

All certificate management is driven by end-user management operations; there is no need to manage certificates separately. Two certificates are issued for each subscriber: one for signing and one for cipher operations.

2.2.3.3 Security Profile and Standards

The following lists the security profile of the ESS platform and services:

- 1024 bit RSA End-user Keys
- SHA-1 hash
- PKIX X.509v3 certificates & CRLs
- PKCS#10 certificate signing request
- PKCS#12 key storage
- 3DES and AES-256 symmetric encryption
- S/MIME PKCS#7 encrypted e-mail format, Internet Email and MIME
- HTML / XML, HTTP 1.1 / SSL

2.2.3.4 CA Key Security

The following lists the security profile of the CA key:

- 2048 bit CA keys
- CA Key Generation/Protection
- CA Keys generated/stored on SafeNet LunaSA HSM
- LunaSA is a FIPS 140-2 Level 3 compliant device
- Keys replicated up to partition on a backup HSM for DR/BCP, with HSM Management for storing keys managed remotely

- Keys signed by WebTrust certified Echoworx ROOT CA for leveraging public trust

2.2.4 Hardware requirements

The minimum hardware requirements for running the Managed Encryption Services are specific to the individual service.

2.2.4.1 Secure Mail

5-10 MB of free hard drive space

Pentium 233 MHz (Pentium 500 MHz recommended)

128 MB RAM (256 MB or greater recommended)

Non-registered users who are recipients of an email from a Secure Mail user have no hardware or platform constraints (apart from access to the internet).

2.2.4.2 Secure DOX

5-10 MB of free hard drive space

Pentium 1.6 GHz or greater

512 MB RAM or greater

NTFS, FAT32, UNIX/LINUX (shared network folder only)

2.2.5 Software requirements

The software requirements for running the Managed Secure Email and Managed Secure Documents are specific to the individual services:

2.2.5.1 Secure Mail

Operating System Support

Microsoft Windows XP Professional with Service Pack 3, 32 bit

Microsoft Windows Vista SP1 or greater, 32 or 64 bit

Note: Installation requires administrative privileges.

Email Client Compatibility

Microsoft™ Outlook® 2007 (Recommended)

Microsoft™ Outlook® 2003 (Recommended)

Microsoft™ Outlook® 2002

Microsoft™ Windows® Mail

Microsoft™ Outlook Express® 6.0 or above

Web Browser Compatibility

Internet Explorer 6.0 or above

Firefox 3.0 or above

Internet Connection Requirements

Minimum 56 Kbps dial-up modem

LAN-based using standard TCP/IP

DSL, ADSL, Cable Modem

Note: If you are using a firewall/proxy the client must be able to communicate with the Secure Mail application back-end.

Note that: for non-registered recipients of an email from a Secure Mail user the software constraints are merely the use of a standards compliant email client and web browser.

2.2.5.2 Secure DOX**Operating System Support**

Microsoft Windows XP Professional with Service Pack 3

Microsoft Windows Vista SP1, 32 bit

Note: Installation requires administrative privileges.

Web Browser Compatibility

Internet Explorer 6.0 or above

Internet Connection Requirements

Minimum 56 Kbps dial-up modem

LAN-based using standard TCP/IP

DSL, ADSL, Cable Modem

2.2.6 Out of Scope

Secure Mail for Lotus Notes or Web Mail clients are not part of the Managed Secure Email and Managed Secure Documents.

The use of this product to encrypt data above IL2 (Restricted or above) is beyond the scope of the CCTM scheme.

2.3 Usage assumptions

2.3.1 Assets

The following assets are to be protected by use of Managed Secure Email (Secure Mail) and Managed Secure Documents (Secure DOX) services:

- Email and their attachments e.g. bank statements, invoices, notices and other forms where protection of the confidentiality and integrity of the document is essential.
- Files and folders selected by the user where protection of the confidentiality and integrity of the files and folders is essential

2.3.2 Threat scenario

The following threats to assets are countered by use of Managed Secure Email and Managed Secure Documents service:

- The threat of email and attachments being intercepted in transit to their intended recipient. Whereupon their confidentiality and possibly their integrity are compromised.
- The threat of files and folders being disclosed to unauthorised individuals, by copying from a desktop or laptop PC, or retrieving from a removable storage device (such as a USB memory stick). Whereupon their confidentiality and possibly their integrity are compromised.

2.3.2.1 Expected operational environment

Secure Mail

Secure Mail operates in the environment where activated Secure Mail users wish to maintain privacy in the email communications they exchange with other Secure Mail users and with other non-Secure Mail users. Secure Mail allows a user to sign, encrypt, decrypt and authenticate email messages using desktop and mobile email clients.

Secure DOX

Secure DOX operates in the environment where activated Secure DOX users wish to protect specific files and folders, and to be able to share those encrypted files and folders with other nominated Secure DOX users. Users can create one or more encrypted files or folders anywhere: hard drives, network drives, and USB keys. All content remains encrypted on the storage device and only the owner or the users that have been granted permission can read and write to the file or folder.

2.3.2.2 Organisational security policies

Secure Mail and Secure DOX rely on the individual to select which content requires encryption.

2.3.2.3 Security requirements on the environment

Secure Mail requires that the subscriber's computer meets certain cryptographic requirements, which it establishes as part of the plug-in installation process.

Secure DOX uses the Microsoft cryptographic key store in which to hold the subscriber's credentials.

3 CCTM CLAIMS FOR THE IS SERVICE

3.1 Claims Statements

3.1.1 Secure Mail

Claims Reference	Claims Statements
CS1	Installing Secure Mail enforces password policy
CS1a	Subscriber registration enforces secure storage of credentials
CS2	The ability to send an encrypted and digitally signed email to another registered user
CS2a	The ability to send digitally signed email to any address
CS3	Sending encrypted and digitally signed email to a non-registered user
CS4	A registered recipient is able to decrypt and read secure email locally on their workstation
CS5	A registered recipient is able to verify origin of a secure email
CS5a	A registered recipient is able to verify integrity of a secure email
CS6	A non-registered recipient is able to read a secure email
CS7	A non-registered recipient can make a secure reply
CS8	A non-registered recipient can verify origin of email
CS9	A non-registered recipient can verify the integrity of email

3.1.2 Secure DOX

Claims Reference	Claims Statement
CS10	Installation of Secure DOX and registration of users enforces password setup
CS11	The user of Secure DOX has the ability to create Secure Folders.
CS12	Data in Secure DOX Files and Folders Remains Encrypted.
CS13	The Secure DOX Encryption Wizard simplifies the process of encrypting files and folders.
CS14	Ability to grant other Secure Dox users access to Secure Folders.
CS15	Ability to generate a list of all Encrypted Folders
CS16	Ability to browse the contents of an encrypted directory.
CS17	Secure DOX maintains a centrally controlled list of applications which are not permitted to decrypt data.

3.1.3 ESS Platform

Claims Reference	Claims Statement
CS18	The ESS Platform is operated and managed securely and meets or exceeds industry recognized security standards and audits, including SAS70, WebTrust, and ISO27001.

3.2 Existing assurance certificates

The existing assurance certificates are referenced below.

Microsoft Windows XP Professional with Service Pack 3, FIPS certificate 989, Windows XP Enhanced Cryptographic Provider (RSAENH), Microsoft Windows Vista Ultimate, FIPS certificate 893, Windows Vista Enhanced Cryptographic Provider (RSAENH), WebTrust Certification for Certificate Authorities

ANNEX A GLOSSARY OF TERMS

A.1 Acronyms

The following table gives all the acronyms that have been used in this ICD and the corresponding description of the acronym.

Acronym	Description
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
BCP	Business Continuity Planning
CA	Certification Authority
CCT	CESG Claims Tested
CCTM	CESG Claims Tested Mark
CSP	Cryptographic Service Provider
DR	Disaster Recovery
EMX	Encrypted Message eXchange
ESS	Echoworx Secure Services
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IA	Information Assurance
ICD	Information Assurance Claims Document
OS	Operating System
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
MIME	Multi-purpose Internet Mail Extensions
RSA	(Rivest, Shamir and Adleman) Algorithm for Public Key cryptography
SHA-1	Secure Hashing Algorithm
S/MIME	Secure MIME
SSL	Secure Socket Layer
Sub CA	Sub Certification Authority
USB	Universal Serial Bus
URL	Uniform Resource Locator
X.509	ITU-T standard for PKI and Privilege Management Infrastructure.
XML	Extensible Markup Language

A.2 Glossary

The table below gives all the technical terms that have been used in this report and the corresponding description of the terms.

Term	Description
Administrator	A user with special privileges and training, who is trusted to administer the system.
User	A user who has none of the special privileges of an Administrator.

ANNEX B MARKETING STATEMENT

The Managed Encryption Service provides simple to deploy, easy to use information assurance for public sector bodies processing data at HMG Business Impact Levels 1 and 2 carrying the Protective Marking PROTECT. The elements available are:

Secure Mail:

Provides standards-based encryption, decryption and digital signatures within supported email clients. Emails can be securely sent to, decrypted and verified by recipients, whether or not they also have Secure Mail.

Secure DOX:

Provides encryption and controllable sharing of sensitive information stored on local disks, removable media and shared network drives, protected by strong credentials.

The Managed Encryption Service provides a Public Key Infrastructure using X.509 Certificates, and handles public/private key administration, completely transparent to the user.