



## CCTM TEST REPORT SUMMARY

### Echoworx

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

<b>VENDOR DETAILS</b>	<b>TEST LABORATORY DETAILS</b>
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

<b>Test Report Summary Reference Number</b>	LGNT-TR-0003
<b>Test Report Summary Version Number</b>	1-0
<b>Test Report Summary Date</b>	5 <sup>th</sup> February 2010
<b>CCTM Certificate Number</b>	2010/02/0068

Reproduction is authorised provided the document is copied in its entirety

Further details about the claims tested are included in [ICD] - published on the CCTM website ([www.cctmark.gov.uk](http://www.cctmark.gov.uk)).

## **1 EXECUTIVE SUMMARY**

### **1.1 Scope of IS Service Claims Tests**

The Echoworx Managed Secure Email (Version 6) and Managed Secure Documents (Version 6) services form part of the Echoworx Secure Services (ESS) platform. The Managed Secure Email service is used to send and receive secure email, including attachments. The Managed Secure Documents service is used to protect sensitive files and folders. The ESS platform provides a fully-managed public key infrastructure (PKI), with automated key and certificate management, digital ID recovery and managed key escrow. For further details, see sections 2.1 and 2.2 of [ICD].

The period of the assessment for the Service, for which the claims were validated using customer questionnaires, was 1<sup>st</sup> January 2009 – 15<sup>th</sup> December 2009.

### **1.2 Test Results**

The CCTM Claims Testing of the Echoworx Managed Secure Email (Version 6) and Managed Secure Documents (Version 6) services, period of assessment January 2009 to December 2009, by SiVenture, concluded that the security functionality claims made within the IA Claims Document [ICD] are valid.

### **1.3 Observations and Recommendations**

Section 2.1 of [ICD] lists the platforms on which the Secure Mail plug-in can be installed. The Secure Mail application interacts with the operating systems FIPS certified Microsoft Enhanced Cryptographic Providers. At present the Windows 7 Enhanced Cryptographic Provider has not fully completed the FIPS approval process, but it is due to complete in 2011. The older Microsoft operating systems Enhanced Cryptographic Providers are all FIPS approved.

It should also be noted that the Secure DOX plug-in application is called Secure Files on the Internet download and help pages.

## **2 CCTM TEST OVERVIEW**

### **2.1 Introduction**

This Test Report documents the results of the CCTM Claims Tests of the IS Service as detailed in [ICD].

### **2.2 Scope of IS Service Claims Tests**

Sections 2.1-2.2 of [ICD] describe the scope of the IS Service to be Claims Tested. The Test Laboratory confirmed this to be accurate for the IS Service tested.

Sections 2.2 and 2.3 of [ICD] summarise the security features, environmental assumptions, expected operational environment, operational security issues and threats, and platforms.

Section 2.2.4 of [ICD] details the security features of The Echoworx Managed Secure Email (Version 6) and Managed Secure Documents (Version 6) that were not tested under the CCTM Scheme. In particular, the cryptographic algorithms used in IS Products and Services are not tested under the CCTM Scheme.

Section 3.1 of [ICD] specifies the CCTM Claims tested by the Test Laboratory on the IS Service. The Claims Tests were only performed with the IS Service running on the platform combinations and IT environment detailed in the Test Configuration section. The platforms themselves were not tested under the CCTM Scheme.

### **2.3 Location and Date of Tests**

Section 3.3 of [ICD] details the location[s] where the Test Laboratory conducted Claims Testing and where witness testing was undertaken.

The start and end dates of Claims Testing were as follows:

10<sup>th</sup> December 2009 – 15<sup>th</sup> December 2009.

Interviews of customer of the IS Services were conducted on:

17<sup>th</sup> December 2009.

## 2.4 Platform Configuration

The platforms supported by the IS Service and used in the Claims Tests are detailed in the following tables.

IS Service: Managed Secure Email (Secure Mail)

Version: v6

Platforms:

Software component	Version / Service Pack
Operating system	Microsoft Windows XP Professional SP3 (32-bit) Microsoft Windows Vista Ultimate (32-bit and 64-bit) Microsoft Windows 7 Ultimate (32-bit and 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 and 64-bit) Internet Explorer 8.0 on Windows 7 (32-bit and 64-bit)

IS Service: Managed Secure Documents (Secure DOX)

Version: v6

Platforms:

Software component	Version / Service Pack
Operating system	Microsoft Windows XP Professional SP3 (32-bit) Microsoft Windows Vista Ultimate (32-bit)
Web browser	Internet Explorer 6.0 and 7.0 on Windows XP Internet Explorer 8.0 on Windows Vista (32-bit)

## 2.5

The test configuration comprised the product running on the platform combinations detailed in the tables below.

User	Service	Operating System	Email Client	Browser
User1	Secure Mail	XP Pro (32-bit)	Outlook 2002	IE6
User2	Secure Mail	XP Pro (32-bit)	Outlook Express	IE6
User3	Secure Mail	Vista Ultimate (32-bit)	Windows Mail	IE7
User4	Secure Mail	Vista Ultimate (64-bit)	Outlook 2003	IE7
User5	Secure Mail	7 (32-bit)	Outlook 2007	IE8

CCTM Test Report Summary: Managed Secure Email (v6) and Managed Secure Documents (v6)

User	Service	Operating System	Email Client	Browser
User6	Secure Mail	7 (64-bit)	Outlook 2007	IE8
User7	Secure DOX	XP Pro SP3 (32-bit)	N/A	IE6
User8	Secure DOX	XP Pro (32-bit)	N/A	IE7
User9	Secure DOX	Vista Ultimate (32-bit)	N/A	IE8
Default	Non-registered	XP Pro SP3 (32-bit)	Outlook Express Thunderbird	IE6 Firefox

The test user configurations were used to test the Claims Statements as shown in the table below.

Claim Reference	IS Service	Users tested (see test platform configurations)
CS1	Secure Mail	User1, User2, User3, User4, User5, User6
CS1a	Secure Mail	User1, User2, User3, User4, User5, User6
CS2	Secure Mail	User1, User2, User3, User4, User5, User6
CS2a	Secure Mail	User1, User2, User3, User4, User5, User6
CS3	Secure Mail	User1, User2, User3, User4, User5, User6
CS4	Secure Mail	User1, User2, User3, User4, User5, User6
CS5	Secure Mail	User1, User2, User3, User4, User5, User6
CS5a	Secure Mail	User1, User2, User3, User4, User5, User6
CS6	Secure Mail	User1, User2, User3, User4, User5, User6
CS7	Secure Mail	User1, User2, User3, User4, User5, User6
CS8	Secure Mail	User1, User2, User3, User4, User5, User6
CS9	Secure Mail	User1, User2, User3, User4, User5, User6
CS10	Secure DOX	User7, User8, User9
CS11	Secure DOX	User7, User8, User9
CS12	Secure DOX	User7, User8, User9
CS13	Secure DOX	User7, User8, User9

CS14	Secure DOX	User7, User8, User9
CS15	Secure DOX	User7, User8, User9
CS16	Secure DOX	User7, User8, User9
CS17	Secure DOX	User7, User8, User9
CS17	Secure DOX	User7, User8, User9
CS18	Secure Mail Secure DOX	Not applicable

## 2.6 Test Method

The Echoworx Managed Secure Email (Version 6) and Managed Secure Documents (Version 6) were tested using the Test Method [TLG and TM] against the security claims made in the [ICD]. Section 3.3 in [ICD] identifies the Test Method for the Claims Tests carried out by the Test Laboratory.

IS Service Claims concerning procedures, performance and user aspects over the period of assessment 01/01/09 – 15/12/09 were validated as follows:

- Questioning clients of the service about their experiences.

## 3 EASE OF USE

**3.1** The installation of the applications necessary to run the IS Service was as described in [UGD] and [UGM].

**3.2** No problems were found either by the test laboratory or by customers (in responses to questionnaires).

## 4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION

The guidance documentation is detailed in [UGD] and [UGM]. These documents are available by following links in the 'Welcome' email of the service installation process. Otherwise the documents can be downloaded from <https://bt-rc.secure-mail.org.uk>.

[UGD] is a user guidance document for the Secure Documents service. It provides information on how to fully use the product as well as having a Getting Started section to guide the user through the installation process. There is also a Frequently Asked Questions chapter for any common problems that may occur

[UGM] provides the same detail as [UGD] for the Secure Mail service.

## 5 RESISTANCE TO PUBLICLY KNOWN VULNERABILITIES

A search for publicly known vulnerabilities on a sample of security websites failed to yield any known weakness in the security of the IS Service. In addition, searches failed to find any publicly known vulnerabilities in the underlying platform for which patches were not available. None of these were relevant to the test configuration. The security websites surveyed were:

<http://www.cve.mitre.org>

<http://www.us-cert.gov>

<http://www.securityfocus.com>

<http://www.nvd.nist.gov>

## 6 VALIDATION OF EXISTING ASSURANCE CERTIFICATES

The Test Laboratory confirms that the existing assurance certificates specified in [ICD] have been validated for the exact version of the IS Service that has been Claims Tested. The certificates [Certs] were correctly stated in [ICD].

Please refer to the Observations and Recommendations section of this report for information on the Enhanced Cryptographic Provider of Windows 7.

## 7 DISCLAIMERS

CCTM Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product/Service, or the IT environment supporting the IS Product/Service.

This Test Report Summary serves solely to summarise the results of testing carried out for the CCTM Scheme and is not an endorsement or otherwise of the IS Product/Service.

## 8 ABBREVIATIONS

The key IS Service abbreviations used within this Test Report are listed below. Generic CCTM Scheme abbreviations used within this report are defined in the Scheme Description [DES].

Term	Meaning
CA	Certification Authority
CSP	Cryptographic Service Provider
ESS	Echoworx Secure Services
FIPS	Federal Information Processing Standards
IA	Information Assurance
ICD	Information Assurance Claims Document
OS	Operating System
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
RSA	(Rivest, Shamir and Adleman) Algorithm for Public Key cryptography
Sub CA	Sub Certification Authority
USB	Universal Serial Bus
URL	Uniform Resource Locator
X.509	ITU-T standard for PKI and Privilege Management Infrastructure.

## 9 REFERENCES

- [Certs] FIPS-140-2 Windows XP Enhanced Cryptographic Provider (RSAENH): Cert #989, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt989.pdf>
- FIPS-140-2 Windows Vista Enhanced Cryptographic Provider (RSAENH): Cert #893, <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt893.pdf>
- [ICD] Echoworx IA Claims Document, Version 3.21, January 2010;
- [TLG] CCTM Scheme Test Laboratory Guide, Issue 3.0.0, March 2009;
- [UGD] Echoworx Encrypted Documents User Guide, Product Release 6.2, October 2009;
- [UGM] Echoworx Encrypted Mail User Guide, Product Release 6.0, April 2009;