



CCTM TEST REPORT SUMMARY

Overtis Group, Ltd

VigilancePro v2009.1.2.6
VigilancePro v2009.1.2.6 tested 31/06/08 – 01/07/09

VENDOR DETAILS	TEST LABORATORY DETAILS
Overtis Group, Ltd	Logica
Overtis Group, Ltd Electron, Fermi Avenue Harwell Science and Innovation Campus Harwell, Oxfordshire OX11 0QR United Kingdom	Logica 250 Brook Drive Green Park Reading RG2 6UA United Kingdom
Telephone Number: +44 (0) 8456 589962	Telephone Number: +44 (0) 1372 369 620

Test Report Summary Reference Number	1007.EC231200:07
Test Report Summary Version Number	V0.2
Test Report Summary Date	3 rd November 2009
CCTM Certificate Number	2009/11/0058

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).

1 EXECUTIVE SUMMARY

1.1 Test Results

The CCTM Claims Testing of VigilancePro v2009.1.2.6, period of assessment 31/06/08 – 01/07/09 by Logica concluded that the security functionality claims made within the IA Claims Document [ICD] are valid.

2 CCTM TEST OVERVIEW

2.1 Introduction

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

2.2 Scope of IS Product Claims Tests

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

As stated in section 2.2.4 of [ICD], the AES cryptographic algorithm is not within the scope of testing under the CCTM Scheme.

Section 3.1 of [ICD] specifies the CCTM Claims Tests performed by the Test Laboratory on the IS Product. The Claims Tests were only performed with the IS Product 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 where the Test Laboratory conducted Claims Testing and where witness testing was undertaken.

Claims Testing took place at the Vendor premises in Harwell on 13th – 14th July 2009.

2.4 Platform Configuration

The platforms supported by the IS Product and used in the Claims Tests are detailed in the following table. This table is consistent with the Security Architecture detailed in section 2.2.1 of the [ICD] and all the platforms specified below require .NET Framework 2 or above as a prerequisite.

With regards to the VigilancePro Server referenced below, it was essential to install the VigilancePro Server initially and set up the rules in line with the Security Claims listed in the [ICD]. Then the Agents running on the various operating systems were configured to act as agent

machines adhering to the rule sets configured on the VigilancePro Server.

Platform Ref	Operating System Name	Version	Browser	Version
VigilancePro Server	Microsoft Windows Server 2003, SP2	V 5.2.3790 SP2	N/R ¹	N/R
VigilancePro Agent – Microsoft Windows XP, SP3	Microsoft Windows XP Professional, SP3	V 5.1 build 2600, SP3 v20080414.031525	Internet Explorer 7.0	v7.0.573.0.13
VigilancePro Agent – Microsoft Windows Server 2003, SP2	Microsoft Windows Server 2003, SP2	V 5.2.3790 SP2 v20070217.021455	Internet Explorer 7.0	V7.0.573.0.13
VigilancePro Agent – Microsoft Windows Vista Ultimate, SP1	Microsoft Windows Vista Ultimate, SP1	V 6.0.6001	Internet Explorer 7.0	V7.0.600.1.18000

2.5 Test Configuration

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

Claim Statement	Operating System	Version	Browser	Platform Ref
CS1 CS2 CS3 CS4	Microsoft Windows XP Professional, SP3	V 5.1 build 2600, SP3 v20080414.031525	None ²	VigilancePro Agent – Microsoft Windows XP, SP3
CS6	Microsoft Windows	V 5.2.3790	None	VigilancePro Agent – Microsoft

¹ N/R denotes that this specific piece of information was ‘not relevant’, as the functionality was not required for any implementation.

² ‘None’ means that the Security Claims are not browser-specific but rather are tested on the Operating System.

Claim Statement	Operating System	Version	Browser	Platform Ref
CS8 CS9	Server 2003, SP2	SP2 v20070217.0 21455		Windows Server 2003, SP2
	Microsoft Windows Vista Ultimate, SP1	V 6.0.6001	None	VigilancePro Agent – Microsoft Windows Vista Ultimate, SP1
CS5 CS7	Microsoft Windows XP Professional, SP3	V 5.1 build 2600, SP3 v20080414.0 31525	Internet Explorer 7.0 v7.0.573 0.13	VigilancePro Agent – Microsoft Windows XP, SP3
	Microsoft Windows Server 2003, SP2	V 5.2.3790 SP2 v20070217.0 21455	Internet Explorer 7.0 v7.0.573 0.13	VigilancePro Agent – Microsoft Windows Server 2003, SP2
	Microsoft Windows Vista Ultimate, SP1	V 6.0.6001	Internet Explorer 7.0 V7.0.600 1.18000	VigilancePro Agent – Microsoft Windows Vista Ultimate, SP1

2.6 Test Method

The VigilancePro v2009.1.2.6 was tested 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.

There were no deviations from the Test Methodology described.

3 EASE OF USE

Overall, the Test Laboratory considers the product straight forward to install. The Administrator Guidance describes how to install the VPro Server components and subsequently describes how to deploy the software onto each VPro Client. The VPro Distribution Kit is a CD which is provided to all customers that contains the normal server side installation files and the extended client site installation files. The VPro Distribution Kit CD also contains a VPro Resource Kit, which contains service packs for Office in addition to installation files for Adobe, dotnet and SQL Server 2005. Administrators should note that there is a prerequisite for .NET

Framework 2 or above to be installed on all Client and Server systems. VPro Resource Kit contains this software.

4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION

All the User Guides referenced follow a similar format in which they are written and are relatively easy to navigate through. Screen shots are provided in order to ease understanding and dependencies are stated in the beginning of each User Guide. However, it is recommended that potential customers read and understand the documentation before installing the product, and as necessary, seek clarification from the vendor should they require any assistance.

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 Product.

6 VALIDATION OF EXISTING ASSURANCE CERTIFICATES

There were no existing assurance certificates.

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.

The results in this Test Report only relate to the security claims specified in the ICD, and also only relate to the items tested.

Note that any opinions and interpretations stated under "[Ease of Use](#)" and "[Quality of Guidance Documentation](#)" in this Test Report are based on the experience of the Test Laboratory in performing similar work under the CCTM Scheme.

8 ABBREVIATIONS

The key IS Product/Service abbreviations used within this Test Report Summary are listed below. Generic CCTM Scheme abbreviations used within this Test Report Summary are defined in the Scheme Documentation.

9 REFERENCES

[ICD] Overtis IA Claims Document, v0.9, 14th July 2009