



CCTM TEST SUMMARY

Vodafone Ltd

Secure Remote Access 2.8

VENDOR DETAILS	TEST LABORATORY DETAILS
Vodafone Ltd	Logica
Vodafone House The Connection Newbury Berkshire RG14 2FN	Logica 250 Brook Drive Green Park Reading RG2 6UA
Telephone Number: +44 (0) 845 8339710	Telephone Number: +44 (0) 1372 369 619

Test Report Summary Reference Number	310.EC231258:7.2.1
Test Report Summary Version Number	V1.0
Test Report Date	20 th January 2010
CCTM Test Certificate Number	2010/01/0066

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).

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY3

1.1 Scope of IS Product Claims Tests3

1.2 Test Results.....3

1.3 Observations and Recommendations.....3

2 CCTM CLAIMS TESTING OVERVIEW4

2.1 Introduction.....4

2.2 Scope of IS Product Claims Tests4

2.3 Location and Date of Tests.....4

2.4 Platform Configuration.....4

2.5 Test Configuration5

2.6 Test Method.....6

3 CCTM CLAIMS TESTING RESULTS7

3.1 Ease of Use7

4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION8

5 RESISTANCE TO PUBLICLY KNOWN VULNERABILITIES9

6 Validation of Existing Assurance Certificates9

7 DISCLAIMERS 10

8 ABBREVIATIONS 11

9 REFERENCES..... 12

1 EXECUTIVE SUMMARY

1.1 Scope of IS Product Claims Tests

The results of this Test Report only relate to the security claims specified in [ICD] for the Vodafone Secure Remote Access (VSRA v2.8) product. For further details, see sections 2.1 and 2.2 of [ICD].

1.2 Test Results

The CCTM Claims Testing of Vodafone Secure Remote Access 2.8 by Logica concluded that the security functionality claims made within the IA Claims Document [ICD] are valid.

1.3 Observations and Recommendations

All of the IT security claims and the environmental security claims relating to VSRA v2.8 have been tested.

The testing showed that it is possible to bypass the VSRA v2.8 if the "launchmsi.exe" application is not sufficiently locked down from access by normal users. It is recommended that a group policy object is used at Domain level. Where local machines are used, users should be denied access explicitly in the laptop/desktop build, to prevent bypass. Vodafone can provide instructions for this on request.

It was also observed while VSRA v2.8 does close barred applications (see claim ApplicationCompliance-5), it does not force their immediate close down. As it takes some seconds for VSRA v2.8 to initiate closure, such applications (e.g. notepad) can still be used, albeit with significant difficulty. This may affect other programs too where system or user activity prevents the product from shutting it down immediately. VSRA v2.8 closes programs gracefully rather than killing the process. No known security vulnerability is implied in this observation, although potential users of VSRA v2.8 should check that the usability of each application they wish to bar is sufficiently impaired for their intended purpose.

2 CCTM CLAIMS TESTING 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.

Section 2.2.4 of [ICD] details the security features of Secure Remote Access 2.8 that were not tested 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 and all tests were run.

2.3 Location and Date of Tests

Claims Testing took place at the Test Laboratory premises on 2nd December – 5th January 2010. The test laboratory used is located at the following address:

Logica CCTM Test Laboratory
Logica UK Ltd
Chaucer House
The Office Park
Springfield Drive
Leatherhead
KT22 7LP

2.4 Platform Configuration

The platforms supported by the IS Product and used in the Claims Tests are detailed in the following table.

Platform Ref	Operating System Name	Version	Browser	Version
Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	Internet Explorer 8.0	8.0.6001.18702

Platform Ref	Operating System Name	Version	Browser	Version
Laptop B (Thinkpad, Lenovo T61) - Microsoft Windows XP Professional	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	Internet Explorer 8.0	8.0.6001.18702

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
Connectivity Control-1	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None ¹	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional
Application Compliance-1	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional
Application Compliance-2	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	Internet Explorer 8.0	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional
Application Compliance-3	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop B (Thinkpad, Lenovo T61) - Microsoft Windows XP Professional
Application Compliance-4	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional
Application Compliance-5	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop B (Thinkpad, Lenovo T61) - Microsoft Windows XP Professional

¹ '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
Security Policy-1	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional
Security Policy-2	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop B (Thinkpad, Lenovo T61) - Microsoft Windows XP Professional
Security Policy-3	Microsoft Windows XP Professional, Version 2002, Service Pack 3	5.1.2600	None	Laptop A (Dell Latitude D630) - Microsoft Windows XP Professional

2.6 Test Method

The Vodafone Secure Remote Access 2.8 was tested using the Test Method against the security claims made in the [ICD]. Section 3.3 in [ICD] describes the Test Method for the Claims Tests carried out by the Test Laboratory.

There were no deviations from this Test Method.

3 CCTM CLAIMS TESTING RESULTS

3.1 Ease of Use

3.1.1 The installation of Vodafone Secure Remote Access 2.8 was described in [IR]. [IR] describes how to install the product from the installation file included in the CD or downloadable from the product's website. [IR] clearly describes the Hardware and Software requirements and the available supported languages. The installation is very simple and easy to understand with the aid of appropriate screenshots at various point of the installation. Likewise the removal procedure is easy to understand and follow, with clear instructions on how to remove each component. [IR] states that you need administrator rights to perform the uninstall instructions. The user guide [UG] provides further details on how to configure and get VSRA 2.8 up and running.

3.1.2 Administrators should note that it is important to understand that Extend 360 Enforcement Agent or BigFix is installed automatically during the installation phase; however it needs to be independently removed. This software provides service hardening of the VSRA Client, and also provides for the method of communication between the VSRA client and the Vodafone Data Centres. This communication is used for the sending of logs and data to the data centres for the reporting capability, as well as to receive policy and phone book updates when they are available.

[IR] describes how to remove the product using Add or Remove Programs. It should be noted that 'Add or Remove Programs' can be accessed via clicking on Start > Settings > Control Panel.

Also, in order to remove BigFix from the registry an administrator will have to locate the BigFix directory. The BigFix directory can be found under the following: HKEY_LOCAL_MACHINE > SOFTWARE > BigFix.

To remove the VSRA folder, an administrator has to delete C:\Program Files\Vodafone\Vodafone Secure Remote Access. The VSRA folder will not be found in C:\Program Files\ but within C:\Program Files\Vodafone.

Another important point is that the icon on the desktop after installation is not the VSRA icon. It is a standard Vodafone icon. The VSRA icon is a shield with a red background; the shield is outlined in white and the right half is filled in white and the left half is filled in red.

It has been noted that for a wireless LAN configuration VSRA takes control of the wireless adapter and the wireless card reports that Windows Zero Configuration (WZC) service needs to start.

However when VSRA is shutdown, this control is released back to Windows.

4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION

There are a number of documents provided to customers to describe how to configure and deploy VSRA for a particular purpose, including:

- VSRA 2.8 User Guide [UG]
- VSRA Product Summary [PS]
- VSRA Implementation Booklet [IB]
- VSRA Installation and Removal Guide [IR]
- VSRA 2.8 SPV3 Release Notes [RN]

The guidance documentation is detailed in [IB], [IR] and [UG]. All documents above (except [PS]) are supplied with the IS Product to the customer on CD. This documentation was received from Vodafone during the test. Only [PS] is in the public domain.

[UG] is a guide that describes the configuration and the various ways to use the product. It provides sufficient information on how to configure the product. The document provides examples of product behaviour when hovering the mouse over the product which makes any user intervention evident along with what options are available. Each option is detailed well and is clear enough to provide an understanding of each function. Various screen shots are provided. The System tray icon is explained clearly, showing the user what outcomes are expected and describing what each icon means. The document also details the updates and the times it will take for an update to complete. [UG] provides guides on the different components including the Help Menu and has a FAQs section to deal with questions that customers may have.

[PS] is an introductory leaflet that provides a prospective customer the key features of the product; what the product is and what it claims to do. It is very clear and succinct. This guide can be easily understood by a customer and has sections which help to give an understanding of how it will benefit the end user. [PS] uses comprehensive, basic and easy to understand diagrams of how the product works (interactions between the client and policy management server). This gives a clear and open description of the product, the various components involved and the communications involved between each component. It is not included with the product on purchase as it is a pre-sales document.

[IB] details the implementation and integration process including customer interaction, delivery times and structure of the Vodafone team. It is clearly written with easy to understand timescale diagrams. This document describes the services available to the customer and how the Product support team can help throughout the entire implementation

phase as well as the interactions involved between the customer and product team.

[IR] is an installation and removal guide. It is a very simple and easy to follow. Each process is clearly defined and followed by appropriate screenshots. This document is furthermore mentioned in Section 3.1.1.

[RN] is a more technical documentation detailing the changes included in the newest release and the impact of any changes.

Overall [UG], [PS], [IB], [IR] and [RN] are consistent and of good quality. They accurately describe each process in sufficient detail. The documents also include various screenshots which are clear and show the expected results/outcome. They are easy to follow and do not inundate the reader with too much information; relevant information is provided. Notes and key functions are highlighted to include additional useful information.

5 RESISTANCE TO PUBLICLY KNOWN VULNERABILITIES

A search for publicly known vulnerabilities on a sample of security websites did not reveal any known weakness in the security of the IS Product. In addition, the testers found no known weakness in the underlying platform. Providing the underlying platform is kept up to date with the most recent patches available, VSRA v2.8 should not be vulnerable to security weaknesses.

In addition to testing the claims, the testers identified a method of deactivation. Vodafone responded by identifying the means whereby the Operating System can be locked down to prevent this vulnerability. Test script "UserShutdown-1" shows the test and the lockdown steps to prevent bypass in the problem scenario.

6 Validation of Existing Assurance Certificates

There are no existing assurance certificates that are applicable to the IS Product under test.

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, or the IT environment supporting the IS Product.

This Test Report 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.

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

Acronym	Description
CMD	Microsoft command line executable
IA	Information Assurance
ICD	Information Assurance Claims Document
IE	Microsoft Internet Explorer
IS	Information Systems
OS	Operating System
RAM	Random Access Memory
SP	A Service Pack is a collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package, in this instance Microsoft Windows.
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USB	Universal Serial Bus (USB) is a serial bus standard to connect a variety of devices to a host computer.
VBS	Vodafone Business Services
VMC	Vodafone Mobile Connect
VPN	Virtual Private Network
VSRA	Vodafone Secure Remote Access
WZC	Windows Zero Configuration

9 REFERENCES

- [IB] Vodafone Secure Remote Access – Implementation programme, v4, 01/ENT/63147, October 2008
- [ICD] Vodafone CCTM IA Claims Document, v4.2, 5 January 2010
- [IR] Vodafone Secure Remote Access – Installation and removal procedure guide, January 2009
- [PS] Vodafone Secure Remote Access – Product Summary, 01/ENT/62076, April 2008
- [RN] Vodafone Secure Remote Access – Release Notes, Version 2.8 SPV3 (2.8.012.8), October 2009
- [UG] Vodafone Secure Remote Access – User's guide version 2.8, v1, November 2009