



CCTM TEST REPORT SUMMARY

GrIDSure Limited

GrIDSure Enterprise
Version 3.3.30.14

VENDOR DETAILS	TEST LABORATORY DETAILS
GrIDSure Limited	Sogeti UK Ltd
Orchard House Heath Road Warboys Huntingdon, PE28 2UW	85 London Wall 3 rd Floor London EC2M 7AD United Kingdom
Telephone Number: 01487 825014	Telephone Number: +44(0)207 014 8900

Test Report Summary Reference Number	GSE080_TRS
Test Report Summary Version Number	V1.0
Test Report Summary Date	8 th December 2009
CCTM Certificate Number	2009/12/0063

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 Scope of IS Product Claims Tests

This document outlines the results from testing the IA claims made by GrIDSure Limited in regard to the suitability of GrIDSure Enterprise Version 3.3.30.14 for use by the UK Public Sector for local and remote secure login to Microsoft Windows Server 2003 domains.

A total of 12 claims were made in the IA Claims Document (ICD). These claims were assessed via a number of tests, each of which was derived specifically to enable each claim to be challenged. The outcome of the assessment process is summarised in the table below:

Assessment	Definition	Claims
FAIL	The product did not pass the tests required to establish the validity of the claim	0
PASS (Conditional)	The product passed all tests, but with reservations	0
PASS (Unconditional)	The product passed all tests associated with the claim	12

The overall conclusion of this evaluation is that the claims made in the IA Claims Document have been validated for GrIDSure Enterprise Version 3.3.30.14.

It should be noted that this report relates solely to the security claims made within the confines of the IA Claims Document, and only for GrIDSure Enterprise Version 3.3.30.14, as it relates to the items tested.

Unique Ref.	Claims Statements	Status
	Authentication	
001	GrIDSure Enterprise enables a GrIDSure pattern to be assigned to an authorised user; only authorised users can then logon to the client using their valid GrIDSure one-time password.	Pass
002	GrIDSure Enterprise provides GrIDSure authenticated access to Microsoft IIS managed websites.	Pass
	Remote Access	
003	GrIDSure supports two-factor authentication via an encrypted seed key and the PIP.	Pass
004	GrIDSure supports two-factor authentication for Sony Ericsson Cybershot and Sony Ericsson W880i java enabled mobile phones via an encrypted seed key and the PIP.	Pass
005	GrIDSure Enterprise provides the means for remote SSL VPN login.	Pass
006	GrIDSure Enterprise supports remote access using a grid generated on an IIS webserver.	Pass
	Time-Limited Grid	
007	GrIDSure Enterprise generates a time-limited grid for authentication.	Pass
	Audit	
008	GrIDSure authentication events are logged providing an audit trail which can be read using standard Microsoft Event viewers.	Pass
	Cached Credentials	
009	GrIDSure Enterprise allows users to continue to login to their computers whilst disconnected from the domain via cached credentials.	Pass
	Management	
010	GrIDSure Enterprise provides centralised administrator tools to manage GrIDSure access (both local and remote).	Pass
011	GrIDSure Enterprise provides policy based controls on the size of the grid and the length of the user's Personal Identification Pattern.	Pass
	Cryptographic Architecture	
012	GrIDSure Enterprise stores ID and Authentication data in an encrypted form in Active Directory.	Pass

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 section 3 of the [ICD]. Testing began on 23/09/2009 and completed on 03/11/2009.

2.2 Scope of IS Product Claims Tests

Section 2.1 – 2.2 of the [ICD] describes the scope of the IS Product to be Claims Tested. The Test Laboratory confirmed this to be accurate for the IS Product tested; with the exception of devices used in respect of the Java enabled phone (see Sections 2.6 and 2.7 of this report).

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 GrIDSure Enterprise Version 3.3.30.14 that were not tested under the CCTM Scheme.

In particular, the cryptographic algorithms used in an IS Product are not tested under the CCTM Scheme. Therefore, the standard Microsoft cryptographic algorithms, including Pseudo Random Number Generators, used by the GrIDSure Enterprise Version 3.3.30.14 product is out of scope for this assessment.

Section 3.1 of the [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. It can be confirmed that all tests were run.

2.3 Location and Date of Tests

Section 3.3 of [ICD] details the location[s] where the Test Laboratory conducted Claims Testing.

All tests were carried out in the Sogeti Secure Test Laboratory, located at 85 London Wall, London, EC2M 7AD. Testing commenced on 23/09/2009 and completed on 03/11/2009.

Witness testing was not necessary for GrIDSure Limited Version 3.3.30.14.

2.4 Platform Configuration

The client platform/browsers supported by the IS Product and used in the Claims Tests are detailed in the following table:

Platform	Operating System / Version	Browser	Other Required Software
Enterprise Server	MS Windows Server 2003 Standard Edition (32 bit) R2 SP2	N/A	Internet Authentication Service (IAS) (Radius implementation) Internet Information Service (IIS) V6 Active Directory
Remote Access (XP)	MS Windows XP Professional SP3 (32 bit)	MS IE 7.0 Mozilla FireFox 3.5.3	N/A
Remote Access (Vista)	MS Windows Vista Business Edition SP1 (32 bit)	MS IE 7.0 Mozilla FireFox 3.5.3	N/A
Client (XP)	MS Windows XP Professional SP3 (32 bit)	MS IE 7.0	N/A
Client (Vista)	MS Windows Vista Business Edition SP1 (32 bit)	MS IE 7.0	N/A

2.5 Test Configuration

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

Claim Reference	Product Name	Prod Ref
004	Any Java-enabled phone but for the purposes of this assessment a Sony Ericsson Cybershot and a Sony Ericsson W880i were used.	

2.6 Test Method

Gridsure Enterprise Version 3.3.30.14 was tested using the CCTM Generic Claims Test Method ([TLG] Appendix B) against the security claims made in the [ICD]. Section 3.3 in [ICD] identifies the Test Approach for the Claims Tests carried out by the Test Laboratory. There were no deviations from the Test Approach.

3 EASE OF USE

3.1 Ease of Use

- 3.1.1 The installation of the IS Product was as described in the [IG]. Installation of the IS product was conducted by a Sogeti tester with some technical support from the Vendor representative. The product is administered via 'plug-ins' to the Microsoft Management Console and requires good knowledge of underlying facilities such as Active Directory, IIS, IAS/Radius for successful administration of the product. Given this, administration of the product is intuitive and relatively simple.
- 3.1.2 Administrators should note that there is a known problem with version 1.0.12.1 of the gsrlASxt.dll used in RADIUS authentication and should check if their distribution has been supplied with this version of the dll. If so they should contact the vendor and obtain the current version of the dll 1.0.14.1.

4 QUALITY OF USER AND ADMINISTRATION DOCUMENTATION

4.1 Quality of Guidance Documentation

The guidance documentation is detailed in [IG], [AG], [UG], [UVG], [WACG], [ATCG], [IASECG], [SCIG], [WebTUG], [WTIG] and [WinTUG]. The documentation is supplied with the IS Product on a CD.

The publicly available address for additional support on the product can be requested from www.gridsure.com

The Gridsure Logon Enterprise Installation Guide [IG], the Gridsure Logon Enterprise Administrator's Guide [AG], RADIUS Logon Administrative Tools Configuration Guide [ATCG], RADIUS Logon Systems Components Installation Guide [SCIG] and RADIUS Logon Win32 Token Installation Guide [WTIG] is aimed at Administrators of the system and provides information regarding the installation of Gridsure Enterprise with both technical and non-technical configuration support.

The documentation provided was found to be clear, easy to follow and intuitive.

Further information on the installation and use of Mobile tokens is available on request from www.gridsure.com

5 RESISTANCE TO PUBLICLY KNOWN VULNERABILITIES

5.1 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/Service. In addition, a search for publicly known vulnerabilities failed to yield any known weakness in the underlying platform that could not be patched in the test configuration.

Security websites inspected are as follows:

<http://xforce.iss.net/>

<http://www.securityfocus.com/>

<http://www.gridsure.com>

6 VALIDATION OF EXISTING ASSURANCE CERTIFICATES

N/A

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 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].

[ICD]	CCT MARK IA CLAIMS DOCUMENT, version 1.3
[IIS]	Microsoft Internet Information Service
[IAS]	Microsoft Internet Authentication Service – this Service is Microsoft’s implementation of a RADIUS server
[PIP]	Personal Identification Pattern – a sequence of squares on a grid which the user remembers and forms the basis of his GrIDSure Authentication

[RADIUS]	Remote Authentication Dial In User Service. Defined in RFC 2865, RADIUS is an Internet Standard protocol used by network devices to authenticate users
[SSL]	Secure Sockets Layer
[VPN]	Virtual Private Network

9 REFERENCES

[IG]	GrIDSure Logon Enterprise Installation Guide, Version 1.7, dated 2009
[AG]	GrIDSure Logon Enterprise Administrator's Guide, Version 1.5, dated 2009
[UG]	GrIDSure Logon Enterprise User's Guide, Version 1.6, dated 2009
[UVG]	GrIDSure Logon Enterprise User Viewer Guide, Version 1.4, dated 2009
[WACG]	GrIDSure Web Access Configuration Guide, Version 1.0, dated 2008
[ATCG]	RADIUS Logon Administrative Tools Configuration Guide, Version 1.4, dated 2009
[IASECG]	RADIUS Logon IAS Extension Configuration Guide, Version 1.2, dated 2009
[SCIG]	RADIUS Logon Systems Components Installation Guide, Version 1.4, dated 2009
[WebTUG]	RADIUS Logon Web Token User's Guide, Version 1.4, dated 2009
[WTIG]	RADIUS Logon Win32 Token Installation Guide, Version 1.2, dated 2009
[WinTUG]	RADIUS Logon Win32 Token User's Guide, Version 1.2, dated 2009