



CCTM IA CLAIMS DOCUMENT (ICD)

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) 207 148 900
Email: enquiries@gridsure.com	Email: ian.mcewen@uk.sogeti.com
Website: http://www.gridsure.com	Website: www.sogeti.com

CERTIFICATE DETAILS	
CCTM Certificate Number	2009/12/0063
CCTM Awarded on	8 th December 2009
CCTM Award Expires on	7 th December 2010
ICD Issue Date	8 th December 2009

TABLE OF CONTENTS

1	INTRODUCTION.....	3
1.1	Background	3
1.2	Objectives	3
1.3	Purpose of Document	3
1.4	Structure	3
2	IS PRODUCT DESCRIPTION.....	4
2.1	Product/Service Identification	4
2.2	Product/Service Overview	5
2.3	Usage assumptions	9
3	CCTM CLAIMS FOR THE IS PRODUCT.....	12
3.1	Claims Statements	12
3.2	Existing assurance certificates	12
Annex A	Glossary of Terms	13
Annex B	Marketing Statement	14

1 INTRODUCTION

1.1 Background

This document outlines 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.

1.2 Objectives

The objectives of this ICD are to:

- Provide a basis for the CESG Claims Tested Mark (CCTM) Scheme assessment of the product ; and
- Act as the basis of an agreement between the vendor and the CCTM Secretariat regarding the marketing claims for the certified product.

1.3 Purpose of Document

This document is the ICD for GrIDSure Enterprise version 3.3.30.14.

This ICD is the baseline document for the CCTM Claims Test of GrIDSure Enterprise version 3.3.30.14.

This document additionally sets out information to agree the scope and process of testing including a description of the test approach and test environment.

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 GrIDSure Enterprise and all the information related to the security of GrIDSure Enterprise version 3.3.30.14.
- Section 3 details the security functionality claims that are being made and the test approach to be used in the conduct of the assessment.

2 IS PRODUCT DESCRIPTION

2.1 Product/Service Identification

Product Name: GrIDSure Enterprise

Version: 3.3.30.14

Platforms:

The client platform/browsers to be used in claims testing are shown in the table below:

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
Mobile Phone Soft-Token	Any Java-enabled phone but for the purposes of this assessment we will use a Sony Ericsson Cybershot and a Sony Ericsson W880i	N/A	N/A

2.2 Product/Service Overview

GrIDSure have developed a patented methodology for generating one-time passcodes. The methodology requires the user to memorise a pattern and sequence of squares on a grid (administrator defined but typically in a 5x5 square arrangement). GrIDSure Enterprise is one such product which has been developed for Microsoft Windows domain environments and replaces the traditional username/password with username/GrIDSure authentication.

2.2.1 Security architecture

GrIDSure Enterprise is a suite of software components which implement the GrIDSure authentication methodology on Windows Server 2003 Domains to provide client user authentication for users requiring access:

- Locally, using XP or Vista client machines.
- To extranet services provided via the web. For example, Outlook Web Access secured behind an IIS server and for which authentication is required.
- Remote SSL VPN access via RADIUS authentication to the corporate network.

Figure 2.1 illustrates how the GrIDSure Enterprise is used in a typical installation.

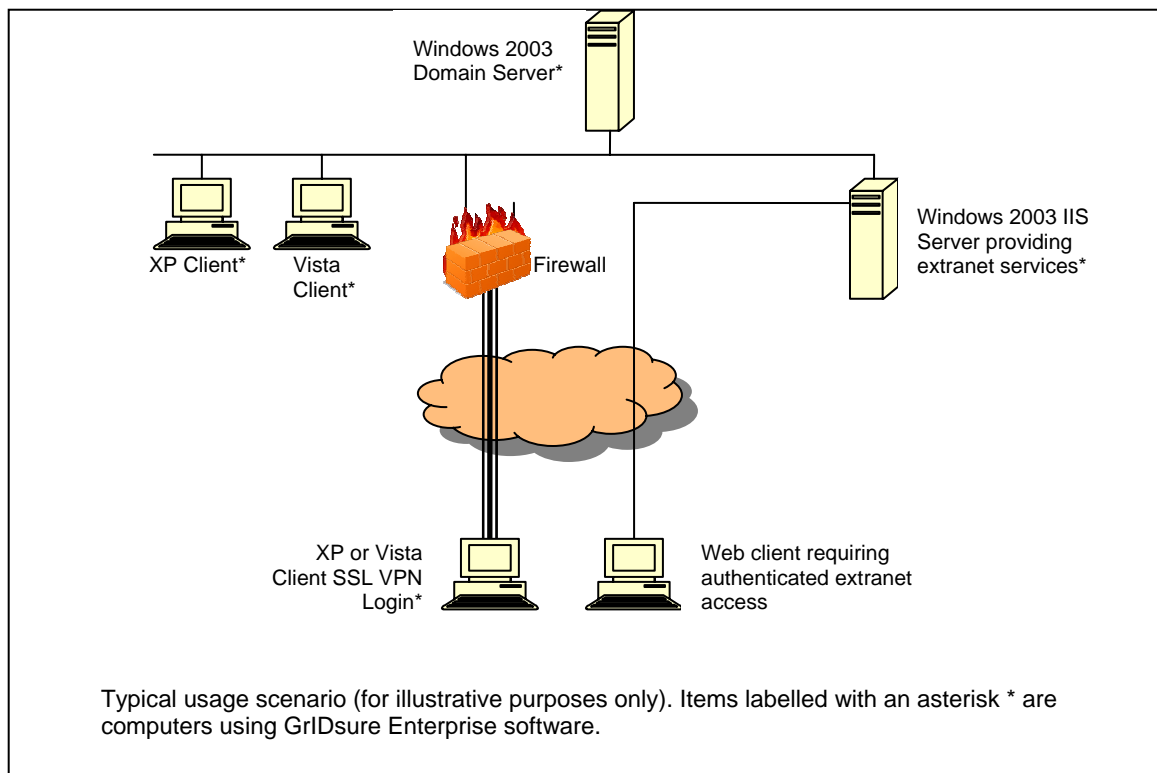


Figure 2.1. Typical GrIDSure Enterprise Environment

The various software components comprising GrIDSure Enterprise provide additional functionality to the extant Windows software on the host computers. Specifically:

- The domain server components extend the standard Windows administrative tools. For example, the Windows Active Directory Users and Groups (ADUC) tool is extended by the addition of two 'tabs' which give the administrator the ability to administer GrIDSure users. The server components also provide a GrIDSure authentication Windows 'Service' as well as policy modules, audit logging etc. Should the administrator wish to provide SSL VPN functionality for his users then he can optionally install the RADIUS authentication modules. These modules extend the standard Microsoft Internet Authentication Service (IAS) service so that back-end authentication is directed to the GrIDSure Authentication services rather than the standard Microsoft username/password authentication.
- The XP and Vista client software components replace the standard Windows username/password functionality with a username/GrIDSure login.
- Clients requiring SSL VPN access are provided with components which allow them to generate 'offline' GrIDSure authentication grids. The user then makes a regular SSL/VPN username/password login replacing the usual password with a GrIDSure one-time passcode.
- The GrIDSure Enterprise components for Windows IIS Webservers alter the traditional Windows username/password authentication that is provided to optionally secure web sites with a username/GrIDSure login. The administration of this functionality and the tools to configure it are provided by an additional tab to the standard Microsoft IIS administration tool.

2.2.2 Hardware requirements

Operating System		Hardware Requirement
Client	MS Windows XP Professional SP3 (32bit)	Network Interface Card 512MB+ RAM (Recommended) 30MB Hard disk space TCP/IP Connectivity
	MS Windows Vista Business Edition SP1 (32bit)	Network Interface Card 1GB+ RAM (Recommended) 30MB Hard disk space TCP/IP Connectivity
Enterprise Server	MS Windows Server 2003 R2, SP2 (32 bit). Configured as a Domain Controller. Microsoft IAS to be installed and configured to support SSL VPN access.	Network Interface Card 1GB+ RAM 1GB Hard disk space TCP/IP Connectivity
IIS Web Server	MS Windows Server 2003 R2 (32 bit) version 6.0	
Firewall/NAS Device	Needs to support standard RADIUS authentication protocol (RFC 2865) For the Purpose of this assessment we will use a Zyxel Zywall SSL10	At least two Network interfaces, one for Internal LAN and one for External network. Device must be configured to delegate RADIUS authentication to the IAS service on the Enterprise server.
Mobile phone	Any Java-enabled phone but for the purposes of this assessment we will use a Sony Ericsson Cybershot and a Sony Ericsson W880i	e.g. Nokia, Sony or Blackberry

2.2.3 Software requirements

The Enterprise server needs to be configured as a Domain Controller.

Microsoft Internet Authentication Server (IAS) should also be installed on the Enterprise server.

The Workstation clients need to be configured to be members of the Enterprise Server domain.

The IIS webserver needs to have the IIS server running and be a member of the domain.

The Firewall/NAS device needs to be configured to delegate RADIUS authentication requests to the Enterprise server.

For all of the Microsoft-based systems it is recommended that all the latest Microsoft Operating system patches are applied.

2.2.4 Out of Scope

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 V3.3.30.14 product are out of scope for this assessment.

GrIDSure Enterprise makes no changes to the functionality of the RADIUS communication between a Firewall/NAS and Internet Authentication Service and this underlying functionality is therefore not tested. The SSL VPN client and its functionality with the Firewall/NAS are unaffected by GrIDSure Enterprise and therefore the VPN security is out of scope. The testing will therefore be confined to determining whether access is granted to the client by the Firewall/NAS following RADIUS authentication with IAS.

The use of the GrIDSure Enterprise product for the protection of assets at IL3 or above is out of scope for this assessment.

GrIDSure Enterprise is supported in a multi-domain controller environment. However this functionality is provided by the underlying Microsoft Operating System so for the purposes of this assessment this feature is considered out of scope.

The web functionality provided by the IIS webserver is supported by all major web browsers. However for the purposes of this assessment only **Internet Explorer 7.0** and Mozilla FireFox 3.5.3 will be tested and all other browsers are out of scope.

GrIDSure Enterprise replaces the standard Windows Username/Password with a username/GrIDSure challenge. Once authenticated, security policies continue to be provided by the

Microsoft Operating system. Consequently the testing will be confined to authentication alone.

GrIDSure Enterprise supports the platforms detailed in the table below. However for the purposes of this assessment, only those highlighted in bold are in scope, all others are considered out of scope.

	Operating System
Enterprise Server	MS Windows 2003 Server Standard Edition R2 SP2 MS Window 2000 Advanced Server R2
Client	MS Windows Vista Business Edition 32-bit SP1 MS Windows 2000 Service Pack 2+ MS Windows XP Professional SP1 MS Windows XP Professional SP2 MS Windows XP Professional SP3
Mobile Phone	The product supports the use of any Java-enabled mobile phone. However for the purposes of this assessment only; A Sony Ericsson Cybershot phone will be used A Sony Ericsson W880i phone will be used Any other mobile phone platform is out of scope.

2.3 Usage assumptions

2.3.1 Assets

The assets to be protected by the GrIDSure Enterprise version 3.3.30.14 product are:

- Access to any sensitive data or intellectual property at IL1 or IL2 on enterprise resources that could pose a risk or threat to an organisation or individual if copied or transferred elsewhere.

2.3.2 Threat scenario

Threats to assets which are countered are:

- T1** Unauthorised access to the network.
- T2** Threats from software Trojans which keylog passwords. Unlike traditional passwords, GrIDSure one-time passwords (OTP) are of no use to keyloggers.
- T3** Eavesdropping on communications where that eavesdropping is aimed at recovering authentication information.

2.3.2.1 Expected operational environment

A typical operational environment is indicated in the diagram in section 2.2. It is primarily designed for corporate office environments where users additionally require remote access.

The business benefits of deploying GrIDSure Enterprise are numerous:

- The GrIDSure methodology is easy to use making training requirements for end-users minimal.
- GrIDSure Enterprise supports secure VPN login for remote users.
- GrIDSure Enterprise remote access is provided using industry standard devices supporting the RFC standard RADIUS protocol combined with grids generated on a device distinct from the one being logged on to. For the organisation this provides a robust two-factor, one-time password solution.
- The server administration functions are provided as extensions to the existing Microsoft Server tools meaning that there are no new applications to deploy or learn.
- Authentication events are logged and can be viewed using the standard Microsoft Event Viewer tools providing the business with a full audit trail.

2.3.2.2 Organisational security policies

The table below identifies the Control Objectives of an organisation's security policy which are supported by the GrIDSure Enterprise v3.3.30.14 product (use of the product, however, does not infer compliance with the ISO 27001 standard).

ISO 27001 Control	Title	Control Objective
A.10.10	Monitoring	To detect unauthorized information processing activities.
A.11.4	Network Access Control	To prevent unauthorized access to networked services.
A.11.5	Operating System Access Control	To prevent unauthorized access to operating systems.

2.3.2.3 Security requirements on the environment

The following assumptions are made:

- The installation and running of the implementation will be carried out by a competent network administrator.
- That end-users are trained in the correct use of the GrIDSure methodology and understand the need to keep their Personal Identification Pattern secret. These policies are very similar to the best-practice guidance normally given to users with regard to traditional passwords and the need to keep authentication data private.
- That the installation and method of deployment is carried out by a competent individual with due consideration for network security, resilience, scalability and failover.

3 CCTM CLAIMS FOR THE IS PRODUCT

3.1 Claims Statements

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

3.2 Existing assurance certificates

None

Annex A Glossary of Terms

CCTM	CESG Claims Tested Mark
GrIDSure Methodology	The GrIDSure personal authentication methodology has been developed by GrIDSure Limited. A description of the methodology is described on the company's website (www.gridsure.com) and covered by a number of International patent applications including International PCT WO2007/063346
ICD	Information Assurance Claims Document
IIS	Microsoft Internet Information Service
IAS	Microsoft Internet Authentication Service – This service is Microsoft's implementation of a RADIUS server
MMC	Microsoft Management Console
OTP	One-time Password – A unique security code generated through a validation network by a hardware or software credential, often used as a second factor for strong authentication.
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

Annex B Marketing Statement

GrIDSure Enterprise provides an easy to use and secure method of authentication to Microsoft networks, containing data at IL1 or IL2, replacing the traditional fixed password with GrIDSure one-time passcodes on Windows XP SP3 and Vista Business SP1 computers. GrIDSure Enterprise integrates with Active Directory and provides centralised policy-based administration using standard Microsoft tools.

Authentication attempts are recorded providing an accurate audit trail of all login attempts.

GrIDSure Enterprise also supports robust two-factor remote SSL VPN access via a combination of a personal GrIDSure secret pattern and a time-limited, locally generated authentication grid to produce a one-time passcode. This provides convenience for users and eliminates the need for costly one-time token generators.

GrIDSure authenticated access can also be provided to corporate extranets allowing users admission to facilities such as Outlook Web Access.

GrIDSure Enterprise offers a unique PC login solution that is more secure than a traditional password, is convenient, easy to use and considerably cheaper than hardware-based alternatives.