



CCTM TEST REPORT SUMMARY

iStorage Limited

diskGenie Hardware Encrypted Portable Drive
--

IS-DG-128-XXX, IS-DG-256-XXX, IS-DG-128-SSD-XXX, IS-DG-256-SSD-XXX
--

VENDOR DETAILS	TEST LABORATORY DETAILS
iStorage Limited	SiVenture
Research House Fraser Road Greenford Middlesex UB6 7AQ	Unit 6 Cordwallis Park Clivemont Road Maidenhead Berkshire SL6 7BU
Telephone Number: +44 (0)20 8537 3436	Telephone Number: +44 (0)1628 651 366

Test Report Summary Reference Number	GHNE-SR-0001
Test Report Summary Version Number	0-2
Test Report Summary Date	2 nd August 2010
CCTM Certificate Number	2010/08/0075

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 SUMMARY	3
1.1	Scope of IS Product Claims Tests	3
1.2	Test Results	3
1.3	Observations and Recommendations	3
1.3.1	diskGenie in all environments	3
2	CCTM CLAIMS TESTING OVERVIEW	4
2.1	Introduction	4
2.2	IS Product Description	4
2.3	Scope of IS Product Claims Tests	5
2.4	Test Approach	5
2.5	Location and Date of Tests	5
2.6	Platform Configuration	6
2.7	Test Configuration	6
2.8	Test Method	9
3	EASE OF USE	10
3.1	Ease of Use	10
4	Quality of Guidance Documentation	10
5	Resistance to Publicly Known Vulnerabilities	11
6	Validation of Existing Assurance Certificates	11
7	DISCLAIMERS	12
8	ABBREVIATIONS	13
9	REFERENCES	14

1 EXECUTIVE SUMMARY

1.1 Scope of IS Product Claims Tests

The iStorage diskGenie Encrypted Portable Drive is a secure removable storage device for all data and documents. The diskGenie Hardware Encrypted Portable Drive uses AES 128-bit or 256-bit ECB real-time hardware encryption engines to securely store all files stored on the drive. The diskGenie comes in four models. The models are differentiated by their encryption type (128-bit or 256-bit) and by their storage media (either a standard hard drive or a solid state drive). The same 128-bit and 256-bit real time AES engines are used in the diskGenie drives with standard hard drives and in the diskGenie devices with solid state drives. For further details, see sections 2.1 and 2.2 of [ICD].

1.2 Test Results

The CCTM Claims Testing of the iStorage diskGenie Hardware Encrypted Portable Drive by SiVenture concluded that the security functionality claims made within the IA Claims Document [ICD] are valid.

1.3 Observations and Recommendations

1.3.1 diskGenie in all environments

Customers or administrators using the diskGenie product in any environment should be aware of the following:

- If a file from the storage drive is still open when the device is locked, or removed from the host system, the file does not automatically close and, hence, unsaved data may be lost
- Users of the diskGenie should be made aware that normal computer security procedures should be upheld even when using the device e.g. always lock the PC (or Mac) when it is not being used
- After a factory reset the iStorage drives need to be re-partitioned and re-formatted to work correctly. This requires the use of the host systems disk management tools. The standard disk management tools in Windows (as described in [UM]) only allow a format into NTFS or exFAT file systems. These file systems can not be used usefully by Mac platforms as they become read only drives. If a reformatted drive is required to be used on both Windows and Mac platforms the drive needs to be formatted as a FAT32 drive. This can be achieved by using the Windows disk management tools to partition the drive and then using the Windows command line "Format" tool to format the storage

partition as FAT32 (format drive_letter /FS:FAT32). However, there is a limit of 32Gb on the size of partitions that can be formatted as FAT32 using these tools on Windows 2000 machines and above. To overcome this limitation the device can be split into multiple partitions smaller than 32Gb, or a third party disk management programme can be used to format the disk. Alternatively, the Ubuntu platform can be used to both partition and format the drive as a FAT32 drive with no size limitations.

2 CCTM CLAIMS TESTING OVERVIEW

2.1 Introduction

This Test Report documents the results of the CCTM Claims Tests of the iStorage diskGenie Hardware Encrypted Drive as detailed in [ICD].

2.2 IS Product Description

Section 2.2 of [ICD] provides an overview of the iStorage diskGenie Hardware Encrypted Drive that was the subject of the Claims Test.

The iStorage diskGenie Hardware Encrypted Drive comes in four versions:

- IS-DG-128-XXX – Version using 128-bit AES encryption and a standard hard drive for storage where XXX corresponds to the storage capacity (250GB, 320GB, 500GB, 640GB and 750GB);
- IS-DG-256-XXX – Version using 256-bit AES encryption and a standard hard drive for storage where XXX corresponds to the storage capacity (250GB, 320GB, 500GB, 640GB and 750GB);
- IS-DG-128-SSD-XXX – Version using 128-bit AES encryption and a solid state drive for storage where XXX corresponds to the storage capacity (30GB, 64GB, 128GB and 256GB);
- 0IS-DG-256-SSD-XXX – Version using 256-bit AES encryption and a solid state drive for storage where XXX corresponds to the storage capacity (30GB, 64GB, 128GB and 256GB);

The same 128-bit and 256-bit real time AES engines are used in the diskGenie drives with standard hard drives and the diskGenie drives with solid state drives.

Details of the platforms and other IT components supported by the IS Product and used in the Claims Tests are detailed in the Platform Configuration section.

2.3 Scope of IS Product Claims Tests

Sections 2.1-2.2 of [ICD] describe the scope of the iStorage diskGenie Hardware Encrypted Drive to be Claims Tested. The Test Laboratory confirmed this to be accurate for the iStorage diskGenie.

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 iStorage diskGenie Hardware Encrypted Drive that were not tested under the CCTM Scheme. In particular, the cryptographic algorithms used in IS Products are not tested under the CCTM Scheme.

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

2.4 Test Approach

Section 3.3 of [ICD] describes the Test Approach. It identifies those Claims Tests that were performed by the Test Laboratory. The Claims Tests of [ICD] were performed using each diskGenie model on all host platforms (where applicable) of the Platform Configuration section.

In several tests trial versions of commercially available software tools were used to prove that the diskGenie storage drive is always inaccessible when it should be i.e. the storage drive was always inaccessible until a passkey was entered. Similarly a trial version of a data recovery tool was also used to confirm the secure deletion of data from the diskGenie storage drive after a factory reset.

2.5 Location and Date of Tests

Section 3.3 of [ICD] details the location where the Test Laboratory conducted Claims Testing. The start and end dates of the Claims Testing were:

- IS-DG-128-xxx: 27th June 2010 – 14th July 2010;
- IS-DG-256-xxx: 27th June 2010 – 14th July 2010;
- IS-DG-128-SSD-xxx: 27th June 2010 – 14th July 2010;
- IS-DG-256-SSD-xxx: 27th June 2010 and 1st – 23rd July 2010;

2.6 Platform Configuration

The platforms supported by the iStorage diskGenie Hardware Encrypted Portable and used in the Claims Tests are detailed in the following tables.

diskGenie models: IS-DG-128-xxx, IS-DG-256-xxx, IS-DG-128-SSD-xxx, IS-DG-256-SSD-xxx

Platforms:

Platform	Operating System	Version	Additional information
PC	Microsoft Windows	2000	Service Pack 4
PC	Microsoft Windows	XP	Service Pack 3
PC	Microsoft Windows	Vista	32-bit and 64-bit
PC	Microsoft Windows	7	32-bit and 64-bit
PC	Linux	Ubuntu 9.10	
Mac	Mac OS X	10.2	
Mac	Mac OS X	10.3	
Mac	Mac OS X	10.4	
Mac	Mac OS X	10.5	
Mac	Mac OS X	10.6	

2.7 Test Configuration

The test configuration comprised the different versions of the diskGenie Hardware Encrypted Drive running on the platform combinations detailed in the table below. The table also highlights which Claims Tests each combination was used to verify:

Claims Test	diskGenie models	Host platforms
CS1	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section
CS2	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power

Claims Test	diskGenie models	Host platforms
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS3	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS4	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS5	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS6	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power

Claims Test	diskGenie models	Host platforms
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS7	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS8	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section
CS9	IS-DG-128-250 IS-DG-128-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-250 IS-DG-256-640	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	Not applicable – the security functionality is host independent; the host is only required for power
CS10	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section
CS11	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section

Claims Test	diskGenie models	Host platforms
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section
CS12	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section
CS13	IS-DG-128-250 IS-DG-128-640	All platforms listed in the Platform Configuration section
	IS-DG-256-250 IS-DG-256-640	All platforms listed in the Platform Configuration section
	IS-DG-128-SSD-30 IS-DG-128-SSD-128	All platforms listed in the Platform Configuration section
	IS-DG-256-SSD-64 IS-DG-256-SSD-128	All platforms listed in the Platform Configuration section

2.8 Test Method

The iStorage diskGenie Hardware Encrypted Drive was 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.

3 EASE OF USE

3.1 Ease of Use

- 3.1.1 The installation of the IS Product was as described in [QS] and [UM].
- 3.1.2 There were no specific points of note for installation, configuration or use of the iStorage diskGenie product.

4 Quality of Guidance Documentation

The guidance documentation is detailed in [QS] and [UM]. It is available for download on the Vendor's website:

www.istorage-uk.com/diskgenie.php

[QS] is a quick start guide outlining the installation and basic functions of the diskGenie device. [UM] is a more comprehensive document listing all functions of the device including installation. [UM] also includes a set of general questions which about common issues with the diskGenie device.

As the diskGenie is a relatively simple device, these manuals provide enough detail to fully describe the installation, configuration and security functionality of the iStorage diskGenie Hardware Encrypted Portable Drive.

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 iStorage diskGenie Hardware Encrypted Portable Drive. 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://rdist.root.org>

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

<http://www.darkreading.com>

<http://www.h-online.com/security>

<http://nvd.nist.gov>

<http://www.securityfocus.com>

<http://www.us-cert.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 iStorage diskGenie Hardware Encrypted Portable Drive that has been Claims Tested. The certificates [Cert] were correctly stated in [ICD].

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
AES	Advanced Encryption Standard
AES ECB	AES in Electronic CodeBook mode
CAVP	Cryptographic Algorithm Validation Program
CCT	CESG Claims Tested
CCTM	CESG Claims Tested Mark
FIPS	Federal Information Processing Standards
IA	Information Assurance
ICD	Information Assurance Claims Document
OS	Operating System
SP	Service Pack

9 REFERENCES

- [Cert] CAVP FIPS-197 AES algorithm validation for the diskGenie chipset; certificate #1174:
<http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>
- [ICD] iStorage IA Claims Document, v2-0, July 2010;
- [DES] CCTM Scheme Description of Scheme, Issue 3.0.1, May 2009;
- [QS] iStorage diskGenie Quick Start Guide;
- [RES] SiVenture Test Results, v1-0, July 2010;
- [TLG] CCTM Scheme Test Laboratory Guide, Issue 3.0.0, March 2009;
- [TM] CCTM Generic Claims Test Method ([TLG] Appendix B) and Specialist Testing method ([TLG] Appendix G), Issue 3.0.0, March 2009;
- [UM] iStorage diskGenie User's Manual;