University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Solid State Testing
Claims Test ADPC0012
ICT Renew Inc.

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.1
Date: October 21, 2014
Distribution: Confidential

DISCLAIMER

The content of this document is based on information shared to date and will be subject to change or modification as requirements are amended, clarified or additional requirements are indicated at a later stage. For this reason this document should be viewed as a discussion document with further qualification and refinement required.

Whilst we make every endeavour to ensure the accuracy of the information provided here and that the recommendations are made to the best of our ability they may be subject to inaccuracies or change.

REVISION HISTORY

11/10/2014	Revision 1.0 issued to Matt Mickelson
21/10/2014	Revision 1.1 issued to Matt Mickelson

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.org.uk

Registration Number: 07390092
Registered Office: Hamilton House, 1 Temple Avenue, London, EC4Y 0HG

University of South Wales Prifysgol De Cymru

University of South Wales

Phone: 0044 845 576 0101

Web: www.southwales.ac.uk

Contents

1.0 Executive Summary

This is the final report detailing the findings in relation to the execution of the ADISA Solid State Testing Methodology on Claims Test ADPC0012 submitted by IT Renew in September 2014. The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Solid State Testing Methodology v1.0, both of which are available from ADISA.

The claim made for the drive was:

> *"The Teraware Digital Asset Disposition Platform v2.15 can forensically sanitise the solid state devices supplied within this claim with reference to the ADISA Risk Levels identified within section Table 1; and generates a Certificate of Sanitisation upon successful sanitisation." - Claim Number ADPC0012. "*

Eight SAS/SATA 3.5" computer hard drives were submitted as part of this test and these are listed below:

Family	***Model***	***Test Level***	***Capcity***	***Description***
ProLiant SSD	MO0200FCTRN	1 and 2	200GB	HP ProLiant SSD 200GB SAS-SSD
ProLiant SSD	EO0400FBRWA	1 and 2	400GB	HP ProLiant SSD 400GB SAS-SSD
320 Series	SSDSA2BW160G3D	1	160GB	Intel 320 Series 160GB SATA-SSD
320 Series	SSDSA2BW160G3L	1	160GB	(Dell) Intel 320 Series 160GB SATA-SSD
X25-M	SSDSA2M160G2GC	1	160GB	Intel X25-M 160GB SATA-SSD
PM800 Series	MMCRE28G5MXP-0VB	1	128GB	Samsung PM800 Series 128GB SATA-SSD
PM810 Series	MZ7PA128HMCD-01	1	128GB	Samsung PM810 Series 128GB SATA-SSD
SS410 Series	MCBQE32G5MPP-0V	1	32GB	Samsung SS410 Series 32GB SATA-SSD

Table 1

After testing it is confirmed that the IT Renew claim is true for all drives tested up to Test Level 1 results. Furthermore, for the two drives tested to Test Level 2 the claim is also true. Full details of these results can be found within this document.

2.0 Test Level 1 Testing.

2.1 Simple Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard COTS forensic tools and techniques. (E.g. encase and access data / FTK)

During this phase structured data was written to the drive which was then forensically imaged in accordance with legal guidelines. Each drive was then placed into the IT Renew Teraware Digital Asset Disposition Platform v2.15 and a data erasure job created as follows:

cli> sanitize method=12 hsn=861526 jid=6

The job was then executed via the "job start jid=6" command. Upon completion of the sanitization job each drive was connected to a forensic analysis workstation and in accordance with the ADISA Threat Matrix, forensic analysis techniques where applied to recover data from the hard-drive.

The two forensic images were then compared and contrasted to ensure that all structured data had been removed. For this test there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on these device being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1

The Results of Test Level 1.

Drive	Result
HP ProLiant SSD 200GB SAS-SSD	Pass
HP ProLiant SSD 400GB SAS-SSD	Pass
Intel 320 Series 160GB SATA-SSD	Pass
(Dell) Intel 320 Series 160GB SATA-SSD	Pass
Intel X25-M 160GB SATA-SSD	Pass
Samsung PM800 Series 128GB SATA-SSD	Pass
Samsung PM810 Series 128GB SATA-SSD	Pass
Samsung SS410 Series 32GB SATA-SSD	Pass

Pass means that IT Renew Teraware Digital Asset Disposition Platform v2.15 mitigates the threat posed by the Threat Actors holding the capabilities outlined by risk level 1 and 2 on the tested drives and the claim made can be confirmed.

3.0 Test Level 2 Testing.

3.1 Simple Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off a chip.

During this phase structured data was written to the drive which was then forensically imaged in accordance with legal guidelines. Each drive was then placed into the IT Renew Teraware Digital Asset Disposition Platform v2.15 and a data erasure job created as follows:

cli> sanitize method=12 hsn=861526 jid=6

The job was then executed via the "job start jid=6" command. Upon completion of the sanitization job each drive was connected to a forensic analysis workstation and in accordance with the ADISA Threat Matrix, forensic analysis techniques where applied to recover data from the hard-drive

Then both the controller chip and NAND memory storage chips were removed and placed into chip reading devices. Forensically sound images of the controller chip and NAND memory storage chips were then created and analysed.

The two forensic images were then compared and contrasted to ensure that all structured data had been removed. For this test there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on these device being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2

The Results of Test Level 2.

Drive	Result
HP ProLiant SSD 200GB SAS-SSD	Pass
HP ProLiant SSD 400GB SAS-SSD	Pass

Pass means that IT Renew Teraware Digital Asset Disposition Platform v2.15 mitigates the threat posed by the Threat Actors holding the capabilities outlined by risk level 3 and 4 on the tested drives and the claim made can be confirmed.

4.0 Summary and Conclusions

All eight drives tested passed the claims test as all forensic data recovery techniques up to and including ADISA Test Level 1 failed to recover any data. The two drives tested to Test Level 2 also passed the claims test as all forensic data recover techniques up to and including ADISA Test Level 2 failed to recover any data once they had the Teraware SAS/SATA SSD data sanitization method applied to them via the IT Renew Teraware Appliance.

Claims Test Carried Out By: Professor Andrew Blyth

Test Facility: University of South Wales

Signature: 

Date: 8th October 2014

Appendix A Claims Test Application Form.

Claims Testing Application Form

Form Number ADPC0012

Section 1 – Applicant Information

Company Name: **IT Renew Inc.**
Address: 8356 Central Avenue, Newark, CA 9560

General Contact
Name: Matt Mickelson
Phone: 001 408 799 4118
Mobile: 001 408 799 4118
E-Mail: matt.m@itrenew.com

Section 2 – Applicant Software Information

Manufacturer **IT Renew Inc.**
Version of software **Teraware v2.15**

Technical / physical architecture of claims test applicant software.

The Teraware platform discovers the target device and capabilities to formulate a multi-stage, forensic-level, sanitization protocol for a solid state device.
Stage 1 - Teraware determines if the target drive supports back-end AES encryption. If so, Teraware will initiate the CRYPTOGRPAHIC_ERASE command to delete the key between the NAND controller and the NAND components. This first step quickly obfuscates the user data making it unavailable.
Stage 2 - Teraware applies the PRNG_OVERWRITE process to the logical capacity. This process is measuring the devices ability to handle host I/O and collect medium statistics that contribute to final disposition decision making.
Stage 3 - Teraware employs a method to issue a BLOCK_ERASE cycle to each of the physical NAND blocks effectively eliminating all previously written data to the physical medium. This step disregards the defect error registers and will address all physical blocks on the NAND chips.
Stage 4 - Teraware performs a DEVICE_ISSUED_OVERWRITE command that will write a designated pattern to all physical NAND blocks using a program cycle. If the drive does not offer self-issued overwrites, then Teraware shall issue a LOGICAL_OVERWRITE command to cover the logical user capacity.
Stage 5 - Verification. Teraware performs a VERIFICATION process on the logical capacity to ensure sanitization of this area is exhaustive.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

TW_Appliance_Users_Guide_v1.0.pdf

Host Information for claims test applicant software to run on. To be shipped by test claimant.

1x Teraware Appliance (contains the application, database, and deployment system)
1x Dell DCS 2100 server w/LSI SAS 9211-4i HBA + Qlogic 4Gb FC HBA (processing station)
1x FC T-Card adapter, SFP, and fibre cable
Teraware User Guide
Setup doc

Section 3 – Test Hardware Information

VENDER	FAMILY	MODEL	CAPACITY	INTERFACE	RISK LEVEL	TEST LEVEL	CERT LISTING NAME
HP	ProLiant SSD	MO0200FCTRN	200GB	SAS-SSD	1,2,3,4	2	HP ProLiant SSD 200GB SAS-SSD
HP	ProLiant SSD	EO0400FBRWA	400GB	SAS-SSD	1,2,3,4	2	HP ProLiant SSD 400GB SAS-SSD
Intel	320 Series	SSDSA2BW160G3D	160GB	SATA-SSD	1,2	1	Intel 320 Series 160GB SATA-SSD
Intel	320 Series	SSDSA2BW160G3L	160GB	SATA-SSD	1,2	1	(Dell) Intel 320 Series 160GB SATA-SSD
Intel	X25-M	SSDSA2M160G2GC	160GB	SATA-SSD	1,2	1	Intel X25-M 160GB SATA-SSD
Samsung	PM800 Series	MMCRE28G5MXP-0VB	128GB	SATA-SSD	1,2	1	Samsung PM800 Series 128GB SATA-SSD
Samsung	PM810 Series	MZ7PA128HMCD-01	128GB	SATA-SSD	1,2	1	Samsung PM810 Series 128GB SATA-SSD
Samsung	SS410 Series	MCBQE32G5MPP-0V	32GB	SATA-SSD	1,2	1	Samsung SS410 Series 32GB SATA-SSD

ADISA Threat Matrix

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3

Section 4 – The Claim

The Teraware Digital Asset Disposition Platform can forensically sanitise the solid state devices supplied within this claim with reference to the ADISA Risk Levels identified within section 3; and generates a Certificate of Sanitisation upon successful sanitisation.

Claim Technical Contact at applicant.

Name: _____

Phone: _____

Mobile: _____

E-mail: _____

Acceptance

I, Matt Mickelson of ITRenew confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of ITRenew

SIGNED:

NAME: Matt Mickelson

TITLE: Director, Product Management

DATE:

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE: 19.05.2014

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: 19.05.2014