CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC0094

SECTION 1 – APPLICANT INFORMATION

Company Name: REDKEY USB LTD

Address: KEMP HOUSE, 160 CITY ROAD

General Contact

Name: Gareth Owen

Phone: [redacted]

Mobile:

E-Mail:

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: REDKEY USB LTD

Version of software: V3.47

Version of user manual: Revision 1

Algorithm to be used: RK1 - Redkey Data Wipe Level 1

Please describe the means of deployment for your software/hardware product:

USB Flash Drive

Please list the equipment you are intending to ship to execute the test, or the means to access/download your software tool:

1 x Redkey USB Computer Data Wipe Tool
1 x Copy of user manual - Revision 1

CLAIMS TESTING APPLICATION FORM

SECTION 3 – MEDIA WHICH YOUR PRODUCT IS TO BE TESTED ON

Solid State Disk Drive (SSD)
Make : Intel
Model : SSDSA2M160G2GC 2.5"
Part Number : CVPO003200K160AGN

Electromechanical Hard Disk Drive (HDD)
Make : Hitachi
Model : 647466-001
Part Number : JP1572FN2NTRUK

ADISA Threat Matrix

RISK LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TEST LEVEL
1 (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. Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
2 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products. 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
3 (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

CLAIMS TESTING APPLICATION FORM

ADISA

SECTION 4 – THE CLAIM

Redkey software called "REDKEY USB ULTIMATE VERSION 3.47", when used in accordance with user manual "REVISION 1", and using the "RK1 - REDKEY DATA WIPE LEVEL 1" algorithm, will remove all user data on the media samples within this test to protect from a forensic attack equivalent to test level 1 of the ADISA Threat Matrix.

I, Gareth Owen of Redkey USB LTD 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 Redkey USB LTD

SIGNED: 

NAME: GARETH OWEN

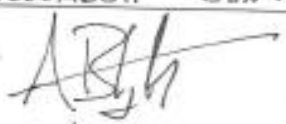
TITLE: DIRECTOR

DATE: 24/10/2020

ACCEPTANCE

Claim Accepted by:

ADISA RESEARCH CENTRE (ARC)

SIGNED: 

NAME: Dr Andrew Blyth, PhD.

TITLE: Director of Research & Technology.

DATE: 28th Oct 2020