

CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC0054



SECTION 1 – APPLICANT INFORMATION

Company Name: Teleplan

Address: Langstone Technology Park Havant Hampshire PO9 1SA

General Contact

Name: Dave Robinson

Phone: 029320444451

Mobile: 07711558404

E-Mail: Dave.Robinson@teleplan.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: Teleplan

Version of software: Proteus.2.16D-14

Background (Explanation of the company and software)

Teleplan has over 30 years experience in the service industry and processes 7 million hard drives annually. The Proteus is the latest in house developed tester to facilitate testing and repairing storage devices. The development group has complete design control of both hardware and software aspects of the system.

Technical / physical architecture of claims test applicant software.

Proteus software is developed on Scientific Linux platform using Eclipse C and C++ integrated development environment. The GUI provides an intuitive interface between independently running cells each running a non join-able thread which makes each cell independent and asynchronous. Low level communication is made through the SCSI-sub system enabling a common access for multi-commodities.

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

Software adheres to industry standard practice for secure coding.
All software engineers are fully qualified in their areas of expertise.

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

The Proteus software is preloaded on a Scientific Linux 6.10 system and requires no additional software.

SECTION 3 – TEST HARDWARE INFORMATION

- SSD
 - o Name: WD Blue NAND SSD 250GB
 - o Model: WDS250G2B0A-00SM50
 - o S/N: 183123803096

- HDD
 - o Name: TOSHIBA HDD
 - o Model: DT01ACA050
 - o S/N: Y78047WBS-X13

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

Teleplan's Proteus, when used in accordance with user manual P-CU-002-001, where by selecting the appropriate HDD or SSD test case, will invoke an algorithm which does a multi-pass overwriting completing with hex pattern 0x00. If supported by subject under test firmware provided algorithms may be used to reinforce the erasure.

All user data on the sample media listed within this claims application, cannot be recovered using techniques aligned to ADISA Test Level 2 after over writing has taken place.

I, Dave Robinson of Teleplan 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 Teleplan

SIGNED:



NAME: David Robinson

TITLE: Research and Development Director

DATE: 16th November 2018

ACCEPTANCE

Claim Accepted by:

Professor Andrew Blyth

Steve Mellings

SIGNED:

SIGNED:

NAME: Andrew Blyth

NAME: Steve Mellings

TITLE: Professor

TITLE: Director

DATE: _____

DATE: _____