CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ACPD0071

SECTION 1 – APPLICANT INFORMATION

Company Name: toolhouse DV-Systeme GmbH & Co. KG

Address: Türltorstr. 16 - 20, 85276 Pfaffenhofen an der Ilm, Germany

General Contact

Name: Volker Denkhaus

Phone: +49(0)8441/5044-22

Mobile:

E-Mail: denkhaus@toolhouse.de

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: toolhouse Entwicklungs KG

Version of software: toolstar®testLX with shredderLX-module 5.10

Version of user manual: inbuilt manual- and help-function

Algorithm to be used: BSI-3 for HDD / Overwrite plus Enhanced Secure Erase SSD for SSD

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

toolstar®testLX with shredderLX-module is made for deep testing and secure wiping of all drives in PCs, server, notebooks and IPCs. All processes and detailed reporting are completely automatable.
The software provides a lot of possibilities for individualisation.
toolstar®software is made for and used by manufacturer, refurbisher, service provider as well as all persons who are responsible for IT- and data security.

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

1 x toolhouse-USB-Stick

1x license toolstar®testLX with shredderLX-module in customer portal
www.licinger.de/customer/login
user: steve.mellings@adisa.global PW: adisa

CLAIMS TESTING APPLICATION FORM

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

1 x Magnetic Hard Drive: WesternDigital WD2500AAKX SATA
1 x Solid State Drive: Samsung 860 EVO V-NAND SATA 250GB

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

SECTION 4 – THE CLAIM

toolstar®testLX Version 5.11 with shredderLX-module, when used in accordance with inbuilt manual and help function will overwrite all user data on sample device when algorithm BSI-3 is selected for HDD and algorithm Overwrite plus Enhanced Secure Erase SSD for SSD are selected, such that no user data can be recovered using forensic techniques aligned with ADISA test level 2.

I, Volker Denkhaus of toolhouse DV-Systeme GmbH & Co. KG 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 toolhouse DV-Systeme GmbH & Co. KG

SIGNED:

NAME: Volker Denkhaus

TITLE: Head of Engineering

DATE: 1.10.2019

ACCEPTANCE

Claim Accepted by:

Asset Disposal and Information Security Alliance Limtied

SIGNED:

NAME: Dr Andrew Blyth

TITLE: Director of Research and Technology

DATE: 1.10.2019