ADISA

PRODUCT ASSURANCE

ADISA.GLOBAL

1.0 ABSTRACT

ADISA has been running a Product Claims Test scheme for data sanitisation tools since 2012. This internationally recognised scheme tests hardware or software against a specific claim about its ability to ensure any data on a piece of media is no longer available, whether by overwriting or by destruction.

During 2019 ADISA developed an enhanced test scheme which augments the product claims test and evolves it to include testing the software vendor's own abilities. This scheme was launched in 2020 and is presented to you as the ADISA Product Assurance Scheme.

This document explains what this scheme is and how applicants should present themselves for evaluation.

1.1 INTRODUCTION

The scheme structure has been defined by ADISA and only complete adherence to each part of this scheme will see a product pass the ADISA Product Assurance scheme.

The scheme is run in two distinct phases. The first is an assessment of the applicant's approach to product development, evolution and support and includes reviews of documentation and interviews with the organisation. The second is a forensic assessment of the tool's performance against a set of target media.

The award/accreditation if successful is made for a three year period with a revalidation test required to extend beyond this period. Should forensic capabilities change during the three year period, the test laboratory reserves the right to retest the applicant's solution at no cost to the applicant.

2.0 APPLICATION

Organisations wishing to undertake assessment against the ADISA Product Approval Scheme, will only be permitted to do so once a Non-Disclosure Agreement has been put in place by the applicant, the test laboratory and ADISA. This can be ADISA's, or the applicant's own document.

Once signed the applicant will be required to complete an application form and to submit this to ADISA. Once approved, ADISA will agree a timeline with the applicant and the test will be scheduled and 50% of the test fees will be due before testing commences.

2.1 TEST FULFILMENT

The applicant will be required to supply the following to the test laboratory:

1. Copies of the software with licensees to be assessed during the test and any hardware necessary to deploy the software which might be considered specialist in nature. An example of specialist hardware may be the deployment rack should the software be used as part of a rack-based solution.
2. A minimum of four drives (including, but not limited to, ATA HDD, SCSI HDD, ATA SSD & SCSI SSD) to undergo destructive forensic testing at the test laboratory (n.b. These will not be returned to the applicant as they will be consumed (broken) during testing. Evidence of disposal will be provided).
3. All documentation required and listed on the application form to permit test phase 1.

The test laboratory will be responsible for the following:

1. Provision of all technology, software and other tools required for the forensic testing to be undertaken, other than equipment listed as being the responsibility of the applicant.
2. Ensuring that all equipment is insured during the test phase.
3. Ensuring that all equipment and documentation is kept secure at all times.
4. Maintaining a line of communication with the applicant throughout the test period.

> It is the applicant's responsibility to pay for shipping to and from the laboratory and to ensure shipping is insured at all times.

At the end of the test period the drive remnants will be disposed of and a certificate provided to evidence this. In addition, all hard and soft copies of documentation, including the laboratory notes, will be retained for a period of four years (length of validity period plus 12 months).

3.0 TEST PHASE 1

The objective of this phase is to assess the applicant's credentials in terms of software/hardware development and support. A range of documents will be required to support each of:

3.1 INTERNAL SOFTWARE DEVELOPMENT ROADMAP

Assessment criteria to include: R&D to understand ongoing changes which could impact on the software requirements, design phase for understanding how to assess and overcome change requirements and testing of proposed solutions in a beta environment.

3.2 NEW PRODUCT INTEGRATION/SUSTAINING SUPPORT

Assessment criteria to include: Staged introduction to production environment with Quality Control and review cycles. For products sold commercially there would be additional checks made on roll out to customers, training, user manual updates and assessment of service and maintenance contracts.

3.3 SOFTWARE REVISION MANAGEMENT PROCESS

Assessment criteria to include: Written policy for change of management, impact on revision nomenclature and communication of changes to customers and users of product. What is the software support process for multiple revisions in the field?

3.4 TOOL REVISION CONTROL

Assessment criteria to include: Assessment made of development process and tools used as part of that process. If test suites are used how are revision changes to those suites assessed?

3.5 IT SUPPORT PROTOCOL

Assessment criteria to include: How the software deals with anomalies and what support mechanisms are in place to address them.

3.6 DATABASE MANAGEMENT

Assessment criteria to include: If the software utilises a data base as part of its deployment or delivery then how is the database secured, partitioned, managed and otherwise maintained? This is to include assessment of how the data overwriting records are stored and recovered by the user of the software.

3.7 RECORDS MANAGEMENT

Assessment criteria to include: Does the software log activities whether in test phase or deployment? Are the logs reviewed and assessed within test phase and during deployment? Are they made available for customers to use to evidence successful use of the software (e.g. provision of wipe reports)?

3.8 SECURITY MEASURES

Assessment criteria to include: Has the software been formally penetration tested to measure vulnerabilities within it which could be exploited? This test could be extended to any web-based portals or databases which are used. Assessment to include how users are managed.

ADISA's method will include an assessment for each test which will start with a set of requirements which all subjects are expected to have with assessment resulting in a score against these requirements. There will be a minimum score required to pass each criterion. This will be based on ADISA and the test laboratory's own opinions on what a minimum expectation on a commercial product should be. These will NOT be published but will be made available to any test applicant under NDA.

Assessment will take place via paperwork review and also remote interviews with key individuals. Site visits will NOT be undertaken as part of this test process unless required by the applicant. At that stage, costs of travel, time and subsistence will be costed in addition to the pricing in 6.0.

4.0 TEST PHASE 2

The objective of this phase is to assess the applicant's software by forensically testing its performance in the ADISA Research Centre in Wales.

4.1 TEST OBJECTIVES

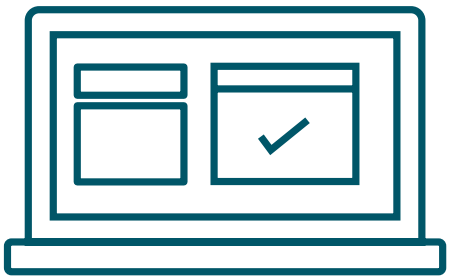
REQUIREMENT 1: PROCESS FOR SANITISATION

The software sanitises user data so that a forensic attack equivalent to ADISA Test Level 2 (See Appendix 1) renders the user data unrecoverable.

REQUIREMENT 2: SOFTWARE FUNCTIONALITY

Software shall have the ability to:

- "leave a Digital Signature or 'Fingerprint' upon the completion of the overwriting process which meets the following requirement:
  - shall be able to identify the specific overwrite on each piece of media present.
  - shall include the date of sanitisation, sanitisation method, sanitisation time, drive serial number, system serial number (if applicable), report ID (so it can be cross-referenced in the database for the certificate), sanitisation software used and version number."
- shall verify the sanitisation of data and create an individual confirmed report of sanitisation for each device which contains the same information as specified for the Digital Signature or Fingerprint. This report shall be stored centrally and be able to be recovered should this be required.
- have the inbuilt ability to verify a minimum of between 1% and 10% of the drive with 10% being the ideal percentage.



REQUIREMENT 3: FORENSIC TESTING

Applicants must present a sample of at least four drives including, but not limited to, ATA HDD, SCSI HDD, ATA SSD and SCSI SSD. When the software is executed the algorithm to be used during this test will be NIST 800–88 Rev 1 and the product should be configured in such a way as to permit the selection of this algorithm.

The test process is designed to prove or disprove the following claim about the software product:

Software evaluation product X, revision Y, when used in conjunction with User Manual Z overwrites all user data including the removal of DCO and HPA, which ensures a forensic attack equivalent to Test Level 2 of the ADISA Threat Matrix cannot recover the user data.

This will be achieved by undertaking a laboratory test including, but not limited to, the methodology outlined in 4.2.1 and 4.2.2

4.2 TEST OBJECTIVES

There are two levels of forensic assessment, each used to attest the software tool's abilities to overwrite data and to prevent data recovery via different forensic tools. The methodology for each of the two levels is below and explained further in Appendix 1.

4.2.1 TEST LEVEL 1 METHODOLOGY FOR SOLID STATE AND MAGNETIC HARD DRIVES

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.

For each computer hard drive device, the following methodology is performed:

1. Structured data, the string 'ADISA', is written to every logical block address on the hard drive.
2. The device is then imaged using Access Data/ FTK to create a base-line forensic image.
3. The device is then erased using the software in accordance with the manufacturer's instructions.
4. The device is then analysed using the following tools to create a second forensic image:
    a. Standard commercial tools and techniques such as Access Data/FTK and Encase.
5. The two forensic images (Stage 3 and Stage 5) are then compared and contrasted to ensure that all structured data has been removed.
    a. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

4.2.2 TEST LEVEL 2 METHODOLOGY FOR SOLID STATE DRIVES

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 the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and placed in a stable state.
2. Structured data, the string 'ADISA', is written to every logical block address on the hard drive.
3. The device is then imaged using Access Data/ FTK to create a base-line forensic image.
4. The device is then erased using the software in accordance with the manufacturer's instructions.
5. The device is then analysed using the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
    a. Software based forensic tools/techniques such as:
        I. Standard commercial tools and techniques such as Access Data/FTK and ENCase;
        II. State of the art data recovery tools such as PC3000 SSD;
        III. Customer designed data recovery software.
    b. Hardware/Chip based forensic tools/ techniques such as:
        I. Flash/NAND TSOP/BGA chip readers;
        II. State of the art data recovery tools such as PC3000 FLASH and Rusolut;
        III. Customer designed data recovery software/hardware.

4.2 TEST OBJECTIVES

4.2.3 TEST LEVEL 2 FOR MAGNETIC HARD DRIVES

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 the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string 'ADISA', is written to every logical block address on the hard drive.
3. The device is then imaged using Access Data/ FTK to create a base-line forensic image.
4. The device is then erased using the software in accordance with the manufacturer's instructions.
5. The device is then analysed using the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
   a. Software based forensic tools/techniques such as:
      I. Standard commercial tools and techniques such as Access Data/FTK and Encase;
      II. State of the art data recovery tools such as PC3000 UDMA/SAS;
      III. Customer designed data recovery software.

5.0 AWARD

An accreditation will be confirmed for a maximum of three years. Any changes to the product which results in a new version of the product (e.g. Version 1.0 becomes Version 2.0) being issued will require re-testing. Any changes to the product which results in a new revision (e.g. Version 1.0 becomes version 1.1) to the product does NOT require re-testing.

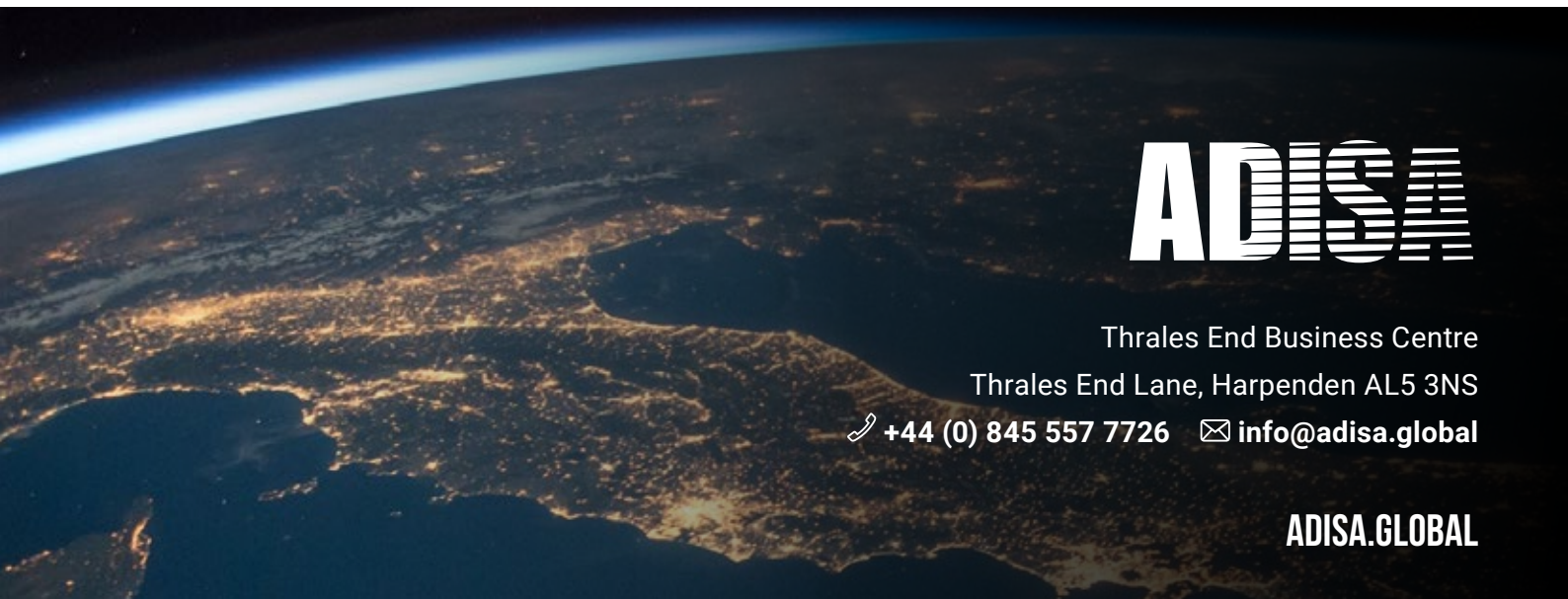
Each applicant will be given a report documenting the findings of the test and, should they pass, will be issued with a certificate to verify compliance with this test (for use in audit etc. not to be displayed publicly on website or in customer facing information) and a standard ADISA claims test logo for them to use commercially as they see fit.

6.0 PRICING

Pricing is available from ADISA upon request.

APPENDIX 1 ADISA THREAT MATRIX

THREAT CAPABILITY LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TYPE OF ATTACK	COMPARISON
1 (Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, COTS and OS tools.	Keyboard attacks from a motivated individual or professional organisation Typical attack could be using open-source forensic tools or commercial tools	Clear NIST 800–88 Rev 1 ISO 27040
2 (Medium)	Commercial data recovery and computer forensics organisation able to mount invasive/destructive software and hardware attack, utilising both COTS and bespoke software.	Laboratory attacks from commercial data recovery experts or specialist forensic scientists. Typical attack could be: Advanced data recover software, Chip Readers and protocol decoders. Typical attack would involve analysis of individual hardware components as well as protocol structures.	Purge NIST 800–88 Rev 1 ISO 27040
3 (High)	Government-sponsored organisations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitised data.	An attack agent of unknown capability and unlimited resource. Typical attacks: Taking theoretical forensic possibilities and making them an actual capability.	Destroy NIST 800–88 Rev 1 ISO 27040



ADISA

Thrales End Business Centre
Thrales End Lane, Harpenden AL5 3NS
+44 (0) 845 557 7726 info@adisa.global

ADISA.GLOBAL