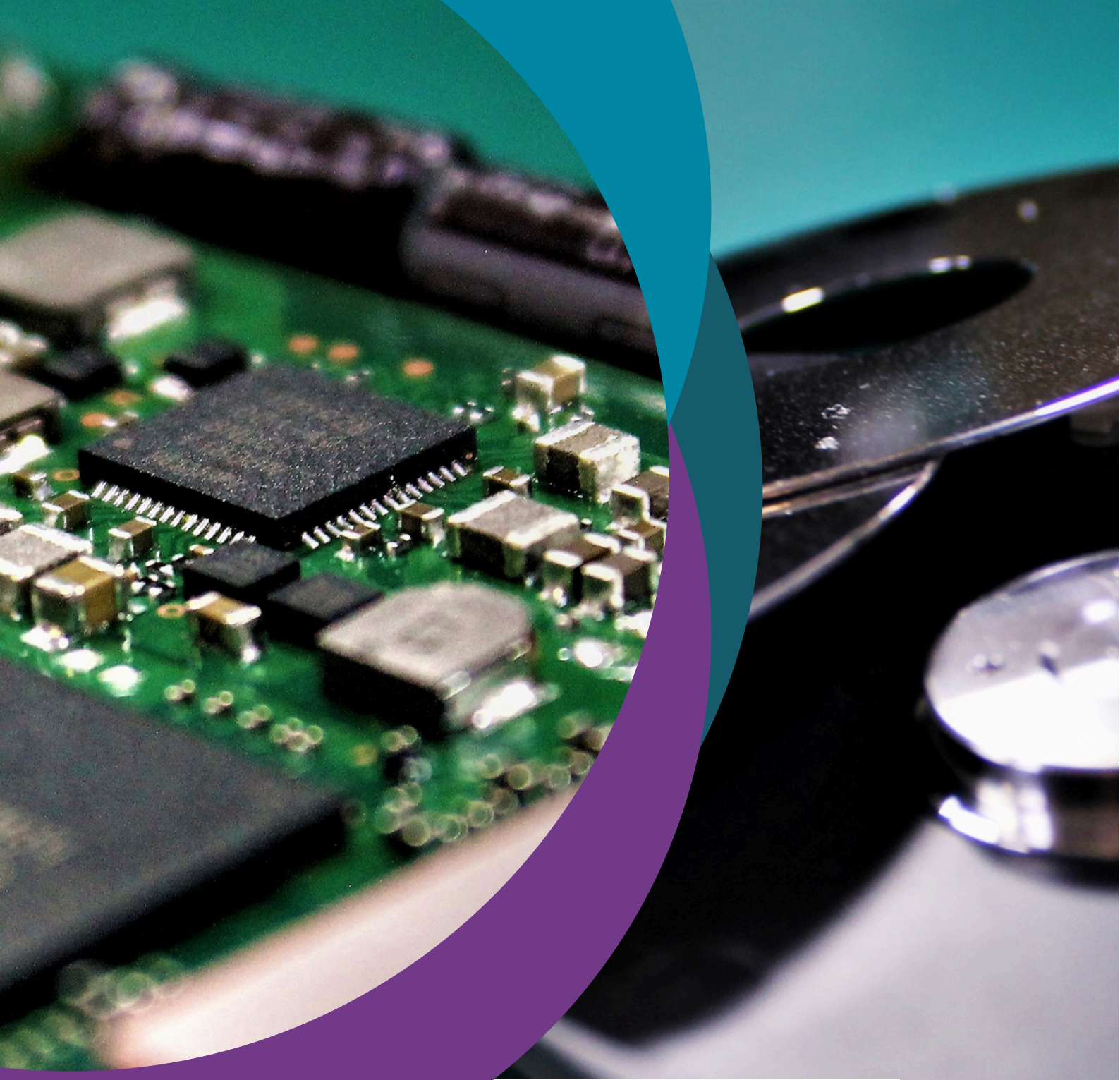


PRODUCT CERTIFICATION BROCHURE

ADISA RESEARCH CENTRE

www.adisarc.com

ABSTRACT

Data Sanitisation is the process of treating data on storage media such that the risk of retrieval and reconstruction is unfeasible using laboratory techniques. This can be a destructive process which impacts the functionality of the storage media or a non-destructive process using software to affect data without impacting on the functionality of the storage media.

Verification of sanitisation techniques is often sought to provide assurance to organisations that their data is not at risk. This can be challenging due to the different storage media formats and the number of variables which can affect the outcome such as operating systems and firmware. Those seeking assurance need to be aware of such variables to make an informed decision on the claims being presented. The use of certifications frequently forms part of the due diligence for organisations seeking assurance when sanitising media.

This brochure presents ADISA Product Certification which has three levels offering increasing levels of assurance to organisations seeking to use or specify media sanitisation products.

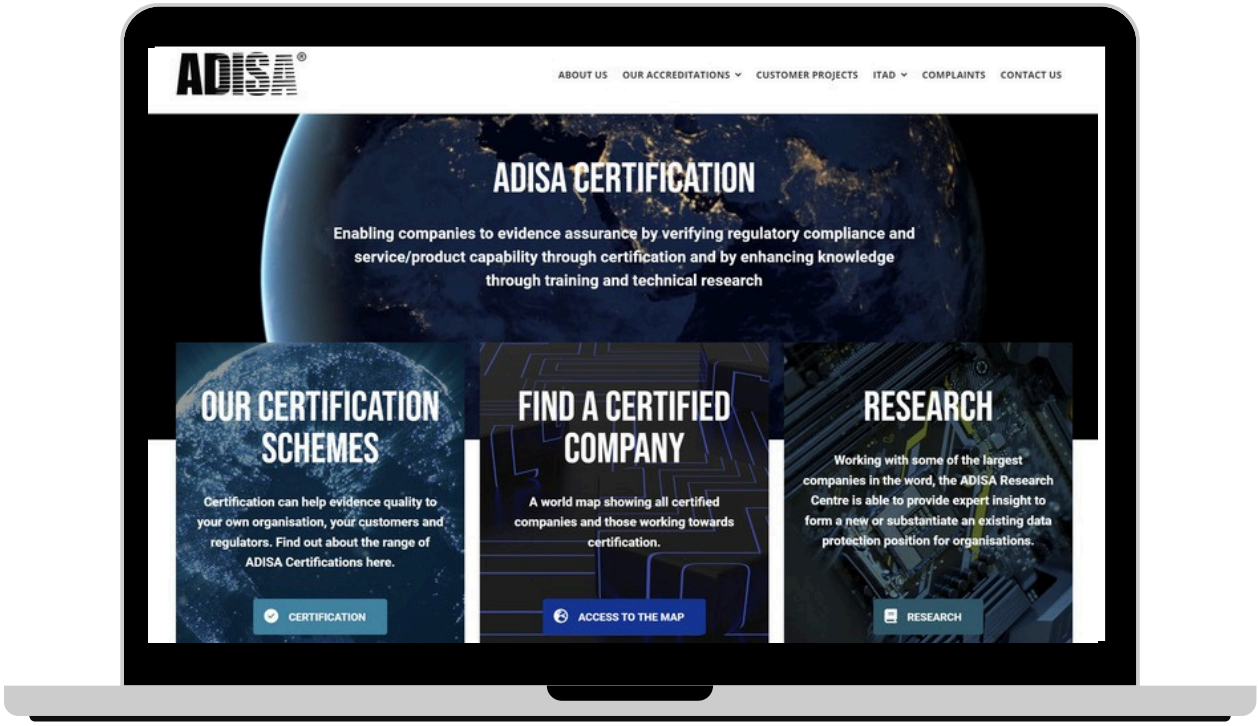
ABOUT ADISA RESEARCH CENTRE

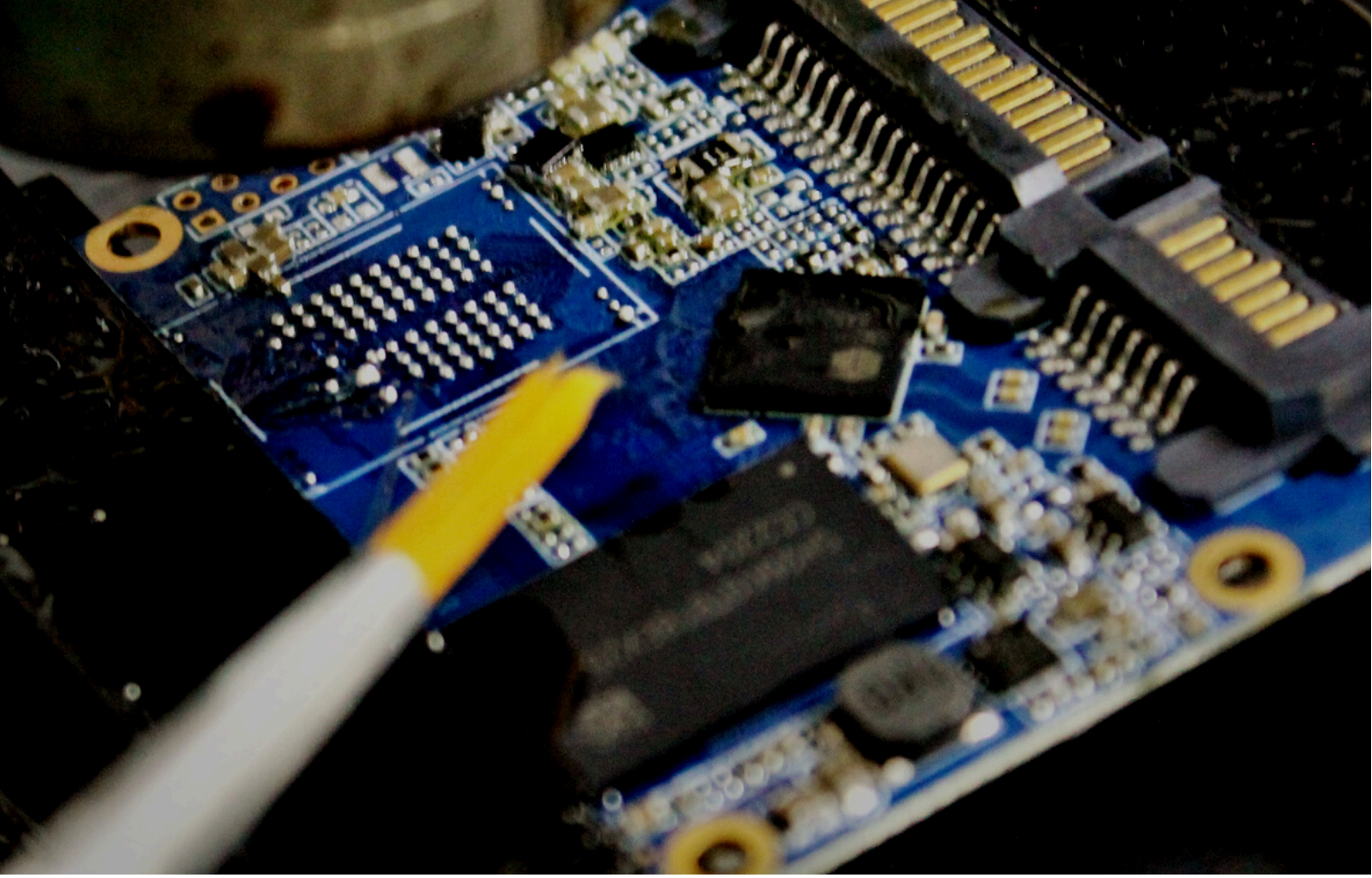
Launched in 2010, ADISA Certification is an independent certification body based in the UK but certifying companies worldwide. ADISA owns several certification schemes including the ADISA Asset Recovery Standard 8.0 which was formally approved by the UK Information Commissioner's Office as a UK GDPR Certification Scheme in 2021. ADISA hold accreditation issued by the UK Accreditation Service (UKAS) for the audit process against this Standard.

ADISA also offers product certification schemes which are included within this brochure which are undertaken by ADISA's own test laboratory, the ADISA Research Centre (ARC), under the control of Dr. Philip Turner, one of the world's leading data sanitisation experts. ADISA is proud to work with organisations across the globe to independently attest to the effectiveness of their products when sanitising media.

The ARC utilises a range of data recovery and media manipulation toolsets including propriety techniques to recreate the capabilities of specific threat adversaries as detailed in table 1, ADSIA Threat Matrix.

In addition to Product Certification, the ARC is the partner house for several blue - chip organisations and government departments.





ABOUT PRODUCT CERTIFICATION

When deciding on a suitable means of sanitising media there are variables which must be considered including risk appetite, threat profile, data type, volume of data, regulatory requirements, and budget. In addition, an understanding of the target media is crucial as different technologies require different sanitisation techniques to be effective. This can cause concern for organisations who are using a sanitisation product themselves or who are writing a specification for a third party as they are unsure what products to place their trust in to sanitise their media.

The ADISA Product Certification Schemes are designed to offer increasing levels of assurance for organisations when looking to use or specify a toolset to sanitise different media. These schemes are:

- Certified Product Claims Test (PCT)
- Certified Product Assurance (PA)
- Certified Sanitisation Software Vendor (SSV)

Each scheme has different characteristics, but a shared core principle is that user data must be rendered irretrievable using compromised methods aligned to particular threat actors.

Each scheme includes a process whereby a laboratory attack is made on a sanitised piece of media to attempt to recover data using increasingly sophisticated techniques to mirror potential threat actors. This approach to verifying the viability of products for use as data sanitisation tools is risk based. The term risk is defined as follows from ISO 13335/1/2004.

"A risk is a potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. It is measured in terms of a combination of the probability of an event and its consequence."

To introduce structure into this process and to allow comparisons to be made, ADISA utilises a Threat Matrix which allows organisations to assess whether the testing undertaken on a particular product is sufficient for their purposes.

The threat matrix defines three test levels which in turn define a series of capabilities that a threat actor/agent may wish to bring against an asset either by direct access to the asset or access via its location within a device.

Test	Threat Actor	Type of attack and compromise method
1	Casual or opportunistic threat actor only able to mount unsophisticated attacks.	Keyboard attacks using the standard device interface using commercial off the shelf (CoTs) or open-source forensic tools.
2	Motivated, targeted threat actor such as organised crime or journalists or hackers applying laboratory methods.	Advanced attacks using specialist hardware and software to interrogate the device / storage media using the device interface and component attacks.
3	State-sponsored organisations using sophisticated techniques with unlimited time and resources.	Typical attack may involve proprietary hardware and software techniques not available on the general commercial market.

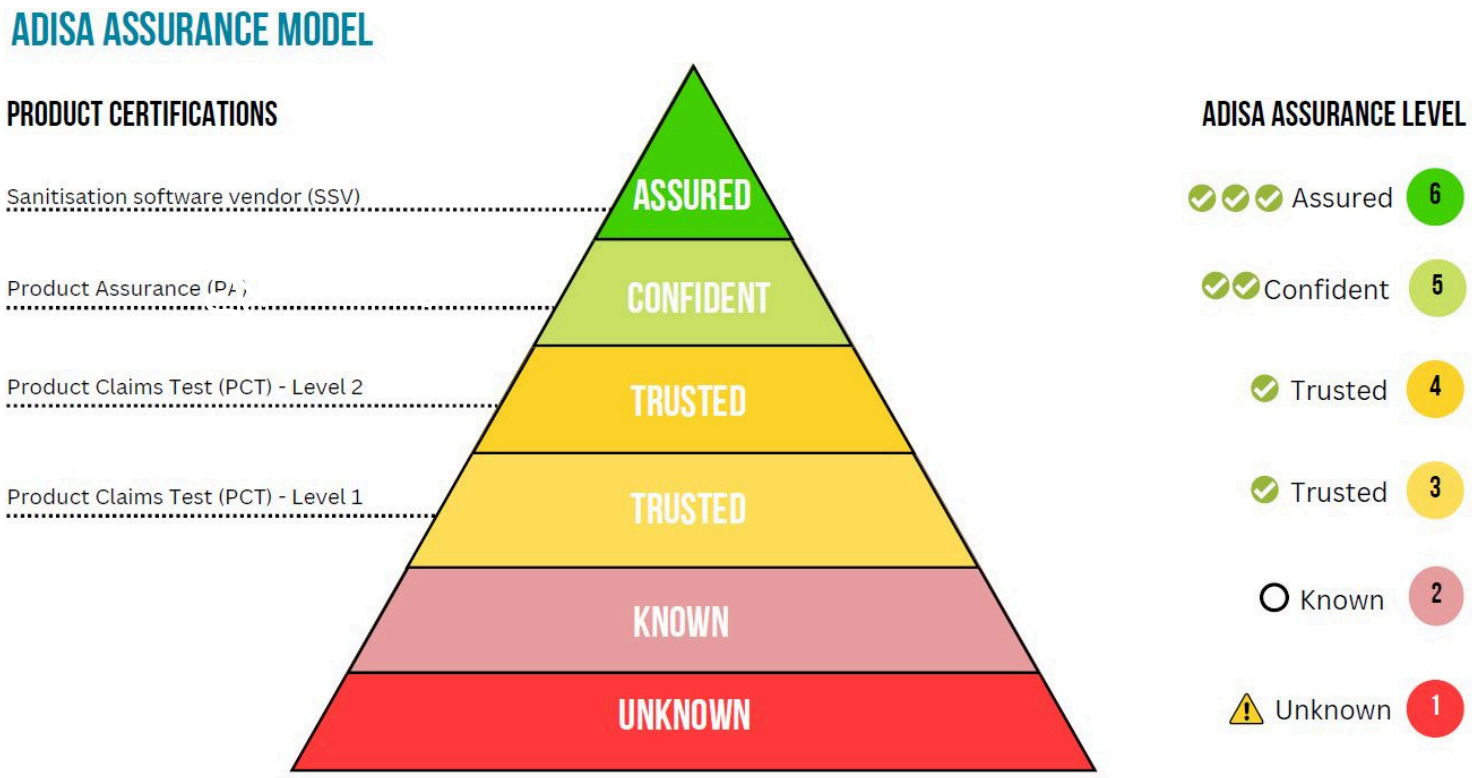
TABLE 1- THE ADISA THREAT MATRIX V4.1

ADISA ASSURANCE LEVELS

The objective of the ADISA Product Certification Schemes is to provide a certification where trust, confidence and assurance can be achieved via an increasing level of testing and validation of the products under evaluation.

- Product Claims Test offers trust that the product under evaluation in a specific media type, renders data unrecoverable.
- Product Assurance offers confidence that the product under evaluation meets the requirements of recognised guidelines and Standards for example, NIST 800-88 and IEEE 2883, such that the outcomes of its use can be assured.
- Certified Sanitisation Software Vendor offers assurance that all sanitisation products presented by the software house can be used with assurance on various media and interface types.
-

For organisations seeking to use or specify a sanitisation product, they can build assurance that the evaluated product can be confirmed and verified as meeting their requirements by requiring certification of that product at the appropriate assurance level.



OUR PRODUCT CERTIFICATIONS

CERTIFIED PRODUCT CLAIMS TEST (PCT)

This provides an entry point for organisations looking to provide their customers with verification that their sanitisation product works in a controlled environment. The process starts with a specific claim being made about the effectiveness of the product to render user data unrecoverable. This claim can select different media types, interfaces or operating systems as determined by the applicant. Depending on their assurance requirement a test level 1 or 2 can be undertaken on their behalf.

The laboratory follows the test method to attest whether the claim made is True or Not True.

FEATURES

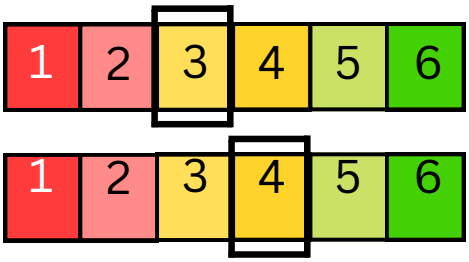
- Forensic Verification that data cannot be recovered using different test levels.
- No minimum sample size to allow for test profiles based on known use cases.
- No limitation on media types.
- Can be hardware or software products tested.

BENEFITS

By holding a PCT certification, an organisation can present third party evidence that the product can be trusted to perform the task for which it is purchased.

Products holding PCT certification should be viewed as more trustworthy than products for which there is either no verification of capabilities or for those where capabilities are self-certified.

ADISA ASSURANCE LEVEL (AAL)



LEVEL 1 TESTING

LEVEL 2 TESTING

AAL 3-4

TRUSTED

CERTIFIED PRODUCT ASSURANCE (PA)

When storage media is viewed in greater detail it can be seen that in addition to there being different types (Magnetic Hard Drive, Solid State etc) there are also different interfaces and media protocols from which the firmware on the media is derived. This is important as the method of sanitisation is typically to issue commands which implement features inbuilt into the storage media whether that is a write command or more commonly an erasure command. These commands differ between media types and interfaces and in some instances are not supported by the media in question.

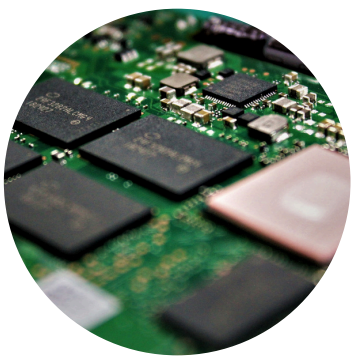
To build assurance, there are two widely accepted data sanitisation guidelines/standards which specify how sanitisation software should engage with storage media to ensure a data safe outcome. These are the NIST Special Publication 800-88 Revision 1 - 'Guidelines for Media Sanitisation' and the IEEE Standard for Sanitising Storage Media 2883.

Within each there are three types of sanitisation techniques, Clear, Purge and Destroy/Destruct. Aligned with these are several recommended commands that can be applied to specific media and devices.

The ADISA Product Assurance scheme performs 13 different tests for either or both NIST 800-88 and IEEE 2883, to verify the command sets which are being sent to the media by interface type. In addition, a 15% sample of media and interface types are selected, and a Test Level 2 process is applied to verify that data cannot be recovered after the execution of the software.

Media and interfaces currently included:

Magnetic Hard Drive – ATA - PATA / SATA and SCSI - SAS
Solid State Drives – ATA - SATA and SCSI - SAS



FEATURES

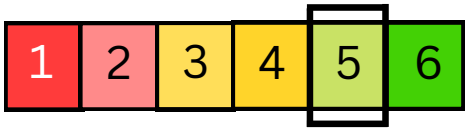
- Verification of compliance to NIST 800-88 and/or IEEE 2883 Clear and Purge for the media and interfaces listed where supported.
- 15% sample of media tested to confirm via forensic verification that data cannot be retrieved using Test Level 2 capability.
- Confirmation of software behaviour when a drive which does not support the required commands is presented for erasure.

BENEFITS

Products which are certified under Product Assurance offer a higher level of assurance by moving from trust to confidence that they will function as designed in all instances. This is based on confirmation of their compliance to the sanitisation requirements laid out in NIST 800-88 and/or IEEE 2883 by interface type and by media type within the scope of the test.

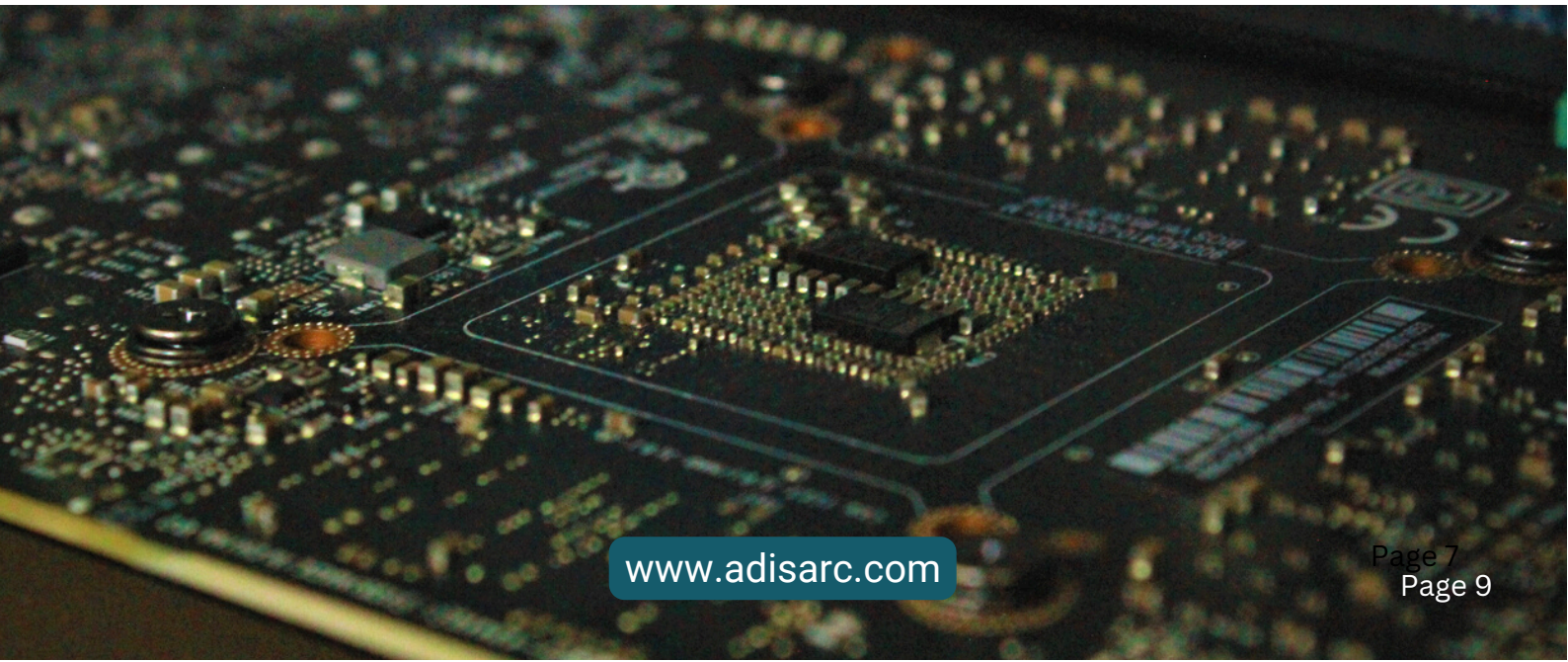
In addition, the data recovery techniques applied evidence that the product under evaluation offers greater assurance than PCT as the commands being issued are confirmed and the outcomes verified.

ADISA ASSURANCE LEVEL (AAL)



AAL 5

CONFIDENT



CERTIFIED SANITISATION SOFTWARE VENDOR (SSV)

The ADISA Certified Sanitisation Software Vendor (SSV) builds on the PCT and PA schemes to provide a broader depth of audit of the software vendor itself plus extending the test environment into an ongoing test profile which is controlled by the laboratory. This shows huge confidence by the software vendor themselves as the lab can introduce variables throughout certification to ensure the real-world environment in which the software is used is reflected by the testing.

FEATURES.

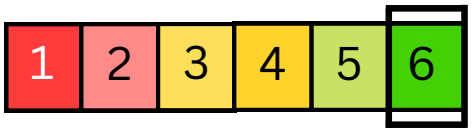
- Audit of software vendor itself.
- Verification of compliance to NIST 800-88 and IEEE 2883.
- Test Level 2 data recovery techniques applied.
- Ongoing monthly testing undertaken by the test laboratory autonomous from the applicant.
- A failed wipe is good! Scheme assesses how drives which the software doesn't support are identified and how the software helps the user identify these.

BENEFITS

This scheme is designed to offer the highest level of assurance possible for software sanitisation software vendors.
By conducting an onsite audit of the applicants' own processes and procedures for software development, this certification builds genuine assurance that all of the products created by the software house have gone through the same rigorous development cycle thus ensuring that their use in all instances can be assured.

Each piece of software offered by the software house will be assessed as per Product Assurance and therefore the outcomes by media type and interface confirmed. In addition, the ongoing perpetual testing sees the number of different drive makes, model and types, increase over time which enables assurance to be achieved through extensive third-party independent certification.

ADISA ASSURANCE LEVEL (AAL)



AAL 6

ASSURED

APPROVALS EXPLAINED

Each test level is carried out in accordance with the current ADISA Test Methodology which is a specification for applying different techniques to attempt to recover data from different media types. This test methodology includes a range of different tools including intrusive and destructive techniques designed to attempt data recovery using non-standard means.

Within each certification type, a positive result would be that the techniques applied to attempt to recover data were not able to recover human readable information. Within all tests, the software under evaluation must operate as an automated tool with no reliance on additional processes other than user prompts which may be required to allow the software to perform its tasks. Examples of not accepted processes would be where the software prompts the user to perform a manual reset on a smart phone to form part of the sanitisation process.

All software being presented shall have a name and version number and be supported by a user manual which itself has a version number. The laboratory will follow the user manual to use the software such that all future users would follow the same steps and therefore reach the same outcome as experienced by the laboratory.

When the sanitisation process has been completed the outcome (pass or fail) shall be presented to the user in a clear and unambiguous way to ensure that there can be no confusion about the result of the process being applied to the media.

When a product is presented for testing the ARC laboratory follows a rigid methodology. The objective of this is to show a consistent, reproducible test to ensure that the confidence in the outcome is absolute.

PCT and PA Test approvals are made on specific version / revision types of products and on specific media types. The testing done is in a laboratory environment and performed by recognised experts within this field.

Where necessary, ADISA may request to repeat the test, at ADISA's cost, to be assured of outcomes.

Should a test result in a failure, all test documentation will be presented to the applicant detailing the results and the process followed. A wash-up call may take place where the applicant can ask questions and / or troubleshoot, and a free re- test will be offered within a 30 days' time window from the original test.

SCHEME REQUIREMENTS.

	PRODUCT CLAIMS TEST (PCT)	PRODUCT ASSURANCE (PA)	CERTIFIED SANITISATION SOFTWARE VENDOR (SSV)
ADISA Assurance Level (AAL)	3-4	5	6
Confirmation that data cannot be recovered	Test Level 1 or 2	Test Level 2	Test Level 2
Test Sample Size	Minimum 1	Minimum 4	Ongoing
Scope of Certification	Specific product version and media type.	Specific product version.	All products.
Verification of:			
Verification of compliance to NIST 800-88 and IEEE 2882 Clear and Purge	✗	✓	✓
Command sets issued to device	✗	✓	✓
That remapped sectors are reported	✗	✓	✓
That reports / certificates are created including unique reference to device being sanitised	✗	✓	✓
Sanitisation failure process to be clear and transparent to user	✗	✓	✓
Practical site audit of software vendor to confirm:			
Internal software development roadmap	✗	✗	✓
New product integration / Sustaining Support	✗	✗	✓
Development tool revision controls	✗	✗	✓
Software revision management process	✗	✗	✓
User support	✗	✗	✓
Data Base / Security Measures	✗	✗	✓
Records management:			
QC / Test Regime	✗	✗	✓

ADISA®

WANT TO KNOW MORE?

CONTACT ADISA ON ± 44 1582 361743

OR INFO@ADISA.GLOBAL

www.adisarc.com