



## Claims Testing Application Form

Form Number ADPC00021

### Section 1 – Applicant Information

Company Name: Aiken Informática, S.L  
Address: Gran Via Corts Catalanes 566, Atico, 08011 Barcelona, Spain

General Contact  
Name: Juan-Carlos Font  
Phone: +34 931 167 443  
Mobile: +34 633 914 554  
E-Mail: jcfont@aiken.es

### Section 2 – Applicant Software Information

Manufacturer Aiken Informática, S.L.  
Version of software Aiken Workbench 2.0

#### Background (Explanation of the company and software)

Based in Barcelona, Aiken are developers of specialized software products for ITAD companies, supporting their full business cycle: equipment processing, warehousing operations and sales.

#### Technical / physical architecture of claims test applicant software.

Aiken Workbench is a client/server solution based on Ubuntu Linux. The clients start from the server using the PXE protocol. The major software functions are: auditing, secure data erasing, testing and imaging.

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

The installation and full operation of the software is described in the Administrator's Guide.

#### Host Information for claims test applicant software to run on.

1. HDD Seagate Barracuda 250GB, model 9SL131-021
2. SSD Samsung 840EVO 120GB, model MZ-7TE120
3. Android tablet Samsung Galaxy Note 10.1 (Android 4.1.2)
4. Apple tablet iPad Air (iOS 10.0.2)

### Section 3 – Test Hardware Information

- O Server: 1 notebook (recommended specifications: i5 processor, 4GB RAM, 160GB drive, DVD reader, Gigabit LAN port. It must be connected via Wi-Fi to the Internet during the installation)
- O Client: 1 desktop computer (recommended specifications: i5 processor, 4GB RAM, Gigabit LAN port).
- O 1 Gigabit network switch

#### 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

The Aiken Workbench product, when used in accordance with the Aiken Workbench Administrator's Guide, will overwrite all available data on the drives and devices within this test to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix.

Claim Technical Contact at applicant.

Name: Juan-Carlos Font

Phone: +34 931 167 443

Mobile: +34 633 914 554

E-Mail: jcfont@aiken.es

## Acceptance

**I, Juan-Carlos Font of Aiken Informática, S.L., 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 Aiken Informática, S.L.

SIGNED:

NAME: JUAN-CARLOS FONT

TITLE: MANAGING DIRECTOR/CHIEF SOFTWARE DESIGNER

DATE: 08/23/2016

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE:

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: