ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC0043

Section 1 – Applicant Information

Company Name: Blackbelt Smartphone Defence LTD
Address: Helm Bank, Natland, Kendal, Cumbria. LA9 7PS

General Contact
Name: Brejesh Chauhan
Phone: 07968280916
Mobile: 07968280916
E-Mail: brejesh.chauhan@blackbeltdefence.com

Section 2 – Applicant Software Information

Manufacturer Blackbelt Smartphone Defence LTD
Version of software Datawipe 3.8.40

Background (Explanation of the company and software)

Based in the UK, BlackBelt Smartphone Defence was founded in 2004, and has been providing Mobile security products ever since. Datawipe has been independently tested, to ensure the software is compatible with the latest devices, also providing a full audit trail which is available real time from your user controlled dashboard. Datawipe will safely remove all user data, restoring your smart device back to an out of box state. This software is used by industry and corporate clients.

Technical / physical architecture of claims test applicant software.

This section describes how the product is deployed, on what hardware it runs and any other technical aspect of using the product.

Operator PC Minimum Specification: Standard desktop / laptop running Windows 7, 8 or 10. i5 machine with full internet access. Each Operator PC must have at least: • 8GB RAM • 250GB+ SSD drive or Magnetic drive • 2 USB host controllers

System Access
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\DataWipe.exe"
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\MobileDevice\idevicerestore.exe
C:\Program Files (x86)\BlackBelt SmartPhone Defence\ BlackBelt DataWipe\BBAppleFirmwareService.exe
C:\ProgramData\BlackBelt SmartPhone Defence\

Firewall Access
https://dashboard.blackbeltdefence.com/ (88.208.233.202)
http://ax.phobos.apple.com.edgesuite.net (184.25.157.104)
http://appldnld.apple.com.edgesuite.net (77.67.87.89)

http://appldnld.apple.com (17.253.15.206)
phobos.apple.com deimos3.apple.com
albert.apple.com
gs.apple.com
gg*.apple.com*
itunes.apple.com
ax.itunes.apple.com*

NB: if you have Anti-virus running, please also add to the exceptions list

Blackbelt uses propriety methods for different operating systems

Blackbelt Device Clean

The BlackBelt propriety application and/or secure commands are sent to the connected device to remove all customer data, including; contacts, call logs, calendars, photographs, videos and user alarms. This process ensures we remove all user accessible data.

Data overwrite

BlackBelt offer both standard and secure wipe, when secure is selected the software will overwrite the storage on the device using a bespoke algorithm to ensure that data is not recoverable using specialist software to rebuild user data.

The BlackBelt Datawipe software allows admin controlled configuration to set number of cycles and passes, to ensure the datawipe process can be configured to meet customer required standards.

Manufacturer Factory Reset

As part of the Data wipe process BlackBelt will always perform a manufacturer factory reset to put the device into an out of box state.

Device Reset Check

To ensure the device is left in a factory reset state, BlackBelt perform a device reset check to complete the process, this ensures the device is left in an out of box state and removes the risk of a false positive response.

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

This is a critical part as the software will be executed by the test lab as per a particular guidance document.

See attached document - BB Installation Guide - Adisa 0811

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

What Hardware (if any) is to be shipped to the test lab in order to run the software?

Do we need to provide a laptop? If yes do we pre-install?

Section 3 – Test Hardware Information

iPhone 8+

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

BlackBelt Smartphone Defence software 3.8.40, when used in accordance with User Manuel "BB Installation Guide – ADISA 0811" will overwrite all available data on the hardware sample within this test to protect to a forensic attack equivalent to test level 1 of the ADISA threat matrix, this wipe method is only for activated iOS devices using the inbuilt protocols.

Claim Technical Contact at applicant.

Name: Brejesh Chauhan
Phone:
Mobile: 07968280916
E-Mail: Brejesh@blackbeltdefence.com

Acceptance

I, Brejesh Chauhan of BlackBelt Defence 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 BlackBelt Defence

SIGNED: B Chauhan

NAME: Brejesh Chauhan

TITLE: Head of Product

DATE: 08/02/2018

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: