CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC0084

SECTION 1 – APPLICANT INFORMATION

Company Name: Shenzhen Anxin Technology Co. Limited.

Address: 11l, Jinyun Century Building, Shennan Middle Road, Shatou Street, Futian District, Shenzhe

General Contact

Name: Luke zhang

Phone: +86 755 23616516

Mobile: +86 13544015430

E-Mail: luke.zhang@litong.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: Anxin Limited

Version of software: MDWv3.0

Version of user manual: MDW Client Operation Manual v3.0

Algorithm to be used: American Department of Defense (DoD 5220.22 M)

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

- The software must be installed on a Windows 10 OS or higher supported PC.
- Once installed the software will connect to MDW server in order to verify operator ID to apply data wiping and at the end of the process the software will return the result / confirmation of the action performed.

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

No equipment needed. Download links will be provided.

CLAIMS TESTING APPLICATION FORM

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

- iPhone 8 - IOS 13.2.3
- Samsung Galaxy S9 - ANDROID 8.0.0

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

Anxin Co Ltd software called MDW v3.0 when used in accordance with MDW Client Operation Manual v3.0 and using algorithm DoD 5220.22 M, will overwrite all user data on the hardware sample within this test to protect against a forensic attack equivalent to test level 1 of the ADISA Threat Matrix.

I, Luke Zhang of Shenzhen Anxin Technology Co, Ltd 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 Shenzhen Anxin Technology Co, Ltd

SIGNED: Luke Z

NAME: Luke Zhang

TITLE: Operations Director

DATE: 10.03.2020

ACCEPTANCE

Claim Accepted by:

Dr Andrew Blyth - ADISA Research Centre

SIGNED:

NAME: Andrew Blyth

TITLE: Director of Research and Technology

DATE: ~~13.08.2020~~ 13.03.2020