



Claims Testing Application Form

Form Number ADPC00027

Section 1 – Applicant Information

Company Name: mce Systems Limited
Address: 8 Yohanan Ben Zakai, Tel-Aviv, Israel

General Contact

Name: REDACTED
Phone: REDACTED
Mobile: REDACTED
E-Mail: REDACTED

Sales Contact

Name: Moshe Reifman
Phone: +972 50 4029289
Mobile: REDACTED
E-Mail: moshe.reifman@mce-sys.com

Section 2 – Applicant Software Information

Manufacturer: mce Systems Limited
Version of software: MCE.9_32_Release.9.32.304

Background (Explanation of the company and software)

Based in the Tel-Aviv, Israel, mce Systems Limited specializes in Omni-Channel Mobile Care solutions, offering consultancy, technology platform and system integration for operators, wireless retailers and mobile logistics centers.

mce proprietary software platform enables automated Device Recognition, Device Software and Hardware Diagnostics, automated Repair, Content Transfer, Device Flashing, Backup & Restore, Device Activation and a wide range of value added services (e.g. Buy-Back and Trade-In automation, Insurance support, Applications side loading and more).

Key benefits are measurable increase in NPS and customer satisfaction, significantly enhanced customer retention, NFF reduction and immediate costs savings through the avoidance of unnecessary device repairs and returns.

Technical / physical architecture of claims test applicant software.

mce solution includes software, certified powered USB hub ("connection box") and USB cables.

An available USB port on the PC is required for the connection box to connect to. The system is designed to work exclusively with the included connection box which has been certified to work with mce.

The system is designed with compliance to current market security standards. Encryption, validation procedures, secured connections, redundancy, reports etc. apply. mce Systems Limited also offer system hardening by providing clients with mce secured environment - mce Shell.

A download link is provided for the installation package which contains all the information required for installation.

Internet connection is required during installation and operation. The system is designed to work a Windows 7 operating system and latest Windows version. Latest updates installed from Windows Update is required as well.

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

User guide is available and can be delivered by email in PDF format. Technical support is available through phone, online desktop sharing or any other kind of online communication that can provide technical services.

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

1 USB connection box, 1 power adapter, 1 Mini USB cable.

Section 3 – Test Hardware Information

- Apple IPAD Air WiFi 16GB running IOS 9.3.5
- Apple iPhone 5S 16GB running IOS 9.3.5
- Samsung Galaxy S5 16GB running 6.0
- Samsung Galaxy Tab 9.6 Quad Core 1.3 GHz 1.5GB RAM 8GB Android running 6.0

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

mce System, MCE.9_32_Release.9.32.304, when used in accordance with User Manual version 1.0 for Wipe process will sanitize user-generated data from smartphones and tablets within this test to protect from a forensic attack equivalent to risk level 2 (test level 1) of the ADISA threat matrix.

Claim Technical Contact at applicant.

Name: REDACTED
Phone: REDACTED
Mobile: REDACTED
E-Mail: REDACTED

Acceptance

I, Liran Weiss of mce Systems Limited 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 mce

SIGNED:



NAME: Liran Weiss
TITLE: EVP Products
DATE: 18.08.2016

Claim Accepted by:

Signed on behalf of University of South Wales



SIGNED:
NAME: Andrew Blyth
TITLE: Professor
DATE: 07.09.2016

Signed on behalf of ADISA



SIGNED:
NAME: Steve Mellings
TITLE: Director
DATE: 07.09.2016