Wipe Whitepaper

Aug. 2019

About mce

mce specializes in digital transformation of mobile operators, wireless retailers and logistics operators in the mobile device world.
By utilizing proprietary technologies, mce empowers our customers to transform operations to the digital world by providing an efficient, seamless and cutting-edge experience for our customers and their consumers.
mce specializes in digitizing business services and programs in the mobile world; creating new touchpoints for once brick & mortar business services only, automating device lifecycle and optimizing device management and routing throughout diverse locations.
mce solutions provide a clear ROI by reducing mobile device handling time in retail and logistics locations, diverting consumer claims to new businesses and provide innovation to the mobile retail world while increasing consumer satisfaction, efficiency and information flow.

mce Wipe

Industry data erasure is focused on a brute-force forensic wipe as standard modus operandi. mce with its extensive mobile experience opts to use a more agile and fast method which provides even better results in a significantly shorter processing time.

ADISA

PRODUCT CLAIMS TESTING CERTIFICATE

CLAIM NUMBER: ADPC0067 MADE BY: MICHAEL BEN-OLIEL OF: MCE SYS LTD

was tested using the
ADISA Product Claims Test Method v1.0.

ADISA CERTIFIES THAT

WIPE ENGINE 12.4.73

was executed on:
Apple Ipad, iPhone 8, Samsung Galaxy S9,
HTC Sensation Z710e and Sony Xperia C1505

and achieved the following results as outlined in the testing method.

TESTING	DATE	VALID UNTIL	RESULT
Test Level 1	17.07.2019	07.09.2020	PASS

This test validates that this product when used in accordance with the specification within claims test document: ADPC0067 can be used to sanitise data against ADISA Test Level 1 on the sample of devices identified in the claim.

Signed
Dr Andrew Blyth

Signed
Steve Mellings – Director
on behalf of ADISA

For further information please contact ADISA today on 0044 845 557 7726
or email us info@adisa.global

mce Wipe is an advanced solution utilizing smart algorithmic (Device and OS oriented) approach and cutting-edge technology that enables a mission-guided, targeted wipe, answering perfectly a wide range of specific user requirements and can be performed in multiple locations along the service chain (POS, Warehouse etc.).
Due to this innovative approach, mce Wipe provides a much better solution in a fraction of the time and with significantly higher degree of customer satisfaction.

mce Wipe provides the top standard in Mobile Data Erasure (MDE) solutions:

- Unparalleled WIPE Efficiency and Speed (>10x)
- Process Aware Architecture (POS2Warehouse)
- Device Auto Detection (Process Automation and Ease)
- Human Error Avoidance (Costs Reduction)
- Standalone and API level systems (Web and/or PC)
- Parallel Processing (multiple device wipe simultaneously)
- Extensive Audit, Reporting and Tracking capabilities

Unparalleled WIPE Efficiency and Speed

mce's advanced erasure protocols (3LEP - described on the previous page) enable up to 10 times faster Wipe process than competitors.
mce utilizes targeted Wipe algorithms for deep specific Wipe of all private data vs. "Zero-Fill" general "bombardment" which is by far less efficient and often misses potential leaks of critical hidden data.
Differentiating between device manufacturers and models dynamically – enables mce to produce the most efficient wipe method per model, reducing wipe time to a minimum by not using one robust method for all devices.
While the Wipe itself is as fast as possible, other efficient actions can be taken to improve the overall journey of customers, by including additional actions before and after the wipe process. Actions such as software update or data backup can be accommodated into a process with specific business need, such as Send to Repair, allowing consumers to avoid a repair (by updating the software) or maintain their data (by backing up content).

Process Aware Architecture

Following the customer service process from Point of Sale (POS) to Warehouse and provides customized procedures for each stage of the process. Allowing logistics centers to have complete visibility of actions performed in stores and service centers – thus automatically selecting the best course of action

Device Auto Detection

Total smartphone support via mce Auto-Detection technology ensures coverage and prevention of POS personnel errors in identification and booking/reporting.

- Android
- iOS
- BlackBerry (not supported for Wipe)
- Windows (not supported for Wipe)

Human Error Avoidance

Our technology is aware of the hidden connections to cloud-services (e.g. iCloud, find my iPhone/Samsung etc.) that are bound to the Vendor Hardware Identifier (i.e. IMEI, PIN…) which pose a major data exposure even after Forensic-wipe. mceWipe™ works in collaboration with vendor connectivity protocols to detect in real-time such connectivity and protect the privacy of users' data in those cases.
Avoidance of human error via:

- Device Auto Detection
- Automated data input
- Centralized/Network-based monitoring and auditing

Early detection of arbitrary security/privacy risk:

- Memory card forgotten inside (SDK)
- Smart cards (SIM and others)
- Find my iPhone
- Find my Samsung
- Passcodes
- Android Factory Reset Protection

Standalone and API level systems

mce provides wipe technology in both Application and API formats.
Enabling seamless integration with existing IT systems (ERP, CRM…) and full web integration
In addition, mce Wipe can be provided as a standalone solution or as an integral part of mce Systems services for extended customer solutions at POS and Warehouse (e.g. hardware diagnostics, trade-in facilitation and automation, applications pre-load, content transfer and more).

Parallel Processing

mce Wipe process is highly efficient and allows a POS agent or Warehouse personnel to perform parallel Wipe procedures on hundreds of devices per day.
mce Wipe concurrently executes over 40 Wipes in one station.

Extensive Audit, Reporting and Tracking capabilities

mce Wipe provides vendors with state-of-the-art audit & reporting support, allowing critical documentation of hardware diagnostics serial numbers, vendor identification codes, complete software details and licensing info.
mce issues full Wipe process report, including Wipe performing personnel ID, device identifiers, station identifiers, dates and time etc.)

Wipe Execution Methods

Multiple Data wipe methods exist and provide different levels of security and speed. Wipe methods can be segmented into the following categories:

Method	Description	Security	Speed	Purpose
Logical	Clearing indexes and other metadata, but not the actual data.	Low. Actual data may be extracted by tools and apps.	High (seconds)	Mostly to free up storage space.
Digital	Overwriting digital media, replacing previous data with arbitrary new data.	High – if indeed all data was overwritten. Wear-levelling technologies and, logical address controllers and redundant storage may lead to un-erased data	Low (hours)	Erasing non cryptographically protected media
Cryptographic	Replacing encryption keys, rendering all data encrypted with old keys undecipherable	High – if all data was previously encrypted	High (seconds)	Recommended wipe method for all but top secret purposes
Physical destruction	Physically destroying the media, beyond ability to extract information	Absolute	Low	When absolute secrecy is required, and media is expandable.

- data, without removal of old undecipherable data.

Each method takes a different amount of time depending on the device manufacturer and the size of user partition on the device.
Due to these variables, each method is utilized by different industries for different purposes.

Wipe Standards

Modern mobile phones have outpaced standards for magnetic media erasure standards. Trusted erasure protocols for magnetic media are irrelevant for sophisticated flash drives and memories, as utilized by modern mobile devices. Notable irrelevant examples include:

- DoD 5220.22-M
- NIST 800-88 Rev. 1 (note: also addresses proper modern media sanitization)
- HMG InfoSec Standard 5
- BSI-GS
- mce's methods adhere to NIST 800-88 Purge levels for almost all modern mobile devices which are encrypted.

Wipe Method selection by mce

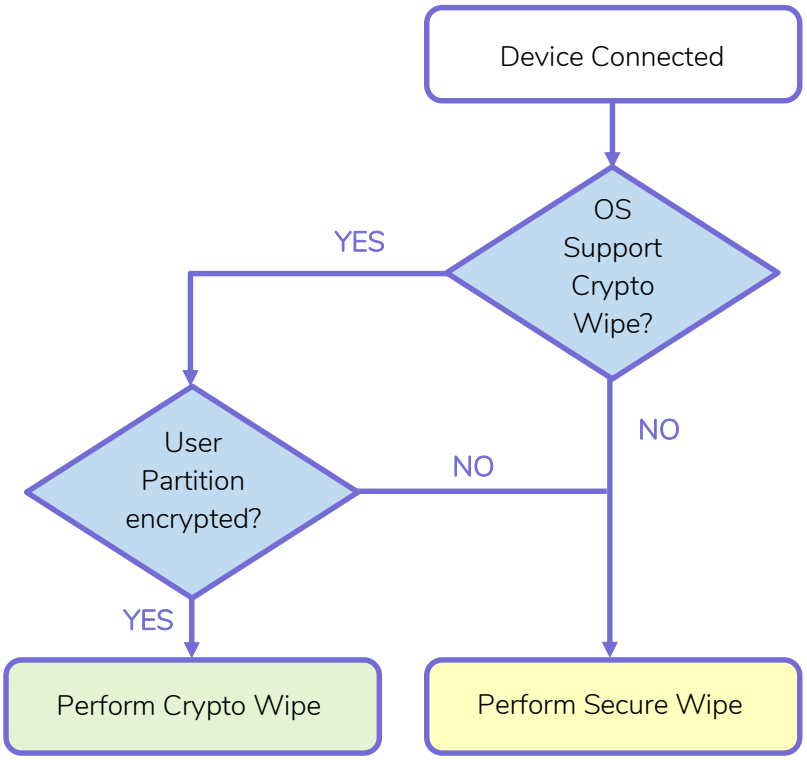
As reviewed above, multiple methods are available and can be utilized for mobile device data wipe.
Our research conclusions, taking into account the requirements of the mobile device industry, security and speed, led to the conclusion of a best fit methodology.
Based on the ability to identify the specific device in real time, its data state and its journey, mce client is able to provide the best solution per device.
Therefore, devices that inherently encrypt user partition enable mce to overwrite the encryption key within seconds, thus de-facto wiping the device from user generated data with a highest security level and within seconds. Older devices, that do not encrypt user data by default, or devices that are not encrypted (for whatever reason) are subjected to a 'Secure Wipe' – logical wipe using vendor tools and protocols - as it meets industry standards and does not consume too much time.

Wipe Architecture and logic

As described above, mce provides a mixture of methods, a best of breads, that is tailor suited to each connected device.
For devices with operating systems:
iPhones 5 and above
Android 6.0.0 (Marshmallow) and above
User partition data is encrypted by default (in most cases), therefore mce client verifies the device data partition is encrypted and overwrites the encryption key

For other devices (lower OSs or non-encrypted user partitions)
mce performs 'Secure Wipe' – It overwrite system partition and user partition with OEM embedded tools that provide their secured wipe mechanism (Manufacturer oriented wipe).
This method provides the fastest and most efficient wipe method tailor suited to the specific device.

On average, the connected device is already encrypted as its operating system mandates it, so wipe takes only a few seconds.



Summary

mce solution comprises many supporting features in the device lifecycle industry. As one of the major ones, Wipe receives our full attention for new methods arising and new devices allowing us to perform the same actions but better.

As operating systems evolve and privacy is becoming imperative for industries and consumers, support features such as Wipe and Flash become more common and more critical. As the attention rises, the importance of performing such actions effectively and without exhausting the consumer is becoming a major concern.

mce continuously investigate and explore new opportunities and technologies to can provide better value and performance for our customers. Any opportunity is measured and reviewed, and if found valuable – immediately incorporated into our products.