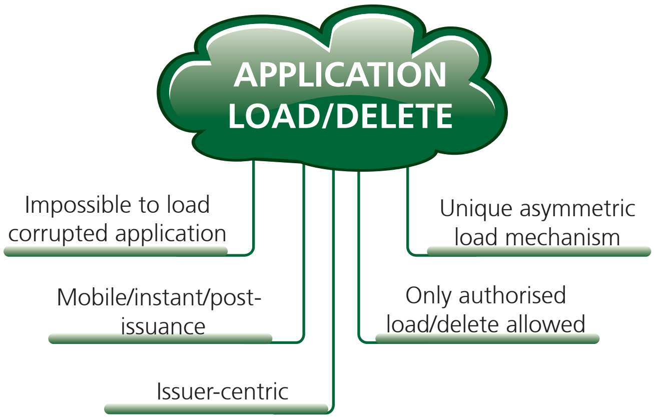
MULTOS IS SECURE

The MULTOS Scheme ensures formidable, best-in-class security across the entire card lifecycle

APPLICATION PROVISIONING... is SECURE

The unique MULTOS application management mechanism secures all aspects of application provisioning.

The MULTOS application load and delete controls are uniquely based on asymmetric cryptography, which allows for the use of digital certificates to secure the load and delete process, and only under Issuer authority. This load certificate contains the all the requisite data needed to verify the unique signature and validated by the device itself, before application load can commence. A similar certificate is also required to allow an application to be deleted.


APPLICATION LOAD/DELETE

Impossible to load corrupted application

Unique asymmetric load mechanism

Mobile/instant/post-issuance

Only authorised load/delete allowed

Issuer-centric

What does this really mean?

The MULTOS loading mechanism guarantees that only genuine applications specified by the issuer can be loaded to a device. Any unauthorised or accidental modifications to either applications or data will cause the device to reject the request.

The issuer maintains full control of all real estate on the device for the entire lifecycle. Corrupt or unauthorised applications will not load to a MULTOS device. Also, this mechanism ensures application management for mobile, instant, or post-issuance retains the same security as that found inside a personalisation bureau. For example, MULTOS application management is based on the same kind of security technology you use to secure corporate emails.

APPLICATIONS CAN CO-EXIST

MULTOS can securely host any combination of applications without the need to do any off-card pre-checks.

Unlike other technologies, MULTOS implements full run-time application memory segregation. MULTOS applications are given a virtual address space in which to run and the operating system checks every memory related operation to ensure that any attempt to access memory outside of the address space is blocked.

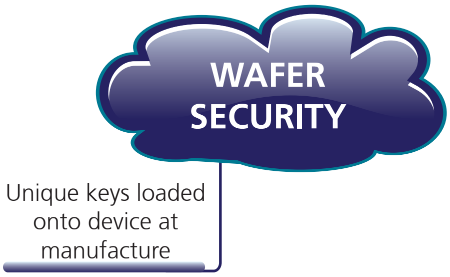
What does this really mean?

MULTOS is truly “multi party secure” and can be used in an environment, such as mobile, where the mix of applications is not known at the time of issuance. Other technologies require the on-card application suite to be approved each time a change is made, making MULTOS the more flexible choice.

WAFERS ARE MORE SECURE

Unique transport keys are given to devices whilst still on the wafer.

IC manufacturers use technology provided by the KMA to inject unique transport keys (and other manufacturer data) into the devices during wafer production.



WAFER SECURITY

Unique keys loaded onto device at manufacture

What does this really mean?

Once a wafer has been made into modules, it is usually necessary to change the manufacturing key for an issuer specific key. This is often performed at pre-perso and implies that the module and card manufacture have to be provided by the same company. Because MULTOS modules already have unique transport keys, the modules can be shipped to any card manufacturer without compromising their security.

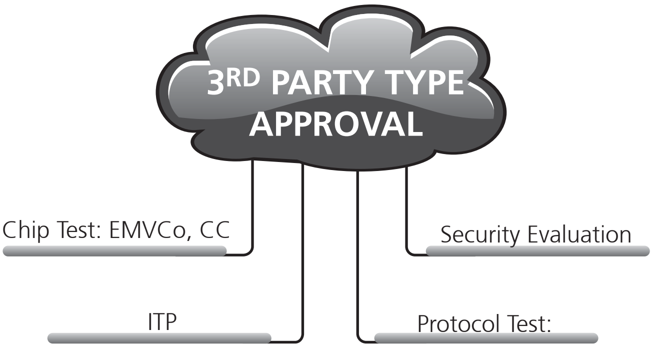
This unique transport key on each MULTOS device also ensures that enablement data can only be loaded onto the target card.

SECURITY IS ASSURED

All MULTOS products must be Type Approved to ensure security and interoperability.

The MULTOS Type Approval process consists of four "pillars";

- The chip must be EMVCo or Common Criteria approved
- The development process must have been security evaluated to either Common Criteria (at least EAL4+) or an approved EMV scheme standard (e.g. C.A.S.T)
- Relevant market protocol testing (e.g. payment, ID, transport) must have been performed
- Each product must have passed interoperability testing defined by MAOSCO.



3RD PARTY TYPE APPROVAL

Chip Test: EMVCo, CC

ITP

Protocol Test:

Security Evaluation

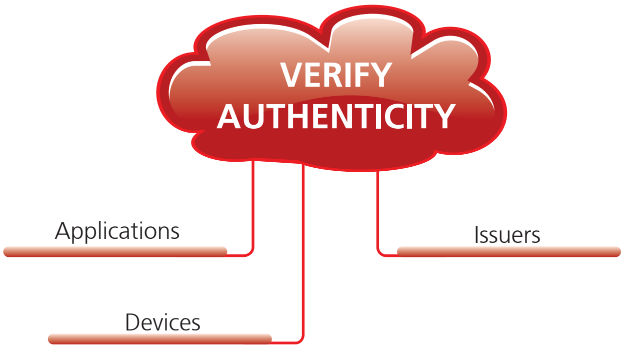
What does this really mean?

If a product has achieved Type Approval, it can be assured that it will deliver the high levels of security and interoperability demanded by the MULTOS Specifications.. A MULTOS product can only be registered on the Scheme at the MULTOS KMA once it has been Type Approved.

AUTHENTICITY IS GUARANTEED

Using certificates makes it possible to check that MULTOS devices and applications are genuine, and from a known issuer.

Each MULTOS device public key is certified using a KMA secret key, and each personalised application is signed by an application provider key, which is in turn certified using a KMA key.



VERIFY AUTHENTICITY

Applications

Devices

Issuers

What does this really mean?

At any stage, whether that be in a personalisation bureau, an instant issuance machine, post-issuance update or provisioning a mobile phone – by using the KMA public keys to verify these certificates, proving applications are genuine is simple, quick and irrefutable.