THE PLATFORM FOR INNOVATION

» Payment
  EMV · Transit · Mobile

» Identity
  Government ID · e-Passport · Campus ID

» IoT
  Smart Metering · Smart Grids · Smart Things

www.multos.com
MULTOS is the highly secure, industry-backed multi-application smart card platform delivering simplicity and innovation to leading card and smart device issuers across the globe.

To date, with over 800 million issued smart devices across 45 countries, hundreds of issuers including national governments, banks, corporate enterprises and transit authorities take advantage of the high security, multi-application capability and speed of deployment to make MULTOS the platform of choice for their smart programmes.

A wide range of applications including, Chip & PIN payment, contactless payment, authentication, digital identity, biometrics, loyalty and mass-transit ticketing maybe implemented using a MULTOS powered chip.

MULTOS allows issuers to relax, knowing they have chosen the most secure, flexible platform that can support their application needs now and into the future.
MULTOS CONSORTIUM

Established in 1998, the openly governed, cross-industry consortium of global organisations continues the objective of promoting MULTOS as a standard for smart cards and devices across a wide range of market verticals and segments. The consortium governs the development of the technology in line with customer needs, sets policies for the open licensing of the MULTOS specifications, and ensures the interoperability and interchangeability of platforms from many vendors through the Type Approval and Security Evaluation policies of the MULTOS platform.

The ongoing process of development and evolution of the MULTOS specifications by the consortium ensures issuers receive a product that is state-of-the-art, fulfilling their market needs with the most secure platform available.

Fig. 1) The role of the MULTOS Consortium
MULTOS is the only multi-application high security platform conceived and designed from first principles specifically to meet the exacting demands of the payments industry, whilst allowing secure co-residency of multiple applications on the same device. This makes MULTOS the ideal platform for an EMV payment implementation. All the internationally accepted payment brands can be issued using the MULTOS platform, as well as a large number of domestic schemes. MULTOS also supports the latest contactless payment technology.

MULTOS is used by several governments to secure their national smart identity card schemes and electronic passports. A wide range of biometric technologies including fingerprint, finger vein or palm vein are available on the platform. As well as providing the highest levels of security assurance that is a core requirement of such programmes, MULTOS gives governments control over the cryptographic key scheme that protects these important elements of national infrastructure. An independent Key Management Authority (iKMA) operated by a national government eliminates any reliance upon the smart card supply chain to maintain the security of keys protecting a national identity scheme.

The MULTOS Scheme utilises a unique provisioning, or application loading mechanism, which secures data as a discreet packet of information. This negates the need for establishing a secure communication channel when sending this data over an insecure network. This, coupled with the ease at which MULTOS can be ported onto any form factor, provides a powerful tool for issuers who are looking to expand their card offering to the mobile world.

Many card issuers wish to combine payments or identity with the convenience of contactless mass transit in a single card. The fast execution speed of the MULTOS Virtual Machine allows open standards based transit applications to be developed and deployed using contactless or dual-interface MULTOS implementations. In addition to this, many contactless MULTOS secure micro-controllers also include the MIFARE Classic application that is widely used in city-wide transportation systems.
The Internet of Things (IoT) and smart metering markets have seen exponential growth with predicted volumes of devices in the tens of billions by 2020. Security of the data passing between these devices is a primary concern, as is the management of digital keys for them. MULTOS, because of its unique provisioning model based on asymmetric cryptography, is perfectly positioned to offer simple post-issuance firmware updates and application loading to devices already deployed, as well as vastly reducing the key management requirements on the system as a whole.

Utilising the same model MULTOS brings to the cards and mobile payments environment, the MULTOS provisioning mechanism enables data packages to be securely transferred across any existing infrastructure and protocol. Of the millions of potential connected devices, only the target device alone, is able to decrypt and load the data package.

This USP is attracting great interest from utility companies, meter manufacturers and systems integrators, as the necessity for greater security and key management increases.
Security threats to smart devices are complex and constantly evolve in line with available technology. One of the original design criteria of MULTOS was to elevate the security of smart devices beyond known threats and continue to provide state-of-the-art protection to the platform and the applications contained therein. As a result, MULTOS has consistently achieved the highest security assurance certification available in the commercial sector, as high as CC EAL7.

**Interoperability guarantee**
The MULTOS operating system is available from multiple vendors. To ensure interoperability, all MULTOS devices are evaluated against identical criteria and achieve the same security assurance level through rigid, mandatory Type Approval process.

**Platform key management authority**
At the heart of the scheme, the MULTOS Key Management Authority provides the ‘Root of Trust’ in the system providing all cryptographic materials used to secure the devices and content throughout their life cycle. The Global KMA performs platform key management on behalf of most commercial issuers worldwide.

**Independent MULTOS schemes (iKMA)**
iKMAs are usually operated by Governments allowing them to own and manage their own MULTOS key schemes giving further safeguards for reasons of national security.

**Securing manufacture**
The MULTOS scheme requires that each and every device is linked to a particular KMA, and has unique identity and cryptographic keys injected at silicon manufacture. The device ID and keys are generated by a KMA, creating the unique link between each device and that particular KMA at the very earliest opportunity. Only this linked KMA can activate the device.

**Open, yet secure device distribution**
The security system limits risk in distribution as no party other than the linked KMA can activate the device, and no keys ever need be distributed. Supply can therefore be open, competitive and highly commoditised, with no risk to the overall security of the system.

**Device authentication**
An issuer is able to validate that an individual device is indeed a genuine MULTOS device and linked to their KMA, regardless of the source of supply.
Asymmetric (Public Key) cryptography
The MULTOS scheme uses asymmetric cryptographic algorithm mechanisms. During activation the KMA creates data that binds a device to a particular issuer, placing it under the control of that issuer for the rest of its life. The KMA also creates a unique asymmetric key pair (a certified public key and a corresponding private key) for each device that is used to secure application content to be loaded to that device.

Controlled content management
Once a device is placed under the control of the issuer, digital certificates are required to authorise the loading and deletion of application content. The issuer requests these permissions from the KMA; certificates will only be accepted by the correct issuer and signed by the correct KMA.

Content provider privacy
Third-party content providers require permission of the issuer to load applications. The provider does not need to share any confidential data with the issuer in order for it to be loaded, and can ensure the content is not tampered with during loading by creating a digital signature which can then be verified by the device.

Multiple content providers
The MULTOS provisioning mechanism permits an issuer to deploy devices containing numerous applications from multiple sources without having to consider risks associated with sharing cryptographic key material.

Post-issuance content management
These same mechanisms used at device issuance permit changes and updates to already-issued devices without any impact or risk exposure to existing on-card applications.
PROTECTING ON-DEVICE APPLICATIONS

MULTOS utilises a secure application execution environment or ‘Virtual Machine’. This is primarily designed to ensure that applications remain separate whilst resident within the device and during execution of any application.

**On-card Firewall**
The virtual machine implements a ‘firewall’ mechanism to ensure that one co-resident application cannot access the code or data of another. When an application attempts to access memory within the device, the virtual machine verifies the memory to be accessed is within the application memory space.

**Built-in secure API functions**
The platform contains numerous API functions known as primitives that permit applications to access the built-in capabilities of the operating system. Primitives provide memory management functions, cryptographic functions, communication protocol access and other functions. The virtual machine also verifies each use of the API, ensuring that all parameters passed are in permitted ranges and that an application may not attempt to misuse the API.

**On-card application communication and co-operation**
An executing application may request execution of another application via delegation. The processing of the delegator is suspended whilst the delegate application is executed in its own separate memory space. Data to be communicated between the applications is placed in untrusted public memory. This mechanism permits the design of card features such as ‘shared PIN’ without compromising application isolation.
A TRULY OPEN PLATFORM

Issuers demand an open, competitive supply chain that offers value with high levels of service. With a truly global spread of vendors, suppliers and system integrators, MULTOS can comprehensively support this requirement, as well as supply openly licensed specifications for application developers and personalisation system developers free-of-charge(1).

Open specifications, open governance
MULTOS has a strong philosophy of ensuring openly available specifications and standards. MULTOS is compatible with both the ISO 7816 and ISO14443 standards pertaining to contact and contactless smart cards, as well as compatibility with application level standards, such as EMV for smart payment cards, FIPS201 for US government and the ICAO LDS specification for electronic passports.

When new specifications emerge, the MULTOS Consortium ensures the platform evolves to support them, protecting future investment of both members and issuers. Most importantly, no single company controls the MULTOS platform; all consortium members democratically decide the policies and changes to specifications through a rigorous open governance process.
ENTRY LEVEL - MULTOS step/one

The MULTOS step/one platform offers the most cost-effective way to initiate an EMV migration programme on a multi-application platform. It is designed exclusively for issuers implementing Static Data Authentication (SDA) EMV applications. MULTOS step/one features the same on-card secure virtual machine and API and is fully interoperable with applications designed for MULTOS. However, the security scheme has been redesigned to permit issuer-centric content management with symmetric key cryptography. This eliminates the need for an RSA co-processor and reduces the memory needed within a MULTOS step/one device.

A card manufacturer or personalisation bureau deploying MULTOS step/one may use in-house key management systems in place of those of a KMA. However, the activation and content management API of MULTOS step/one cards is compatible with MULTOS-capable software and systems.

MULTOS step/one offers an economic, simple point-of-entry for EMV with a defined migration path to MULTOS and full DDA/CDA capabilities.

CONTACTLESS & DUAL-INTERFACE

MULTOS enables existing contact-only payment card deployments to be quickly and easily enhanced to contactless with no major changes to card issuing or data preparation systems.

The efficient MULTOS virtual machine allows fast code execution ideal for mass-transit ticketing applications using open standard ISO 14443 Type A or B contactless interface. Many city-wide mass-transit schemes use proprietary application protocols, so some MULTOS and MULTOS step/one platforms also support the MIFARE Classic application alongside regular MULTOS applications.
MULTOS smart cards are manufactured and personalised by all the major globally-operating card vendors and most of the smaller more regional card vendors. This gives issuers the ability to choose the provider that meets their specific requirements. Issuers often require local, responsive suppliers who understand their unique needs. Our MULTOS consortium partners, with their extensive global presence, can satisfy these requirements or assist new suppliers in delivering MULTOS-based cards for the first time.

Smart card personalisation and complete lifecycle management systems are equally important for issuers. MULTOS works with all major systems vendors to ensure they support the MULTOS KMA and smart card OS platforms. As the specifications are freely available, anyone can build software and solutions to support card and application deployment.

MULTOS platforms are available from:

- DNP/Hitachi,
- Multos International,
- Samsung SDS
- UbiVelox

on silicon manufactured by:

- Infineon
- Renesas
- Samsung Electronics
- STMicroelectronics

MULTOS step/one platforms are available from:

- Multos International
- Samsung SDS and
- UbiVelox

on silicon manufactured by:

- Infineon
- Samsung Electronics
- STMicroelectronics

All MULTOS products contain an RSA cryptographic co-processor for PKI and EMV DDA/CDA support. Memory sizes extend up to 144k.

Memory sizes range from 4k to 32k.

MULTOS and MULTOS step/one products may also support contactless and dual interfaces in accordance with ISO14443 A or B and MIFARE. For a complete list of available products visit: www.multos.com/products.
When you need a secure, flexible platform for your smart device implementation, MULTOS offers the total solution. Our open, global network of industry leading suppliers, manufacturers and developers ensures MULTOS provides the ideal platform for you.

(1) Fees apply for MULTOS Implementation licence and MULTOS stepone Off Card licence. (2) Check for availability. ©2015 MAOSCO Limited. MULTOS is a trademark of MAOSCO Ltd. MIFARE is a trademark of NXP. All other trademarks acknowledged. Published by MAOSCO Limited. 1F GPS House, 215 Great Portland Street, London, W1W 5PN, United Kingdom.