

MULTOS - The High Security Smart Card OS



MULTOS – the High Security Smart Card OS

**Tim France-Massey, Business Development Director,
MAOSCO**

14th September 2005

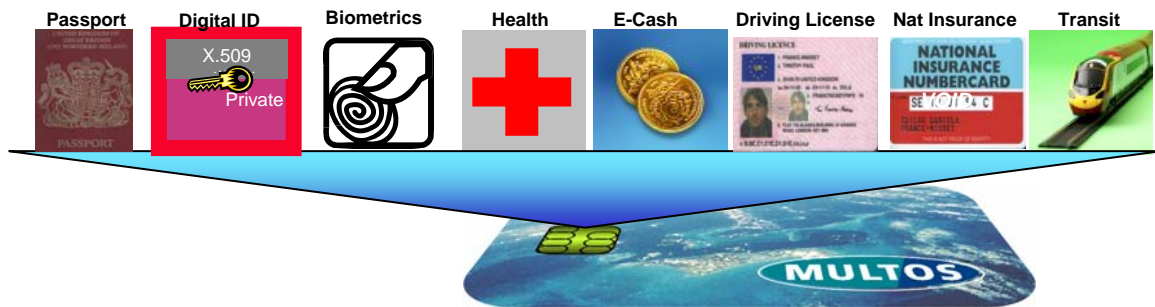
Contacts

Tim France-Massey	tim.france-massey@multos.com	Phone :+44 (0)20 7557 5462 Fax : +44 (0)20 7557 5472
-------------------	--	---

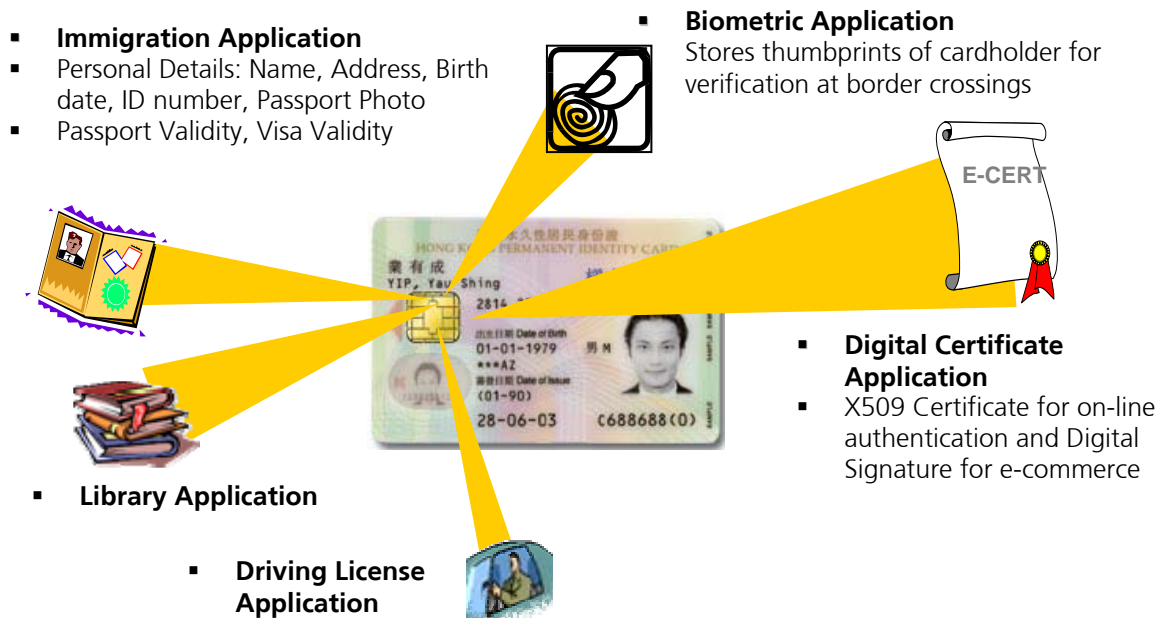
MULTOS - The High Security Smart Card OS

If you are involved in the smart card industry, then by now, you will have heard of MULTOS – the high security smart card Operating System. As standards in the IT industry go, it has already achieved something of a heritage, having been born in the last century – 1997 to be precise. MULTOS was founded by a consortium of companies that had a vision of a standard secure smart card operating system, that could be implemented on any silicon chip, and execute any smart card application, be it payment, identity or ticketing in a standard and secure way.

The vision also foresaw that different application providers – such as Government and Commercial bodies – would want to share the same smart card, for the convenience of the individuals that carried them, perhaps combining identity, biometrics, healthcare, payment, travel and other functions all on one card:



As time has gone by, this vision has been realised by some of the pioneering governments around the world. The most significant smart card project in the world today (as voted by Industry Experts in Washington DC last year) being that of the Hong Kong Citizen's ID card, launched in August 2003, which combines an Immigration application, with a variety of optional applications for citizens from other government or commercial bodies such as Driving License, and Post Office Digital Signature applications:



MULTOS - The High Security Smart Card OS

As more and more trust is placed in the ability of smart cards to prove who we are, whether for making payments in a shop, clearing immigration or signing a contract over the internet, then the more attractive it is for fraudsters, organised crime gangs, people traffickers and terrorists to replicate a genuine identity to gain access to funds, benefits, locations or identities that they are not entitled to.

That means that if we are to vest our trust in the ability of smart cards to prove who we are, either face to face, or over remote channels such as the internet, then it is essential that the personal information and unique data, such as biometrics or unique encryption and signing keys that prove who we are, remain protected.

MULTOS has achieved a reputation for being the most secure smart card operating system in the world. But what does that actually mean? Aren't all smart cards "secure" these days? Don't they all protect our identity?

The answer is that security is a relative thing. EMV cards are more secure than magnetic stripe cards, because it takes more know-how and it costs more to copy a chip card than a swipe card.

But when a security measure like chip cards becomes ubiquitous, then the weakest link becomes the chip or the software in the chip and its ability to protect your personal data from a hacker. Techniques exist for penetrating the physical silicon chip hardware of some chips – with electron microscopes and lasers – and with enough knowledge to deduce the values of encryption keys that protect the data stored in the chip. The latest chips from the silicon manufacturers will incorporate defences against the latest known forms of attack developed by evaluation laboratories. Hopefully the laboratories, and the silicon manufacturers always stay ahead of the hackers. In this respect, yes, the latest microprocessor smart card chips represent the most secure form of storage for digital information or executable code.

Similarly, the software of the smart card, which contains the operating system and the actual applications that run on the chip – such as your Passport, Payment or Healthcare applications – also needs to contain measures to protect the personal data and unique keys that identify you. After all, a smart card is like a mini computer. It has the memory and processing capacity of a home computer of just less than two decades ago. So called "open standard" multi-application smart card platforms like MULTOS and JavaCard allow applications to be installed and executed on the smart card, even after the chip card has been "issued" to the recipient. So like PCs, there needs to be a mechanism in place to protect applications on the card that contain sensitive data from trojans or denial of service attacks. It should be the job of the smart card operating system to make sure that all the applications are protected from unauthorised external and internal attempts to read or change sensitive data.

This is where MULTOS earns its reputation for being the most secure smart card platform in the world. When a smart card OS developer writes a MULTOS operating system on a silicon chip of their choice, they have to ensure that the chip and the operating system comply with the strictest of security assurance targets. Specifically, the MULTOS security target demands that:

1. Applications can only to be loaded onto a card or removed from the card with the permission of the Card Issuer – this means that the card issuer can ensure that applications can only be loaded by trusted third parties. This objective is met by means of cryptographic load certificates that the card issuer uses to authorize the loading of an application.
2. Applications are to be segregated from other applications - an application may not read from or write to another application's code or data. This means that once the card is issued with for instance an Identity application, the Government or Corporation that issued the card does not need to worry that a subsequently installed application masquerading as one from a trusted third party could gain access to the memory areas of the identity application. MULTOS ensures that

MULTOS - The High Security Smart Card OS

one application cannot access the memory of another application through the use of “on-card” firewalls which police the execution of each application during runtime. If one application illegally tries to access the memory space of another application, then the MULTOS OS will immediately detect this violation and end the execution of the offending application. This differs from JavaCard, whereby the “fire walling” is achieved when the byte codes of each applet are “verified” off-card to check that there is no unauthorized object sharing between applets. This has the consequence that if one wishes to load a new applet post issuance, then the new combination of applets needs to be “verified” by someone. This means the new combination undergoing a new security evaluation (an expensive and time consuming process). The MULTOS on-card firewalls on the other hand mean that you CAN add a new application to MULTOS, without needing to re-evaluate the whole combination.

3. Loading or Removing an application must have no effect on the code and data of existing applications – when a new application is loaded, it is allocated a fixed area of memory in which it can store its static and dynamic data and executable code. A MULTOS application cannot grab more memory after it has been loaded. If, as with JavaCard, it could, then there would be a risk of a denial of service attack on the other applications on the card, whose own memory requirements could be restricted by the denial of service applet.
4. The application load process must be able to guarantee the authenticity, integrity and confidentiality of the application code and data. This means that an issuer can send new applications, such as a healthcare application, to the identity card, after it has been issued, and the new application and the data in it are completely private to the application provider (the health authority) and are encrypted in transport to the card. MULTOS uses an “asymmetric” key mechanism to allow third parties to encrypt their application with the target card’s public key and download it on the card without needing to send it over a secure network or via a secure session. The MULTOS card then decrypts the application code and data with its unique private key. This is a patented feature of the MULTOS OS, so it is the only smart card operating system that offers the ability to protect code and data in this way.



- Each application’s data is protected from other applications by on-card firewalls enforced by MULTOS.
- MULTOS Chip Hardware must be tamper resistant to prevent against latest hardware attacks
- MULTOS allows applications to be added during the smart card’s lifetime without affecting the security of existing applications.

- MULTOS is the only multi-application smart card operating system to meet all these requirements, and be awarded an ITSEC E6 High accreditation by the UK & Australian Govts – the highest IT security assurance level achievable.

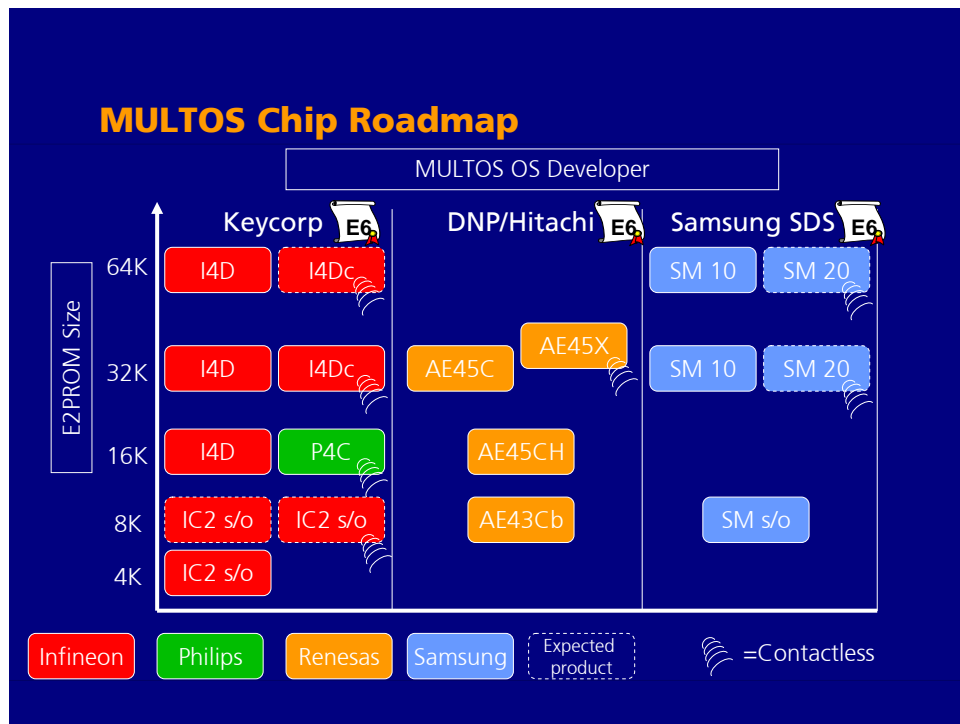
The above 4 security claims form part of a standard security assurance target against which, all implementations of the MULTOS operating system must be evaluated to the highest achievable level of security assurance. Today, the two internationally recognised security evaluation criteria are ITSEC

MULTOS - The High Security Smart Card OS

(to level E6 High) and Common Criteria (to EAL4). As stated by CESG, the UK Government Certification body: "Both ITSEC and Common Criteria (CC) provide an equally effective process for security evaluations. The UK ITSEC scheme has been firmly established since 1990 and CC has recently been established as an international criteria ITSEC Certificates are currently recognised by France, Finland, Germany, Greece, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland, and the United Kingdom. Common Criteria Certificates up to and including EAL4 are mutually recognised by the USA, Canada, France, Germany and the UK."
 (CESG, UK Govt – www.cesg.gov.uk)

Common Criteria							
ITSEC							

All MULTOS implementations (listed below) must be evaluated to either ITSEC E6 High or its Common Criteria equivalent before they can be sold as MULTOS Assured products:



It is because of this common security target, and mandatory evaluation of all MULTOS products to a common level of security assurance, that MULTOS products can claim to offer the highest level of security assurance in the smart card industry. So next time someone tells you their smart card is secure, just ask them if it is MULTOS Assured.

For more information, visit the MULTOS website – www.multos.com or contact Tim France-Massey at the MULTOS consortium HQ in London on tim.france-massey@multos.com