



MULTOS for ePassport

Maintaining a secure ePassport for a decade with MULTOS

Why is there a need for an updateable chip in an MRTD?

ePassports containing sensitive biometric data are being issued to citizens around the globe. But as standards evolve, and new threats emerge, how will Governments be able to protect their technology investment, whilst protecting the identities of citizens?

Evolving standards and Threats

Today, the ICAO standard defines how the contactless chip in the ePassport stores the citizen's passport data in a Logical Data Structure, along with one or more biometric images, how the chip performs mutual authentication with an ePassport reader and transmits the data via its contactless interface, and how the reader can verify the authenticity and integrity of the ePassport data and biometric image presented by the MRTD. But as standards and threats evolve, so the functionality of the ePassport chip will need to evolve. Many countries are discussing the addition of an eVisa capability, and perhaps airlines could make use of the chip for storage of electronic boarding passes. To counter new software attacks that emerge during the lifetime of the MRTD, encryption keys that protect the citizen's data or perform authentication may need to be lengthened, or new algorithms introduced. Any of these changes would require the chip in the ePassport to install executable software updates, but the vast majority of ePassports being issued today do not support the capability to make changes to the software in the chip.

Why don't most ePassports support software changes?

The risk of issuing an ePassport that can have its software updated, is that in theory, a hacker could install a virus application that could render the chip unusable (a denial of service attack), which could extract sensitive data from the ePassport application (such as encryption keys, or biometric data), or could install a fake identity into the chip. As a result most ePassport chips use a fixed, unchangeable operating system, that cannot support software updates or installation of enhanced application versions.

The weakness of a fixed operating system

The problem with an ePassport chip that cannot be updated, is that as soon as a vulnerability in the OS is identified, then all the issued ePassports are potentially vulnerable to the attack and may need to

be withdrawn and reissued. An updateable chip on the other hand, can be automatically installed with a security enhancement (like a "Windows Update" on your PC) when it is next used. But of course, the mechanism by which the update can be installed needs to be carefully controlled, and only initiated by the issuer of the ePassport.



The need for a securely updateable ePassport

The solution is to use the securely updateable smart card operating system called MULTOS. Which has been deployed for many years in the financial and national identity smart card industries. Over one hundred banks and several governments have issued over 60 million MULTOS smart cards and now ePassports since 2001.

Why MULTOS for ePassport?

MULTOS has the reputation for being the world's most highly assured smart card operating system. That is because the MULTOS standard defines a rigid operating system security architecture that protects the application code and data inside each application, and mandates a rigorous security evaluation by Government recognized evaluation facilities (such as GCHQ in the UK) to the highest achievable levels of security assurance – such as ITSEC E6 High or Common Criteria equivalent.

In addition, MULTOS implements a highly secure and efficient mechanism for installing updates – a mechanism known as Secure Trusted Environment Provisioning (STEP). STEP defines a mechanism by which the Government is in complete control of the all the keys used to manufacture the ePassport chips, right from the moment they are created in the silicon factory, and the keys that control the process by which new software can be installed to the device



MULTOS for ePassport

throughout its lifecycle. As a result, the Government is in a position to update the functionality of the Chip in the MRTD to meet business and technical requirements for today and tomorrow, without reissuing the document.

How does Secure Trusted Environment Provisioning work?

“STEP”, as described in the diagram below, essentially enables the issuing Government to maintain complete control over the issuance of ePassport chips, and over the software that can be installed into them. At the centre of “STEP” is a so called “StepNexus Server” (also known as a “MULTOS Key Management Authority”), that generates chip specific transport keys, asymmetric key pairs, and application load and delete permission certificates. The transport keys lock the MULTOS chips until the chip is “enabled” with encrypted data containing chip configuration parameters, and a public / private key pair used to encrypt and decrypt new applications. The permission certificates ensure that only applications that are “approved” by the ePassport issuer can be installed.

Who is issuing ePassports using STEP on MULTOS?

The most advanced deployment of smart card technology in the world – as voted by Card Technology, an independent industry publication – is in Hong Kong, where the Immigration Department of Hong Kong Special Administrative Region has deployed a single identity document infrastructure

for managing the issuance and usage of 7 million Smart Identity Cards supporting biometrics and Digital certificates since August 2003, and 4 million ePassports starting from the end of this year.



Although the Hong Kong ePassport will be issued as a single application chip, by using MULTOS, the Hong Kong Government has complete control over the lifecycle of the chip, has the flexibility to update the chip with new versions of software or new applications in the field, and has the ability to multi-source the silicon that is used inside the ePassport.

Where can you get ePassport on MULTOS solutions?

ANY passport manufacturer can source the contactless MULTOS chip inlays, so every Government can continue to buy from its existing passport manufacturer. Fully interoperable and high performance contactless MULTOS ePassport modules are available now in 36K, 64K and 72K E2PROM versions from Hitachi (Renesas), Keycorp (Infineon), and Samsung SDS (Samsung) respectively. For more info contact services@stepnexus.com

