



MULTOS for Identity

Securing Identity, Protecting Privacy, Enforcing Sovereignty



Carrying a Smart National ID card is like having an embassy in your pocket – it enables the citizen and the Government to interact remotely from anywhere in the world, and is trusted by third parties as a valid proof of identity. In most smart identity schemes, the secure tamper resistant environment of the chip contains software for authenticating the cardholder's identity in a variety of situations:

- Basic identity data – digitally signed by the issuing government, proves that the card is a genuine ID issued by a sovereign Government.
- A possible biometric match on card application, that proves that the citizen carrying the card is the one to whom it was issued. Can be used for automated passenger clearance at borders.
- A possible digital signature application with PIN or biometric authentication – enables virtual world interactions with the citizen and enables private sector eCommerce with Digital Signatures

Securing Identity, Protecting Privacy, Enforcing Sovereignty

Just as in the real world where the sovereignty of the embassy must be maintained within a secure environment, so the Government ID functions in the ID card must be protected against:

- hardware or software attacks aimed at exposing or altering sensitive code or data. This is essential for **protection of Citizens' privacy**
- issuance of fake ID cards
- corruption of Government applications on the card

WHILST ALLOWING:

- new Government functions or security enhancements to be installed on the card - remotely
- (Possibly) permit others to install applications on the card without impact on existing Government ID applications and whilst maintaining **privacy** of third party data

Why MULTOS for ID?

MULTOS is the most secure, flexible and future proofed smart card platform for securing identity, protecting citizen privacy and enforcing government sovereignty and is deployed in the world's largest and most advanced biometric identity contact and contactless interface smart card projects around the world. When security matters, MULTOS is the safest choice.

Assurance:

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 against a core set of security enforcing functions:

1. Applications are only to be loaded onto a card or removed from the card with the permission of the Card Issuer
2. The application load process must be able to guarantee the authenticity, integrity and confidentiality of the application code and data
3. Applications are to be segregated from other applications - an application may not read from or write to another application's code or data
4. Loading or Removing an application must have no effect on the code and data of existing applications

Certificates are awarded by Government recognized evaluation facilities (such as GCHQ in the UK, and the DSD in Australia) to the highest achievable levels of security assurance – such as ITSEC E6 High or Common Criteria equivalent.

Enforcing Sovereignty

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 maintains complete **sovereignty** over all the keys used to manufacture the ID 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 throughout its lifecycle. As a result, the Government is in a position to update the functionality of the Chip to meet business and technical requirements for today and tomorrow, without reissuing the card.



MULTOS for Identity

How does Secure Trusted Environment Provisioning work?

STEP™, as described in the diagram below, enables the issuing Government to maintain complete control over the issuance of ID card chips, and over the software that can be installed into them. At the centre of STEP™ is a 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 ID card issuer can be installed.

Who is issuing MULTOS ID cards?

Hong Kong Smart ID Card & ePassport



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.

Hong Kong Immigration operates its own highly secure StepNexus Server to enforce sovereignty over the content of the Smart ID card.

Turkish Armed Forces

The Turkish Armed Forces (TAF) is the second largest armed force in the NATO Alliance. In 2006 it has deployed a multi-application smart card based on dual interface MULTOS technology for to all

2.2m servicemen and their families. The new military ID card incorporates a number of applications:

- e-purse application is supplied by Oyak Bank, a leading Turkish financial institution that provides financial and pension management services to the Turkish Military. The application is based on the open EMV standard, using MasterCard's M/Chip payment function configured as "Pre-Authorized Debit". This allows the card to be used in standard EMV payment terminals, and transactions can be processed using standard EMV networks.
- Physical access control – for access to controlled areas on Turkish Military bases.
- PKI application for logical access control and digital signature
- Healthcare application – storing emergency healthcare details, of soldiers and family members.



Middle Eastern Govt ID card

A major middle eastern Govt is deploying the largest national ID card scheme with StepNexus Server and MULTOS to over 17 million citizens an residents

Norwegian Lottery

In a joint venture called "Buypass", the Nowegian State Lottery and Post Office have issued 2.1m PKI MULTOS cards to enable citizens to authenticate themselves online for eGaming and other eCommerce services.

Where can you get MULTOS ID solutions?

ANY Systems Integrator or card manufacturer can

source MULTOS chips, so every Government can continue to buy from its existing ID card manufacturer. Fully interoperable and high performance contact and contactless MULTOS chip modules are available now in 32K, 64K and 72K E2PROM versions from Hitachi (Renesas), Keycorp (Infineon), and

Samsung SDS (Samsung) respectively. For more info contact info@multos.com

