The future of National eID: increased security and citizen-centric services

As the number of programs for national electronic IDs (eIDs) continues to grow, there is an increasing need for IC solutions that ensure security, reduce fraud and support multi-application functionality. NXP, the preferred partner for eGovernment projects around the world, supplies best-in-class secure microcontroller solutions that enhance security and performance in every type of eID, from entry-level to very advanced eID schemes.

National governments around the world are making a dramatic shift, moving away from traditional, paper-based identity cards to eID cards. The shift is being driven by several factors, including the widespread desire for heightened security and increased government transparency.

The changeover is happening quickly. According to Acuity Market Intelligence, by 2015, the number of countries issuing national eIDs will exceed those issuing traditional IDs by a ratio of 4 to 1. Europe currently has the highest country adoption rate, but Asia, which includes the enormous populations of China and India, dominates in terms of market volume and revenue share. In total, Acuity predicts that the global market for national eID programs will reach $11 billion annually by as soon as 2013.

The need for multi-application

In addition to providing secure and convenient citizen identification, modern eID implementations let citizens use the cards for multiple applications.

At the entry level, eIDs may add functions like access to electronic voting or social-security systems. More sophisticated solutions offer added levels of security, to support such features as digital signatures or online authentication. A secure online authentication function can provide easy access to eGovernment and eCommerce services, replacing traditional face-to-face services.

The heightened security achieved by embedding a chip in the ID may have been the primary goal for early eID projects, but multi-application functionality has emerged as one of the most compelling aspects of embedding a chip in an ID. The ability to support multiple applications makes it possible to manage several citizenship-related issues with a single eDocument, and that provides significant value. As a result, multi-application is helping drive demand for eID solutions in general.

A number of countries around the world have already introduced multi-application eID cards. In Europe, for instance, the European Citizen Card (ECC) framework provides guidelines on recommended functionality in a super-regional context. The eIDs issued by members of the European Union do double duty within the EU region as Machine Readable Travel Documents (MRTDs).

Developing countries are targeting multi-application setups as well. There are several eID schemes designed to support multiple functions, from eVoting and social-security system access to driver's licenses and access to electronic healthcare services.

Some governments are adding payment applications to the eID card, and that opens up even more possibilities. Supporting multiple applications also helps governments reduce the overall costs of the required infrastructure, since one system can be used for several functions and there is a level of technical consistency that can lower the long-term maintenance costs.

Unlike electronic passports (ePassports), which are required to comply with international standards, national eIDs can be more flexible in their design. They can be tailored to support the local infrastructure and can be budgeted to meet a range of project objectives. In some ways, this added flexibility is helping to push adoption, because even countries with limited resources can implement an adequate eID scheme.

Why NXP?

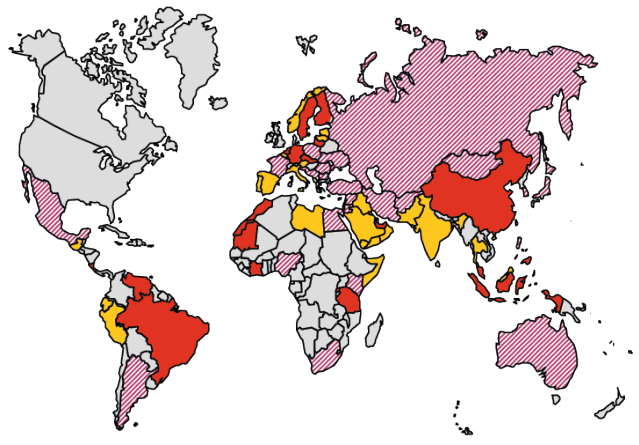
From a semiconductor standpoint, the secure microcontroller platform is central to the overall design of any eID solution. Security is a key concern, since personal data needs to remain safe at all times and fraud is always a risk. At the high end of performance, to support more advanced multi-application functionality, the controller needs to provide a large memory configuration and support strong cryptographic algorithms. And, as always, the IC platforms, along with the overall system solutions, have to meet certain price points.

NXP is the leading IC supplier in identification, and is the preferred partner for eGovernment projects around the world. Close to 80% of all ePassport and eID projects worldwide rely on our products.

Our best-in-class product portfolio covers the complete range of requirements for national eID systems. The SmartMX and SmartMX2 families of secure microcontrollers, which work with an impressive array of operating systems, have been implemented by all major vendors. Options for the OS include multi-purpose, application-specific, or open-platform, such as JAVA Card operating systems. Our products scale to the highest levels of transaction performance, and meet the most demanding requirements for security.

We provide all the cryptographic algorithms required by any national eID program, including symmetric triple-DES and/or AES cryptography, hash algorithms like SHA-1/SHA-2, and asymmetric RSA or elliptic curve cryptography that supports different key lengths.

Overview National eID projects on a worldwide base



Market Status Jan 2012

- More than 40 projects in deployment
- More than 60 projects in preparation
- More than 25 projects rely on NXP solutions to date
- New projects mainly targeting hybrid, dual interface or contactless solutions

Contact based deployed

Hybrid/contactless/dual interface deployed

In preparation

*Not all projects considered on map

CASE STUDY 1

Fast asymmetric transactions for Germany

Germany began issuing national eID cards in late 2010. The design, first specified in 2005, has a strong focus on citizen value and prompted the development of new cryptographic protocols and authentication methods. NXP's SmartMX is a key element in this demanding project.

As required by German law, the design takes into account the cardholder's privacy. It uses unique techniques to address the issues of minimal disclosure and the self-determination of data.

An online authentication function verifies the cardholder's identity, so citizens can securely access eGovernment or Business-to-Consumer (B2C) services via the Internet. Mutual authentication requires terminals to authenticate and prove access rights, based on card-verifiable certificates, before the card releases any personal data. A multi-level public key infrastructure was implemented in the background to support the scheme. The advanced functionality demands fast asymmetric transaction performance.

To add legal certainty to online correspondence, the cards can support a qualified electronic signature (QES) scheme protected by the highest levels of security.

Individual cards are expected to be in circulation for roughly 10 years, so the platform needs to be rugged and durable. Using a contactless IC solution supports the long lifetime requirements, and reduces the cost of maintenance for the reader infrastructure.

The combination of identity card, online authentication token, and QES function on a single smartcard places high demands on the security controller. The design is an excellent example of a high-end solution, and serves as a successful reference project for other national eIDs.

CASE STUDY 2

High-volume symmetric transactions for Indonesia

The eKTP project in Indonesia is one of the largest national eID projects to date. The deployment, which started in late 2011, will provide roughly 170 million citizens (out of a total 240 million) with an eID card. In addition to the identity function, the eKTP card will further the goals of democracy by including eVoting capabilities. The card will also store biometric data and support data updates in the field.

As major supplier for this project, NXP is delivering a cost-effective secure microcontroller platform that supports symmetric cryptography and offers an optimized memory configuration.

The need to support multiple applications, along with support for post-issuance data updates, as well as offline authentication, make the eKTP project a good fit for NXP's secure microcontroller solutions. As a high-volume project, the eKTP example also illustrates how relatively advanced design specifications can still be met even when resources are limited.

Indonesia selected a contactless format for their eID card, in part due to the need to support long lifetimes. The contactless approach also helps optimize the total cost of ownership, and increases system reliability by providing a robust interface.

To learn more...

For details about our SmartMX and SmartMX2 platforms, please visit www.nxp.com/smartmx2.

www.nxp.com

Date of release: April 2012
Document order number: 9397 750 17234
Printed in the Netherlands