MEDEA+

2A303: Biometric platform for next-generation identification, authorisation and digital signatures (BioP@ss)

SMART CARDS SYSTEMS FOR SECURE APPLICATIONS

Partners:

CEA-Leti
CompuWorx
Gemalto
Giesecke & Devrient
ID3 semiconductors
Infineon Technologies
NXP Semiconductors
OKsystem
Precise Biometrics
STMicroelectronics

Project leader:

Patrice Plessis,
Gemalto

Key project dates:

Start: July 2008
End: January 2011

Countries involved:

Czech Republic
France
Germany
Hungary
Sweden

The BioP@ss project targets development of advanced microelectronics and embedded software in secure and interoperable dual-interface or contactless smart-card platforms for all e-administrative applications required at European level. It assembles a powerful consortium including major chipmakers, global smart-card vendors, software developers and integrators, small and medium-sized enterprises, and academia. It will deliver a series of innovative options such as high-speed contactless interfaces, advanced biometrics and near-field communication connectivity that will enable the delivery of public services to European citizens from a personal e-identity platform and will open up global markets.

As the EU expands, it needs to ensure public administration can work across its borders and be easily accessible by all citizens. This is essential to increase freedom of movement for citizens and business throughout the Union. The EU i2010 information society framework set out a strategy to address the main challenges in improving efficiency, modernising administration, reducing bureaucracy and enabling citizens to communicate with public authorities more easily.

A key element is a secure national identity (ID) card allowing citizens to access to services in an expanded e-administration. The challenge is the need for secure electronic authentication and interoperability within and between countries. The European Commission has clearly indicated that compatible national electronic ID (eID) cards are essential whatever the technology – contact and/or contactless.

At the same time, member states have been requested to include additional biometric information and in particular digital fingerprints on e-passports. This marks a major step in biometrics as it creates a strong link between document and owner.

Meeting European standards

Prime applications targeted by the MEDEA+ 2A303 BioP@ss project are eID cards based on the European Citizen Card (ECC) family of standards currently under finalisation at the European Committee for Standardisation (CEN) and the next generation of electronic passports and residence permits.

The BioP@ss consortium supports the ECC approach, which combines the benefits of standardisation with the flexibility to adapt to national requirements by introducing individual ECC profiles. A specific goal is to ensure that components generated will comply with the ECC profiles representing French contact-based and German contactless-based implementations. The project will also cover areas such as e-health cards, electronic voting and electronic residence permits.

This project will leverage on the results of the earlier MEDEA+ Onom@Topic+ project and reuse its proposed open middleware architecture, now undergoing approval by several standardisation committees. BioP@ss will capitalise on the Onom@Topic+ hardware and embedded results and on all the proofs of concept in advanced very high

data rate contactless interfaces, embedded biometric components, advanced modelling techniques and embedded software platforms.

Key technology elements

BioP@ss will introduce new key technology elements, such as power-optimised contactless chips for next-generation passports, and will pursue definition and standardisation of a single more than 3 Mb/s contactless interface extending ISO 14443 and similar near-field communication (NFC) technologies and new cryptographic blocks supporting the recommended European extended access control (EAC) policy.

This work will include elliptic curve cryptography as well as the new supplemental access control (SAC) in combination with the basic access control (BAC) authentication protocol. SAC is supported by the German Federal Office for Information Security (BSI) and the French national information security agency ANSSI.

There will also be research into advanced match-on-card (MOC) biometric techniques and BioPIN, software-embedded privacy techniques aimed at providing users with a reasonable level of control over private data when dealing with administrations. The project will demonstrate embedded software platforms enabling plug-and-play connection between an identification, authorisation and digital signature (IAS)-based platform and an Internet protocol (IP) architecture. Client and server middleware for the citizen will be demonstrated.

Applications targeted have large economic, social and technical impacts and are expected to represent a substantial part of the smart-card market by 2012. There are stringent common security and interoperability needs at European level for eID and services, residence permits and e-health cards as well as at international level for International Civil Aviation Organization (ICAO) travel documents.

Rights across Europe

All EU citizens have rights and obligations that they expect to exercise all around Europe and web-server middleware is well adapted to this. The mechanism involved should be simple, technology independent, easily understandable and accessible anywhere and at anytime within member states to propose a migration path from existing solutions dedicated to citizens. Access to public services at pan-European level is key. Supplying basic enabling technologies to meet this goal is expected to be a prime impact.

BioP@ss will provide compliant implementations of the ECC standard, based on a standardised IAS kernel, for practical cross-border interoperable services. These implementations will be accompanied by technology options that open the way to develop extended government services on a more local level, based on cross-administration or private/public partnerships. Options could include IP plug-and-play, high-speed contact interfaces or web server plug-ins.

The eID concept is largely driven by legislation and standards. Several countries have already adopted a national eID scheme: eight European countries have contact-based interfaces as do other countries that include China, Ecuador and Saudi Arabia. Other dual or contactless-based schemes are in development.

There are several standard initiatives for national eID including Europe with the ECC, the Gulf Co-operation Council and the US NIST programme. BioP@ss will develop platforms that are compatible and interoperable with some of these initiatives. Project results should be usable for all new eID projects in the 27 EU countries and will enhance existing schemes such as those of Belgium and Spain.

Numerous impacts

The results of this project will have numerous impacts, especially in terms of external border controls. The most visible aspect will be the installation of new terminals for fingerprint scanning at borders. Not only will scanners be required but the entire border control reader will have to be compatible and equipped with document-authentication software linked to the passport-controlling authority.

In terms of market opportunities, BioP@ss targets applications such as e-passports and e-identity cards. More than 70 countries had adopted the first version of the ICAO e-passport by end 2009. The first ICAO standard was finalised in 2004, while the EU adopted EACv1.11-secured biometry from end 2009. This represents a potential market for BioP@ss of more than 200 million units.

Success will speed the availability of a European information society benefiting public authorities, citizens and technology suppliers alike. And the inherent proof of concept is likely to be exported outside Europe, as already demonstrated by convergence between CEN and ISO standards.