PROJECT RESULT

Smart card systems for secure applications

MEDEA+

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


# Speeding secure electronic identification for passports and citizen services cards

**The BioP@ss project has developed advanced microelectronics and embedded software for secure and interoperable smart-card platforms essential for pan-European e-administration, including electronic identity (e-ID) cards, residence permits, healthcare cards and driving licences. The results have laid the technical foundations for future e-ID documents in the EU, while reducing administrative costs for government, raising security levels of electronic documents, accelerating data transfer between ID documents and contactless readers, and simplifying use of public electronic services by citizens.**

Some 380 million identity (ID) cards are in circulation in the EU with its 500 million population. However, there is a strong need to raise the security level of future electronic ID (e-ID) cards and passports, speed their reading and simplify access to and use of public services for citizens across Europe. The latter makes it possible to replace time-consuming and costly paper correspondence between citizens and the state by electronic communications – reducing governmental expenditure.

The MEDEA+ 2A303 BioP@ss project brought together the three major European chipmakers associated with two major secure operating systems developers, digital security specialists and research organisations as well as biometric equipment manufacturers, integrators and card-reader makers to develop new high security chip-card technologies. The initial focus was implementation of e-ID solutions based on the European Citizenship Card standards for e-passports and residence permits with their associated public key infrastructure (PKI). Applications were also envisaged for health-service access, electronic voting and driving licences.

BioP@ss built on the earlier MEDEA+ Onom@ Topic project. It focused on the proofs of concept achieved in the areas of advanced contactless interfaces, biometric components, advanced modelling techniques and embedded identification, authorisation and signature (IAS) software platforms.

### Match-on-card environment

Facial image verification is the main use for biometrics with e-passports and e-ID cards. The goal of BioP@ss was to develop an innovative match-on-card (MOC) biometrics environment, suitable for on-card processing, and to develop an environment enabling users to interact from a biometrics e-ID personal device with a set of multiple near-field communication (NFC) enabled mobile terminals using web services.

In addition, biometric MOC solutions can be supplied as a Java applet which means countries introducing national e-ID cards have greater flexibility regarding choice of smart card. It also combines strict personal privacy with secure authentication – such as a biometrics personal identification number (PIN) or used as a password for extended access control for contact or contactless platforms.

All this required new chip technologies which have provided several innovative options such as very high bit rate (VHBR) contactless interfaces and protocol, advanced biometrics and NFC connectivity enabling the delivery of innovative services to citizens from a personal e-ID platform.

Advances included further development of security chips and their encryption technologies, and security software for the Internet personal computers (PCs) used by citizens and

public authorities. Data transfer rates between e-ID cards and readers have been increased more than tenfold – from 800 kb/s to 10 Mb/s. Moreover, a new chip-card operating system will make it possible to use future e-ID documents on the Internet without the need for additional software components on the PC.

## Supplemental access control

BioP@ss worked also on proof of security for the supplemental access control (SAC) standard for e-passports, contributing to the Password Authenticated Connection Establishment (PACE) protocol. E-passports are biometrics-enhanced, machine-readable travel documents based on specifications defined by the International Civil Aviation Agency (ICAO) to strengthen border security. The EU and the ICAO will enforce use of this mechanism for all travel documents issued from 2014.

E-passports incorporate a contactless microprocessor chip on which information on the passport holder is stored – biometrics as well as name, date and country of birth. The EU required extended security to ensure the contactless chip could not be read without physical access to the travel document and that data exchange between chip and reading device is encrypted.

SAC takes such security even further, based on PACE v2. This implements asymmetric cryptography with data encryption based on a shared key between reading device and chip during authentication. The result is enhanced data confidentiality which makes skimming or eavesdropping impossible.

## Products and standards

Overall advances include:

- Development of web-server-based software and middleware, ensuring operations are more transparent and facilitate the migration phase for today's programs;
- Proof of security for new protocols for third-generation passports, e-ID cards and resident permits – important for the new travel regulations from the end of 2014; and
- Speed of access to data that will cut waiting times for security checks at airports and simplify access to data such as X-rays in medical card records.

The technologies developed are being incorporated into card platforms by the BioP@ss partners. Middleware packages are already in products, while card specialists Gemalto and Giesecke & Devrient are working on complete contactless identification, authorisation and digital signature solutions.

Moreover, BioP@ss has contributed to several standards, including:

- ICAO SAC/PACE V2, adopted in mid 2011;
- A new ISO contactless VHBR standard, currently under consideration by the relevant ISO work group; and
- The CEN IAS standard for the European Citizen Card.

Benefits include increased mobility in Europe with faster and more flexible access to e-government, better protection of personal data and the availability of a series of building blocks in middleware/software and hardware, biometrics and protocols that can be used in other projects and platforms to improve European security and competitiveness.

Smart card systems for secure applications

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

**PARTNERS:**

CEA-Leti
CompuWorx
Esterel Technologies
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

**CATRENE Office**
9 Avenue René Coty
F-75014 Paris
France
Tel.: +33 1 40 64 45 60
Fax: +33 1 43 21 44 71
Email: catrene@catrene.org
http://www.catrene.org

EUREKA Σ!

MEDEA+ Σ!2365 is the industry-driven pan-European programme for advanced co-operative R&D in microelectronics to ensure Europe's technological and industrial competitiveness in this sector on a worldwide basis.

MEDEA+ focuses on enabling technologies for the Information Society and aims to make Europe a leader in system innovation on silicon.