Smart card systems for secure applications

MEDEA+

2A302: European smart card platform for citizenship and mobile multimedia applications (Onom@Topic+)

Powering up smart cards for powerful ID and mobile multimedia applications

The ONOM@TOPIC+ project has developed powerful European smart-card platforms for citizenship and mobile multimedia applications. The primary goal was to develop complete hardware and embedded software components to enable industrial and government operators, terminal and smart-card companies, and chipmakers to take full advantage of the enormous potential offered by fixed or mobile e-services. The second aim was to demonstrate the added value of the platforms, showing interoperability and new service delivery potential in EU citizen ID cards and powerful multimedia applications for network operators.

The ever-increasing level of integration possible in integrated circuits means many more functions can be added to chip-equipped smart cards. The MEDEA+ 2A302 ONOM@TOPIC+ project brought together chip-makers, software developers and systems integrators not only to add functions but also to design new architectures to improve service interoperability, end-user acceptability and ease of use by seamless handling of complex functions that could not have been possible with previous technologies.

ONOM@TOPIC+ was split in two:

1. Development of a citizenship platform; and
2. Extension of multimedia possibilities in a new generation of subscriber identity module (SIM) cards and mobile terminals.

International interoperability

The citizenship subproject focused on international interoperability of digital identities, contributing to European and global standards, and extending identification, authentication and signature (IAS) functions. Onom@Topic worked with partners worldwide to develop the CEN European Citizenship Card (ECC) norm, contributing to the stabilisation of the first three parts – work on the fourth part could not be completed within the project. It also influenced ISO 24727, mostly led by US and non-European companies.

Unlike previous projects, ONOM@TOPIC+ targeted a fully open approach – including private/public partnerships – and demonstrated interoperability between different countries on complex services. This prepares the way for future national ID card interoperability within Europe: five countries – France, Germany, Italy, Spain and the UK – have already agreed to work on such schemes in the Porvoo Group.

ONOM@TOPIC+ came up with a set of card-embedded and middleware-oriented functions that make possible the future deployment of the next-generation ECC compatible with cross-border services access. In addition, several innovative features were prototyped, including match-on-card biometry, high-speed contactless interfaces, formal verification of security property and support for new protocols such as near field communication (NFC).

Other advances include mechanisms for terminals to discover automatically which services can be hosted on the card, how these services can be accessed by the terminal and how efficient communication can be established between card and remote servers without compromising security for either card issuer or user. This strong security is implemented in hardware and software.

In future, it will be possible to use chip-equipped cards in a variety of terminals, enabling cardholders to be recognised everywhere as European citizens and get seamless access

to government services such as pensions or document delivery at home or in other countries, using interoperable web-based delivery mechanisms. The card should also be able to incorporate applications such as financial, retail or information services.

The Onom@Topic+ technology is now very close to market. Several ID projects based on the results will be industrialised in Europe by 2010.

Next-generation SIM cards

The mobile multimedia subproject set out to make major improvements in SIM cards and mobile handsets to handle multimedia content more efficiently. Efforts resulted in new technology concepts, with two new standards now recognised worldwide.

Key advances included a SIM card supporting very high speed connectivity with mobile terminals using the well-recognized USB communication interface technology. This is crucial as mobile personal computers and mobile multimedia converge completely. In addition, the project developed the single wire protocol (SWP) to handle NFC technology from the SIM card for proximity contactless interfaces with external devices such as kiosks, TVs and consumer electronics. Both interfaces have been endorsed by ETSI and 3GPP.

The new interfaces ensure a high level of security and the project targeted simultaneous use of both interfaces in the SIM platform, without changing the existing standard packaging and pin count. This required efficient use of the eight pins on the standard card: five for the ISO-standard connections between handset and card, two for USB and the last one for contactless management thanks to the clever SWP full-duplex protocol. Working prototypes were produced in the project with a suitable handset to host the new cards. Such cards should be available commercially early in 2009.

A second major innovation was in terms of enabling very large memories on the SIM card. Current memories are in range of several hundreds of kilobytes, while the MEDEA+ project led to hundreds of megabytes or even gigabytes using clever packaging and side-by-side or stacking technologies. Another advance concerned a completely new software design. The SIM card can now act like an Internet node, having a TCP/IP connection with the mobile handset so that it is possible to browse the content of the SIM card in the same way as in a standard Internet browser.

Finally, substantial developments were made at handset level to enable mobile terminals to take full advantages of these new SIM card features.

New operator services

It is now also possible for the mobile operator to develop new services – including complete remote configuration of the handset and management of operator identity from the SIM card, and downloading applications directly to the SIM card for later use on the handset. This is a key advantage for the service provider as the operator owns the SIM card and not the handset.

The operator will be able to control the SIM card, check what is in it and manage both operator and customer applications efficiently, opening up new opportunities. Several advanced use cases were developed – such as fast phone book restore, video on demand, mobile blog and anonymous secure purchase – and some will be marketed from the end of 2008.

Smart card systems for secure applications

2A302: European smart card platform for citizenship and mobile multimedia applications (Onom@Topic+)

PARTNERS:

CEA-LETI
CompuWorx
Esterel Technologies
France Telecom - Orange
Gemalto (Axalto and Gemplus)
ID3 Semiconductors
NXP Semiconductors
Oberthur Card Systems
Oksystem
Philips CE iLab
Precise Biometrics
Purple Labs
Safe Layer
STMicroelectronics
Telefonica

PROJECT LEADER:

Jean-Pierre Tual
Gemalto

KEY PROJECT DATES:

Start: January 2005
End: December 2007

COUNTRIES INVOLVED:

Czech Republic
France
Hungary
The Netherlands
Spain
Sweden

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.