PROJECT PROFILE

A302: Enhanced smart-card platform for accessing securely services of the information society (EsP@ss-IS)

SMART CARDS FOR SECURE INTERNET

Partners:

CEA-LETI
INPG-TIMA
Interpay
Philips Consumer Electronics
Schlumberger
STMicroelectronics
Thomson Multimedia
TIM
Trusted Logic

Project leader:

Jean-Paul Thomasson,
STMicroelectronics

Key project dates:

Start: January 2001
End: December 2004

Countries involved:

France
Italy
The Netherlands

The growth of value-added electronic and mobile commerce services can be greatly enhanced by the availability of both hardware- and software-based open smart-card platforms. At a secondary level, the development of such open platforms can provide a set of reusable innovative technological bricks from which future generations of high security smart-card products may be created. The EsP@ss-IS project aims to deliver all of the necessary hardware and software for open smart-card platforms destined to support the availability of value-added electronic and mobile commerce services. These are intended to meet the needs of operators in the mobile telecommunications, banking and pay-TV sectors.

Within four years, the number of users accessing the Internet from consumer appliances, such as personal digital assistants, pen-based devices, mobile phones or TV set-top boxes, is forecast to far outnumber users gaining access to the Internet from a portable or desktop PC. The reasons for this changeover include: ease of use of consumer appliances compared with PCs; early availability of fast Internet access using wireless, mobile phone, cable, satellite and ADSL (asynchronous digital subscriber line) technologies; and the lower cost of such appliances compared with a PC.

The development of mobile and electronic commerce in Europe will nevertheless only be achieved if the consumer can be guaranteed a full level of security and privacy. Without care in the development of e-business practices, consumers and operators could be exposed to risks that may seriously endanger their activities. Smart-cards offer a particular secure solution to these problems.

Secure Internet connections

With its wide vertical partnership, the MEDEA+ A302 EsP@ss-IS project is intended to be the flagship for all MEDEA+ smart-card projects. Overall, it supports the European aim of achieving a leading position in the development of secure Internet applications.

Europe has two key strategic advantages in this area:

1. European phone manufacturers lead the world in mobile telecommunications, which will deliver the most widely available Internet access platforms using new generation wireless application protocol (WAP) and later universal mobile telecommunications system (UMTS) terminals from 2003 onwards – and Europe has the most powerful mobile telecommunications operators worldwide; and
2. Europe leads the world in the smart-card market, with all major players in the value chain being Europeans. This is true for card software suppliers as well as manufacturers of micro-controllers for smart-cards.

The EsP@ss-IS project is dedicated to smart-card platforms for the support of e-commerce applications and fully encompasses the goals of the European Commission's *e*Europe initiative, for which it will provide the technical background in a pre-competitive, industry-led consortium. This will also

be achieved through a dynamic communications and project promotion policy, with substantial effort dedicated to targeting standardisation bodies worldwide.

E-commerce still on trial

E-commerce already represents an increasing portion of all purchasing of goods in the USA, where most payments are made with standard credit/debit cards, using unsecured magnetic-stripe technology. Payment over the Internet represented about 5% of purchases in the USA in 1999 – and about 50% of all litigation through denial of service, repudiation, unpaid services, etc.!

In Europe, some e-commerce pilot programmes have started, with e-purse schemes, such as Proton in Belgium, the Netherlands and Sweden, the German Geldkarte and chip-based debit/credit cards like Cybercomm in France.

Most of the innovation is centred on the mobile telecommunications field, where all major operators have already started mobile commerce services based on a combination of mobile network/equipment and Java SIM Toolkit smart-card technology. Large operators such as BT/Cellnet, France Telecom, Sonera, Vodafone-Air Touch and TIM offer stock-exchange access services, location-based services, or payment using dual-slot GSM mobile handsets.

Some content providers offer large mobile- and e-commerce portals with many services ultimately accessible through mobile terminals, set-top boxes or PCs.

In Asia, the major on-going experience is that of the NTT DoCoMo I-mode project in Japan, which has apparently attracted over eight million users since its launch in 2001. It already offers news, gaming and financial services –- a preview of what will be achievable over the future UMTS mobile networks.

In the public key infrastructure (PKI) field, besides the US majors, European companies have already started to be successful, especially from the mobile communications perspective.

Innovation proposed

The EsP@ss-IS consortium intends to deliver generic smart-card platforms to supply and deploy mobile- and e-commerce services. These platforms will be based on best available technologies at silicon process, open embedded software and middleware levels. They will include:

- High performance 8- and 32-bit platforms with large user memories, full optimisation of power consumption and high bandwidth, full support of high-speed contactless and wireless protocols;
- Highly innovative technology bricks supporting future generations of smart-card, such as very large user memory (flash, FeRAM), and card-embedded copyright protection software for video and audio compression (MPEG, MP3, etc.);
- Open embedded, layered software architecture based on secure real-time operating systems, on-board card application management with a firewall between application, embedded virtual machine and application programming interfaces such as Java, MEL or Visual Basic, with secure application downloading;
- Dedicated embedded middleware at terminal level aimed at enforcing end-to-end security for transaction processing, based on state-of-the-art techniques such as mobile PKI or virtual private networks;
- Methodology framework supporting efficient hardware/software co-design, formal support of Common Criteria certification scheme and secure intellectual property reuse; and
- Architectural concepts aimed at optimising the functional split between various components in the infrastructure and specifying the security, performance and cost trade-offs.

Developing a generic platform

While aimed initially at the mobile telecommunications, banking and pay-TV sectors, these platforms will be of use to all software or service companies intending to develop or promote such services. The target of the consortium working on this project is to bring to the smart-card, mobile and e-commerce user community the equivalent of the 'Windows/Intel' platform in the traditional IT field.

In addition, the MEDEA+ project will deliver many basic innovative technological bricks to enable achievement of these goals as well as preparing for future generations of smart-card platform. This objective will include new non-volatile memories for large on-chip storage, high-speed cryptography and digital signal processing with MP3/MPEG audio/video compression capabilities, open embedded software with downloading capability, high-speed interfaces and wireless protocols.

The project will be phased over two two-year periods, corresponding to two generations of hardware/software smart-card platforms. The second generation will benefit from all of the basic technology components developed in the first two years of the project.

MEDEA+ Office
33, Avenue du Maine
Tour Maine-Montparnasse
PO Box 22
F-75755 Paris Cedex 15, France
Tel.: +33 1 40 64 45 60
Fax: +33 1 40 64 45 89
Email: medeaplus@medeaplus.org
http://www.medeaplus.org