

Smart cards
for secure
internet

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

Smart-card systems secure Internet applications

The rise of electronic and mobile commerce is accompanied by increasing concern for the security of transactions conducted over the Internet. As a result of the MEDEA+ A302 EsP@ss-IS project, the foundation has been laid for the development of open smart-card hardware and software platforms that will provide the protection necessary to foster the growth of value-added services in sectors such as mobile telecommunications, banking and pay-TV. Open standards and the definition of core building blocks consolidate the strength of Europe's competitive position in this technology growth area.

The rise in the numbers of people accessing the Internet using consumer appliances such as mobile phones and TV set-top boxes is outstripping that of personal computer users. This trend is driven by the accessibility and lower cost of appliances, coupled with the increasing availability of high-speed connection via wireless, satellite and cable links.

However, today's newspapers are filled with stories of identity theft and network attacks by increasingly sophisticated criminals. The full potential of electronic and mobile commerce (e- and m-commerce) will only be realised if consumers and businesses can be guaranteed an adequate level of security and privacy.

A recent market survey estimated the current volume of e-commerce in the EU to be worth €30 billion, of which €20 billion was paid using card-based products. With the Internet becoming an even more dominant medium for electronic transactions, there is a strong incentive for Europe to promote this combination of technologies as the way ahead.

Leadership threat

By their very nature, smart cards with embedded circuitry to store and process data are highly appropriate to today's models of business mobility. The latest microcontroller

architectures, controlled by more efficient operating systems, allow fast execution of crypto-protocols required for public key infrastructure (PKI) operations. Together with new connectivity options, this makes it possible to set up secure end-to-end channels with distant web servers, and to support a wide variety of Internet protocols.

With much more extensive use of second and third generation mobile communications devices, European industry will provide the most widely available Internet access platforms, while the region has some of the world's most powerful mobile telecom operators. All major smart-card players are also European.

Yet this is no guarantee of success. The card market experienced its first major downturn in 2000 to 2002, which resulted in a rationalisation of the companies involved as well as a diversification of product portfolios. Recovery is underway, with the need for new and even more trusted security features in mobile telecoms and growth expected in public sector, multimedia and network security applications. But new competitors, notably from the Far East, are entering the arena – and IT manufacturers are pursuing non-card-based solutions.

In order to protect and reinforce the competitive position of Europe, several of its leading names joined forces with SME partners and

a top research institute in the MEDEA+ A302 EsP@ss-IS project. This is regarded as major cornerstone for all MEDEA+ smart-card activities.

Card/service vision

Coordinated by STMicroelectronics, the partnership spanned the whole card value chain, from chip manufacture to content provision and network operation. Its vision was to provide the smart-card and service provider/user communities with a generic equivalent to the traditional IT world's Windows/Intel platforms.

The prime objective was to deliver the hardware and software to form a basis for open platforms permitting the development of secure value-added services in telecoms, banking, pay-TV, health and other sectors. A secondary goal was to define basic technological building blocks supporting high-speed wireless and contact-less protocols. It was also seen as essential to exploit the power of the consortium in winning acceptance for the project's innovations by the international standards bodies.

Two generations

The MEDEA+ project was divided in two phases, corresponding to two successive platform architecture generations: the first was an enhancement of existing state-of-the-art prototypes and is now commercialised by one of the project partners (ST22 Product Family). In the second, long-term requirements identified in an initial user survey were integrated into proven intellectual property (IP) blocks developed during the first phase. This approach produced the 'low cost platform' and '.NET smart card' for web-services access control, plus a

more advanced 'high-end platform' and 'flexible multimedia card' architecture.

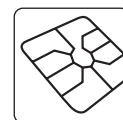
Although not fully integrated on silicon, the flexible multimedia card concept was presented at several major shows, including the November 2004 MEDEA+ Forum in Paris. Video transfer was demonstrated via a contact-less interface at up to 1.7 Mbit/s, with a refresh rate of 21 images/s – approaching the traditional 25 images/s film refresh rate – demonstrating high-speed biometrics-based identification using secure smart cards.

And a real embedded .NET smart card was shown at a number of Microsoft symposiums to be capable of supporting various authentication schemes allowing ID provisioning on portable devices.

Global dominance

European companies hold some 80% of the world smart-card market, with well over half of all the cards in use globally produced in European smart-card factories. This market has led to the creation of over 10,000 direct high skilled jobs in Europe since the early 1990s. But continuous innovation is essential to retain this dominance. The EsP@ss-Is open smart-card platforms will stimulate new patterns of collaboration in Europe's card-related industries, and could encourage creation of start-up companies to exploit the additional power and security of the technology. As end-users, citizens will benefit directly from developments that will allow an unprecedented secure access to new and wide-ranging services.

Knowledge sharing with a number of parallel projects during the lifetime of the project ensured that maximum value would be derived from its results.



Smart cards
for secure
internet

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

PARTNERS:

Axalto (incl. former part of Schlumberger and CP8)
CEA-LETI
INPG-TIMA
Interpay
Philips
STMicroelectronics
TIM
Thomson
Trusted Logic
Viaccess

PROJECT LEADER:

Jean-Paul Thomasson,
STMicroelectronics

KEY PROJECT DATES:

Start: April 2001
End: December 2004

COUNTRIES INVOLVED:

France
Italy
The Netherlands



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



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 for the e-economy.