PROJECT PROFILE

A306: Technology responses to ubiquitous security threats for e-security (TRUST-eS)

SMART CARDS FOR SECURE INTERNET

Partners:

Atmel
Axalto
Bioret
CEA Leti
CNM
Gemplus
GET
InnovaCard
INPG-TIMA
iRoC Technologies
STMicroelectronics
SystemPlus
Telefonica
Thales
Uni Madrid (Carlos III)
Uni Tarragona (URV-URJC)

Project leader:

Laurent Manteau,
Gemplus

Key project dates:

Start: July 2004
End: December 2006

Countries involved:

France
Spain

During the past decade, Europe has led development of smart cards into complex media able to store, compute and securely manage multiple applications. Global terrorist activities have now driven governments, national authorities and large companies to consider cards and other options to upgrade security. But, there is a need to overcome technological limitations currently encountered in card-based transaction platforms, and pre-empt foreign competition to provide reliable and cost-effective solutions for the e-security and e-government applications needed. The MEDEA+ TRUST-eS project is targeting authentication technologies addressing multimode identification with smart-card-based biometrics.

Credit-card size smart cards containing memory and processing circuitry have developed rapidly since the early 1980s to handle banking transactions, support mobile communications and act as electronic 'purses'. Under the strong influence of European industrial companies, such systems have been widely adopted in applications where no other options were available.

More recently, a major market opportunity has been created by the fact that, especially since the terrorist attacks on New York on 11 September 2001, most governments have become increasingly concerned about national security. The control of access to restricted and sensitive areas such as airports and government buildings requires secure smart-card solutions similar to those for other e-government applications like citizens' identity cards and e-signatures.

Timely action essential

Market analysts forecast compound annual growth of 27 to 50% for smart cards in Europe, and 97 to 120% worldwide. This clearly indicates that, even though Europe invented the concept, it could lose the initiative unless appropriate and timely action is taken.

However, despite the fact that the technology has become increasingly sophisticated, the industry faces major hurdles to the pervasive use of smart cards for such purposes.

On the one hand, the need to manage and secure rapidly growing information networks is creating a demand for even more advanced capabilities than now available. On the other, Europe is confronted with a situation where cards will have to compete with alternative solutions promoted by the USA and Japan, especially for e-security and e-government.

In the MEDEA+ A306 Trust-eS project, a consortium of European industrial players, SMEs and academic partners, led by Gemplus, is pushing smart-card performance and adding new features by addressing technological developments from the system-on-chip (SoC) component level to interfaces with external network architectures.

University partners will develop longer term technologies, while partners such as Telefonica will act as end users. And Thales will bring in systems integration know-how, complemented by the results of the

MEDEA+ A302 EsP@ss-IS project, to ensure application of Trust-eS-developed technologies. Standardisation will be promoted to facilitate wider dissemination.

Pragmatic approach

To reduce the total resources needed and avoid duplication of effort in tackling these issues, the Trust-eS team is liaising with other European initiatives covering related areas – including the MEDEA+ T123 Crescendo and T206 CMOSSOI projects.

Cards employing conventional identity verification – such as passwords and personal identification numbers (PINs) – are easily compromised. But use in conjunction with biometrics offers one of the most reliable methods of determining individuals' identities.

Iris and fingerprint scanning are considered today as the most reliable authentication, but are largely limited to professional applications due to their perceived invasiveness. A number of companies are nevertheless already proposing fingerprint-scan systems coupled with smart cards via microelectronic components. If the political will and public acceptance can be mustered, such systems could be widely and cost-effectively deployed.

With the development of multi-application solutions, the usual trade-off between silicon area, SoC performance, power consumption, security and the division of functionalities between hardware and software has to be totally re-engineered for both cards and interfaces. Also, it is desirable that architectures allow cards to be used in a wider environment and interfaced with standard IT systems that are not 'card-centric'.

Five aspects

Trust-eS work focuses on five main areas:

1. System architecture – in terms of performance, portability, attack detection and resistance. This entails in-depth analysis of SoC designs, incorporation of system-on-insulator (SOI) and non-volatile memory technologies from other MEDEA+ projects, and design of reconfigurable blocks for improved security or greater silicon efficiency;
2. Client/server applications – in which the card is integrated into distributed architectures so it can function as a server or securely run applications that do not reside on the card itself. To date, even the most high-end smart cards have been developed in a fully card-centric manner, which poses serious limitations on their proliferation in the established information and communication technologies (ICT) world. Trust-eS is developing new hardware/software resources to bridge this gap, entailing a totally different organisation of communications protocols, memory management and allocations on the card, as well as of the commands to the card;
3. Reconfigurable blocks for secure SoCs – making the card more customisable and secure by integrating a configurable hardware block and software-embedded driver. The target is a robust, flexible platform offering reduced customisation costs;
4. Authentication techniques and technologies – essentially addressing fingerprint sensor technology, new multimode fused biometric identification algorithms and biometric systems architecture based on smart cards. Enhancing sensor resistance to fake-finger fraud is an important aspect in extending the potential for secure services through unattended terminals and mobile phones. The goal is to reach a stage where biometrics can replace PIN code identification on the card and be coupled with cryptography for applications such as e-signatures;
5. Integration of smart-card interfaces in systems environments – combining highly secured embedded technology with connectivity to secure smart card interface platforms. Reliable and integrated contactless features are being developed for cards and platforms. The consortium intends to develop a demonstrator suitable for security and access control in residential service areas – including those lacking Internet access – as well as in the next generation of intelligent office workspaces.

Careful dissemination

Industrial partners in Trust-eS will exploit project results in their own product lines, while vertical co-operation will enable them to determine optimal solutions for interfacing the various elements into complete systems for e-government applications.

Clearly, the secure nature of the solutions and technologies developed in this context would be devalued by public revelation of certain results. Hence the consortium will pay particular attention to the dissemination. Characterisation and assessment of techniques, methods and technology blocks or demonstrators will be released as far as possible – while implementations, source codes and detailed architecture descriptions will probably remain confidential or be patented where practical.

MEDEA+

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

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 for the e-economy.