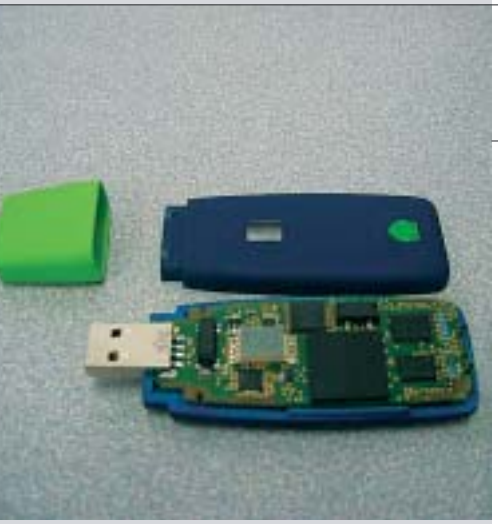
PROJECT RESULT

Smart cards for secure internet

MEDEA+



A304: Cryptographic system on a chip (CryptoSoC)

Data security begins at home

Safeguarding stored data against increasingly sophisticated threats is crucial to administrations, industry, commerce and citizens. Access control, electronic signatures and the confidentiality of proprietary information all depend on cryptographic protection. But with most systems interconnected either directly or indirectly via the Internet, reliance on software-based methods is no longer adequate. CryptoSoC has developed interoperable hardware components that will enable Europe to assemble its own system-on-chip devices providing improved security and generating business opportunities worldwide.

Rising levels of criminal attack and terrorist action make the protection of critical information system infrastructures a growing concern for administrative, business, communications, finance, distribution, energy and transport networks. But, with the Internet becoming a near-universal medium for data exchange, the use of commercial security software to fulfil essential functions such as encryption, electronic signature, key generation and storage can no longer be relied upon to provide an appropriate level of security and trust. For this reason, the adoption of hardware-based cryptographic resources is becoming mandatory at all system levels.

Weakness creates risk

Although Europe has a strong position in smart card technology for personal terminals, US industry has so far dominated in the field of hardware cryptographic components for the fast-moving server and networking equipment market. As well as posing a commercial threat, reliance on externally sourced microchips could even leave national security and defence installations in Europe open to penetration by foreign intelligence organisations. Provision of secure and trusted key management cannot be achieved with general purpose central processing units (CPUs), because they lack sufficient built-in security features for tamper response, critical data path insulation and the separation of buses for different types of data. Moreover, it is not that easy to load the cryptographic computation that will be required for future applications onto a CPU without exceeding the heat-dissipation capabilities of securely constructed equipment.

In the MEDEA+ A304 CryptoSoC project, a group of French and Italian partners set out to address these issues by creating a cryptographic system-on-chip (SoC) device architecture that would be entirely under the control of European companies.

Major chip manufacturer STMicroelectronics had already produced a number of hardware structures that could be exploited in the security market, while computer manufacturer Bull is a leader in the field of Internet security with its TrustWay product portfolio. Amtec acted as the provider of hardware/software-based security solutions within the Marconi group — and Sagem could contribute its experience as a prominent supplier of mobile terminals and security products. This industrial strength was complemented by the research expertise of institutions in Italy and France.

Response to real market needs

The project began with a user requirement

survey to assess the evolution of the server market, in terms of volume and of the security requirement of current and expected applications.

Based on the results of this exercise, the consortium devised a suitable architecture, which they realised through a series of interoperable building blocks. The focus was on very high performance, capable of supporting large scale public key infrastructure (PKI) and key tetrabyte/s class networks. High-level trusted security is guaranteed by an internationally recognised Common Criteria evaluation and certification.

The aim of the project was not just to produce a single chip, but rather to develop the know-how needed to construct interoperable cryptographic components including SoC architecture adapted to specific application requirements. The resulting building blocks are programmable elements that represent the stage before commitment to actual chip production. In this way, the costs and uncertainties of silicon implementation based on early user specification could be avoided within the project itself — they will be incurred at a later stage, in response to actual market demands.

In addition, intellectual property (IP) developed within CryptoSoC is enabling the partners to synthesise components matching requirements ranging from those of smart card systems and mobile handsets to virtual networks in which business partners conduct transactions and share essential information on-line. By granting licences to other European players, the CryptoSoC project is providing them with access to the same technology and thereby helping to ensure that CryptoSoC components become an established standard.

All-round success

Shortly after the end of the co-operative research project, Bull was ready to launch three new products. In co-operation with Amtec and STMicroelectronics, it also demonstrated that IP exchange between partners was possible and worked well. This essential feature at the heart of the MEDEA+ project allowed for the rapid introduction of new developments based on the mutually adopted CryptoSoC application programming interface (API).

All of the industrial partners eventually produced new IP and have adapted their existing blocks to the common API. This collaboration has allowed rapid constitution of a rich library of proprietary cryptographic modules, several of which — for example, configurable IP from CEA, I2E and Sagem — are ready for integration in a new generation of cryptographic components targeting all class of application.

Such elements can now become part of standard devices without exposing any of their highly confidential design details. The new architecture itself, simulated by Politechnico di Milano, has proved to be compliant with the many different requirements of both high-end servers and low-power mobile applications.

The very good relationship established between all the partners remains a key factor in proceeding with the promotion and extension of an architecture that is the foundation for future European cryptographic developments. The architecture and IP developed are scalable for products with both high level security, such as military applications, and low level security, such as personal computer applications.

Smart cards
for secure
internet

A304: Cryptographic system on a chip (CryptoSoC)

PARTNERS:

AMTEC
Bull
CEA-LIST
I2E
Politechnico di Milano
Politechnico di Torino
Sagem
STMicroelectronics

PROJECT LEADER:

Patrick Le Quéré,
Bull

KEY PROJECT DATES:

Start: October 2001
End: December 2004

COUNTRIES INVOLVED:

France
Italy

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.