A304: Cryptographic system on a chip (CryptoSoC)

SMART CARDS
FOR SECURE INTERNET

Partners:

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

Project leader:

Alain Filée,
Bull

Key project dates:

Start: April 2002
End: December 2004

Countries involved:

France
Italy

The world of e-business, where customers and business partners are all connected using a common global infrastructure, has arrived. One of the key challenges related to this new reality is the level of confidence that can be placed in the infrastructure itself. Can anyone really be sure that only the intended recipient reads the information they are sending? Because the majority of IT security technologies are of US origin, Europe faces a potentially dangerous lack of independence and control in this area. MEDEA+ project CryptoSoC seeks to redress the balance by developing the basic trusted security hardware components necessary to protect future Internet servers and high-speed data networks.

Protection of critical information systems infrastructures for business and financial communication will become a fundamental issue in the future. Cryptography addresses this need.

Today, cryptography can be applied using hardware, software or communication protocols such as secure socket layer (SSL). Some co-processors exist or are being proposed for computation of ‘algorithmic kernels’ for both public- and private-key cryptographic systems. However, rather than being used directly on main processor system boards, these components are incorporated into add-on accelerator cards that demand high level application program interfaces. Consequently, cryptography is now still carried out mainly by software that performs the essential operations such as encoding, electronic signature, key generation and storage.

Policy change needed

Current protection policies tend to provide safe communication ‘pipes’ between remotely executing co-operating applications, and are consequently designed to safeguard network data streams transferred mainly using Internet protocols. Next-generation storage area networks (SANs) that integrate input/output traffic and message-passing over the same high performance channels may require major changes to avoid serious security gaps in communication path protection.

Given the high vulnerability of commercial software, it cannot continue to provide an adequate level of protection for information technology systems directly or indirectly interconnected over the Internet. Therefore, incorporation of hardware-based systems will be mandatory in tomorrow’s terminals, servers and networking equipment. But – apart from personal terminals, where Europe has a strong position in smart card technology – US industry enjoys a monopoly in this market.

While smart cards provide a solution in ‘client’ environments such as mobile terminals, new technology is needed for next-generation Internet servers and networks.

Trust and confidence

Cryptographic hardware on a server must fulfil two main functions:

1. It should ensure secure and trusted key

management. This cannot be achieved currently with general-purpose central processing units (CPUs), which lack built-in features such as tamper response mechanisms, critical data path insulation and separate buses for different data types. Although such facilities are likely to be achievable in future general purpose CPUs, their heat dissipation capabilities will not be compatible with the design of highly secure cryptographic devices, which are generally encapsulated in poorly dissipating tamper-proof packaging.

2. As the heart of a cryptographic device is its encryption components; these cannot have hidden weaknesses or limitations. This fundamental 'trust and confidence' consideration makes it vital to ensure adequate control over development and production. As various unfortunate events over the past decade have demonstrated, the protection of European IT infrastructures for business, administration (and even national security and defence) cannot be assured if they have to rely on foreign cryptographic technology. Unwanted interventions could have dramatic impact on commercial competitiveness and the safety and privacy of citizens' lives.

The CryptoSoC consortium aims to avert this by introducing a cryptographic system-on-chip (SoC) architecture entirely under the control of European industries. Based on interoperable intellectual property (IP) blocks developed collaboratively by the partners, it will permit the synthesis of various components offering precisely the features required for different types of target equipment.

The focus is on providing very high performance – for example, allowing the creation of large scale public key infrastructures (PKIs) and networks running at terabytes per second – plus very high levels of trusted security, made possible by a common criteria evaluation and certification.

Participants in this MEDEA+ project, co-ordinated by leading cryptographic device supplier Bull, cover the technological and market spectrum from basic research institutions to silicon and systems manufacturers. Horizontal co-operation and dissemination, notably cross licensing of IP blocks, will be instrumental in establishing a viable European SoC architecture for tomorrow's security components. CryptoSoC is complementary to the MEDEA+ EsPass-IS smart card project aimed at developing a secure access platform for commercial services.

Ambitious project

The principal goals of CryptoSoC are to:

- Perform a user survey to assess the evolution of the server market in terms of quantity and types of application. In particular, this will evaluate the level of security needed by future applications exploiting Internet and high-speed network equipment. It will measure the impact of ongoing trends that are reshaping the industry, and allow determination of computational requirements;
- Define a suitable system architecture for implementing the desired security level, based on the findings of the study;
- Examine, specify and develop all the IP building blocks necessary to produce a state-of-the-art cryptographic SoC;
- Provide a measure of flexibility, making the cryptographic component adaptable to different security requirements and evolving standards;
- Use the IP blocks in developing SoC prototypes that include, for example, crypto-wired logic, user-programmable logic, secure storage for keys, tamper-detection and response logic, and very high bandwidth bus interfaces; and
- Produce system demonstrators of CryptoSoC-enabled cryptographic boards for high-speed network equipment (in the Gb/s range) and large e-business/commerce servers (handling over 1,000 Tb/s), and field-test them.

Meeting market requirements

The overall aim of the project is not simply to make a single chip, but rather to develop synthesisable IP blocks of validated architecture, from which cryptographic components adapted to specific market requirements can be produced. Consequently, eventual silicon implementation will not be carried out within the limited timeframe of the project, but rather proceed in line with market demand. Non-inclusion of costly silicon diffusion activities will also eliminate the uncertainties and delays often associated with this phase.

'Smart cards & security', a dedicated MEDEA+ application area, is gaining more and more political importance and enjoying the fundamental support of society, as the majority of people have increasing concerns related to personal safety and to full transparency of data in their personal sphere. Products and services integrating CryptoSoC technology can be expected to appear in the 12 months following the availability of the first field-programmable gate array prototypes resulting from this project, making its benefits quickly visible.

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+ ∑!2365 is the new 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.