

2A502: Trusted secure computing (TSC)

SECURITY

Partners:

Bertin Technologies
 Bull
 CEA-LETI
 Celestica Valencia
 EADS
 Ecole Nationale Supérieure des
 Mines de Saint-Etienne
 FT R&D/Orange
 Fundacion European Software
 Institute
 Gemalto (Axalto SA and Gemplus SA)
 Philips AT
 STMicroelectronics
 TB-Security
 TB-Solutions Technologies Software
 Technikon
 Uni Paris VI (LIP 6)

Project leader:

Jean-Pierre Tual,
 Gemalto (Axalto SA)

Key project dates:

Start: September 2006
 End: December 2009

Countries involved:

Austria
 France
 The Netherlands
 Spain

The MEDEA+ 2A502 TSC project aims to develop a family of silicon hardware components and embedded software to ensure secure and trusted computing in the consumer, computer, telecommunications and wireless areas. It also intends to develop trusted concept and architecture elements that will be usable in other European industrial segments such as the automotive, industrial and aerospace sectors – especially in content acquisition, payment, ticketing and digital rights management aspects. Finally, this MEDEA+ project will develop a European alternative to US-initiated initiatives related to trusted-computing standards while keeping interoperability with existing US and Asian approaches.

Computing systems and devices in industrial, automotive, information technology (IT), aerospace and wireless environments are vulnerable to outside attack or interception, even when protected by internal and external security measures. Current security methods have varying degrees of penetrability as they are mostly based on *ad-hoc* software layers not necessarily directly connected to the protection of critical assets commanding the bootstrap and initialisation of the platform.

There is a need therefore to develop embedded silicon components with a trusted level of security that will be impervious to attack, so providing an impenetrable screen while maintaining interoperability with legitimate external services.

Why trusted computing?

Current security and privacy methods are based on specific add-on software layers or especially-protected hardware. In either case, security and privacy are treated as external to the system. This has worked reasonably well but there is a fundamental problem with this approach: malicious users or code can circumvent security fea-

tures relatively easily since their foundation is insecure.

The MEDEA+ 2A502 TSC project is taking a new approach, following the concepts initiated by the Trusted Computing Group (TCG), based on low-level layer security and integrity protection. This means that protection mechanisms are present in the basic hardware as well as in the basic input/output system (BIOS) and the operating system.

This new design principle will not only apply to traditional IT devices such as servers or personal computers (PCs) but also to all of the new generation of personal devices connected to packet networks – such as personal digital assistants, mobile handsets, Internet service set-top boxes and personal video recorders.

Security and privacy need to be integrated instead of being added in an *ad hoc* manner. Software on its own cannot provide the trust necessary to match technological progress and the threats that come with it. An operating system cannot counter the threat of unauthorised software mounting an attack before the operating system itself has taken control. The starting point of trusted computing must be an integral

2A502: Trusted secure computing (TSC)

component that can be trusted and cannot be modified. Such trusted processor modules (TPMs) can then ensure other devices in the system can be trusted. Coupled with external user authentication such as smart cards or secure tokens, TPMs can provide a high level of trust in platform and user management.

What is a trusted device?

Functionally, a trusted device must check platform integrity and protect privacy attributes and credentials of users and stakeholders by ensuring a high level of tamper resistance and not allowing any information disclosure when communicating with the outside world. It should provide a specific level of user interaction and control, and refuse to perform any activities imposed by unauthorised third parties.

Such a trusted device should minimise the risk of identity theft, information leakage, data destruction, sensitive data loss or illegal access to corporate or private networks. In short, a trusted security device has to provide critical infrastructure protection and survivability.

However, there are some additional fundamental conditions which must be met to enable the stakeholders of a system to become fully confident with its use:

- *Full control of critical technology* – No EU organisation or group of users will trust a system in which critical parts are made completely by US or Asian companies, sometimes with a monopolistic position;
- *Full-system approach* – The overall security level of a system is no higher than its weakest part. Development of trusted

components has to take security of the complete system into account; and

- *Evaluation and certification by independent third parties* – Security by invisibility is no longer valid in a highly networked and technological world. Security and the trust level of critical components must be proven and certified by independent bodies with the credibility and expertise to assess robustness of critical components against potential threats.

So the TSC project will also address these three fundamental conditions.

Reducing US dependency

The hardware and embedded software components developed in TSC, coupled with home-made trusted operating systems, will enable European administrations and enterprises to reduce dependency on US companies such as Intel, AMD and Microsoft in critical IT infrastructure components, so regaining sovereignty. It will also minimise exposure to the current high level of fraud from Internet piracy. Such piracy is also starting to reach disquieting levels in mobile and multimedia networks with music and video piracy, pay TV hacking, etc.

In addition, the results of TSC will provide a higher level of protection against business intelligence attacks and offer a greater degree of security for sensitive data such as, intellectual property and business accounting – SOX spreadsheet or international financial reporting standards (IFRS) files for example.

This MEDEA+ project will therefore ensure competitive power in European industry sectors covering open servers and PCs, mobile chipset providers, smart cards and

trusted personal devices, consumer electronics and professional mobile radio communications.

High market demand for servers and client platforms based on open-source operating systems together with the stable *de facto* specifications issued by the TCG for TPMs has already driven US industry to develop fully-featured trusted computing platforms. The MEDEA+ TSC project – and companion software projects such as PFC (France), EMNSCB (Germany) and OpenTC (FP6) – will ensure Europe has the technologies required to build an independent alternative to full US offers.

One particular innovation is expected in the development of a European generation of TPMs coupled with advanced smart-card technology and open-source software kernels that will make it possible to manage simultaneously trusted computing, user identification and privacy concerns. Specific effort will also be allocated to the infrastructure aspects of such components.

The result overall will be better integration of security features in sensitive products and infrastructures, better security practices and acceptance among integrators and end users, and better interoperability of security products at all levels of product design – not only in the computer area, but also in new mobile and consumer platforms. Success will be similar to that obtained by smart-card technologies in everyday life, with for example a better trust in and use of electronic payment means, a gain of activities and competencies in security and a strong enabler for the development of value-added services over mobile or multimedia home networks.



MEDEA+ Office
140bis, Rue de Rennes
F-75006 Paris
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.