ITEA
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

PROJECT RESULTS

A Trusted, European Security Infrastructure

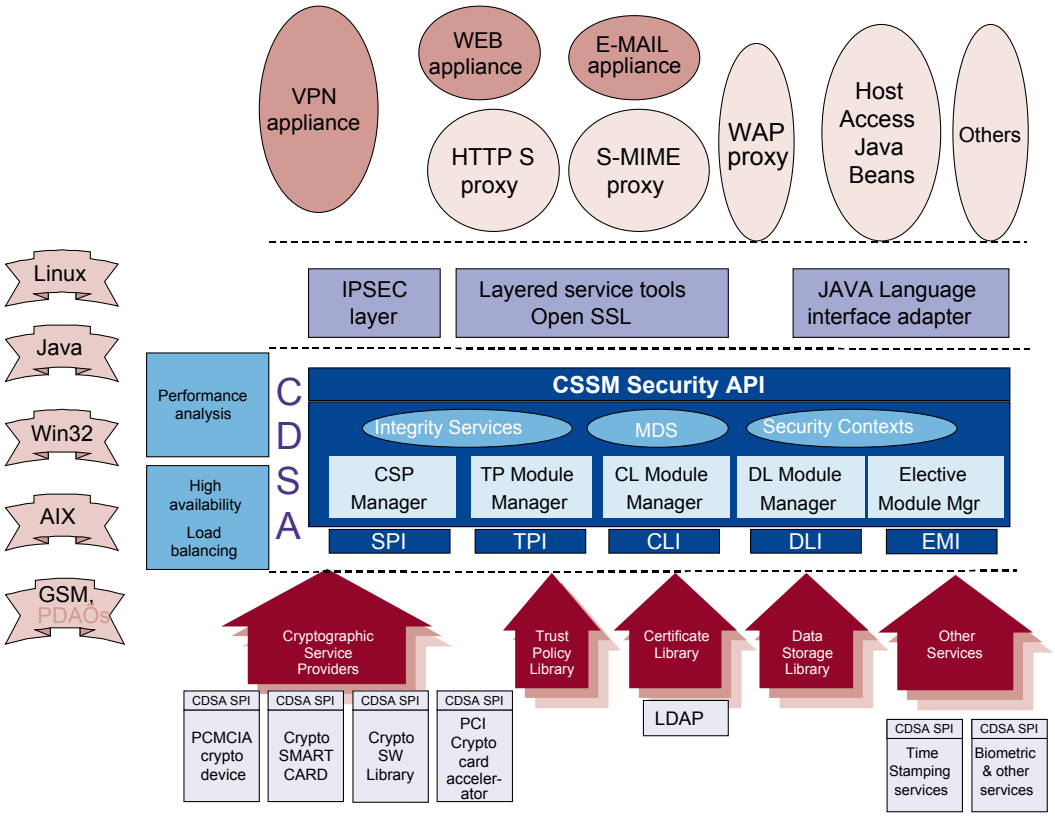
The aim of TESI was to develop an open security software architecture with inter-operable, pluggable security components. The project has created a commonly accepted and trusted 'de facto' standard development environment for Europe's security software industry.

The need for reliable European security software

Electronic commerce and exchanges are fundamental tools for businesses and governments alike. They have a huge impact on the economy and on society. A secure IT infrastructure is therefore essential for Europe, both to protect corporations and public administrations against unauthorised access to the data on their information systems, and to protect citizens' privacy.

Infiltration of Internet-based Information Systems (IS) presents a serious challenge to government departments and companies. European parliamentary reports on 'Communication Intelligence in 2000' published in 1997 *[GFR]* and 1999 *[DC]* reveal the potential impact of 'cyber war' on business competitiveness and privacy. They recommend using highly reliable cryptography-based systems to protect European IS.

Due to the current lack of such a European platform, the security of critical IT-based infrastructures for business, communication, finance, distribution, energy and transportation cannot be reliably guaranteed. The risk of this precipitating a major crisis cannot be discounted.



TESI (ITEA 99037)

Partners
Amtec
Bouygues Télécom
Bull
Ercom
Flextel
I & T
i2e Telecom
Politecnico di Torino
Q-Labs
Simulog
Sistech
Utimaco

Countries involved
Belgium
France
Italy

Start of the project
February 2000

End of the project
June 2003

ITEA

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

PROJECT RESULTS

A European security platform
TESI has built a complete security infrastructure with a set of reliable middleware security components, that is:

- entirely designed and managed by European companies
- compliant with relevant IETF standards so that they can be easily integrated into any application by any middleware software vendor
- fully compatible with standard Web server and browser software and e-mail
- based on The Open Group CDSA (Common Data Security Architecture) specification to ensure applicability worldwide.

Innovative solutions have been provided in a number of areas:

- strong modular cryptography (e.g. 3DES) that was 100% developed by a European consortium, guaranteeing users a 100% reliable solution that works with almost any commercial-of-the-shelf (COTS) Internet application, yet without the limitations of currently available US products (key size reduction factor, unwanted key recovery mechanisms, and design flaws).
- Through standard high-level Application Programming Interfaces (APIs), TESI provides the flexibility for application developers to address the security concerns of all major e-commerce and Web-based applications, such as e-mail and Electronic Data Interchange (EDI), virtual private networks and electronic payment systems.
- The solution is open for future third party extensions, thanks to the implementation of the Open Group Common Data Security Architecture (CDSA) framework (with 100% source code control by the consortium) adapted for specific European security requirements.
- The TESI framework is equally suitable for implementation on client and server operating systems.
- European cryptographic algorithm researchers/developers are offered a reliable standards-based environment.
- Research on architecture and protocols to support advanced e-business services such as 'time stamping' and PKI-enabled (Public Key Infrastructures) services in a common framework.
- Advanced research, enabling the TESI infrastructure to be implemented in embedded applications for mobile phones and Personal Digital Assistants (PDAs).

The TESI infrastructure has been made widely available to all European security developers and actively promoted as the 'de facto' European standard security infrastructure and API. It is fully compliant with CDSA and other international Internet standards.

Promoting a common standard
The results of this project have been exploited and disseminated through a variety of channels:

- TESI results now are being used to create new products such as VPNs and Web security systems.
- Components developed in the project have been packaged and distributed as OEM building blocks, enabling the development of fully trusted European security solutions for e-commerce and e-exchange applications at the lowest possible cost and fastest time to market.
- The TESI CDSA core middleware has been 'open sourced' (SourceForge) for the targeted platform, and is thus freely available to both the scientific and industrial community (European IS Vendors, OEMs and developers).
- The high level of awareness of TESI activities among IT security companies has been proved by the successful re-use of TESI components in other ITEA and IST projects.
- A TESI Interest Group has been established.
- The consortium has contributed to standardization activities within the CEN ETSSI W-Sign Working Group.

Major project outcomes

Exploitation

- 5 new products
- 1 new service

ITEA Office
Eindhoven University of Technology Campus
Laplace Building 0.04
PO box 513
5600 MB Eindhoven
The Netherlands
Tel : +31 40 247 5590
Fax : +31 40 247 5595
Email : itea2@itea2.org
Web : www.itea2.org

ITEA - Information Technology for European Advancement - is an eight-year strategic pan-European programme for pre-competitive research and development in embedded and distributed software. Our work has major impact on government, academia and business.

ITEA was established in 1999 as a EUREKA strategic cluster programme. We support coordinated national funding submissions, providing the link between those who provide finance, technology and software engineering. We issue annual Calls for Projects, evaluate projects, and help bring research partners together. We are a prominent player in European software development with more than 5,000 person-years of R&D invested in the programme so far, and another 10,000 anticipated over the next five years.

ITEA-labelled projects build crucial middleware and prepare standards, laying the foundations for the next generation of products, systems, appliances and services. Our projects are industry-driven initiatives, involving complementary R&D from at least two companies in two countries. Our programme is open to partners from large industrial companies, small and medium-sized enterprises (SMEs) as well as public research institutes and universities.

Σ! 2023

October 2003