

Project profile

TOISE

Trusted computing for European embedded systems



In the future, critical applications such as smart grids for electricity networks, smart metering, environmental or infrastructure sensor networks and the management of trusted components will require development and implementation of secure technologies to provide smarter and safer operation. Trusted computing systems used in personal computers and workstations offer a proven security mechanism and could be adaptable for this purpose. The ENIAC JU project TOISE aims to develop such tamper-resistant solutions for embedded applications and boost European leadership in secure integrated devices.

Sub Programme

- Nanoelectronics for energy efficiency
- Nanoelectronics for wireless communications

Malicious behaviour is a minor threat for classical energy distribution networks. Physical or technical attacks result in a relatively small financial loss or minor disruptions in energy supply. The situation is more complex in smart grids. Bi-directional flows of energy and information, and different types of communications interfaces, coupled with other infrastructures, result in new attack vectors. Co-ordinated and distributed attacks are well known from computer networks and now become feasible in energy networks. Such attacks could result in major destabilisation of networks and large financial losses for the different stakeholders.

The ENIAC JU project TOISE aims at reducing the risks through cost-effective and resource-compliant security solutions. TOISE will provide new security building blocks such as monitoring and intrusion tolerance functions suitable for smart grids. It will define, develop and validate trusted hardware and firmware mechanisms that will be applicable both to lightweight embed-

ded devices and as security anchors within related embedded platforms.

Future applications

TOISE will focus on the study and development of secure solutions for future critical applications. These include electricity distribution grids, which will require significant dependence on distributed intelligence and broadband communication capabilities. Smart meters are also needed to control appliances in consumers' homes to reduce consumption. These essential capabilities require the latest in proven security technology for large, wide-area networks.

Another use is in sensor networks for applications such as environmental monitoring, airports and critical site safety, infrastructure monitoring and healthcare. In unsupervised environments, an attacker can easily compromise a network once the characteristics of the sensor devices are known. Security and survivability are, therefore, important for applications using wireless sensor networks.

Wireless-connected devices are another area of concern. These have to deal with two major security issues: protection of content and of personal information. Robust stakeholder segregation, security policy enforcement and isolation of mutual assets are significant challenges in increasingly open computing, with devices that are exposed and vulnerable to new malware, software and hardware attacks on a daily basis. Some of the related security challenges address trusted open platforms and trusted execution environments, identification and authentication procedures and secure storage.

Hardware and firmware

TOISE will study and extend hardware and firmware tamper-resistant device architectures and/or the use of lightweight trusted platform module (TPM) concepts applied to smart grid and smart-meter environments. It will also investigate anti-counterfeiting architectures and implementations for communications, wireless networks and the management of trusted devices.

There are three key objectives:

1. Energy efficiency – investigating and implementing secure solutions for the design of smart-grid applications and their deployment in large-scale networks and systems. These solutions will be based on hardware trust anchors in devices located in unsupervised environments and will use advanced trust establishment mechanisms.
2. Security of communications – investigating and implementing

secure wireless sensor networks, addressing secure authentication devices, studying and implementing a new generation of trusted portable devices as well as securing storage in memory, and studying secure hardware items by adding TPMs for embedded systems. Proposed solutions will target both lightweight low footprint secure devices and trusted anchors with complex system-on-chip (SoC) platforms.

3. A new generation of tokens that will demonstrate optimal cost through full SoC integration, enforced privacy management with new authentication interfaces, secure channel establishment with TPMs for secret secure updates and the management of various entities.

Common position

A substantial initiative is proposed to align a common European position in the domain of secure systems and devices. Several TOISE partners are already involved in related standardisation working groups and their work in parallel with TOISE will encourage the development and promotion of European solutions in conformity with the new standards to be announced.

The successful outcome of TOISE will maintain European manufacturers and peripheral suppliers as worldwide players in the efficient implementation of secure integrated devices. It will also enhance employment opportunities within the European software and hardware environments.

Energy efficiency

Partners:

- Azcom Technology
- CEA-LETI
- EADS Defense and Security Systems
- EADS France Innovation Works
- Gemalto
- Hellenic Aerospace Industry
- Institute of Communication and Computer Systems
- Magillem Design Services
- Numonyx
- Politecnico di Milano
- Proton World International
- Secure-IC
- Spanish High Council for Scientific Research (CSIC)
- STMicroelectronics France
- STMicroelectronics Italy
- Tecnologías Servicios Telemáticos y Sistemas
- Telecom ParisTech
- Thales
- University of Cantabria
- University of Milano-Bicocca

Project co-ordinator:

- Bernard Candaele, Thales

Key project dates:

- Start: January 2011
- Finish: December 2013

Countries involved:

- Belgium
- France
- Greece
- Italy
- Spain

Total budget:

- €21.7 million

Details correct at time of print but subject to possible change. Updates will be included in the project summary at the end of the project.



The ENIAC Joint Undertaking, set up in February 2008, co-ordinates European nanoelectronics research activities through competitive calls for proposals. It takes public-private partnerships to the next level, bringing together the ENIAC member states, the European Commission and AENEAS, the association of R&D actors in this field, to foster growth and reinforce sustainable European competitiveness.