

## Project profile

# SMART

## *Secure memories and applications-related technologies*



Growth in digital multimedia and in wired and wireless Internet-based services focuses attention on the need for protection of personal data and identification. Various electronic certification devices have been used – from magnetic-strip cards to increasingly sophisticated smart cards. Convergence of applications such as personal or private data, connectivity and multimedia requires high performance, large storage capacity, rapid data transfer and extended security against fraud. The ENIAC JU project SMART is developing a new generation of small, portable smart secure devices with enhanced performance.

### Sub Programme

- Nanoelectronics for Security and Safety

The primary objective of the ENIAC JU project SMART is to develop a new generation of smart secure devices (SSDs) which enable the holder to perform trusted operations with other devices connected to the information technology infrastructure. These SSDs have to be reliable and capable of protecting the holder's privacy through the use of authentication and identification protocols, pseudo-anonymity or anonymity of the holder and trusted attestation. The SSD has to protect against the leakage of any information, be tamper resistant against different forms of attack and provide tamper evidence to the holder.

The objective of the project SMART is to define and develop new hardware and firmware technologies for the secure storage and communication of large, multi-form data files. The project will focus on new memory blocks based on the intrinsically safer phase-change memory (PCM) technology rather than conventional non-volatile memory (NVM);

tamper-resistant techniques and authentication/identification mechanisms for remote objects within ambient computing to allow the scaling and optimisation of various applications in new-generation SSDs.

Different forms of SSD are considered as driving applications within SMART. These include new subscriber-identity module (SIM) cards; high capacity secure mass storage modules; smart cards and secure microcontrollers, system on chip. It is expected that those devices will be deployed in personal digital assistants (PDAs), in new ambient computing applications, in government terminals and in related supporting infrastructures.

SMART addresses four challenges:

1. New-generation NVMs with high capacity and secure architecture;
2. Access time and processing improvement;
3. Related cryptography engines with configurable firmware; and
4. Resistance to state-of-the-art attacks.

## Enhanced device capabilities

This new generation of SSDs will represent a substantial improvement in data-storage capability, data-transfer rate and security by comparison with existing devices. However it requires technological innovation in several fields such as memory technology, security mechanisms, low power security features, side attack countermeasures and architecture security. Key characteristics will include:

- Secure storage of larger, multi-form sets of data; efficient, fast and adaptive process cryptography;
- Process-sensor information and authentication/identification of distant objects within ambient computing;
- Integration of secure tokens to support application convergence; and
- Integration of secure middleware supporting virtualisation in line with authentication of running applications and prevention of state-of-the-art attacks.

To satisfy all these basic needs, a new non-volatile PCM technology, well suited to this application domain, will be used, as well as innovations at design and firmware level.

## Advanced technology

Memory technology is probably the most disruptive innovation introduced in this project. Until now, floating-gate flash memory has been the mainstream technology for both embedded NVM in secure devices and large-scale secure memories. While such memory technology offers high integration densities and can rely on a large production and reliability base, it presents drawbacks for spe-

cific applications: memory can only be erased in large blocks, high voltages are required for programming and the programming speed is relatively long – in the order of tens of microseconds.

PCMs are reaching maturity; they now have bit programmability, require only moderate voltages and can be programmed in hundreds of nanoseconds. However, they do not have a long history behind them, have never previously been used in embedded applications and their resistance to tampering has never been investigated.

SMART therefore is developing embedded PCM technology and memory blocks, testing their immunity against tampering, defining programming mechanisms in secure mode and developing hardware and firmware security features that will allow the characteristics of the PCM to be securely exploited when targeting smart secure device applications.

## Maintaining global position

This ENIAC JU project is a combined effort from major European chip-makers, experts in the domain of countermeasures against invasive and side-channel attacks, specialists in the design of secure hardware, a skilled group in the development of secure middleware, a public-key infrastructure company and leaders in the market for secure solutions.

The overall aim is to maintain Europe as a worldwide player in the field of efficient implementation of secure integrated devices with new memory generations targeted at trusted devices and smart secure portable objects.

## Nanoelectronics for Security and Safety

### Partners:

- Aristotle University
- CNES
- Gemalto
- Integrated Systems Development
- MultiCert
- Numonyx
- STMicroelectronics France
- STMicroelectronics Italy
- Teletel
- Thales Communications
- University of Milano-Bicocca
- University of Minho

### Project co-ordinator:

- Giancarlo Forlanini, Numonyx
- Jérôme Quevremont, Thales Communications (technical co-ordination)

### Key project dates:

- Start: January 2010
- Finish: December 2012

### Countries involved:

- France
- Italy
- Greece
- Portugal

### Total budget:

- €15.2 million



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.