MEDEA+

Taking a smart approach to security

EUREKA

Practically rocket science

Smart cards are very much a European success story with their birth almost literally rocket science: German rocket scientist Helmut Gröttrup invented the 'portable memory' concept in 1968 with colleague Jürgen Dethloff — practically at the same time as Japanese scientist Arimura and US engineer John Ellingboe; the patent featuring the close-to-final smart-card concept was filed by Dethloff on 6 June 1976 and was finally approved in 1982. Almost simultaneously, Roland Moreno patented the concept of memory card — 25 March 1974. The first mass use of such cards was in France from 1983 with their adoption for payment in pay phones.

The first microprocessor-equipped smart card was developed by French computer company CII-Honeywell Bull. French engineer Michel Ugon patented the self-programmable one-chip microcomputer (SPOM) that defines the necessary architecture to auto-program the chip on 26 August 1977. And Motorola produced the first chip based on this patent three years later.

Bull sold its smart-card operations to Schlumberger in 2001. Schlumberger combined these operations with its own smart-card department, and then created the independent Axalto spin-off in 2004. In 2006, Axalto — by then the world's number two smart-card manufacturer — merged with world leader Gemplus to form Gemalto, a key player in MEDEA+.

In 1992, microchips were integrated in all French Carte Bleue debit cards — requiring a personal identification number (PIN) before a transaction can be accepted. Europay, MasterCard and Visa (EMV) agreed in 1993 to develop a joint specification for smart cards that could be used as either debit or credit cards. The first EMV specification emerged a year later with a stable release in 1998. Subsequent updates retain compatibility with the 1998 specification. The EMV system is now used widely around the globe, albeit with some exceptions, such as the USA — EMV contactless smart cards are developing there very rapidly. In the mid 1990s, smart-card-based electronic-purse systems also began to emerge in Europe — such as Geldkarte in Germany or Proton in Belgium. Here the value is stored on the card, making it unnecessary to check with an external account — and so avoiding the need for on-line connectivity.

But it was the introduction of smart-card-based SIM cards for mobile phone equipment in the 1990s that led to a major increase in smart-card use. This ever-growing market is still driving smart-card technology today as SIM cards offer access to an ever wider range of services — security, value added and financial under operator control.

Taking a smart approach to security

As smart cards enter a new phase of ubiquitousness with the growing convergence of consumer, information technology and telecommunications worlds, new and compelling applications are starting to emerge that build on the standards and technologies established in MEDEA+ and its predecessor MEDEA programme. By bringing together both the manufacturers and users of smart cards, MEDEA+ has served as a catalyst to preserve and increase European dominance of the global smart-card market. The result has been a direct increase in employment in the electronics industry, greater levels of security by encryption and conservation of digital rights and personal data, and higher levels of citizen comfort and welfare.

Smart cards — also called chip or integrated-circuit cards — are credit-card or subscriber identity module (SIM)-sized plastic cards with embedded electronic circuitry that are now the most widely found computing device worldwide. There are two main types: memory cards, incorporating non-volatile storage and sometimes specific security logic; and microprocessor cards — now by far the majority — containing non-volatile memory, specialised analogue and digital blocks, and of course highly cryptographically secured microprocessors.

Key element in our lives

Developed originally in Europe — see opposite page — and still dominated globally by European companies, smart cards have become a key element in our everyday lives. We use them for:

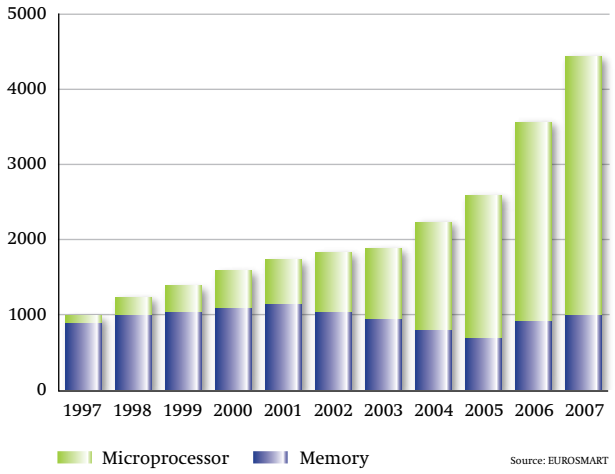
- Controlling our financial transactions, providing much higher security than magnetic stripes;
- Protecting and enabling telecommunications through the SIM cards in our digital mobile phones that provide access to GSM/3G/WiFi networks worldwide and to a fast-growing range of value-added services from information kiosks to mobile multimedia;
- Faster and simpler subscription and payment of everyday travel, particularly with the development of contactless smart cards that mean we do not even need to stop as we dash for the train;
- Storage and protection of our medical data and easier access to care in the health sector;
- Ever greater corporate security in the workplace; and, increasingly,
- Private storage of personal authentication data such as biometric templates and other data to prove our identity for public sector applications such as electronic passports, driving licences and city-life cards, providing simpler and interoperable access to public information, healthcare and government services within individual countries and even across borders.

As both system users and owners, we all have assets to protect, be it our personal identities, our money, our privacy, our intellectual property, our commercial income from added-value services or state security. Therefore access and proof of identity are crucial — and the more valuable the asset, the higher the level of security that is required. At the same time, in an increasingly connected world, access should be as simple as possible without the need for multiple log-ins. And there is the overwhelming concern about protection of personal privacy.

Booming market

More than four billion smart cards were forecast to be shipped worldwide in 2007 according to European smart-card association EUROSMART — a fourfold increase over the past decade. Of the four billion, more than 500 million were expected to be secure contactless devices.

Worldwide smart-card shipments



Strong growth was expected in:

- Public service and healthcare applications — up over 50% on 2006 figures, particularly with the growth in e-identity documents;
- Financial services, with a 20% growth, aided by increasing use of EMV cards in Asia Pacific; and
- Telecommunications — with some 2.4 billion cards expected for the mobile communications market alone, an 18% growth year on year.

Global smart-card shipments 2007

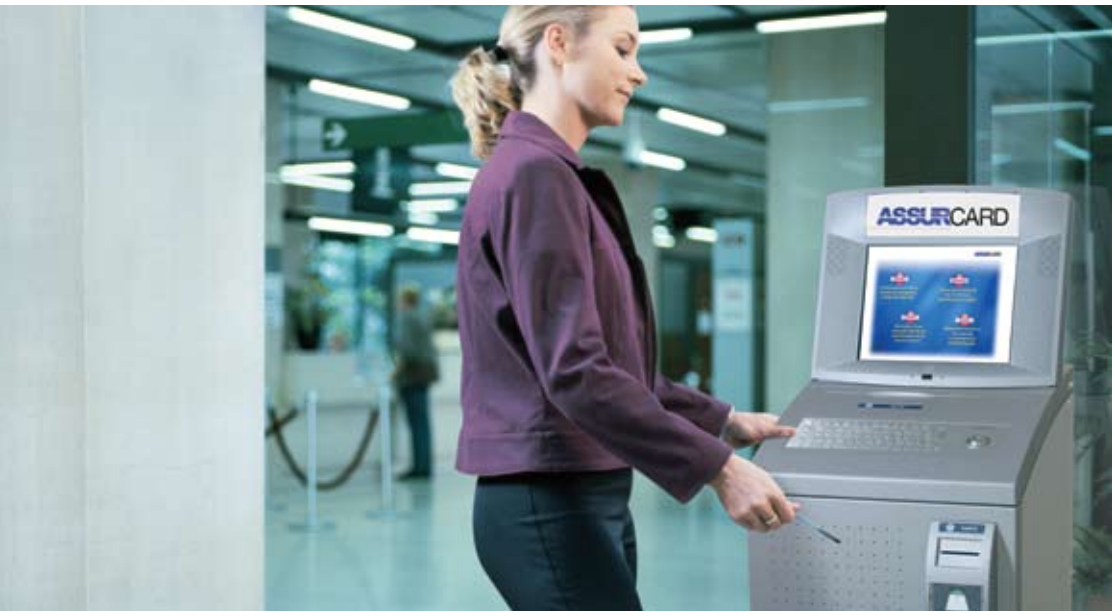
(millions of units)

Segments	Memory	Microprocessors
Telecommunications	440	2650
Financial services/Retail/Loyalty	30	510
Government/Healthcare	300[1]	105
Transport	160[2]	30
Pay TV	-	85
Others (incl. corporate security)	80	65
Total	**1010**	**3445**

Source: EUROSMART

[1] Includes 250 million Chinese national ID cards

[2] Does not include one-time trip tickets



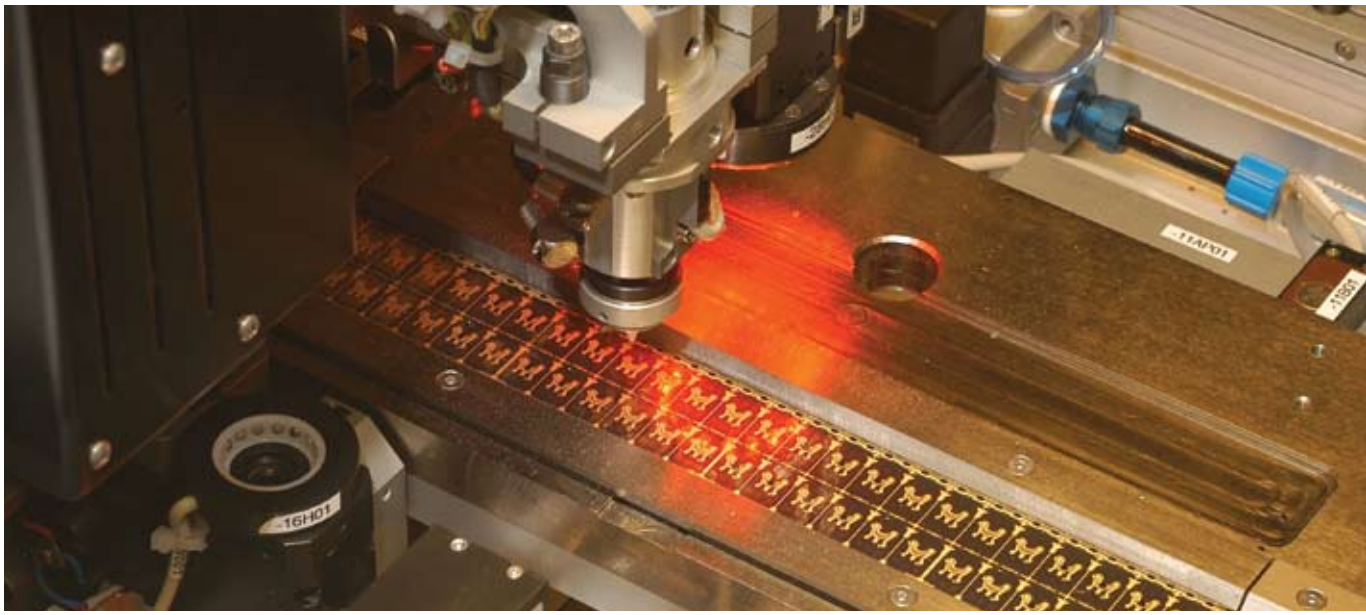
Leading edge of security

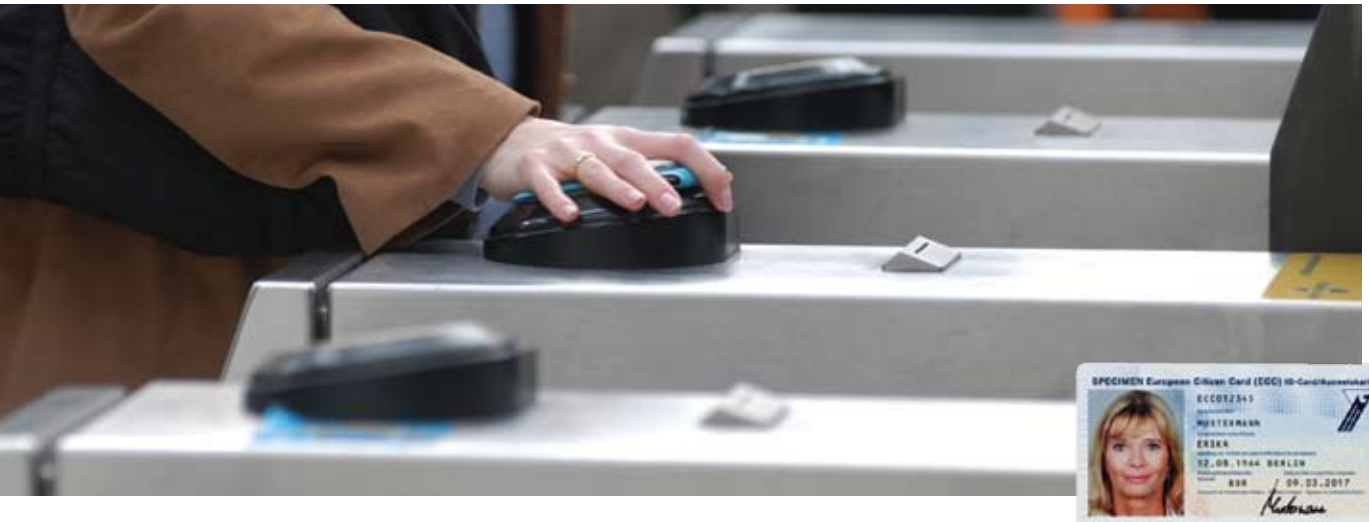
MEDEA+ has been instrumental in keeping Europe at the leading edge of security systems through the use of smart cards. EUREKA Clusters first made their mark on smart-card development in the multi-application secure smart cards (MASSC) project that ended in 2000, The MASSC project ran in MEDEA — the predecessor programme to MEDEA+ — and resulted in a system-on-a-chip card platform using an open architecture that provided a baseline for security mechanisms and led to standardisation. The success of the project served as a launching pad for much further industry co-operation.

Three smart-card projects featured in the first phase of MEDEA+: enhanced smart-card platform for accessing securely services of the information society (EsP@ss-IS); cryptographic system on a chip (CryptoSoC); and technology responses to ubiquitous security threats for e-security (TRUST-eS).

In 2002, the volume of e-commerce in the EU was estimated to be worth €30 billion, of which €20 billion was paid using card-based products. The MEDEA+ A302 EsP@ss-IS project set out to meet increasing concerns about the security of financial transactions over the Internet with the continuing rise in electronic and mobile commerce. It involved the whole value chain from chip manufacture to content provision and network operation.

The project laid the foundation for the successful development of the open smart-card hardware and software platforms required. The protection provided fostered a fast growth in value-added services in mobile telecommunications, banking and pay TV. Open standards and the definition of core building blocks consolidated the strength of Europe's competitive position in this technology growth area.





Cryptographic protection

Internet security was also the focus of the MEDEA+ A304 CryptoSoC project. Safeguarding stored data against increasingly sophisticated threats is crucial to public administrations, industry, commerce and citizens alike. Access control, electronic signatures and the confidentiality of proprietary information all depend on cryptographic protection.

With most systems interconnected either directly or indirectly via the Internet, reliance on software-based methods was seen as no longer adequate. Hardware methods existed but the hardware cryptographic market had long been dominated by the USA. CryptoSoC focused on very high performance approaches, capable of supporting large scale public key infrastructure (PKI) and key tetrabyte/s class networks.

The project developed interoperable hardware components that enable Europe to assemble its own system-on-chip devices providing improved security and generating business opportunities worldwide. High-level trusted security is guaranteed by an internationally recognised Common Criteria evaluation and certification. TRUST-eS was a somewhat parallel project. Europe led development of smart cards into complex media able to store, compute and securely manage multiple applications.

Global terrorist activities have now driven governments, national authorities and large companies to consider cards and other options to upgrade security.

Conventional identity verification — such as passwords and PINs — are easily compromised. Combining these approaches with biometrics offers a particularly reliable method of determining individuals' identities — iris and fingerprint scanning are considered as the most reliable authentication. The MEDEA+ A306 TRUST-eS project targeted authentication technologies addressing multimode identification with smart-card-based biometrics.

Piling on the functions

Phase two of MEDEA+ saw the emergence of the smart cards systems for secure applications (Onom@Topic+) project. The MEDEA+ 2A302 Onom@Topic+ project brought together two original ideas to develop a European smart-card platform for citizenship and mobile multimedia applications. A basic premise was that – with the enormous capabilities of silicon integration – chipmakers, embedded software developers and systems integrators could pile up functions on the card itself and simplify interoperability by carrying out complex tasks not possible previously.

The primary goal was to develop complete hardware and embedded software platforms that would enable industrial and governmental operators, terminal and smart-card companies, silicon vendors and citizens to take full advantage of the enormous potential offered by the development of fixed or mobile e-services. These services included EU citizen identity cards and mobile multimedia applications providing added value for both user and network operator.

Key developments in the citizenship subproject included card-embedded and middleware-oriented functions that make possible deployment of next generation European citizenship cards as well as preparing future interoperability between European and worldwide identity projects. As a result, citizens will be able to carry a smart card that provides access to healthcare, administrative and governmental services in other countries as the card will be recognised and mechanisms interoperable. These cards should also be able to incorporate private services such as banking and information.

The objective for mobile multimedia was to push the capabilities of existing SIM cards and mobile terminals to handle much more multimedia, while fully protecting digital rights and payments for services. This involved firstly a new generation of SIM cards supporting very high speed connectivity with the mobile terminal using the USB technology standard in personal computers. The project also developed a new standard for the SIM card using near field communication (NFC) technology for proximity contactless interfaces — it is only necessary to touch devices to enable an information flow between them.

A second major innovation was in memory. By using clever packaging technologies, side-by-side or stacking technologies and a new generation of software, the project managed to increase memory from the current hundreds of kilobytes to hundreds of megabytes or even gigabytes. As a result it is now also possible for the SIM card to act like an Internet node, using a standard connection with the mobile handset to visualise the content of the SIM card.

Onom@Topic+ resulted in three major contributions to world standards: an interoperable e-identity smart-card platform with a standard middleware architecture, compatible with projects in the major European countries and with the US-backed ISO standard was proposed to and endorsed by the CEN — building the so-called European Citizen card norm; development of a high speed/low-power interface between SIM card and mobile terminal for mobile multimedia; and development of a single-wire protocol (SWP) enabling contactless data exchange between SIM card and an NFC module — now both accepted as ETSI/3GPP standards.

Not out for the count

Providing all the connections required for the new functionalities — particularly simultaneous use of both USB and NFC interfaces — while ensuring a high level of security required clever use of the fixed standard pin count in the standard SIM card package. Efficient use had to be made of the eight pins available: five for the ISO-standard connections between handset and card, two for USB and the last for contactless management thanks to the clever SWP full-duplex protocol.

Advanced electronic identities

Two projects were intended to increase the functionality and reliability of smart-card technology: the first is developing secure access to public services through the biometric platform for next generation contact-less IAS (BioP@ss) project, while the second is working on secure and trusted computing in the consumer, computer, telecommunications and wireless areas with the trusted secure computing (TSC) project.

The MEDEA+ 2A303 BioP@ass project is targeting the development of advanced secure and interoperable smart-card platforms based on microelectronics and embedded software for all e-administrative applications requested at European level — e-identity, e-health, driving licenses, etc. It is building on the results of the Onom@Topic+ project — especially with reuse of the open middleware architecture proposed by the consortium partners and currently under final approval by CEN and ISO standardisation committees.

The prime applications are:

1 Electronic identity cards fully compatible with the European Citizenship Card (ECC) family of standards currently being finalised at the CEN; and

2 The next generation of electronic passports complying with EU and International Civil Aviation Organisation (ICAO) requirements that should come in force by the end of 2009.

The European Citizenship Card combines the benefits of standardisation with the required flexibility to adapt to national requirements by introducing individual ECC profiles.

A specific goal of the BioP@ss project will be to ensure that all solution components generated in the project comply with the ECC profiles that represent the French and the German implementation of the electronic ID card. It is nevertheless expected that the project application fields could cover other areas such as electronic health, electronic voting or electronic driving licenses.

Several new key technology elements are envisaged:

- Power-optimised contactless chips to improve transaction speeds — a serious issue in airport or seaports where queue management is a prime concern;
- Full 'match-on-card' biometric techniques targeting better privacy management and improved interoperability of infrastructure components — i.e. the card, and not the terminal, is processing the biometric data;
- Definition and standardisation of a single more than 1Mb/s contactless interface — potentially up to 5 Mb/s;
- Support of NFC technology to enable better simultaneous support of government and private services; and
- New cryptographic blocks supporting the recommended extended access control (EAC) policy for the next generation EU passport that includes several advanced match-on-card biometric techniques — such as fingerprint, facial or iris recognition. Implementation of this new security scheme together with advanced cryptographic schemes -such as elliptic curves — for the second generation of e-passports is a global first and requires a significant amount of co-ordinated work from all EU members.

At the same time, software-embedded privacy techniques are being developed to provide users or citizens with a reasonable level of control over their private data when dealing with administrations.

Applications targeted by BioP@ss will have large economic, social and technical impacts and are forecast to represent a huge part of the complete smart-card market by 2009 to 2012. They share some stringent needs in terms of security and interoperability at European — electronic ID, driving licenses, health service cards — and international, ICAO travel documents, levels.

Success in this project will speed the availability of a European information society, beneficial to public authorities, citizens and the main technology actors supplying the public sector. And the concepts are exportable outside Europe, as already demonstrated by the convergence between CEN and ISO in these fields. The USA is already using European technology in this area.

Trusted processor modules

Software on its own cannot provide the trustworthiness needed to keep up with technological progress and the possibilities and threats that come with it. Therefore, the starting point of trusted computing must be a device that can be trusted and cannot be modified. Known under the generic name of trusted processor module (TPM), this device can then ensure that other devices in the system can be trusted.

This approach is based on low-level security and integrity protection, which means that protection and detection — such as hash or signatures — mechanisms must be present in the basic hardware as well as in the basic input/output system and in the lower layers of operating system. This design principle will not only apply, with some variations, to traditional IT devices such as servers or PCs, but also to all the new generation of personal devices connected to packet networks — including personal digital assistants (PDAs), mobile handsets, IP set-top boxes, storage devices, network components and personal video recorders (PVRs).

Fully integrated security

Most current methods of protecting computers rely on software solutions. But this is no longer sufficient. The MEDEA+ 2A502 TSC project takes the concept of security even further with the concept of trusted computing. TSC starts from the premise that security and privacy need to be integrated in a system from the beginning instead of being added on top of it in an *ad hoc* way. The international US-led Trusted Computing Group (TCG) promotes a standard for a 'more secure' platform like a PC or mobile phones. This result in strategic requirements and issues for the further development of 'European-made' security technology that generate a lot of political and sovereignty issues — such as the transparency of processing of personal data enshrined in the EU data protection directive over IT infrastructure of private, enterprise and government customers.

TSC is providing answers to these potential concerns by capitalising on key EU-originated technologies such as smart cards — or secure USB tokens — and open-source software. It is developing a family of hardware/embedded software silicon components that enforce secure and trusted computing in the consumer, computer, telecommunications and wireless areas. It is also working on trust concepts and architecture elements usable in other European industrial segments such as automotive, industrial and aeronautics — especially in their content acquisition, protection and payment, subscription and rights management aspects.

The components developed in TSC will enable European administrations and enterprises to:

- Minimise their current dependency on US companies in critical IT infrastructure components, hence regaining sovereignty;
- Minimise their exposure to the current high level of fraud coming from Internet piracy — such as music and video piracy, pay TV hacking and identity spoofing;
- Offer higher levels of protection against business intelligence attacks; and
- Offer higher levels of protection for sensitive data: such as intellectual property or business accounting.

One particular innovation is expected in the development of a new European generation of trusted platform modules (TPMs) – the basic trusted hardware devices – for IT, mobile and consumer applications coupled with advanced smart-card/secure-token technology and open-source software kernels that will make it possible to manage simultaneously trusted computing, user identification and privacy concerns.

Vision 2020

The EUROSMART vision for 2020 is for 20 billion smart cards with 4 billion mobile phone users, and 4 billion e-identity documents in circulation. The smart cards would be using advanced technologies in 45 or 32 nm silicon processes and offer highly secure, tamper-resistant and citizen-friendly solutions. Smart cards will be a key focus in CATRENE, the successor to the MEDEA+ programme, where they feature in the security lead project segment. They will also be a focus of co-operation with other relevant EUREKA Clusters such as ITEA2 that deals with embedded software and CELTIC, concentrating on telecommunications.

CATRENE
Cluster for Application and Technology Research in Europe on NanoElectronics

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

EUREKA Σ!

MEDEA+ ∑!2365 (2001 to 2008) was the industry-driven pan-European programme for advanced co-operative R&D in microelectronics. Its aim was to make Europe the global leader in systems innovation on silicon. Some 90 projects were labelled, covering challenges in microelectronics applications and enabling technologies, and involving 2500 scientists and engineers annually from 23 European countries. The more than 600 partners included major microelectronics manufacturers, systems houses, SMEs, universities and institutes.