RESET Roadmap 5.0

Roadmap for European research on
Smartcard rElated Technologies

Project Deliverable Ref.: D5

Deliverable Title: "Final Roadmap"

Date of Preparation: 15 May 2003

Version: 5.0

Status: Final

Dissemination Level: Public

Table of Contents

1 EXECUTIVE SUMMARY

The objective of RESET (Roadmap for European research on Smartcard related Technologies) is to investigate the RTD needs corresponding to current and expected future technology gaps, identified by the industry and resulting from market and product trends foreseen by smart card industrial players. The goal of this initiative is to describe current and future RTD challenges and deliver roadmaps for RTD on secure devices and platforms, relevant for European RTD programmes beyond FP5 and for national and international RTD programmes.

Smart cards are key components addressing security needs in a number of well established consumer applications. Although the smart card industry is currently experiencing a decreased development rate - mainly resulting from the global slow down of ICT markets and in particular mobile phone markets - experts are convinced that there is still an enormous potential for smart card deployment in traditional, and new application areas.

Traditional high-volume applications include banking, telecom, pay-TV, etc. (see also section 3). There is still a strong need for innovation to address the requirements of those applications to overcome existing limitations and anticipated evolving environments. But an even higher potential for smart card technology applications is expected from upcoming ubiquitous computing and ambient intelligence environments. These environments create a need for "handy" personal keys that can provide the required level of trust and confidence to users in networked applications. Current smart card technology has an advance over other solutions to address these needs - however some of the existing technology limitations should be overcome to enable the integration of smart card technology-based personal devices as integral components of networked applications.

In order to establish a suitable roadmap, the RESET project had to take into account a specificity of smart card systems, which is to integrate a wide range of technologies. The investigation to be carried out has therefore been divided in 6 main technology areas, each of them covered by one expert working group:

WG1: Communication and networking

WG2: Systems and S/W

WG3: Smart card accepting devices, interfaces and biometry

WG4: Card embedded peripherals, subsystems and micro-systems

WG5: High-end cryptography, tamper-proof and security technologies

WG6: Micro-electronics

The investigation of the working groups was carried out following a common framework which included the following topics:

- State of the art: existing and emerging technologies, their limitations, competing technologies
- On-going research: inside and outside the smart card world
- Evaluation of technology and marketing requirements: evolution of the smart card technologies in information / communication / transaction systems, scientific and technical challenges, market requirements, etc.
- Research orientations for improvement: short / medium and long term

Furthermore, each of the WGs was invited to come up with a research roadmap for its specific domain as contribution to the global roadmap. Finally, following the process of gathering and consolidating R&D needs in each domain, the participants to the WGs were invited to think of scenarios for collaborative RTD project that could answer these needs with a perspective to reach a real impact in smart card technology within a timeframe of 5-6 years from now.

The results of this investigation and consultation process are presented in this report. It starts from a short description of the socio-economic context that influences the development and deployment of smart card applications. Then a summary of the main outcomes of the 6 working groups is introduced. As the complete material prepared by the WGs is too large to be integrated in this report, result of their investigations and discussion is available in the form of material resulting from dedicated workshops or self-standing consolidated reports that can be read for a more in-depth understanding of each of the 6 mentioned technology domains.

Section 5 of the roadmap summarises the main driving and blocking factors that condition the evolution of smart cards and then identifies the technical challenges that need to be mastered to enable the European smart card technology suppliers to deal with these factors, address anticipated requirements and exploit new market opportunities.

Section 6 contains a summary list of the resulting main R&D targets and RTD programmes and resources that have a capacity to carry out smart card technology related research.

Section 7 contains a table which consolidates the identified main RTD topics in an integrated collaborative research programme that would have the potential to federate a sufficient number of European R&D resources to address these R&D targets.

2 INTRODUCTION

RESET is the first ever made attempt of the European smart card industry and academic stakeholders to assess and introduce technology and marketing priorities, with the view to provide global R&D orientations.

This initiative is reflecting a situation shortly described hereunder, where:

- Smart card industry is facing a new economic environment, where global players of the information society aim at providing technology and systems building blocks upon an integrated way, in order to deliver solutions which fit global market requirements, especially in terms of security and trust
- Global growth rate of traditional smart card markets, especially in the telecom area, is no more at the level of the 90s. This means that companies have to carefully select R&D priorities fitting their business development strategy, in order to optimize use of human and financial resources
- Smart card has yet to improve its performances and features for being fully acknowledged as an element of the new generation networked environments, especially in the IT and consumer domains
- 6th Framework Programme, with new instruments and improved R&D integration, provides a valuable opportunity for helping the smart card industry to better structure its effort towards common technology excellence achievements by a coordinated joint RTD effort

Smart card industry has therefore to identify and address major challenges of the global information and communication society, such as:

- Improved interconnection with IT infrastructures, specifically in the context of the new generation Internet, for enhanced access to trusted e-services
- Evolution towards extended open HW and SW platforms, addressing requirements for secure, interactive and personal devices
- Overtaking of current technology bottlenecks, through provisioning of technical features required by rapidly evolving systems and networks environments. Main expected improvements are faster data communication, extended and manageable memory capacity, secure co-design of elements integrated in the value-chain (µcontrollers, crypto algorithms, multi-tasking OS,…), embedding of new components for security (sensors), energy (power supply), user convenience (display), etc.
- Implementation of standard architectures, supporting open OS, multi-application schemes management, interface bus, etc.
- Extended cooperation in test suites implementation and security certification procedures

In this context, RESET roadmap deliverable is aiming at:

- Accurately identifying the **common priorities** of the smart card industry, in terms of technology improvement and marketing requirements
- Being of a highly manageable instrument, acknowledged as such by any current or potential player of smart card related activities
- Providing a sound basis for efficient co-operation in R&D programmes, with regards to FP6.

3 SOCIO-ECONOMIC CONTEXT

3.1 CURRENT MARKET CONTEXT

Smart cards offer several basic security services that, in fact, underlie other smart card applications (e-commerce, medical identification, etc.). They allow secure logging to systems and webs, secure signature of electronic documents, encryption and decryption of digital information, etc.

Accessing a network or some information using a smart card provides the parties (users, networks, devices and information) with mutual authentication and trust. On the other hand, in an increasingly on-line environment, where information transactions are performed over an insecure network such as Internet, security is a key issue. In general, the market requires high security products that can be implemented at a low incremental cost.

Smart cards are used in a variety of different applications. Due to the increasing computing power of processors embedded in cards, more and more security-related actions are performed by means of the smart card itself. Use of high-end-cryptography (assuring high security) can result in relatively high execution times of encryption and decryption processes. The market needs high performance of the smart card applications including short calculation times for the cryptographic procedures.

The implementation of new and enhanced security technologies should not increase the price of the smart card products. Elegant ways for developing and implementing new security technologies in a cost-efficient manner are sought.

Europe is still the main marketplace for smart cards, from supply and demand standpoint. However, global growth rate for µprocessor cards is faster in Asia, with special notice to inland China, and in South America for memory cards, with special notice to Mexico.

Smart card industry is currently experiencing significant evolution as regards business. The telecom sector, which remains the first revenue generator for smart card-based solutions, is facing since 2001 a heavy reduction in rate of increase, due to market saturation.

Meanwhile, the financial sector is meeting a steady though regular 15 to 20% yearly growth rate, mainly due to the EMV roll-out.

Finally, the so-called emerging markets, which have been termed as such for many years, are now offering real business opportunities, through government ID and public transports projects.

Table 1. Smart card market. Millions of units shipped per year per sector, world-wide

(Source: Eurosmart, November 2002)

	Year 1998	Year 1999	Year 2000	Year 2001	Year 2005 (forecast)
Telecom	930	1 113	1 390	1 440	2 750
Pay TV	25	30	20	25	80
Banking	73	108	120	142	150
Loyalty	-	-	-	48	40
Transport	16	44	13	35	210
Healthcare ID	35	58	27	32	160
Internet ID	-	-	5	5	150
ID	-	-	-	-	200
Others	75	77	28	24	70
TOTAL	**1154**	**1429**	**1603**	**1751**	**3810**

Table 2. Memory and microprocessor smart cards market in 2002

in millions of units, world-wide (Source: Eurosmart, April 2003)

Sector	Card (Mu)	
	Memory	Microprocessor
Telecom	950	430
Financial Services / Retail - Loyalty	23	175
Government / Healthcare	30	32
Transport	60	15
Pay TV	0	35
IT / Security	9	7
Others	13	7
TOTAL	1085	701
TOTAL 2002	**1786**	

Table 3. Smart card market by geographical areas. Millions of units (memory & µprocessor cards) shipped per year per region (Source: Eurosmart)

	Year 1999	Year 2000	Year 2001
Europe & ME	903 (63%)	888 (55%)	786 (45%)
Asia & Pac	262 (18%)	424 (26%)	447 (25%)
America	264 (18%)	291 (18%)	518 (29%)
TOTAL	**1429**	**1603**	**1751**

3.2 MAIN APPLICATION FIELDS

3.2.1 TELECOM

SIM cards for mobile telephony and prepaid public telephone cards are the main outlets for smart cards in telecommunication services.

About 1500 million units of mobile phone and prepaid telephony cards were sold in 2001 (this quantity has steadily increased from the 930 millions of units shipped in 1998). According to Eurosmart's forecast, sales of about 2700 millions of smart cards are expected in 2005 in the telecommunications sector (see Table 1 & 2), with µprocessor SIM cards greatly overtaking memory cards at that time.

In telephone systems, the growth of prepaid telephone cards is expected to drop as mobile phones increase their share of the market. A new market cycle is expected in the telecom area, supported by two major drivers: extended delivery of added-value services and implementation of the next generation wireless networks (GPRS and UMTS).

Telecom operators (telcos) have been very active in provisioning new services to subscribers, and smart card suppliers have compensated to a certain extent price drop by improved-technology products, such as extended EEPROM capacity (from 2 to 64 Kilobytes in 8 years) or open OS platforms for improved added-value services management.

Due to a lack of standards and a fragmented set of technical solutions, m-Commerce has not yet fully reached its target. However, it remains a strong priority for telcos, provisioning services such as Information on Demand (IOD), games and multi-media message services (MMS) supported by new colour-screen handsets, with the view to improving ARPU (average revenue per user).

The churn rate (volatility of subscribers) is still high and could become worse with telephone number portability (same phone number for subscriber, irrespective of the network operator). However, compared with handset, SIM card remains for telcos a valuable tool for optimizing security management (personalisation) and keeping a direct and loyal link to their subscribers.

The 3G revolution, expected in Europe for 2004, should provide the smart card industry with a new cycle of dynamic business, thanks to securely managed (and packaged) third party services to customers.

3.2.2 FINANCIAL SERVICES

The market growth in banking sector is mainly resulting of the conversion of magstripe debit & credit cards to smart cards, for improving trust and security and providing enhanced marketing payment schemes. The major part of worldwide markets has adopted precise deadlines for migration towards international EMV standards for chip-based payment. The value behind deadlines is a shift in liability, for any type of card fraud to whichever party - card issuer or merchant acquirer - which would not accept EMV cards.

Europe is on the front line for this liability transfer application, targeted for January 1st, 2005. However, the pace for migration is very much depending on the situation regarding fraud.

Banks are also exploring the use of high end card products, running either multi-application schemes, or enhanced functions as e-signature. In Central Europe and Turkey for instance, banks are experiencing real differentiation schemes thanks to privileged agreements with a large range of service providers (retail, petrol, airline…), thus offering their customers the possibility to really access services on a frequent and regular basis.

However higher "product mix" is still at a preliminary phase in the banking sector, mainly due to the high level of investment required by the EMV migration (cards, terminals, back-office,…). Real differentiation schemes, as compared with the wireless telecom sector, are still at an investigation stage. The main real multi-application scheme is still the provision of an electronic purse application twinned with a debit/credit function.

3.2.3 IDENTIFICATION

As government, public and private organizations move towards electronic methods of service provision, the need of secure electronic personal identification (ID) becomes more critical. According to this, shipment of about 200 millions of smart cards for personal identification purposes is expected in 2005. At the moment of this writing, a few millions of smart cards are sold yearly for Internet identification purposes. An important market niche is related to health services, for identification and storage of personal insurance and health records.

Every organization (university, company, library, etc.) is a potential consumer of smart cards for identification purposes. Issuing smart cards to employees, students, etc. is becoming widespread as the card is a valid device for multi-application schemes in these closed environments.

Smart cards are a clear identity product. Managing identity information is one of the smart cards' roles in most of the areas which they are used in. Smart card-enabled PKI (public key infrastructure) technology is expected to play a growing role in the implementation of smart card-based network access for enterprise IT systems and the roll-out of national ID card programs. Thus, identification might be considered the next killer application in smart cards industry. Biometrics is likely to be a key issue in smart card based ID applications.

The memory requirements are about from 2KB to 8Kbytes, but larger amounts will be needed in order to accommodate new applications based on identification card usages.

3.2.4 MULTIMEDIA AND PAY-TV

The sales volume related to pay-TV amounts to about 30 millions of units per year. Substantial increase of this figure is expected in the next years, because of the new interactive and Internet television market. For payment TV, microprocessor cards do need to increase memory, in order to store larger keys and be able to participate in interactive TV applications. In pay-TV only microprocessor cards are used.

Digital Asset Protection (DAP) is a type of software developed to enable secure distribution - and perhaps more importantly, to disable illegal distribution - of paid content over the Web. DAP technologies are being developed as a means for fair use of commercially marketed material, in particular in the context of the widespread use of peer-to-peer file exchange programs. Smart cards will play an important role in DAP, in order to meet the requirements needed to protect the interest of copyright holders of multimedia contents, software or large amounts of data.

3.2.5 TRANSPORTATION

There are several uses of smart cards in the transportation sector. For instance: 1) contact smart cards can be used for highway toll payment or parking control; 2) for public transportation, contactless smart cards are being deployed at several cities (the user does not need to physically plug her/his card at the metro station barriers). Replacing magnetic stripe or paper cards by chip cards in a new generation of ticketing systems is a major trend in transportation. The volume of sales related to new ticketing systems is expected to reach 150 millions of units in 2005, to be added to the 20 or 30 millions of smart cards annually sold for other transportation purposes.

In Europe, two programmes are in the spotlight in 2003, Paris and London. Paris mass transit operators (RATP and SNCF) have already issued more than 500 K contactless chip cards and equipped 800 subway stations.

In London, the "prestige" project (Transport for London) should provide access to network for commuters from spring 2003, and within 18 months, 2 to 3 million people are expected to use smart cards.

Rome and Berlin should be the next two European capitals to issue card-based automatic fare collection for their public transport networks.

System integrators of card-based solutions often provide operators with licenses which permit the combination of low-cost systems for short term ticketing schemes, and long-term agreements for implementation of adding added-value services.

3.3 CURRENT FRAMEWORK FOR ACTIVITIES IN THE SMART CARD INDUSTRY

Smart card industry is still under the control of Europe-based companies, which have installed settlements all over the world for product trade and manufacturing, often via joint ventures with local companies. However, due to serious economic factors, such as reduced market growth in mobile telephony which is the first revenue generator for smart card industry, or the slow emergence of new market opportunities such as ID or e-ticketing, the global activity is currently facing, as other fields of electronic industry, high pressure on product cost and profit margin.

This has an impact on financial results of many market players and, in parallel, on the motivation of the investors’ community to support its development.

In this context, smart card industry is considering ***innovation as a key factor*** for preventing evolution towards provisioning of pure "commodity" card products, which are doomed to be manufactured in low labour cost countries.

Re-adjustments are seen in the value-chain, with increased overlaps between components suppliers (IC, card and CAD manufacturers, application/service providers, system integrators), which have begun to extend their business position beyond their current limits. For example, card manufacturers could have their own IC design and architecture development team, and IC manufacturers could go right ahead with IC packaging and micro-module assembly, through existing or new device form factors, memory configurations or protocol implementations (USB, MMC, …).

System-On-Chip design is now providing great deals of embedded SW, thus decreasing cost of ownership for issuers and users and reducing product time to market through enhanced solution interoperability. This could speed industry restructuring through merge & acquisition operations, generating major changes in the smart card supplying chain in the years to come.

3.4 IMPACT OF LEGAL ISSUES AND REGULATIONS, ETC.

With regard to information society requirements, smart card industry has to deliver products and solutions which comply with the legal and regulation framework. Smart card is a key instrument for secure access to network and online services, and for trusted management of user consent in transactions. Therefore, two major regulation domains have to be seriously considered:

- electronic signature
- protection of personal data and privacy management

As far as e-signature is concerned, an enormous amount of new legislation governing the way that companies and consumers do business in electronic environments has been issued worldwide. In this process, the electronic signature has made much progress towards gaining the same legal recognition as its hand-written, paper-based counterpart. Electronic signatures - whatever type - have been accepted as a means to identify e-commerce participants and thus constitute a common approach to identification and authentication in e-commerce.

The European Union has issued a European Electronic Signature Directive, in order to provide a legal framework to guarantee EU-wide recognition of electronic signatures - a prerequisite for ensuring the security of data that is transmitted electronically (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures).

The purpose of the Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a common framework for electronic signatures and certain certification services, in order to harmonise this type of activity in the internal market.

Detailed **technical specification** of the requirements for qualified certificates, certification service providers and secure signature creation devices that are generally provided for in the Annexes will have to be officially endorsed by the **Article 9 Committee** which has been tasked by the Directive to follow the technical developments. Suggestions related to these specifications have been discussed and agreed upon within the scope of the **European Electronic Signature Standardization Initiative (EESSI)**. Proposals for Secure Signature Creation Devices (SSCD), for a general format for Advanced Electronic Signatures, for Qualified Certificate Profiles, for Policies for Certification Providers issuing Qualified Certificates, for Time Stamping Profiles and for Procedures for Electronic Signature Verification have already been published and circulated for comment.

The smart card as a SSCD is more specifically addressing requirements for "advanced" or "qualified" signature, and targeting a great deal of business opportunities in e-Government applications, which most often require the setting of Public Key Infrastructures, for providing trust and confidence over open networks. Compatibility of national legislations and acknowledgement of wireless networks as infrastructures offering the required security mechanisms for such services and applications will be key issues for supporting the position of smart card as a SSCD in the years to come.

Privacy and personal data protection issues have as well a major impact on smart card technology and marketing requirements, as the card is most often holding -and protecting- the identity of users.

Most consumers are extremely reluctant to give out personal information, such as credit card number and expiry date, for fear that it will be intercepted by a third party and fraudulently used.

Again, the European Union has the most advanced regulatory framework as regards data protection. Two European Directives have to be mentioned, as directly relating to the T2R infrastructure:

- Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of Personal Data 95/46/EG adopted 24th October 1995
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

These two directives have been up-dated in 2002.

In most European countries, personal data protection is a constitutional principle and the right to privacy is enshrined in the European Convention on Human Rights (Article 8). However, until now, differences between national data protection laws have resulted in obstacles to transfers of personal data between Member States. Both Directives therefore lay down common rules, to be observed by those who collect, hold or transmit personal data as part of their economic or administrative activities or in the course of the activities of their association.

However whereas the Directive 97/66/EC relates only to data processing by telecommunication service providers, the Directive 95/46/EC holds the general principles for processing of personal data and regulates the transfer of personal data to third countries outside the European Union.

4 TECHNOLOGY CHALLENGES

Smart card related technology challenges are presented hereafter for the 6 main technology areas identified by RESET:

- Communication and networking
- Systems and S/W
- Smart card accepting devices, interfaces and biometry
- Card embedded peripherals, subsystems and micro-systems
- High-end cryptography, tamper-proof and security technologies
- Micro-electronics

4.1 COMMUNICATION AND NETWORKS PROTOCOLS

This chapter addresses the evolution of smart card communication protocols and the integration of smart card in new networks such as wireless home or corporate mobile networks.

Communications relate to physical and logical means that are needed and used by smart card to exchange information with at least a CAD. Usually communication operates with electrical and logical protocols.

Networking means that smart card is able to exchange data with other applicative entities, located somewhere on the network. It belongs to a distributed computing architecture and includes peers identification, as well as how to involve them. Networking uses communication services to work with external application in a peer to peer mode.

Hereinafter three areas for research and improvement of smart card in the domain of "Communication & Networking" are considered:

- Physical link
- Communication protocol
- Integration of smart card in networks.

4.1.1 TECHNOLOGIES TRENDS AND MARKET REQUIREMENTS

Evolution of the smart cards technologies have to be assessed in relation with the evolution of information systems and network infrastructure.

SMART CARDS

From the beginning smart cards were developed on proprietary platforms and mostly used for one single application. One major change, driven by a lack of interoperability between smart card vendors, has been the move to open platform and more precisely Java. Aside from cutting costs and development time, Java is supposed to increase personalization of the service after the smart cards has been issued. This requires an evolution of the communication model for keeping its promise. Unfortunately, smart cards are still using ISO 7816 protocols which are not well suited for solving these new challenges.

INFORMATION SYSTEMS

As far as communication and networking are concerned, the major changes in the IT industry are:

- Internet protocols: TCP/IP everywhere, broadband Internet access, new application models (Web, peer-to-peer)
- High speed peripherals: USB, IEEE1394

TELECOMMUNICATIONS

Another major evolution concerns the telecom sector, where mobile phones are progressively replacing fixed network connections.

New requirements in communication and networking correspond to an interest for cooperation with IT industry, with the view to use the same communication standards in order to ease the convergence in the networks infrastructure managed by the different operators.

WIRELESS LOCAL AREA NETWORKS (W-LAN)

Wireless LAN is a new networking technology providing high speed data rate, which has rapidly gained much popularity. Different technologies exist which support different needs. The main players are:

- 802.11, for connection within a range of around 300 m
- Bluetooth, for personal environment (a few meters)

The improved convenience of wireless access to networks has increased the range of situations where people can perform computing, thus increasing security concerns.

CONCLUSION

In recent years, smart card has evolved from a specific device to a more open platform, offering multiple applications and enhanced security. At the same time, network connectivity has become an integral part of computing environments.

However, neither the smart card application model nor its communication protocols have evolved accordingly with regards to the evolving external computing world.

4.1.2 SCIENTIFIC AND TECHNICAL CHALLENGES

Smart cards should carry on being used as trusted personal devices, with a better integration within their environment and high speed interfaces. Experts believe that the greatest challenge will be to integrate networking features inside the devices, with the view to make them a part of the interconnected IT world. For the time being, networking features are supported by the card accepting device. For the future, the trusted personal device should be able to virtually connect to an arbitrary Web page for getting up-dated information, as well as authenticating a transaction via a high-speed and secure direct link to a server.

PERFORMANCE IMPROVEMENT

In the context of the emergence of new protocols, it becomes urgent for the smart card to enhance its communication capabilities, according to the state of the art in the world to which it is connected.

It is necessary to improve the interface in both the wired and wireless modes. As an example, following targets should be considered:

- from Kbit/s to 100Mbits/s for data exchange speed rate
- low power consumption for enhanced portability
- full-duplex for multi-protocol

CONNECTIVITY ENHANCEMENT

From the communication and networking point of view, evolution towards open platform will become possible when smart card is in the position of being smoothly integrated in the interconnected IT world.

Following targets should be considered:

- TCP/IPv6 for Internet protocols
- Security of connection link
- Wireless communication protocols

The use of protocols such as IPv6 could compromise the privacy management required by a wide scope of applications. Therefore, the possibilities provided by IETF regarding privacy and security (such as IPSec or RFC3041) should be investigated.

SUPPORT NEW COMMUNICATION MODEL

Real multi-application smart card requires that different applications could have simultaneous access to available resources (communication stack, NVM memory, etc.). This will undoubtedly impact the underlying Operating System and the following aspects will have to be considered:

- Multi-tasking OS
- faster access to NVM
- improved RAM capacity

Further to interoperability and adaptability, new applications, such as secure peer-to-peer applications, will require smart cards being considered as real network nodes.

4.1.3 RESEARCH ORIENTATIONS

Three areas for research and improvement are considered hereafter, as elements addressing smart card communication and networking: physical link, communication protocols, integration in networks.

4.1.3.1 Short / Medium term

PHYSICAL LINK

Enhanced standard link between terminal and smart card

High speed protocol

COMMUNICATION PROTOCOLS

Non-exotic / non proprietary communication protocols easy to implement (in program) and available every where (e.g. IPv6)

INTEGRATION IN NETWORKS

Integration in wired and wireless Internet access specifications

4.1.3.2 Long term

PHYSICAL LINK, COMMUNICATION PROTOCOL AND INTEGRATION IN NETWORKS:

Migration path to Smart Objects

Wireless Objects Protocols

Depending on the type of approach (smart card as a specific ISO device or as a "platform"), improvements could be assessed upon items introduced here under:

	Device Current SC	**"Platform" extended SC**
Physical link	Full duplex High speed Clock recovery Pin(s) number Wireless	Multi-interface (USB, Bluetooth,…)
Communication protocol	Card to something (1 to 1 and 1 to any) Multi-protocol Protocols used in IT and consumer (like Ipv6) Wireless protocols	Peer to peer Multi-protocol Protocols used in IT and consumer (like Ipv6) Wireless protocols
Integration in network	Internet Security	Internet Security

ASSESSMENT OF PRIORITY TECHNOLOGIES

Operating system:

Multitasking operating system (cf Ch 4.2)

Hardware requirements:

Embedded RF

Embedded Battery

Faster non volatile memory access

Larger RAM

Network requirements:

Connectivity with IT

Implementation of mobiles nodes connected through wireless links

Improvement of W-LAN technologies for large and dense networks

Security requirements:

Maintenance of privacy and security level

TENTATIVE TIME SCHEDULE

IPv6 integration: Short term (2 years from now)

High speed protocol: Short term (2 years from now)

Multi-tasking: Medium to long term (2 to 5 years from now)

Wireless solution: Medium to long term (2 to 5 years from now)

4.2 SYSTEMS AND SOFTWARE

To cope with the broad range of topics involved with the technology domain "Systems and Software", three different sub domains were created:

- Operating Systems (OS) and High Level Languages
- Development Tools
- Systems Integration and Card Application Management

4.2.1 TECHNOLOGY TRENDS AND MARKET REQUIREMENTS

Several general and sub-domain specific requirements can be identified. First of all, smart card systems should be dependable and trustworthy, which should be proven by high levels of certification. In contradiction to this, the development costs for new products have to be affordable and a short time to market is required for new products and applications. To meet both requirements, sophisticated development tools are needed.

From the IT systems side, smart cards must be easy to integrate into large networked systems, by appropriate middleware concepts.

The general future view is that with a single smart card, a given user should be able to connect anywhere, anytime, to all the value-added services he or she has subscribed to. It should also be easy for the user to add/remove any new type of service to/from the lot of subscriptions. In addition, this requires a sophisticated management of smart cards and their content.

4.2.1.1 Operating systems and high-level languages

Future operating systems will have to support new upcoming hardware features. Mainly new communication and network protocols must be integrated. In addition multi-application capacity will be of importance. This does not only mean to store several applications on the card and to select between them, which is current state-of-the-art, but also to integrate the concurrent execution of applications on the card. Future programming languages must better support the special requirements of smart cards, either as high-level multi-purpose languages or as portable and efficient low-level languages (possibly with dedicated features).

4.2.1.2 Development tools

In general research results from the software engineering field have to be adapted to the field of smart cards. Therefore, smart card specific requirements like the restricted resources and special security needs have to be considered. These tools have to support all aspects of certification and clearly defined validation techniques will be needed. An integrated design of on-card and off-card applications has to be considered.

4.2.1.3 System integration

There is a strong need for improved system integration, which is currently on a very low level (proprietary APDU definitions).

Three main fields can be identified. First, smart card middleware will enable an easier integration. The card of the future will adapt itself to the end-user terminal or network to which it is connected, while still maintaining a high level of security for the applications. Second, smart cards that become smart objects need an improved management of the cards themselves, the applications, and the content stored on them. Third, project management tools will support the prediction of (human) resource requirements, distributed development, and the interaction between development and validation.

4.2.2 SCIENTIFIC AND TECHNICAL CHALLENGES

4.2.2.1 Operating systems and high-level languages

The main barrier that could be identified is the variety of smart card hardware that might hinder the development of more sophisticated operating systems and programming languages, due to the enormous porting costs.

The second barrier are the limited resources available on the smart card, since state of the art IT operating system techniques like multi-tasking and multi-threading cannot be easily adapted to the smart card hardware.

4.2.2.2 Development tools

Concerning the development tools the main challenge will be to improve security and the certification process. Formal methods must be defined on different levels. Formal modelling with description languages should support concurrent and mobile computations. Formal verification should be as automatic as possible through the use of static analysis, model checking and automated theorem proving. Last, program verification that complements security issues has to address challenging issues like applet life time, persistence, atomicity and reset, specific runtime environments and libraries, etc. All of the before mentioned methods have to be supported by appropriate development tools. In addition, on-card analysers that verify applets have to support strong security models.

4.2.2.3 System integration

Although middleware and integration tools have already been investigated in Software Engineering to a certain extend, these concepts have to be adapted to the special characteristics of smart cards (e.g. restricted resources, I/O capabilities,...). A second challenge of importance is the management of smart cards and their content, which lacks a fundamental approach for defining the model(s) sustaining the card management system, thus conducting to difficult integration of card management systems in information systems.

4.2.3 RESEARCH ORIENTATIONS

4.2.3.1 Short / Medium term

OPERATING SYSTEMS

– The key themes for Operating Systems are: Open source OS., Multi tasking/multi-threading OS , File System management/Memory Management Models , Modularity (Multi layered OS), Real Time OS , I/O speed enhancement , High-speed communication protocols.

OPERATING SYSTEMS

Enhanced execution environment	Dynamic and symbolic on-card linking: this is a great way to reduce the burden on both the application developers and the card issuers, because it reduces the management cost of the card. For example, loading class files complicates a bit the design of the OS, but reduces a lot the learning curve, which is today a big problem, encountered by developers when they try to figure out what they can do with the card. Multi-threaded OS: it is very useful to support true multi-application models. It is also mandatory to deploy applications developed independently, without à priori knowledge, which is not the case with current cards. High-level memory management: it is necessary for the developer to reduce the work that has to do with memory, and it can help a lot on performance issues traditionally encountered with today's cards. Discussing persistent and transient memory managements and abstractions is a major issue.
Support for non-functional properties	Enhanced transactions (with regards to multithreading) QoS for e.g. streaming applications, but also for the management of generic latencies.
Resource control	Deadlock prevention/detection Improved use of the card resources shared by multiple applications Lease model for resources: static/dynamic guarantees
System adaptability and flexibility	Static scalability of the system with regards to hardware capabilities and applications requirements.Post-issuance update of the system components e.g. for real and safe OS patches rather than proprietary card filters! Dynamic reconfiguration e.g. on the fly communication buffer resizing for optimization. Dynamic extension e.g. for adding on-the-fly an application protocol (ftp) required by a newly installed applications
Real-time	For example, the SIM application has deadline constraints that are managed in the application code without any support/guarantee by an operating system. Facing real-time issues will be more and more critical in future applications· – Mastering the execution time of the OS primitives.· – Predicting execution time of application codes.· – Scheduling real-time tasks in accordance to their respective deadlines.

HIGH LEVEL LANGUAGES

Better general-purpose programming languages

A first direction for improvement is to enhance the expressiveness of the programming languages used for smart card programming, while keeping them general-purpose: for instance, to replace the Java Card subset of Java by full Java, including garbage collection and threads. This requires a significant engineering effort, both on the system software side (implement garbage collection in the virtual machine) and on the hardware side (to revisit the RAM/Flash trade-off).

Alternative high-level languages should also be considered. An obvious alternative to Java is C#. However, C# shares much the same traits and limitations as Java; the choice between C# and Java is yet more political than technical. Other languages of interest include Eiffel and Modula-3: both include native support for features that could help writing reliable and secure smart card applications. Eiffel supports logical assertions and programming by contract, while Modula-3 offers strong type abstraction and genericity mechanisms.

Rather than switching languages entirely, a "mix and match" approach is possible, whereas new language features of interest are added to a, say, Java base. For instance, Generic Java adds genericity to Java, and the JML modelling language (see below) adds logical assertions.

Domain-specific and scripting languages

Domain-specific languages (DSL) are a complementary alternative to general-purpose languages. By design, a DSL tries to reflect the characteristics and idioms of the intended application domain directly as language concepts, constructs, and notations. For instance, a DSL for financial analysis could have primitive notions of contracts, financial products, indicators, etc, with special syntax to express them -- just like integers or arrays are primitive notions with special syntax in general-purpose programming languages. DSLs do not emphasize generality -- many are not able to express arbitrary computations -- but aim at supporting a particular application domain with maximal clarity, safety and conciseness, and in such a way domain experts that are not professional programmers can write that programs.

The so-called scripting languages often start as domain-specific languages specialized in e.g. command scripting (command shells), Web programming (PHP), or text processing (AWK). Some scripting languages later evolve into full-fledged general-purpose languages via feature accretion (e.g. Perl, Python).

Besides allowing shorter, clearer programs, DSLs offer two advantages stemming from their limited expressiveness. First, they can often be compiled down to table-driven automata, or byte-code for specially designed virtual machine, leading to small compiled code that can be executed very efficiently. Second, DSLs often have a strong declarative flavour, thus facilitating the application of formal methods (proofs, model checking, test generation).

There have been relatively few attempts to apply the DSL / scripting approach to the smart card world. The only example we are aware of is the SIMspeak scripting language to describe succinctly customer interaction on GSM phones. Some examples of smart card programming situations where adequate DSLs could improve software quality and compactness:

- Implementation of APDU-based communication protocols, perhaps via ASN1-style notations for bit- and byte-level manipulations, and automatic generation of robust encoders and decoders.
- Expressing concurrent computations in the synchronous reactive style (as in Esterel or SCADE), from which state machines interfaced with an asynchronous I/O API can be generated.

Other opportunities for using DSLs might emerge in the near future, once careful domain analyses are conducted.

DEVELOPMENT TOOLS

Connections with modelling and specification languages

Applying formal methods to a program requires that both the actual program and the specification it is intended to fulfil are expressed in a common framework that can be processed by machine. Sometimes, the program is obtained as a by-product of the specification, via incremental refinements of the specification up to a fully executable specification (as in the B method).

At the other end of the spectrum, the specification can be embedded as annotations inside the program: pre- and post-conditions on functions and methods, invariants for loops, etc. For the latter approach, the programming language must be extended with the ability to express these conditions and invariants in a suitable logic, and attach them to program points. The Java Modelling Language (JML) is an example of such an extension for the Java language. Significant work remains to be done to

– Design modelling languages that are sound and expressive, yet remain usable in practice, and
– Develop adequate interfaces between these modelling languages and existing theorem provers and model checkers.

In the longer term, efforts on modelling and specification languages can have significant fallbacks on the design of the programming languages themselves. Rather than considering formal methods as an afterthought, it could be worthwhile to take into account provability and testability early in the design of future programming languages. For instance, emphasis on program proofs favours declarative language constructs over imperative ones; and emphasis on model checking and formal testing favours programming via finite-state machines.

SYSTEM INTEGRATION

Integrated tools

Integrated set of tools for the development of applications in a global framework, permitting to test all types of elements, such as card applets, midlets, and all other sort of software components that fits in the framework. These tools should fit in very different usage scenarios: 3G Mobile networks, digital Pay-TV networks, TCP/IP based networks, etc.

Enabling technologies

RMI and others

Regarding Java Card, RMI seems the middleware of choice to use. From Java Card 2.2, the elements needed to bring RMI to the smart card begin to appear on scene. But the RMI, as it has been proposed in the specification aforementioned, is far from being optimal. In one hand, only unidirectional remote calls are foreseen, from the outside world to the applet inside the card. On the other hand, even this part is still lacking some services that should make use of remote objects inside the card completely transparent for the developer.

This gap should be filled in a first phase, so as that calls from client applications outside the card, to the applets inside the card, appear to be exactly the same as standard RMI. Then, RMI in the other direction (from inside to outside) should also be considered, since this would simplify the development of applets in some cases, or create new types of uses for these applets in other cases.

Other types of middleware technologies also could be considered to be ported to the card: Corba, SOAP based RPC, .NET Remoting, etc.

MIDP and others

Mobile Information Device Profile (MIDP) has been defined by Sun and other participants of the corresponding Java Community Process (JCP) expert group (MIDPEG). As it reads in one of their docs: "The goal of this specification is to define the architecture and the associated APIs required to enable an open, third party, application development environment for mobile information devices, or MIDs". The idea is that this kind of specification will greatly simplify development of applications (midlets) for mobile devices that use the Java 2 Platform, Micro Edition (J2ME).

Many of these devices use smart cards (mobile phones, Set-Top boxes) and more will use them in the near future (PDAs, for example), the profiles considered in MIDP talk only about of aspects such as User Interfaces, Networking or Persistent Storage, among others. There isn’t even a single reference to smart cards. There is a need to carefully study the possibility of enlarging the scope of MIDP to include smart cards.

This subject should be addressed outside of the Java world as well. It would be important to define standard mechanisms for communication between the terminal and the smart card in very different scenarios such as telephones of PDAs using PocketPC, PalmOS, and so on.

4.2.3.2 Long term

SYSTEM INTEGRATION

Design models

Design methodology for identifying the right application model to be used by on-card software when an application is delegating parts of its functionality to a smart card.

Also implementation choices and techniques of application models with smart cards taking into account the smart card constraints, the level of security offered by the card and the identified part of an application model to be resident on-card. This activity could impact on the following topics:

- On-card framework understood as APIs and services needed to support application models (e.g., RMI APIs and RMI engine),
- Middleware supporting application model (e.g., CORBA for synchronous request-response application model)
- Application protocols (e.g., HTTP for the servlet application model)

Design models related to management of smart cards:

- Management entity definition: artefacts, packaging, granularity, etc.,
- Management functionality (e.g., load, install, update, remove, set security level/domain, etc.)
- Multi-application card management issues when smart cards are considered as real application servers deployed in million of units.

Design technologies

Design technologies applied to smart cards to be considered are

- **XML**. Definition in XML of many of the specifications used today in different industrial processes related to smart cards. In particular, data employed in pre-personalization and personalization phases.
- **UML**. Use UML to model design patterns. This could be used to model server component patterns, and define and model patterns in card application development. For example, the use of these models would greatly simplify the development of server side component and applets for Java Card, using tools like Rational Rose or Objecteering.

On-card and off-card framework

Specific card framework or existing framework adapted to advanced smart card programmability and usage include

- Extensible and scalable on-card and off-card framework.
- Dynamic management of card framework services.
- Framework for distributing codes that interact with smart cards taking into account security, performance, ease of use, dynamic behaviour, off-line operating mode, etc
- Dynamic (or ad-hoc) vs. static deployment operations such as e.g., card announcement, application/ service publications, card/applications interface/proxies installation, etc.

OPERATING SYSTEMS

Open source OS is an important long-term research topic with expected benefits of portability, flexibility and interoperability. The Linux model could evolve smart cards towards full-fledged, secure autonomous computers and makes the smart card full partner on the network:

- Connecting to a smart cards like to an ordinary web server,
- Connecting to a smart card from web browsers via IP address or network name,
- Log in to a smart card across the network with a standard telnet client,
- Use XML protocol to enable XML based card applications,
- Supports a variety of application frameworks (Java, .NET, HTML, XML) in a single card, etc.

Main issues of this topic are of course security (due to public availability of the code), capacity constraints, etc.

4.3 SMART CARD ACCEPTING DEVICES, INTERFACES AND BIOMETRY

Smart card is to a large extent a slave of the reader or terminal. In the future the relation between card and terminal will be more balanced, and the connection between card, reader, terminal and networked server should be optimised in terms of security and cost-effectiveness.

The main elements to be considered at the card accepting device (CAD) level are:

- Secure interconnection with ambient intelligent environments (domestic, public, professional)
- Man-machine interface for user convenience
- Integration in new generation information systems, platforms (languages, protocols,…) and infrastructures

4.3.1 TECHNOLOGY TRENDS AND MARKET REQUIREMENTS

4.3.1.1 Evaluation in specific areas

Information and transaction

This area is referring to devices connected to IT platforms such as PCs, information kiosks, cash registers, etc. and addressing security of stored information on the device itself, or secure link with a device to access remote information systems, identification devices, etc.

For this purpose the following types of technologies are addressed

1. *Secure readers - device readers and protocols are:*

   a. *Contact (USB, Fire Wire, etc.)* - Readers for Smart cards with contacts that utilise some means other than an RS232 connection to communicate with a host device.

   b. *Contact less (Wi-Fi, IR, Blue Tooth, etc.)* - Readers for contact less Smart Cards that utilise some wireless means other than an RS232 connection to communicate with a host device. The communication between the reader and the Smart Card needs to be encrypted for preventing "eavesdropping" of the transmitted data.

2. *Secure Smart card reader with keypad* - A reader with an inbuilt keypad for safely processing authentication/identification data (generally a PIN) during a transaction. The PIN (or biometric data) must be secured itself and requires to be kept proof from environments where it could be exposed to Trojan Horses.
3. *Biometric interfaces for Palm, Finger, Iris, etc.* - Readers that allow for identification corroboration using some biometric function, in a secure manner.
4. *Miniaturization and cost effectiveness*. - To become a pervasive technology, devices should evolve towards smaller, cheaper and low-voltage features

On its own side, the card itself could improve its inherent interfacing capability, through evolutions mentioned below (cf more in chapter 4.4)

Interface components embedded in the card

a. *Biometrics* - Miniaturised sensors placed on the Smart Card device itself, such as for "match on card" finger print

b. *Keypad* - Miniaturised keypad for data entry on the smart card itself

Form factor: Wearable or proximity devices that can either be incorporated into objects such as a watch or a ring, with contact-less capabilities etc. At the opposite part of the spectrum, incorporating a card interface as a removable device onto a hard disk to allow for removable data security.

Communication

This area is referring to communication devices in any type of form: mobile cellular telephone, satellite phone, PDA, etc.

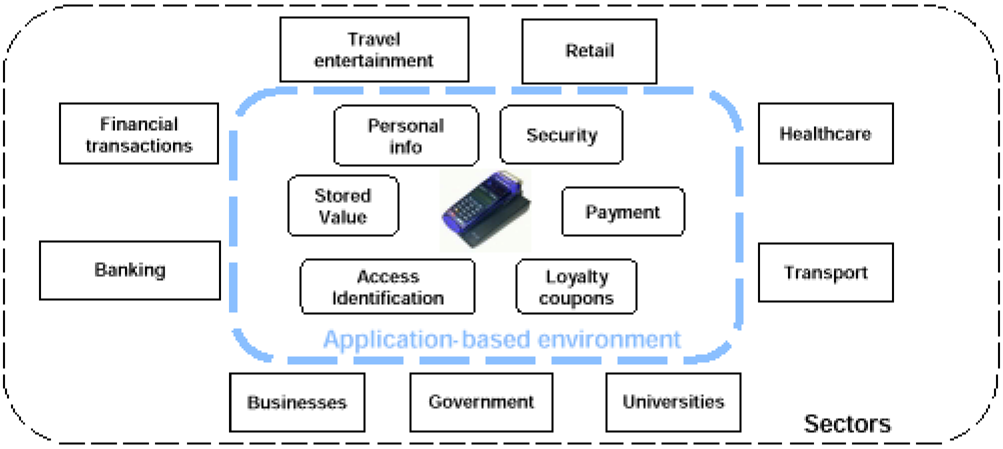
1. Miniaturization and low power - to bring the interface devices in-line with the lower energy requirements of both the receiving devices and the smart cards themselves.
2. High speed protocols - interface devices need to support new protocols that will allow for higher data rates.
3. Multi-application -from user identification in a mobile phone to other applications relating to e-commerce, such as an electronic purse or home banking, and extended wireless connection through protocols such as Blue Tooth.

4.3.1.2 Market requirements

GLOBAL MOVE TOWARDS MULTI-APPLICATION

A global move for multi-application around smart card accepting devices brings need for an interoperable, software-driven device that can be tailored to each party needs. The following picture is showing the path to the required combination of functions, at the core system level, and of applications, at the environment one.

Figure 1.



SECURITY IS A TRANSVERSAL ISSUE

Pervasiveness of security highlights the necessity for each component to be designed upon specific security requirements. The evolution towards open CAD platforms should be supported by the implementation of tamper resistant mechanisms for preventing data leakage or corruption.

USER FRIENDLYNESS: USE WILL GREATLY INFLUENCE USER INTERFACE

The use of the smart card accepting device (advertising, web browsing, multi-application management, etc.) will influence user interface. Main requirements are:

- easy-to- install SW interface and easy-to-use readers for consumer everyday life
- enhanced displays (size, touch screen interface, colour), supporting e-marketing requirements

4.3.2 SCIENTIFIC AND TECHNICAL CHALLENGES

4.3.2.1 Generic aspects of smart card systems evolution

The table below summarises the main fields for smart card systems evolution, covering aspects such as performance, compatibility / interoperability, market penetration, etc.

Performance	State of the art	Next steps
Partitioning between Terminal and Smart Card	Die size of the smart card is limited by reliability requirements (today about <20mm²). This limits the functionality for a given technology.	The complexity of systems embedded into the smart card will increase in the future due to: – Thinner flexible wafers, – Smaller dimension of the die, – Multi-chip concept. This will influence the partitioning of the functionality between the smart card and terminal. E.g. in biometric applications: processing inside the smart card itself will become feasible and cost effective.
Compatibility / Physical Interface	Physical layer is defined by ISO standards: **Cardswith contacts:** ISO/IEC 7816-2, -3 based **Contactless IC cards:** ISO/IEC 14443-2 based	Additional physical interfaces to ease integration in existing infrastructure, e.g. PC interface through USB protocol.
Protocols	**Cards with contacts:** ISO/IEC 7816-family **Contactless IC cards:** ISO/IEC 14443-3, -4	New protocols to consider: USB, Secure Devices (SD), Multi Media Cards (MMC)
Interoperability	Protocols are based on ISO/IEC 7816 and ISO/IEC 14443-3, -4 COS are today mask programmed in ROM and patched into NV memory.	Java will offer a high flexibility for multi applications systems, through both card and CAD.
Voltage and Power	5 Volt operation is the de facto standard for POS terminals. 3 volts is the standard for Mobile phone Power consumption: a few mW for card with contacts and some hundreds of µWatts for contactless operation.	Future applications will make use of lower voltages as defined in ISO/IEC 7816-3 3.0 Volts and 1,8 Volts. Mobile phones will make use of it. However, POS terminal lifetime will require 5 Volts for longer periods in the future. Contactless operation will drive the technology and architecture for low power operation.
Physical size	Dimensions of smart card are defined in ISO/IEC 7810 (ID1-format). Other form factors are available in the market (e.g. Memory stick, xD memory)	Cards and trusted personal devices featuring other forms and dimensions are under consideration. Evolution towards thinner ID1 cards (<0.4 mm) will impact the contact read/write interface.
Access control	PIN code is the de facto standard.	Biometric methods will come in addition or as alternative
System on card aspect	Smart card has no additional elements as user interface.	Applications will request enhanced interfaces, such as: display, buttons, acoustics, biometrics. They may shift partly from the terminal to the card.
Terminal/Reader	Dedicated solutions for contact and for contactless smart cards.	– Dual interface Terminal/Reader – Standardised specifications for generic card readers (e.g. STIP, PC/SC, FINREAD) to enforce interoperability – Java will offer high flexibility for multi application smart card readers

4.3.2.2 Specific challenges

TRUST

The first challenge relates to the users' feeling about the system: can they trust the card and the terminal for the purpose they want?

The card accepting device must provide integrity of the data related to the transaction:

a) data prompted to the user: characteristics of the goods or service provided, transaction amount & currency…

b data entered by the user (for the e-government applications, salary amount, items ordered & quantities…)

c) user identification, such as PIN, biometric data…

Let us consider the frequent pop ups Internet users are confronted with, such as whether to trust a certain certificate, whether to turn on active x controls etc. Many users do not understand the questions and routinely click OK to continue. The technical issue here is that designers must know what the effect of a security exception could be, and how systems and users will cope with these exceptions.

A smart card specific example is provided by the use of prepaid cards. How can users trust the card to keep their money safe, and how can they be sure that the terminal does not ask for more than it should? One common business model assumes that the user is always wrong, which clearly does not inspire confidence in a system.

Another example may be found in the use of smart cards for e-government purposes. Web forms, smart cards and other technical means are in use for online applications. How to get the same level of trust and confidence people have in a face-to-face relationship with the agent? Would it be possible to develop adaptive interfaces that could provide a feeling of sympathy?

To address the problem of fostering trust in smart card based interfacing, prototypes of systems based on different trust models are considered. Such systems would comprise the smart card as the basis of trust, but would also necessarily comprise the remaining infrastructure. For reliable assessments, complete prototype systems would have to be evaluated by large user communities. Focus groups would study and discuss the implications, with the objective of developing trust models for smart card applications that enable evaluation of levels of trust.

MANAGEMENT

The second challenge relates to the management of a system of applications, specifically in the context of deploying multi-application smart cards.

In a multi-application context, the card and the terminal use a shared infrastructure. Generic, open frameworks are needed to build that infrastructure because:

1. Sharing an infrastructure is less expensive than deploying several infrastructures
2. A shared open infrastructure can be scrutinized by independent experts, thus allowing an increased trust in the infrastructure
3. A shared infrastructure would benefit from best practice experience by the partners involved in building the structure

Cost savings would result from the judicious choice of algorithms and protocols that are known to interwork, that have been tried and tested, and that are free from undocumented feature interaction.

The most important feature of a shared infrastructure would be the ability to manage different user credentials (such as numbers, keys or tickets), depending on specific application environments.

Link could be made with the Liberty Alliance Project, which addresses requirements for IDs and credentials sharing over the infrastructure.

TOOLS

The third challenge is to develop appropriate tools to foster trust into a shared infrastructure. This challenge can be met by developing new programming models for card and terminal that enable code on both platforms to inter-work in an optimal fashion. Ideally designers would not have to know where their code would run. To foster trust, the designers would have to be able to predict the levels of trust experienced by the users. This requires the ability to quantify levels of trust, as well as modelling and measurement tools for trust.

4.3.3 RESEARCH ORIENTATIONS

4.3.3.1 Physical Properties and Types of card accepting devices

MINIATURIZATION OF DEVICES AND REDUCTION OF POWER CONSUMPTION

as regards the mobile handsets integrating a chipcard in a plug-in format, their size is continuously optimised. Therefore, there is a requirement for reducing the size of the interfaces into those devices. In the mean time, it’s necessary to bring the interface devices in-line with the lower energy requirements of both the receiving device and the smart card itself.

SECURE CAD WITH KEYPAD

a CAD with an inbuilt keypad should permit processing data (e.g. a PIN) in a secure manner. The issue to be addressed here is the safety and integrity of the PIN or biometric data and protect them from environments where they could suffer attacks such as Trojan horses transmitted through the host device.

INTEGRATION OF BIOMETRICS FEATURES IN CADS

this is a major evolution is terms of authentication process, especially in ID application contexts. However, the level of security is higher if the matching of the biometric template is performed inside the card, in order to prevent any data leakage or corruption between the card and the CAD.

FORM FACTOR

The possibility of having wearable devices incorporated into everyday objects such as watch or ring, etc. is to be considered, thanks to improved contact-less performances, packaging and chip optimisation.

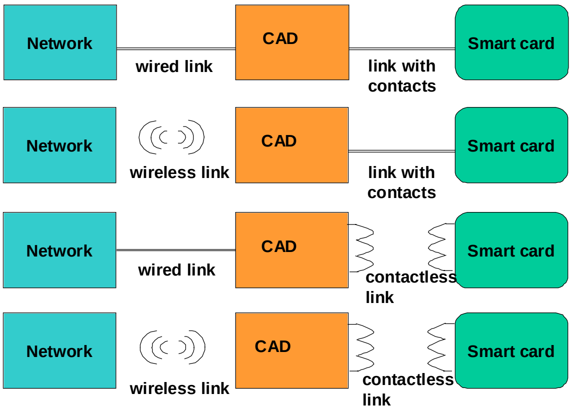
COST EFFECTIVENESS FOR PERVASIVE TECHNOLOGY

In order to achieve a successful evolution towards devices acknowledged as a pervasive technology, it is essential to develop smaller, cheaper, and user friendly CADs, with enhanced energy management, making it possible to implement a migration towards cards and CADs fully considered as consumer appliances.

4.3.3.2 Data Transmission / Communication

The diagram hereunder illustrates the possible scenarios for the integration of a CAD into a system infrastructure connecting Smart cards and Network.

Figure 2. Scenarios for card / reader / network connection modes



1a. Wired link between CAD and Network (USB, Fire Wire, etc.) - CADs for Smart cards with contacts that utilise some means other than an RS232 connection to communicate with a host device.

1b. Wireless link between CAD and Network (Wi-Fi, IR, Blue Tooth, etc.) - CADs for contact less cards that utilise some wireless means other than an RS232 connection t communicate with a host device. The communication between the CAD and the Smart Card needs to be encrypted to prevent "eavesdropping" of data transmitted.

2. High speed protocols - The CAD need to support new protocols that will allow for higher data rates in data transmission, for improved connectivity to network. Open Multi-application platform - implementation of multiple applications generally relating to e-commerce.

3. Peripheral wireless Communication protocol - Printers, displays, off-load data storage, etc. - Develop a protocol to allow a contact less smart card with a suitable wireless technology to output data directly to a relevant peripheral.

4. Large range wireless link (toll use, Identification devices, etc.) -Develop an interface device (CAD) for smart cards that are to be used in applications such toll roads (OBU - On board unit), Identification devices, tracking devices.

4.3.3.3 Transactions and Security

This area addresses requirements for transactions in e-commerce, m-commerce, loyalty or e-purse schemes, etc.

The table below is featuring the main orientations for CAD improvement, on short/medium and long term:

Feature	1 to 3 years	3 to 10 years
Hardware platform	Multiple components in the device	Evolution towards one unique system on chip component
Software platform	– Small Terminal Interoperability Platform (STIP)· – Ability to load / unload applications· – Remote terminals management systems	– OS may be standard or specific· – Software should be portable to several hardware platforms· – certification & agreement through test suites should be facilitated
Functional architecture	Architecture may be distributed (concentrator / terminal) On-line payment improvements Payment servers	Personal devices. Home gateways will appear. Terminal device may be separated into2 parts in the future: – the card acceptor's one – the card holder's one Improved modularity (loading of new functions without changing the core platform)
Application	Mono application to multi applications Several applications in the accepting device. Interfaces and accepting devices suitable for different sorts of application specific smart cards. => User still needs several cards, but may use them with the same accepting device	Shared devices by different organisations (sharing of security features) Multi application smart cards. => User only needs one card for different applications
Security	New cryptography (ECC, AES…) The whole transaction must be secured, including integrity of the data related to the transaction Terminal authentication…	According to the evolution of cryptography, and available computing power Anti collision and card/terminal peering (wireless mode)
User's interface for security	PIN processing & security improvement	New modes of authentication = biometrics features
User's interface for user convenience	Accepting contact & contactless cards	– Device will become portable and autonomous· – ·Graphical display, keyboards, etc… for improved user interface· – Disabled persons requirements:, tactile screens, speech recognition, speech input & output, adapted keyboards…· – Biometric-based input acquisition
Services	Devices & cards will be used for new types of service: secured delivery, vending machines, secured delivery for non-physical goods such as software, movies or music	Continuous improvement

Feature	1 to 3 years	3 to 10 years
Connectivity to smart card Contacts Contactless	Card interface – ISO 7816, – ISO 14 443, – USB Network	Fast link Near Field Communication (NFC)
Connectivity to hosting device Wired Wireless	Improvement to present technologies & new technologies: – RS232 – Universal Serial Bus (USB) – Wide area Network (WAN) – Bluetooth – WiFi – GPRS	UMTS, 4G IP protocols
Market acceptance	Standard architectures: FINREAD, STIP, Global Platform, PC/SC	New generation smart card accepting devices: mobile phones, PDA, Set-top boxes
System Configuration with biometrics	Template-on-Card or Match-on-Card (application dependent)	System-on-Card as improvement of Match-on-Card
Standardisation of biometrics in smart cards	Standardisation of specific encoded/extracted data templates on smart card	Standardisation of algorithms to be implemented in smart cards: Unique feature extraction algorithms for unique data representation, unique matching algorithms for unique decision criteria.
Protection of biometrics data against replay and data acquisition attacks	Cryptographically protected data transfer.	Complete biometrics system in tamper proof environment.
Avoidance of paper printouts and further security documents	Adding more intelligence to accepting devices to further process data from card electronically.	Adding the functionality of storing requested valuable and sensitive data, as payload data to authentication device.

4.4 EMBEDDED PERIPHERALS, SUBSYSTEMS AND MICRO-SYSTEMS

The main requirement for future smart card applications is to provide the card holder with trust and confidence, thanks to the protection of personal data that are stored or transmitted through a direct, instant, permanent, and convenient control on them.

In order to achieve this goal, the card should be able to communicate with the environment, exchange information on the services that are supported by the card itself and by the environment, present it to the user in a convenient way and allow him to interact through the card with the global information system, e.g. by selecting one of several proposed services or options.

User convenience is therefore a key word.

The smart card must turn into an interactive and secure personal device that will integrate new features such as displays, keyboards, identification sensors and power sources, and that will communicate with the environment through contact or contact-less interfaces.

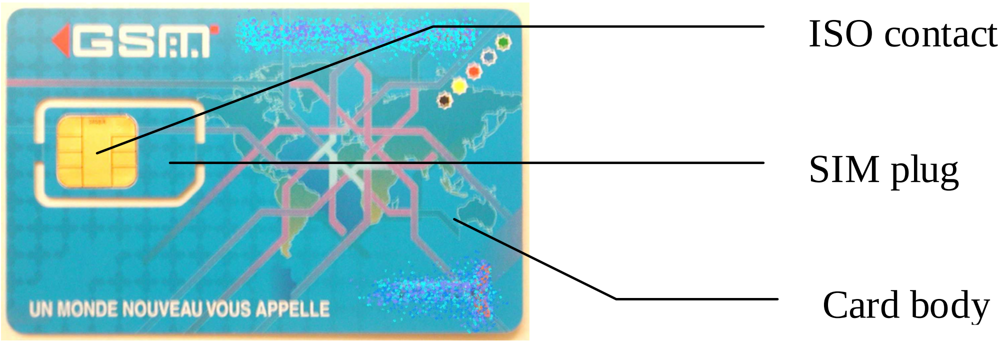
4.4.1 TECHNOLOGY TRENDS AND MARKET REQUIREMENTS

Three main categories of smart card can be considered, depending on the way the card communicates with terminals. However, all three are made of a plastic body containing one or several components with specific features.

- Contact cards use the module (packaged chip) ISO contact to communicate and require to be inserted in a reader or a terminal.
- Contact-less cards communicate by the means of an antenna and driver, embedded into the card body.
- Dual interface cards combine both modes of communication.

In the case of mobile phone SIM cards, the contact card body is punched to the SIM plug size.

Figure 3.



DIMENSIONS

Card body dimensions are specified in ISO/CEI 7810, ID-1 type 85.90x54.18 mm, the thickness being within 0.80mm+/-0.04mm.

Positions of the 8 'ISO' contacts are defined in ISO7816 in reference to card body edges.

SIM plug dimensions, position on the card and ISO contacts position on the plug are defined in ETSITS 100977 (GSM 11.11). Plug outer dimensions are 25x15mm.

MODULE MANUFACTURING

Chips wafers are delivered to assembly plants thinned (grinding or chemicals) to a common thickness of 150 to 180µm and a diameter 6 or 8 inches.

Chips Wafer is mounted on an adhesive tape supported by a frame.

Then separation of the chips is performed by sawing the wafer (dicing).

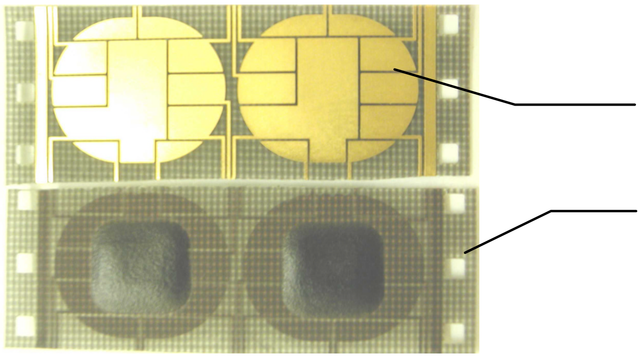
Chips dimensions for regular applications may vary from about 1x1mm to 5x5mm.

The substrate of the module consists in a 35mm wide glass epoxy tape (usually there are 2 modules in tape width).

On one side of the tape, copper has been laminated etched and plated with Nickel and Gold (or Palladium) to form the ISO contact.

For some applications the other side of the tape may be plated too (dual interfaces and other specific).

Figure 4.



ISO contact face

Encapsulated chip face

DIE ATTACH

Wafer and reel of tape are loaded in a pick and place machine.

Adhesive is dispensed on the tape by the mean of a nozzle in appropriate shape and amount.

The adhesive may be electrically conductive (silver particles loaded for bulk bias) or non conductive.

The chip is picked up from the wafer placed towards the adhesive with controlled position, speed, force and time.

Then the adhesive is cured. In this filed standard die attach is competing with flip chip processes

WIRE BONDING

Electrical connection between the die contacts and tape contacts is established by wires.

Most of time, Wires are made out of high purity gold (99.99%) and have a diameter of 25µm.

They are bonded by automatic machines equipped with vision system for accurate placement.

Ultrasonic welding is used to connect wire ends chip or tape metallurgy.

Wire loops length above the chip are typically around 100µm. Using flip chip this process will be no longer needed.

ENCAPSULATION (POTTING)

Protection of the assembly is insured by resins (generally epoxy based).

Many kinds of resins can be found on the market, depending on the application requirements.

Different encapsulation (potting) processes are existing, among which:

- dispensing a single resin (glob top)
- dispensing a couple of resins a viscous one first constituting a dam then filled up with a low viscosity self levelling resin (dam and fill technique)

- filling applications polymerisation of the resin may be obtained by UV exposure (UV cured resins) or thermally activated depending on the resin type.

Using flip chip this process will be no longer needed. The mechanical stability of the module will be realized by the embedding process.

GRINDING

Depending on the encapsulation process, it may be necessary to grind the resin to get the module height required by the card thickness.

Overall module height is commonly about 600µm.

ELECTRICAL TEST

Typical electrical test sequence will consist in:

- punching electroplating lines to unshort the modules
- parametric tests: continuity, open/short, leakage, power
- functional tests: ATR (answer to reset) memory write and erase

Fail parts are invalidated by a punched hole which will be detected by embedding machines and not used.

ANTENNA

Antenna is a metallic coil supported by a polymeric inlet (PVC, ABS, PC).

The coil may consists of

- winded copper then glued on a polymer layer
- etched pattern on a copper or aluminium clad polymer sheet
- screen printing on a polymer layer

The antenna shape depends on the performances requirements of the application.

In simple contact-less cards the interface between the antenna and terminals is insured by a chip attached to the antenna by different techniques (soldering, flip chip…).

In dual interface cards, antenna driver may be integrated as a function in the module chip.

Different flip-chip techniques are available either for Direct Chip Attach to the antenna or for the micromodule manufacturing:

- gold-bumps on chips attached with anisotropic conductive adhesives (ACA tape or liquid)
- gold-bumps and conductive adhesive with underfill
- tin/lead soldering with underfill
- gold to gold using gold bumps thermal-sonic bonding with underfill

After driver assembly, the antenna sheet is stacked and laminated with other layers to get the final card body.

CARD BODY MANUFACTURING

Two processes are used to manufacture card body: moulding and lamination.

Molding is a card to card process while lamination uses sheets of about 40 positions

Subsequent processes remain quite the same.

CARD BODY MATERIALS

- moulding process makes use of pellets of following polymers in 4 (or more) cavities mold:
  - ABS (Acrylonitrile Butadien Styren), PET (Poly Ethylenglycol Terephtalate)
  - PS (Polystyren), PC (Poly Carbonate)
- lamination uses sheets containing 40 cards (or more) made of:

PVC (Poly Vinyl Chloride), PET, PC

In the case of lamination different layers may be co-laminated to achieve required performances.

In the case of contact-less cards, the layer supporting the antenna is placed between the 2 cores, which are then thinner, to keep card thickness in specs.

4.4.2 SCIENTIFIC AND TECHNICAL CHALLENGES

Future smart card applications will require improved reliability, autonomy and user-friendliness, and should take into account environmental constraints. These features will depend on additional components to smart card, such as displays, keyboards, sensors, and extended interfaces (contact & contact-less) with external environment. They will greatly impact technologies for assembly and embedding, materials and components, as well as techniques for interconnection of elements.

In order to ensure compliance with the installed infrastructure of CAD, the form factor of contact smart card should preserve the position of the ISO contacts, for security concern.

The main technology challenges will address the following aspects:

SC HARDWARE ARCHITECTURE

Market requirements for increased smart card functionalities include cost effectiveness of solutions. Therefore, available standard internal bus, such as I2C or SPI, should be proposed for the short and medium term.

Data integrity requires a secure internal data transmission link between e.g. micro-controller and extended memory, when applicable. Standardisation of the positions of additional components should ensure a maximum of possible applications (current ISO activities: NI17.4 TF SOC and NWI SC17 N2047).

FORM FACTOR

Established infrastructures for smart cards, especially for financial services applications, will prevent deviations from the ID0 and ID1 format in the short and medium term. However, smart card used for contact-less only applications (without any ISO contact) may be an exception, as long as customer acceptance for other formats with respect to handling and safekeeping can be generated. On a long term perspective, any deviation from the current standards depends on the installation of appropriate infrastructure by major card issuing organisations.

The card thickness, in addition to the required flexibility, prevents using available technologies for additional components, for contact smart card applications.

INTERFACES /COMPONENTS

Additional components and / or interfaces are probably the main market requirement in terms of increased functionality. However, thickness, reliability and cost effectiveness are limiting access to usable technologies for any kind of additional components.

DISPLAYS

Currently main R&D activities target the implementation of small and flexible displays, e.g. to check the content of an electronic purse. On a short term range, one or two line of 7-segments displays may be considered as sufficient. For higher information content in the mid/long term, matrix displays may become necessary. The reliability of the smart card as well as the lifetime should not be limited by an additional display.

KEYBOARDS

Low functional keyboards, such as knobs to scroll the display or simple confirmation buttons for contactless applications are sufficient for the currently required functionality. An increased number of components and further functions may require more complex keyboards, as far as they comply with the requirement of the form factor (thickness) and can be easily operated.

BIOMETRIC SENSORS

Due to technology (currently limited capacity of the processor on the smart card, thickness and reliability of the card body) and economical reasons, biometric sensors are currently not integrated into the card, but into the CAD (for contact applications).

In the medium or the long term, however, card integrating biometry sensor could be required for high-end applications, with enhanced micro-controllers able to process complex algorithms.

Voice sensors may be considered as well as an interesting opportunity on a long-term perspective.

ADDITIONAL INTERFACES

Market demand for data exchange to PC-peripherals, e.g. for secure data transmission via Internet, already results in smart card with additional contact interfaces, via the not reserved ISO contacts C4 and C8 (USB). Contactless Interfaces (Dual interface Card) are also already well established for e.g. access control. New standards for near field communication will be available as well in the near future. Due to the expected fast development of new Bus standards for data transmission with IT peripherals such as PCs or PDAs, compliance with such standards will also be a market requirement for future smart card applications.

POWER SUPPLIES

The use of active components such as displays or keyboards requires self contained power supply in the Smart Card. On a short term, price, life time and reliability are the main factors for the selection of an appropriate technology. As long a 2 years lifetime, with 10 operations a day for the display, is required for the card, primary cells are sufficient.

The employment and acceptance of secondary, rechargeable, cells in the mid and long term depend on suitable loading technologies, via contacts or inductive coupling during the transaction, or solar cells. Form factors in terms of thickness, reliability and safety requirements are also key factors for embedded power supply in smart card.

PACKAGING TECHNOLOGIES

The need for improved packaging technologies for Smart Card applications are primarily considered from a price and reliability standpoint. The necessity for cost effectiveness, accompanied with higher functionality for integrated circuit, will result in a higher integration density of IC and thus smaller chips. Increased reliability requirements in terms of flexibility will result in reduced silicon thickness (<100µm).

Use of flexible interconnection technologies or flip chip technologies, in combination with decreased lateral dimensions of the IC, will be a quite challenging technical improvement in the near future. As a consequence, full flexible IC technologies (<50µm Silicon) or polymer electronics will find interesting applications in smart card manufacturing, on a long term range.

INTERCONNECTION TECHNOLOGIES

Reliability, especially when considering use and integration of different components, and cost effectiveness are the main market drivers for the interconnection technology. Anisotropically Conductive Adhesives (ACA) and Isotropically Conductive Adhesive (ICA), in combination with chipscale packages for additional components, will meet the short term requirements. Hot Melt ACA, UV-curing ICA, Laser welding are possible alternatives for further increased requirements.

EMBEDDING TECHNOLOGIES

Here again, product reliability, price and production capacity, along with compliance with card body materials, will drive the development of embedding technologies. Hot Melt Adhesives (with lower bonding temperatures and faster bonding times) are likely to be adequate technologies in short term.

Further increased reliability at low cost will require a more comprehensive approach in the mid and long term, with direct processing of components into the card body during the card manufacturing process.

MATERIALS FOR CARD BODY AND INLETS

Currently used materials for Smart Card body, such as ABS (Acrylonitrile Butadien Styren), PET (Poly Ethylenglycole Terephtalate), PS (Poly Styrene), PC (Poly Carbonate) and PVC (Poly Vinyl Chloride) are all meeting the mechanical requirements for the card body in the short term. Compliance with additional various security features (OVDs, OVIs, laser printable features) is required. In mid and long term also compliance of the card material itself with more sophisticated technologies for packaging, embedding, and interconnection technologies for the different components is required.

The development of assembly and packaging materials such as die attach, glob top, and tape materials is primarily driven by cost improvement and need for increased reliability.

DURABILITY ASPECTS

Currently banking applications requires a lifetime of 2 years. In short term, minimum requirement to 3 years is likely. Due to additional components, the number of electrical interconnections is definitely the main challenge in terms of increased reliability and durability.

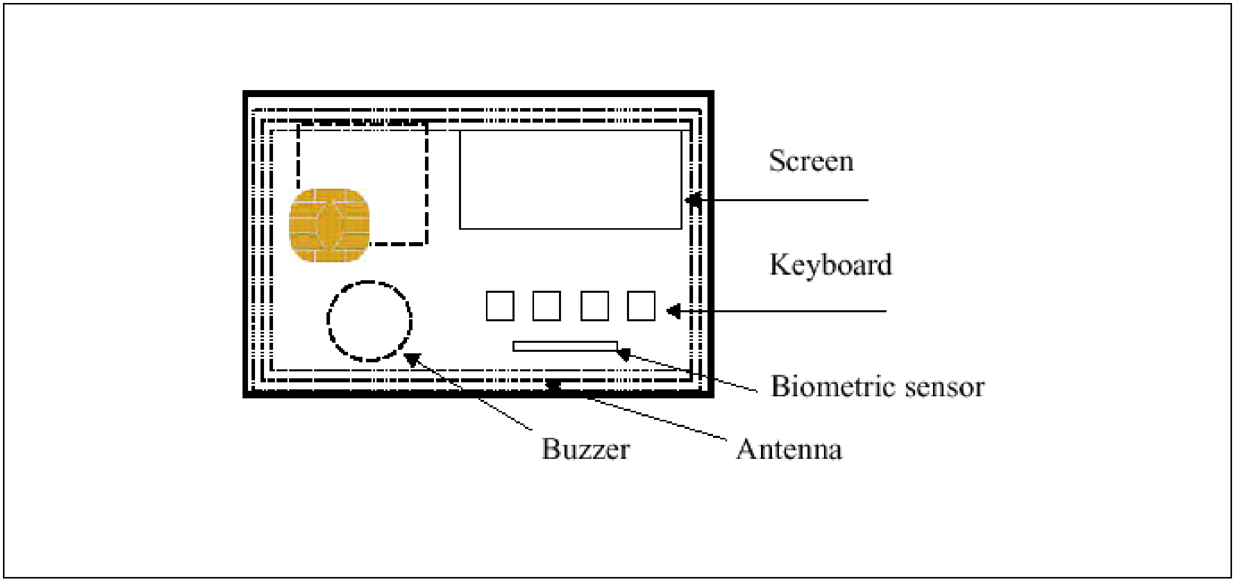
ENVIRONMENTAL ASPECTS

Compliance to general Semiconductor/Industrial Standards is required (halogene free, lead free) with regard to materials and processes for short and long term considerations.

There is currently no standard for the card body material itself. However, some customers require halogen, chloride or styrens free material.

4.4.3 RESEARCH ORIENTATIONS

Figure 5.



4.4.3.1 Card Hardware Architecture

SHORT TERM

I2C or SPI bus (6 wires maximum)

Interface between main chip and bus: managed by a separate interface chip (the interface should not be included in the main chip).

Interface between bus and display: managed by a chip "already mounted on the display".

Interface between the separate interface chip and the knobs: direct connection, no need to be driven by the bus.

Interface between the separate interface chip and the battery: direct connection, no need to be driven by the bus.

Display: most likely mono-stable, segmented or pixel.

ISO 14443 (13.56MHz) optional RF interface included in the separate interface chip: the antenna is connected to this chip and not to the main chip.

MEDIUM TERM

Same as above with a fingertip sensor and a keyboard both managed by the bus and supplied with their interface chips "already mounted on".

Display: bi-stable and mono-stable either possible, segmented or pixel.

Possibly new standards for RF interface

LONG TERM

Extended range of peripherals (biometric sensors, MEMs), all supplied with their interfaces "already mounted on".

Increased amount of application on one card increases the demand of memory on card: up to 512K on the smart card controller, over 1Mb on addition silicon (e.g. FRAM, SRAM)

4.4.3.2 Form factor

SHORT TERM

D-001 & 000 formats with slight shape variations are tolerated (small and local thickness variations, rounded corners, notches.) as far as applications are in a first step managed in closed environments, which means with terminals easy to adapt to special card format, and as far as the card format will still comply with ISO ID-001 & 000 existing industrial infrastructure.

Smaller than ID-000 format: not in the scope of this workshop as this format does not comply with embedded peripherals.

Plugs should keep the ID-000 format and the ISO 7816 contacts layout, and module size should be left free (upper limit: plug sized) in order to give room for large silicon sizes.

MEDIUM TERM/ LONG TERM

ID-001 & 000 formats, no shape variation tolerated in contact card technology

4.4.3.3 Power Supplies

SHORT TERM

Primary and secondary batteries.

Voltage: 3V and 4V.

Capacity: up to 25 mAh, depending on application profile.

For secondary batteries: loading by contacts or power cells & loading control unit included into the interface chip. Hot reset function.

MEDIUM TERM/LONG TERM

Primary batteries for low-end applications.

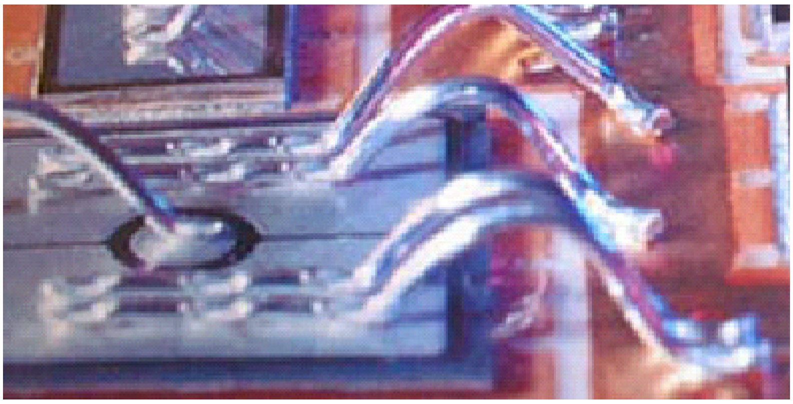
Secondary batteries for high-end applications.

Voltages: 3V and 1.8V, Capacity: probably lower than 25mAh.

For secondary batteries: same as above + flash loading feature + adapted power management unit.

4.4.3.4 Packaging technologies.

Figure 6.



Main focus in the development of packaging should be the reduction of component costs and component thickness. The conventional die attach technology followed by wire bonding and encapsulation will be substituted by flip chip technologies and improved interconnection technologies. This will result in thinner packages. This new technology will need a new process design and new materials. The standard glass/ epoxy tape has to be replaced by a thinner two sided polymer tape. Process specific conductive or non-conductive glues have to be developed in cooperation with a process specific bumping technology for the IC's.

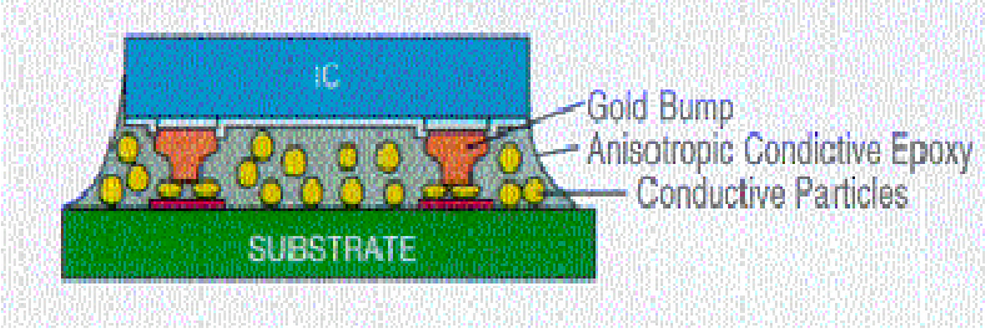
A further aspect is the realization of more than one chip on one module. This is done following the need of tamper proof modules and the integration of sensors on card.

MEDIUM TERM/ LONG TERM

Equipment required for handling thin wafers (below 100µm).Thinner and more reliable chip packaging technologies: thinner and more reliable modules (<300µm).

4.4.3.5 Interconnection technologies

Figure 7.



SHORT TERM

Wire bonding.

Flip chip for contact less card and tags.

MEDIUM TERM/LONG TERM

Interconnections will have to be

- Thin, flexible and reliable
- Lead-free
- Cheap

For this purpose, the chip will have to comply with the following requirements:

- Very thin (below 100µm), pads plated with stainless metal
- Pads layout with a minimum pitch (say 300µm)

Chip manufacturers test pads location layout with a minimum pitch (say 300µm) to be specified.

4.4.3.6 Embedding technologies

SHORT TERM

- Hot melt and technologies for the largest amount of contact card.

MEDIUM TERM/LONG TERM

- Integrated technologies: flexible handling equipment for the mounting of various additional card components at different stages of the production chain (these equipments already exist for SMT and other industries, they just need to be adapted to the smart card) Low temperature pressure sensitive adhesives (<80°c), ideally room temperature

4.4.3.7 Materials and material transformation

SHORT TERM

- ABS, PVC, PC, PS.
- Evolution towards biodegradable material if the additional cost is acceptable.

4.4.3.8 Hardware protection

SHORT TERM

- Coating on the micro-Chip.

4.5 HIGH-END CRYPTOGRAPHY, TAMPER-PROOF AND SECURITY TECHNOLOGIES

4.5.1 EVALUATION OF TECHNOLOGY TRENDS AND MARKET REQUIREMENTS

Smart cards are already playing an important role in electronic transaction systems. Especially for smart-card assisted electronic payment systems, chip security becomes more and more important. Only smart card controllers with appropriate security certifications (e. g. by Common Criteria, ITSEC or by the payment card issuing organizations) will be authorized in the future. Besides that, for sake of security enhancement, longer cryptographic keys will be used in payment-related smart card operations. As the overall performance of the system should not decrease, however, new ways for speeding up the cryptographic procedures even with longer keys and both secure and practicable key management systems are required.

Smart cards are going to be used in the Internet environment, connected via an input/output unit at every personal computer. The security implications for smart cards in the PC and Internet environment have to be assessed. The security of the whole application namely involving the smart card and the security protocols have to be addressed rather than the cryptographic algorithms alone.

Smart cards, for which additional applications or executable code can be downloaded via the Internet or mobile networks (e.g. UMTS- Universal Mobile Telecommunication System), will especially be prone to software attacks and viruses and therefore require special protection mechanisms. For multi-application smart cards, firewalls preventing unauthorized access to card file systems or confidential data and making data manipulation unlikely must become highly reliable. The market demands to ensure strict separation and integrity of the individual applications on multi-application cards. This requirement will have to be scrutinized from the security point of view.

The security environment in contactless smart card applications differs from the scenario with contact smart cards because the data transfer takes place without physically interconnecting the card to a card reader. This is the reason why data can be read out, or transactions could be initiated without the deliberate consent of the owner. Especially the data stream from the terminal to the contactless card is subject to interception due to the wide reach of the electromagnetic signals. Illegally building up an electronic communication with contactless cards, in particular in applications with a non-closed user group, must be prevented. Elaborated overall security concepts for contactless smart card applications are required at least to ensure the security of the transaction protocol and the resistance against side channel and fault attacks when using this interface.

On the other end, huge demands for (very) low cost smart cards, namely for financial and access control applications, will remain important. In that context, "light" cryptographic algorithms like e.g. the GQ (Guillou-Quisquater) protocol, not necessarily requiring a dedicated hardware (coprocessor) or high-end 32-bit processors, will play an important role (at least at the smart card side).

A more and more important trend in secure applications is the possibility to introduce biometric identification. This does not necessary remove the usage of the PIN code but reinforce the link (mainly) between the secure token (smart card) and the owner of it. In that framework, the card will play an important role, in a first stage to hold the physical characteristics to match with the person during the identification phase but also to secure the whole identification process itself. The card could even, in some cases, include the biometric sensor (e.g. fingerprint detector) for an improved security. On-board biometric enrolment (computation of the physical characteristics to be held in the card for the matching) is also a possible future feature.

To reduce personalization costs, parameters of cryptographic algorithms (e.g. public-key, private key and modulus for the RSA (Rivest-Shamir-Adleman) algorithm or the equivalent CRT (Chinese Remainder Theorem parameters) will be more and more generated on (by) the card. This is particularly important for high-end smart cards for which applications could be downloaded during the life cycle of the card and not only during the initial personalization. This nevertheless induce important problems to be solved namely on how to prove the exactness of a key generation and the link with someone’s identity - usually solved using a PKI (Public Key Infrastructure).

Another evolution that can be expected is that standardization bodies will develop sets of security tests (e.g. linked to CC, FIPS 140-2, ITSEC, ...) that will later be endorsed by both users and regulators. Users will then require that a smart card platform passes these tests before accepting it for use in highly sensitive applications.

4.5.2 SCIENTIFIC AND TECHNICAL CHALLENGES

Smart cards are used extensively in security-sensitive applications such as banking, SIM cards for mobile phones, pay-TV systems, etc. In such applications, the smart card is considered to be a tamper-resistant device. It is used for the secure storage of sensitive data like secret cryptographic keys and for performing sensitive computations involving such secret keys. These sensitive computations include operations like encryption, the generation of digital signatures and the generation of message authentication codes.

4.5.2.1 Cryptographic functionalities and protocols

Cryptographic algorithms (or primitives) are the building blocks used for these operations. These cryptographic primitives can be divided into symmetric algorithms and asymmetric algorithms.

DES (Data Encryption Standard) and Triple-DES are still the main symmetric algorithms used because they are well established, and they are well suited for HW implementation which are faster and more secure than SW ones. A new crypto algorithm, AES (Advanced Encryption Standard) developed in Europe and successfully introduced and standardised in the US in 2001 should in the longer term replace DES. AES is more secure and it is well suited for implementations on various platforms, in both HW and in SW.

Asymmetric algorithms, also called public key (PK) algorithms, are needed to address the key management requirements. PK require support from more complex/performant/costly smart card devices and infrastructures. Currently PK deployment is quite limited, and RSA algorithms are mostly used. The future is seen in new algorithms like elliptic curve (EC) algorithms that are able to reach the same or higher security levels with shorter keys, hence consuming less resource.

INCREASE OF KEY SIZES FOR MORE SECURE AUTHENTICATION PROTOCOLS

One of the most important technical challenges is the development of more secure authentication procedures and protocols. The performance of the key generation and the efficiency of the key management systems, especially for asymmetric algorithms, must be improved in order to achieve a high overall performance of the systems of tomorrow. High-end cryptography will be necessary. Key lengths of 2048 bits will be applied and integrated. The interdependence of key length, implementation in the cryptographic smart card controller and performance will have to be investigated and optimized. The challenge here is to design a system that can handle the increased key size, in particular how to deal with the problem of increased memory size and the need of a better input/output speed.

NEW SIGNATURE ALGORITHMS

Instead of the RSA algorithm in public key cryptography special digital signature algorithms such as the DSA (Digital Signature Algorithm) which resulted in the standard "DSS" (Digital Signature Standard) have also been proposed. However, these algorithms generally require costly crypto processors to be used by the smart card. Here the challenge is to find new signature algorithms that can be used in low-cost smart cards, without crypto processors, and have improved security characteristics.

ADVANCED SECURITY PROTOCOLS

It is already a challenge to implement privacy enhancing technologies on current smart cards due to the complexity of the protocols, the large number of cryptographic operations required or the size of the credentials that must be stored or transferred. With the appearance of multi-application smart cards, a new threat to the privacy of the cardholder appears. For example, a user using his or her banking card to buy and store a movie theatre ticket on line, runs the risk of revealing his movie tastes to the bank or his debt to the theatre. More complex unlinkability and untraceability protocols must be implemented on the smart cards to prevent this.

ELLIPTIC CURVE (EC) GENERATION ON-CARD

The recent years have borne a significant progress in point-counting algorithms for elliptic curves over finite fields. Still, as yet, the implementation of such algorithms on smart cards for on-card elliptic curve generation seems to be prohibitive due to time- and memory-consumption.

However, the usual practice today is to use "standardized" elliptic curves, because these are well studied curves, which one can trust (they avoid all known "weak" classes of elliptic curves)

Hence, the challenge here is the following: find a way for the smart card to generate its own elliptic curve, together with a "proof of validity" (i.e. the absence of accidental or malicious weakness for the generated curve).

4.5.2.2 Tamper-proof and security technologies

As key component of a secured application and in particular in untrusted environments, the smart card is exposed to different attack techniques aiming at extracting secret information from the card. Attack techniques used depend on the attacker's available means and knowledge, such as reverse engineering on smart card chips, provoking and analysing responses of the smart card in normal and abnormal (e.g. disturbed power supply, exposure to electromagnetic fields) operating conditions.

The exposure to and sophistication of attacks is steadily increasing due to widespread availability of ICT equipment, multiplication of computing power, growing general knowledge on IT, security technology and attack techniques, number of potential attackers, potentially combined means and effort through the Internet, etc.

Smart card chips have built-in countermeasures such as sensors, glue logic, shielding, constant current mode, etc. to make these chips tamper resistant. These countermeasures need, however, to respect a major constraint which is the implementation cost, an especially critical issue for low-cost/low-margin smart card mass applications.

NEW PARADIGMS OF ATTACKS

Smart cards and the internet: new threats

The use of smart cards in the internet environment requires enhanced security concepts. End-to-end security as well as security measures supporting connectivity and interoperability have to be established. Data integrity and trustworthiness have to be achieved as well. Traceability of smart card data in the internet and liability in case of attacks are issues to be investigated. In the future smart cards will be accessible via the internet. The communication via the internet bears the danger of data transfer to and from the smart card without the knowledge of the owner by an unknown third party in the internet. Besides that, unintentional disclosure of secret information via internet server operators is likely to augment. Due to the ubiquitous internet, the number of potential smart card attackers will increase drastically. Attacks employing the combined power of hundreds of computers to break security mechanisms of smart cards could be performed via the internet more easily. Novel security schemes for smart cards and smart card readers in the internet will become necessary. Furthermore, smart card protocols must become "fault tolerant": they must be ready to handle accidental of intentional faults induced by the connection to the untrusted network.

Hybrid attacks

In order to be ahead of any potential attackers, the smart card industry must find security leaks and possible new attacks regarding their smart card systems by themselves and also develop suitable countermeasures. Different diverging attack techniques (e.g. mathematical methods and applied physical methods) must be combined in an intelligent way to conceive new security attacks and measures against them.

The ultimate scientific challenge is to develop smart card operating systems and implement cryptographic algorithms so that the complete systems are immune against crypto-analysis and implementation attacks. Only dedicated research activities enable the smart card industry to achieve that goal.

Here a "crypto-analysis" attack means an attack that is only mathematical: it considers the algorithm or protocol as a black box, and tries to find secrets, or to circumvent the protocol, by using only logical information (e.g. inputs or outputs of the black box).

In contrast, an "implementation" attack makes use of additional information given by the real smart card running the protocol (side-channel information such as timing, power consumption, etc.). To perform such an attack, the attacker needs to make experiments on the very smart card performing the computations.

Composition attacks: combining pure cryptanalysis and implementation attacks

Side-channel-attacks are likely to become even more threatening in the future when combined with real crypt-analysis: many attacks on cryptographic algorithms (or rather the implementation of such) portrayed so far are straightforward and uses only knowledge about the algorithm under attack (and its implementation), but not any deep (cryptographic) insight into it; the leaked information being sufficient to compromise an entire secret key.

However, given a real good crypt-analytic understanding into a particular algorithm, even seemingly harmless fractions of information (leaking, for instance, through an inadequate DPA (Differential Power Analysis) -defence) could be used as an oracle, and still suffice to compromise a system.

Such effects have not been studied sufficiently yet, since pure cryptographers do not yet consider the assistance of "foul play" in their research work. Therefore there is a need to carry out research on the prospects of the sophisticated interaction of theoretical cryptanalysis and physical attacks, i.e. to study the admission of physical attacks to purely crypt-analytical ones in detail (and on detailed examples), in order to become more aware of the future prospects of such "composition attacks". Here, the physical attacks under consideration need not be limited to passive ("side-channel") attacks, since active ("fault-induction") attacks underlie the same concerns.

SECURE HARDWARE RECONFIGURABILITY FOR SMART CARDS

So far, to speed up the insufficient performance of genuine software implementations of cryptographic algorithms invoking complex mathematical computations (like finite field arithmetic for ECC), IC-manufacturers offer specifically designed crypto-coprocessors for smart card ICs.

Recently, the opportunities of scalable, configurable hardware accelerators for such coprocessors have been demonstrated. (For instance, on the CHES (Cryptographic Hardware and Embedded Software) 2002 workshop scientists of the TU Darmstadt presented an FPGA-implementation (Field Programmable Gate Arrays) of a finite field coprocessor for speeding up elliptic curve arithmetic.)

In the future, FPGAs could be a standard feature even on smart card ICs, allowing in principle to re-configure cryptographic coprocessors even during the usage life-cycle (for instance, by the card issuer, to update an improved version of a crypto-accelerator). This raises concerns towards security policies and security evaluations of Smart Cards involving FPGAs.

The opportunity of an "FPGA-update" (in contrast to a "software update") is currently hardly addressed by the whole scenario of Common Criteria (CC) evaluation for Smart Cards. For a medium or long term perspective, though, it seems to be imperative.

The specific problem of Common Criteria is the following: if a given configuration for a product has been completely evaluated within the Common Criteria framework, means and ways are to be found to reduce the rework of evaluation to be done if one "reconfigures" the FPGA to the minimum.

ON-CARD RANDOM NUMBER TESTS

There is a variety of standard tests for random numbers currently available. (For instance, FIPS 140-1, FIPS 140-2, the NIST "Test Suite" Special Publication 800-22, BSI's AIS publication for physical random-number generators, etc.). For testing a smart card's random number generator (RNG) on-card (i.e. by the card itself, for instance during usage), most smart cards invoke only the most rudimentary tests, in particular, even those are often performed with only a minimum number of random bits to be tested. The latter fact often further weakens the evidence of such a test's response.

Random Number Generators (RNG) are used in several contexts for security, for the generation of random "challenges" for authentication algorithms, numbers for probabilistic encryption, "masks" for protections against side-channel attacks, seeds for signature algorithms (e.g. DSA). The theory underlying these applications makes the hypothesis that the used (pseudo) random generator is indistinguishable from a real random generator.

There are two challenges related to RNG tests and usage: the first one is that a specialized battery of tests for RNG must be found that is well-suited to the inherent limitations of smart cards (speed, memory) and ensures a good enough trust level; these tests should be standardized to be included in the context of formal security evaluation.

The second one is to build such applications with a weaker hypothesis (such as: "the RNG passed the specific random number tests"), instead of the strong (and mainly theoretical) hypothesis above.

FORMAL MODELLING

It is important for the industry to improve the sub-field of tamper-proof and security technologies, which requires the greatest improvement. This still requires considerable research effort before they will produce useful results.

The global challenge is the following: give a formal modelling of the implementation attacks and of the required security in the smart cards and give well-defined methods to avoid these attacks (i.e. countermeasures), that can be formally proven to be efficient.

4.5.3 RESEARCH ORIENTATIONS

4.5.3.1 Short / medium term

Short and medium term development and research on a variety of different areas is proposed to enhance security in smart card environments.

INVESTIGATION AND PREVENTION OF ATTACKS

Existing invasive (= physical) **attacks and non-invasive attacks** have to be investigated further and refined. New attacks, especially active attacks which do not require too expensive equipment to be carried out, have to be developed. Only with the know-how about the attacks can new hardware and software countermeasures be developed and new effective security mechanisms be implemented.

Existing active attacks (e. g. by radiation) have to be further examined. Light sensitivity of the integrated circuits in smart cards, dependencies on the wavelength of the incident light and possibilities to manipulate data or software processes should be investigated.

SECURE CHIP DESIGN AND TAMPER RESISTANCE

It is generally acknowledged that the field of secure chip design and tamper-resistant hardware needs considerable effort in terms of research in order to reach the level of maturity of the field of e.g. cryptography. Research and development must be performed to enhance the physical security for smart card chips by principally adding active protection mechanisms to the chips.

Information leakage (side-channel) effects (e. g. electromagnetic radiation of the chips during the various actions of operation) must be prevented by modifying the chip hardware accordingly and by designing the software programs adequately. The Central Processor Units (CPUs) of the future should not release information through execution times, power consumption, radiation, or others (such as for example diagnostics information) or through the combination of the above mentioned effects. Considerable efforts are necessary to achieve these goals.

Secure logic cells of the processor are needed, which destroy data (or significant portions of the chip through physical destruction) when being manipulated or probed.

Hard, opaque, tamper-evident and removal-resistant coatings for the semi-conductor chips in smart cards must be developed and applied to better protect the processor against physical attacks. A secure coating is hard to remove or, optionally, when removed destroys significant data or portions of the chip.

Top-side and bottom-side shields that prevent various invasive attacks (e.g. by focused ion beam (FIB) probing) and semi-invasive attacks (e.g. by light, laser, X-ray) are to be developed.

Masking techniques against power, radiation and timing analysis (possibly combined with the on-chip random number generation (RNG)) must be further developed.

The smart card chips must employ both environmental failure testing and protection features. Therefore, tamper detection and protection mechanisms via sensors and actors on the chip must be devised. In addition, active tamper response must be integrated resulting in zeroizing confidential information on the chip in case of a detected attack

Secure Built-in Self Test (BIST) techniques must be developed and applied in designing the smart card controllers of the future to overcome obvious contradiction between security and testability.

Chip-hardware design tools must be improved to automatically take security precautions into account (e. g. the place and route functions).

SECURE SOFTWARE (OPERATING SYSTEM, TOOLS, PROTOCOLS, TEST, CERTIFICATION, ETC.)

The whole area of "secure software updates" on smart cards must be carefully investigated. Procedures and features, such as loading applets onto cards employing the flash memory technology, downloading software from networks to cards and susceptibility to viruses while carrying out these procedures, must be thoroughly examined and secured.

The on-chip random number generation (RNG) must be improved in order to achieve an affordable RNG technology which produces high quality of true random bits.

Authentication procedures and protocols which are more secure are necessary. High-performance key generation methods and novel, secure and powerful key-management systems have to be developed.

Secure software mechanisms against non-invasive attacks must be further developed, including software intrusion detection and software defence features against brute force attacks (e. g. by appropriate counting methods). Ways of enforcing security policies have to be developed.

Finally, evaluation methods and measures for hardware and software security in smart card must be developed to be able to classify smart card security.

SECURE HARDWARE-SOFTWARE INTERPLAY

Hardware and software co-design. The goal is to reach a reasonable balance between performance and security in smart card chips and operating systems. Some chips make available a hardware support for cryptography, enhancing both performance and (sometimes) security. However, other features used in secure software components could also greatly benefit from a hardware support. In particular, adding hardware modules dedicated to security could be used by the system to implement smart countermeasures with good performance, such as integrity (checksum) facilities.

The combination of classic cryptanalytic methods with the exploitation of side-channel effects must be carried out further to gain insight in new security improvement potentials.

ADVANCED CRYPTOLOGY

The security of smart cards in the PC and internet environment must be enhanced, due to the increasing hacker community in the internet and the threat of viruses creeping into smart card applications. Digital fault tolerance features have to be investigated. Novel cryptographic security schemes for smart cards in the internet will become necessary.

The performance of high-end cryptographic procedures in smart cards should be improved. Execution times in case of long key lengths must be optimised. The safe integration of the DSA (Digital Signature Algorithm) in smart card applications must be carried out and measures to protect this algorithm against attacks have to be developed.

Especially, cryptographic algorithms which enable on-the-fly encryption and decryption must be developed.

New smart card interfaces, such as the USB (Universal Serial Bus) interface, and the corresponding protocols must be analysed with respect to the fulfilment of security requirements.

Research has also to be done in the field of signature algorithms, in order to be able to compute signatures in low-cost smart cards. There are several such "alternative" signature algorithms that are particularly well-suited to smart cards but their exact security still has to be determined.

In addition, further research in the design and validation of cryptographic protocols must be undertaken, especially in the context of privacy protection and fault tolerance (more rigorous treatment of unexpected card tear, communication errors, etc.). This is particularly relevant if smart cards increasingly become "ordinary" members of a large distributed system.

For contactless card applications algorithms must be developed which are fast enough to meet the short interaction times with the contactless terminal and which are suitable for the low power environment in the contactless card scenario. The security of the air interface between the contactless card and the card reading device must be enhanced.

4.5.3.2 Long term

The following long-term term research and development is proposed to enhance security in smart card environments.

SECURE SOFTWARE (LANGUAGES, COMPILERS, VALIDATION TECHNIQUES AND SOFTWARE CERTIFICATION)

Research in software security for smart cards has as its aim to provide methods, theories and tools that can help increase the confidence in the software that executes on a card. This issue should be addressed both at the programming platform level (design of programming language, development of certified operating systems and optimising compilers) and at the application level (software engineering of efficient, secure, certified applets).

The Java Card language has become a de facto standard for programming smart card applications. Research should contribute to the successors of this language (be it object-oriented or other) and notably its security architecture in order to obtain a language well suited to handle the secure dynamic loading of applets. The design of the Java Card firewall and the accompanying notion of shareable objects should be analysed to provide a security architecture that is both light-weight and flexible.

Optimised compilers are necessary for fitting high-level programs on smart cards. At the same time they are notorious for introducing subtle errors that potentially can be exploited to compromise security. It is thus necessary to develop compilation and optimisation techniques that can be proved correct formally and automatically. Functional correctness is not sufficient to ensure security, but it is clearly required. At the same time, compilers that produce safe code must be developed. For example, in case of failure of a critical or security related test, it should not be possible for a single glitch to be able to override the result of the test (a "glitch" being an external interference such as voltage or radiation etc. that causes the smart card chip to behave abnormally.)

At the application level, techniques and tools should be designed to prove that applets adhere to a given security policy. Such techniques could stem from static program analysis, automated theorem proving or software testing, or a combination of these. The integration of these techniques into a validation methodology is still an issue of research that should be pursued. Another issue requiring substantial fundamental research is to what extent these validations can be carried out on-card, thus freeing the card from relying on third-party verification and signed code.

Security policies must be analysed and transformed into a collection of formal security, specified in a formalisms that allows their verification by formal methods. The generally acknowledged problem of specifying availability (or denial-of-service) type properties is particularly important in the smart card setting, and a special effort is required here.

The results emanating from the above activities should be integrated with the software certification process such as that outlined in the Common Criteria. To reach the highest level of certification a considerable effort in terms of formal software development is required. Research should be conducted aiming at developing methods and tools that can assist and facilitate this process. This would cover formalisms for specifying smart card software such as (subsets of) the Unified Modelling Language UML or or the Java-oriented Java Modelling Language (JML) together with techniques for refining high-level specifications into low-level code. This would also include a methodology for automatic test case generation for secure smart card software (formal methods) that should be developed. Most challenging is the quality of testing, which not only translates into various forms of specification and implementation coverage. Notable development efforts for improvement include: (1) firmly grounded and automated measures of testing quality and (2) quality guaranteed by construction, e.g., using a systematic methodology and test generation tools

Work to make Field Programmable Gate Arrays (FPGAs) a standard feature on smart card ICs must be carried out. By using FPGAs on smart-card IC for crypto-coprocessors, it will become possible to re-configure cryptographic co-processors even during the usage life-cycle, for instance by the card issuer to update an improved version of a crypto-accelerator. The concerns with re-configurable hardware in smart cards towards security policies and security evaluations of smart cards involving FPGAs must be investigated. The opportunity of an "FPGA-update" (in contrast to a "software update") is currently hardly addressed by the whole scenario of evaluation (e. g. Common Criteria) for smart cards but becomes imperative on a short to medium-term perspective.

Research work aiming at secure smart card operating systems which are tamper-proof against invasive and non-invasive attacks must be carried out.

HIGH-END CRYPTOLOGY

It is generally acknowledged that good cryptographic tools (e.g. for signature, encryption, authentication) exist and continue to be developed by researchers. Generally, the tools and their limitations are well understood. It will be necessary to continue in enhancing the security of known, popular techniques that are in common use today. Breakthroughs in cryptography that will force increase in key-sizes, especially in public-key cryptography, are very likely. It will be very likely that new weaknesses are discovered in newly introduced symmetric algorithms (such as the new AES). The impact of such findings on the smart card industry must therefore be investigated and estimated very carefully.

In practice, due to price and performance limitations, the best cryptographic tools available are not always used. The recent years have borne a significant progress in point-counting algorithms for elliptic curves over finite fields. Currently, the implementation of such algorithms on smart cards for on-card elliptic curve generation is impeded by the time- and memory-consumption. It is therefore necessary to continue research into the issue of how these novel encryption techniques can be implemented on a smart cards.

4.6 MICRO-ELECTRONICS

4.6.1 SEMICONDUCTOR TECHNOLOGY TRENDS AND MARKET REQUIREMENTS

4.6.1.1 Technology trends

MICROELECTRONICS PROCESS APPLICATION TO SMART CARDS DEVELOPMENT WITH REGARD TO ITRS REFERENCE AND ANALYSIS

Smart card Integrated Circuit (IC) development follows the evolutions of the semiconductor technology in terms of front-end process, mixed technologies integration, power consumption constraints and design technique. The smart card IC has become a real and complex Secure System on Chip (SeSoC) including new CPU core, memory management, security functions, dedicated IP blocks and native embedded software. Due to the technology trends, the die size of the chip is decreasing following the technology features process but the market needs contribute to increase the data processing capabilities, the memory size and the global processing power requirements of the smart card integrated circuit.

The scope of RESET is not to redefine a global technology road map already done and updated in the ITRS, the International Technology Roadmap for Semiconductors (a Semiconductor Industry Association’s Initiative), but to highlight the main differences between the ITRS road map and the Smart Card requirements, with the view to reduce the gap between both.

The International Technology Roadmap for Semiconductors (ITRS) is the result of a worldwide consensus building process. It predicts the main trends in the semiconductor industry spanning across 15 years into the future. The participation of experts from Europe, Japan, Korea, and Taiwan as well as the U.S.A. ensures that the ITRS is a valid reference for the semiconductor industry as regards to historical advancement of semiconductor technology and to worldwide integrated circuit (IC) market. The Semiconductor Industry Association (SIA) coordinated the first efforts for producing what was originally the National Technology Roadmap for Semiconductors (NTRS). The NTRS provided a 15-year outlook on the major trends of the semiconductor industry. As such, it was a good reference document for all semiconductor manufacturers. The NTRS documents provided useful guidance for suppliers of equipment, materials, and software and clear targets for researchers in the outer years.

Table 4. Technology characteristics/requirements (according to 2002 ITRS update):

key lithography-related characteristics by Product types:

Year of Production(in nm, current or estimate)	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2010**	**2013**	**2016**
DRAM ½ pitch	130	115	100	90	80	70	65	45	32	22
MPU ½ pitch	150	130	107	90	80	70	65	45	32	22
MPU Printed gate-length	90	75	65	53	45	40	35	25	18	13
MPU Physical gate-length	65	53	45	37	32	28	25	18	13	9
Smart card chip MCU	**<500**	**250**	**180**	**150**	**130**	**115**	**100**	**TBD**	**TBD**	**TBD**

Due to its market share (less than 1%), smart card industry is not a significant market driver for the semiconductor technology. Nevertheless it is facing some complex/multiple technologies integration issues (NVM, very low power, wireless interface, limited die size, tamper-resistance, etc.).

It has to be noted an acceleration (pull-in) of the requirements for more advanced technologies in the global electronic industry, which is not necessarily compatible with the long smart card deployment cycle-time, although new threats and security attacks would require the opposite (i.e. to be synchronized or in advance compared to the technology introduction cycle).

SMART CARD IC DEVELOPMENT MAJOR CHALLENGES

The generic features for evolution are the following:

- Die size optimization (for cost effectiveness)
- Packaging environment
- Security requirements
- Performance optimization:
  - Platform architecture
  - Power consumption continuous reduction
  - Easy third party IP integration and re-use
  - IP protection through design
  - Rapid and cost effective development environment
- Compliance with Semiconductor Industry technology road map (ITRS reference)
- Integration of reliable, flexible and fast high-density Non Volatile Memory technologies, with high density RAM.
- Dynamically re-configurable devices, on a longer term
- Endless challenge for meeting the security requirements versus the technology limits created by the ITRS road map, as well as cost and testability constraints.

Memory types

In addition to EEPROM, several new Non Volatile Memory (NVM) technologies are considered as valid for meeting the requirements of advanced smart card applications, such as faster access time, higher memory capacity with smaller cell size, low power consumption and higher endurance and retention times.

FeRAM technology, where volume production started in 1996, will support very fast writing and low power consumption features required by card software programmes. Flash memory is an alternative technology for increasing the capacity of NVM into smart card ICs.

Next generation of FeRAM, MRAM, PCM (Phase Change Memory) and more recently introduced RRAM, which are currently undergoing heavy R&D programmes in laboratories, will provide ideal features to replace the whole range of memories, ROM, RAM and NVM, for the next generation smart card.

	FeRAM	**MRAM**	**PCM**	**Floating gate memory**	**Charge trapping device**	**Notes**
Data storage	Ferroeclectricpolarization	Magnetic polarization	Phase conversion between crystalline and amorphous	Charge on floating gate	Charge trapping oxide	
Switching time	Less than 1ns	Less than 1ns	Less than 10ns			Switching time of PCM is limited by heating and cooling
Access time	Over 30ns	Over 2ns	Over 50ns	Over 30ns	Over 30ns	Access time of FeRAM depends on bit line capacitance like DRAM
Write endurance	10^{12} ~ unlimited	Unlimited	10^{12} ~ unlimited	10^{6}	10^{5} ~	Fatigue
Read endurance	10^{12} ~ unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Since FeRAM read is destructive and requires rewrite, read endurance is limited
Switching energy	C*V^2 (a few pJ/bit)	I*V*t (a few hundreds pJ/bit)	I*V*t (a few hundreds pJ/bit)	10-100 times on page basis ***	100 times (1 kcell)***	
Cell size	50F^2 (0.35um, FJ*) 40F^2 (0.18um, FJ) 35F^2 (0.13um, TI) 15F^2 (0.25um, Samsung **)	9F^2 (0.6um, Motorola)	8F^2 (0.18um,Intel)	16-20F^2 (0.13um)	4-8F^2 / bit (including multi-level storage)	DRAM over 8F2SRAM over 100 F2NAND Flash, 5F2

Note: C: capacitance, V:voltage, I: current, F: design rule
* embedded (CMOS technology) under volume production
** stand alone (DRAM technology)
*** write energy, comparing to FeRAM

Low power design

Asynchronous design provides new capability for smart card IC, as it needs reduced power consumption, thus better complying with security requirements. Today smart card asynchronous design has been demonstrated in the US (ASYNC technology) as well as in the European Union. European projects, such as MEDEA Espass-IS or IST G3 Card, are addressing study and design of RF platforms based on asynchronous logic.

Dynamically re-configurable devices

Re-configurable devices are not currently part of the smart card design, but re-configurable techniques are used in the semiconductor industry to perform rapid prototyping through flexible and updated products. The process evolution in smart card allows investigating the use of re-configurable blocks into the smart card IC, and providing adaptable ICs for a large amount of applications such as cryptographic functions, HW acceleration, new I/O modellisation ,...

4.6.1.2 Market requirements

From both smart card and semiconductor industries standpoint, the market requirements are:

ON A SHORT/MEDIUM TERM:

– Telecoms

  Multiple applications services / very large account oriented
  Semi complex on board services
  Full applications download (Over the Air for Applet size < 10 / 15 KB)
  Limited applications update (1 to 2 KB, OTA)
  ID proofing
  End Users access applications
  Operated services (customer profiling, Customer Relationship Management)
  Continuity of services
  Dual interface communication (Contact / contact-less)
  New PK / non PK algorithms (AES, RSA 1024 & 2048, EC)

– IT / ID markets

  Complex matching algorithms for biometry
  Hi- speed communication secure protocols (like MMC / USB for DRM applications)
  Complex encryption hi speed algorithms (Full speed on line encryption for Digital Right Management)
  New PK / non PK algorithms (RSA 2048, EC, AES)

– Financial services

  Dual interface communication (Contact / contactless)
  New PK / non PK algorithms (RSA 2048, EC, AES)

ON A MEDIUM/LONG TERM:

Generic services

- Services management service (locate, instantiate and operate new services)
- Communications services (Unified API for ISO 7816, 14443, Full duplex, TCP/IP, USB, XML)
- Repository services (Unified way to access any type of data)
- Power management services (configurable power regulation)
- Security events services (Security audits configurations, log, reports, actions etc..)

Telecom

- Highly interoperable multi-application platforms (non very large account oriented)
- Complex on board services
- Full applications download and management (OTA) (Applet size ~ 32 KB)
- Full applications update
- End-users access applications
- Advanced interactions with handsets
- Complex operated services (Profiling, CRM, RDM, Privacy management …)
- ID / IT markets

- Biometry on cards (fully integrated)
- Secure Multi Media Card-like products
- Distributed applications model for the card in the IT world
- CRM, DRM applications

Other markets

- Multimedia cards
- Multi-components cards (Displays, power on board, sensors)

4.6.2 SCIENTIFIC AND TECHNICAL CHALLENGES

The main objective here is to define how smart cards technologies (applications, functions, utilisations) and marketing requirements will influence the architecture of smart card SOC (System-On-Chip) devices, in the next 3 to 5 years period.

4.6.2.1 On a short/medium term

	Impact on Chip technology
Javacard standard evolution (→ V 2.2)	
Stronger interoperability	Silicon independent card O/S
Use of RMI (remote method invocation)	Comm, I/Os / CPU performances
Logical channels to access memories	NVM technology
Garbage collection	Memory Protection/Management Unit
New cryptographic API (RSA 2048, AES, Elliptic Curves)	Dedicated H/W or ISA
Biometric API	
Embedding card manager (for install / uninstall of applets)	Memory Protection/Management Unit
Javacard O/S will reach 200 / 300 KB	Memory size
Improved security levels (→ EAL 5+, 6, 7)	
Resistance to fault attacks	Chip architecture or design methods
Tamper resistance	H/W sensors
Applets verifiers	
New algorithms and appropriate countermeasures	Specific ISA
Memory protection and partitioning	Memory Protection/Management Unit
Better resistance to non invasive attacks	Design methodology
Card interface with external networks and systems	
High speed communications protocols	Comm. I/Os
Distributed applications architectures	Comm, I/Os, CPU speed
Client / server architectures	
Increasing need for computing power	CPU architecture
Contactless / contact communication capability	Multiple I/Os / UART
Multiple browsers on board	Memory size / NVM technologies
Dynamic memory management	Memory Protection/Management Unit
Low power compliance (GSM / 3G)	Chip architecture / PM
Card manufacturing Process	
Smallest die size as possible	IC process technology
Low cost assembly process	Reducted test flow / quality
Personalization	Specific I/Os / Fast writing NVM

4.6.2.2 On a medium/long term

	Impact on Chip technology
Javacard standard evolution (→ V 3.0)	
Evolution toward J2ME	Size of ROM / RAM
Javacard O/S may reach 512 KB	Size of ROM
Migration of Toolkit (STK) toward Javacard Applet	
Distributed Javacard applications becoming a de facto model	Computing power / I/O communication speed / MMU
Card will run in a client / server environment	Memory Protection/Management Unit
Addressable memory size will reach 1 Mbyte	CPU architecture / memory techno.
Average size of applets will be above 32 KB	NVM memory technologies
Enhanced interoperability	Open architectures for CPU
Enhanced garbage collector / No persistent heap	MMU
Multithreading / Multitasking operations	Logical memory access
Performances will request all Java Object in RAM	RAM size or technology
O/S will be optimised for 32 bit chip architectures	32 bit CPU - ISA
Biometry API / Full Java compliance	Specific H/W, FPU
Improved Security level (Above EAL 7)	
On Card applet verifiers	Dedicated hardware
Embedded Security audit systems	
Improved tamper resistance	
Improved fault tolerant architectures	Chip architecture / design methodology.
New algorithms	Specific H/W or ISA
Card Interface with external world	
Distributed Javacard applications	Fire wall / comm I/Os/ MMU/CPU
Integration of cards in frameworks for back offices, handset, terminals	Comm,I/Os,chip architecture/CPU
Operated services	NVM technology and MM
High speed communications protocols	Comm. I/Os
Low power compliance	Chip architecture / PM / Chip technology.
Card manufacturing/ management requirements	
Low cost manufacturing	Chip size / Auto test features
Performant personalisation process	NVM technology, Comm, I/Os
OTA management	NVM technology, MM, Comm, I/Os

4.6.3 RESEARCH ORIENTATIONS FOR IMPROVEMENT

4.6.3.1 Short/Medium term

Memory management unit/memory partitioning unit

High speed communication interface

Standard communication protocol support with card acceptor and network servers

High performance Non-volatile Memory (size and type)

Power consumption optimisation

Improved tamper-resistance

4.6.3.2 Medium/long term

The same as above, plus:

Fault tolerant design

H/W device re-configurability

Easy manufacturable & cost effective Camouflage technology

Single memory technology to replace RAM and NVM with same performances

Multiple IP integration, intensive IP re-use for both hardware and software with proven security and IP protection.

CONTRIBUTION TO THE ROADMAP

The main market drivers mentioned are:

Open card platform (mainly Java)

Security level for value-chain stakeholders IP protection and consumer’s privacy protection

Card interface with external environment

Manufacturing process

4.7 SYNTHETIC OVERVIEW

The following table contains a synthetic overview of the technology challenges described in the previous sections.

ITEMS	COMPONENTS	SYSTEM	Trend	TIMEFRAME
Communication / Networking	Multi-tasking OS Mass storage memory Low power/energy	Internet IPv6 High speed communication protocols	Consumer appliances Peer to peer exchanges	Short / medium term
Software platforms	Multi-application OS High level programming language Trusted development tools	Card SW management	Dynamic and remote SW management within Information Systems Mobile information devices	Short / medium term
Card accepting interfaces	Integrated HW component platform Extended authentication protocols (biometry) Wireless communication to network (low power)	Interoperability for multi-application schemes Integration into hosts Reader SW management	Dynamic and remote SW management within Information Systems	Short / medium term
Smart objects	Embedded peripherals (display, sensors, keyboard, interface chip, antenna)	HW & SW architecture Power supply for wireless interface	Consumer appliances Peer to peer exchanges Preventing central databases management	Medium / long term
Security technologies	SW: Enhanced cryptographic components Embedded random number generator HW: Secure logic cells design	Certification of security HW and SW attack modelling HW & SW codes co-design	Safe access to open networks and content Increasing user’s control of the personal device	Medium / long term
Micro-electronics	Non volatile memory Asynchronous designChip dynamic reconfigurability Memory management/partitioning	Tamper resistance Single memory technology Dual interface Configurable power management	Continuity of operated services Consumer’s privacy	Medium / long term

5 SMART CARD ENVIRONMENT FOR BUSINESS AND TECHNOLOGY DEVELOPMENT

5.1 DRIVING FACTORS

5.1.1 BUSINESS OPPORTUNITIES AND MARKET REQUIREMENTS

Enhanced business opportunities for IC Card will rely upon two major drivers:

- Local markets where smart card lags way behind other types of installed technology. This situation can be found in areas as strategic as North America, where magstripe cards are still widely used
- Application markets where smart card has not yet met technical and/or marketing requirements

In both cases, smart card will have to closely stick to the emergence of new networked environments, to innovative business models enhancing provision of services and applications and to users' expectation for convenience, trust and cost effectiveness.

The "smart card for everyone" scenario still clashes with serious obstacles, relating to both card and CAD features:

– card:	security in remote dynamic application management
	cost effectiveness, compared with other two-factor authentication tokens
	privacy management in multi-purpose schemes
	service providers branding in multi-application schemes
– reader:	lack of interoperability, preventing card multi-acceptance
	need for cheap, portable and easy-to-use CADs

Therefore, service providers and retailers still endorse a "show me the value" position.

However, strong business opportunities still emerge on the smart card market roadmap, linked to its safe data storage/processing capabilities, its personal and ultra-portable device features and to the benefit it provides to the issuer of a strong and loyal link with subscribers/consumers.

e-business services

Open wired and wireless networks will require personalised online access to e-business and e-government applications, supported by chip-based strong authentication and e-signature mechanisms. The e-Europe 2005 initiative reflects member states' requirements for secure infrastructures and accelerated deployment of e-government services. Smart cards and trusted personal devices will have the responsibility of safely handling users' digital identity, for both consumer and business applications. Therefore, smart card position as proven technology to support access and consent in e-services will be reinforced.

Protection and management of digital content

The Internet has become a global copy machine of protected digital content. Music industry is already paying the price of huge piracy activity with decreasing business; same will happen for film/video industry with even higher potential economic impact. Protection mechanisms implemented at this stage are not strong enough to resist hackers' combined effort. Awareness for safer solutions should support increased demand for "trusted web assistant" devices.

Next generation wireless framework

The 3G revolution will bring smart card industry into a cycle of dynamic business through a renewed eco-system, where online multimedia services, information on demand, gaming, "daily life services" will rely on data management, supported by high-end SIM cards twinned with new generation handsets. The ground for m-commerce, which has not yet reached its targets due to a lack of standards and fragmented technical implementations, will be therefore established and the card will have the opportunity of reinforcing its position of ID trusted carrier, supporting ubiquitous and interactive links between network operators, third party service providers and subscribers/customers.

Ambient intelligence and smart portable objects

The need for secure tokens to identify users and reflect his/her personal preferences, in both home and professional environments, offers a sound business opportunity for smart card, as far as it fits with required evolutions in terms of shape and format, secure and fast communication channels, user-friendliness,… In this area, a migration towards a concept of "trusted personal device" built upon a smart card technology platform approach is expected. Evolution towards wireless local area (W-LAN, WiFi) access points to network will support as well this evolution.

Contactless access to services and goods

The current market share of contactless card products is still low, due to lack of shared standards, absence of product security certification, difficulties to implement multi-application card schemes,… However, market analysts forecast that contactless technology will progressively replace contact in most of applications where twinned physical and logical access is required, be it for information, communication or transaction. The current migration to electronic fare collection in public transport infrastructures will support the evolution towards large scale implementation of reliable contactless technologies, with a good level of acceptance from users.

Traceability

The smart card technology assets can be obviously transposed into systems required for goods traceability, where disseminated identification management through portable contactless objects is progressively replacing centralised database management systems, at least in closed environments. This provides a huge opportunity for assembly and packaging technologies when contactless traceability systems take place in open environments, such as retail logistics.

5.1.2 SECURITY: "ARMS RACE" BETWEEN ATTACKS AND COUNTER-MEASURES

Smart card technology evolution will be impacted by the continuous competition between attacks and counter-measures. The smart card technology providers must keep an advance on the techniques used by the hackers, whilst the pressure of potential attacks on key components for secured applications will be steadily increasing in the future, because:

- The means at the disposal of hackers and organised crime increases continuously: sophisticated SW and equipment is at the reach of everybody, PC computing power has reached the level of supercomputers in the past
- The Internet has increased potential threats as far as:
  - knowledge on security and attack techniques is spread around the world
  - number of potential hackers and cooperation within hacker networks is increasing, along with level of "creativity" generated in hacker competitions
  - combined computing power (e.g. 100s of PCs involved in breaking into the security mechanisms)
  - etc.

This situation forces smart card technology providers to continuously improve security techniques, while fulfilling constraints of limited system resources, meeting requirements for low implementation cost and preventing decrease of overall performance (e.g. for the implementation of high-end cryptography).

In order to maintain and increase trust of card issuers and consumers in smart card technology, they need to keep an advance on potential new attack techniques or weaknesses that have appeared and develop counter-measures. It is also anticipated that the need for trust and confidence will also result in an increased demand for security certification and standards.

5.1.3 INCREASED CONSIDERATION FOR CONSUMER REQUIREMENTS

Privacy concern, trust, confidence and convenience will be major drivers (or blocking factors) in the deployment of smart card applications. Consumer expectations must be better taken into account in the definition of smart card features and in the design of smart card products and applications. In that sense, meeting the following targets is important for evolution of smart cards:

- **Direct interactivity** between user and smart card: this will drive development of technologies to implement user interface components and power sources on the card,
- **Fraud reduction**: the consumer should be confident that the risk he takes when using the card for e-transactions is clearly managed through agreement with card issuer and service/product provider
- **Multi-application** card, for reducing the volume of plastics in the consumer's wallet, pin codes to remember, and extending its use to a role of "web assistant" or "convenient data storage device".

5.1.4 PRODUCT COST AND INTERNATIONAL COMPETITION

The opening of new markets is stimulating competition. East-Asian countries, with particular notice to China, offer tremendous market opportunities for smart cards and the current growth rate of µprocessor cards is already higher in this part of the world than in Europe. Local production is a political priority (development of the smart card industry is a target mentioned in China's 5-years plan from 2001-2005) and the smart card industry leaders have installed manufacturing facilities in the most important Asian countries. However, price pressure for standard mass-application smart cards (e.g. banking cards) is already tough; it is anticipated that competition for supplying such products will be multiplied with products from low-labour cost countries

In another part of Asia, namely Japan and Korea, major investments are made in contactless technologies, targeting market opportunities for smart ID cards.

Therefore, innovation and technology leadership are key assets for European smart card providers, with the view to tackle new industry competitors and to limit financial margins erosion.

Innovation is also the way forward to maintain a position in entry level products:

- Security technology used in smart cards (cryptology, attack counter-measures, etc.) needs to be optimised for low cost implementation
- Manufacturing cost can potentially be reduced with improved production technology.

Faster time to market is also a factor to improve the competitive position. Again innovation and technology advance are key to improve performance in this area. In particular more standard smart card HW and SW components, more powerful development and integration tools, etc. are needed to speed up the process from product specification to commercialisation.

5.2 BOTTLENECKS

5.2.1 HETEROGENEOUS CHIP ARCHITECTURES AND OPERATING SYSTEMS

In the early days of micro-computers, many architectures, operating systems, coexisted, system resources where very limited, one could hardly find a decent programming language and there was no interoperability. The situation changed when IBM introduced the PC and DOS, which was immediately considered by the whole micro-computer industry as a reference and market standard. This fact has enabled optimisation of RTD effort, accelerated innovation, and extremely fast evolution of powerful hardware and software components targeting this platform.

A similar evolution has not (yet?) happened in the smart card world. The lack of common hardware and software architectures is an obstacle for the provision of more sophisticated and optimised development tools, compilers, adapted languages, test and integration tools, etc.

Much effort is consumed for porting exiting software from one smart card product to another w/o real added value (other than e.g. ensuring a second source).

It also hinders the development of more sophisticated operating systems. In order to achieve a certain level of HW independence, platform independent OS and interpreted languages are used, but these solutions have major constraints in environments where system resources are scarce.

The current situation is generating important drawbacks, such as:

- SW development effort / cost / time
- Less efficient code optimisation which is more difficult; partial hand-coding is still required for specific SW routines
- Increased cost for test / qualification / conformance test / certification.

5.2.2 WEAK CONNECTIVITY TO IT AND CONSUMER WORLDS

There is currently no smart card slot in PCs or consumer appliances, except for encrypted TV decoders. This situation is the demonstration that smart card is not yet a fully acknowledged "networked object". Therefore, specific effort should be undertaken for enhancing card connectivity to the three major environments of the global information society:

- IT/PC systems
- Consumer/home appliances
- Mobile wireless networks

In terms of technical improvements, the major efforts should address the communication performance: speed and security of the link with accepting device, be it wired or wireless, then the card memory capacity, targeting megabytes instead of Kilobytes, and power consumption for improved autonomy of portable devices. Particular consideration should be given to Internet and IPV6, with regard to the management of applications, cards and readers over the network.

5.2.3 LACK OF CARD ACCEPTING INFRASTRUCTURES

A "smart card for everyone "scenario is not so much putting a card in everyone's hand. The key issue is to provide end users with card accepting devices that are small enough, easy to use (or to install if it is not a stand alone reader), and cost effective, for making them familiar with this device. Accessing networks from ubiquitous connecting places is already a reality with individual wireless devices (SIM in handset), but there is no equivalent in IT/PC and consumer appliances, although requirements for security are the same (authentication, proof of consent). The chicken and egg scenario between availability of services and provision of CADs will end when standard device architectures facilitate acceptance of the same card towards different services. Industry convergence around common specifications such as STIP or FinRead should help solving card readers' availability problem.

5.2.4 LIMITATION OF AVAILABLE COMPONENTS, MATERIALS AND CARD ASSEMBLY TECHNOLOGIES

SC CHIPS

The production of chips for smart cards is a quite small part of the total business of silicon founders - less than 1% of the total chip market. Price pressure on smart card chip is quite strong: components must be cheap, whilst at the same time they have a number of specific constraints: mix techno (microprocessor cores + logic + RAM + NV memory + sensors, etc.), chip size, specific security requirements, etc.

Investment in smart card specific chip design, production technologies and equipment is quite limited in view of the potential revenues. Furthermore inerty in innovation is increased due to severe requirements regarding to security and certification.

Problems resulting from this specific context include:

- Smart card chip technology behind state of art in other IT domains (e.g. components for PCs)
- Most smart card chips are still based on very old 8 bit µC cores, with limited processing power, limited memory capacity, etc.
- More sophisticated system resources are difficult to implement: memory management units, multi-tasking OS, etc.

OTHER COMPONENTS

Although the "traditional" smart card has only one chip, in future smart cards with extended functionality more components are needed to enable autonomous functioning of the card or for increased interactivity with the user would. For the time being the offer of existing components does not reach the level of functionality, size, robustness, cost, etc. targets that are mandatory for smart card applications.

Strongest demand for such components is expected for:

- **Power sources**: current smart cards are mainly powered through card reader, hence operational whilst inserted in a card reader (contact cards) or in the proximity of a terminal (contact-less cards). An on?card power source is needed to break the barrier of card reader dependence and to allow the smart card to be operated anywhere. However on-card batteries are still expensive and life time too much limited. Furthermore embedding of multiple components is more complex and innovation is required for enhanced manufacturing processes, including assembly, interconnect, testing, etc. (see below).
- **Components to support smart card extended features**, in particular to enable a certain level of direct interactivity with the user (card holder): innovative solutions concerning displays, sensors, keyboards and knobs, buzzers, etc. that can meet the requirements of the smart card environment and cost and manufacturing constraints are needed.

MATERIALS

Smart cards are exposed to a strong environmental stress. Current smart card applications are typically targeting life time of 1 to 2 years (e.g. loyalty cards, bank cards). The most cost efficient materials are chosen to meet these requirements.

However for new smart card application, such as electronic ID cards, drivers license, travel documents etc. or future secure personal devices a longer life times (>3 years) would be more appropriate. New materials for card bodies, interconnect, etc. are needed that meet the new life-time requirements, cost constraints and manufacturing specificities of smart cards applications.

New materials are needed to:

- Produce cards with increased durability but low impact on production cost,
- Compatible with environment protection and workmanship safety policies, etc.

ASSEMBLY TECHNOLOGIES

Card assembly, interconnectivity technology needs to be enhanced in order to:

- Handle thin chips
- Handle and interconnect multiple components on an card
- Increase reliability, robustness to environmental stress, life time connectivity standards.

5.2.5 LIMITATIONS OF AVAILABLE DEVELOPMENT, TEST, INTEGRATION AND CERTIFICATION TOOLS

The means at disposal of smart card industry product development units are behind the average in other IT sectors; because of the issues mentioned above, the software, tools and equipment needed for development, test and integration is less powerful and optimised.

In particular:

- There is no language support for smart card specific aspects, some general features of Java are missing
- For cost and scalability problems formal methods are used only for some parts to be certified; limitations of code optimisation by compilers, poor simulation and debugging tools
- No dedicated tools/equipment for system Integration and Card application management,
- Poor middleware: middleware concepts not yet well established in the smart card world
- Lack of suitable environments to carry out CC evaluation

The drawbacks of this situation are:

- Increased development cost,
- Longer time-to-market,
- Risk of products not being optimised for robustness,
- Difficulty (or impossibility) of certification,
- Reduced take-up by system integrators of smart card who do not know how to integrate them.

5.3 CHALLENGES

This chapter will introduce the main technology priorities assessed by each of the 6 Working Groups of the RESET project.

5.3.1 COMMUNICATION AND NETWORKS PROTOCOLS

The smart cards will continue to be used as personal and trusted devices, with a better integration within their environment and high speed interface. However, a major challenge will be to fully integrate them into an interconnected IT world. For the time being, networking features are supported by the card accepting device, which has a privileged physical connection with the card. This current communication model should be overcome, through an evolution where card becomes a non-limited node of the network, as regards its embedded communication capabilities.

The scientific and technical challenges introduced hereunder are targeting three levels of requirements:

- physical link between card and terminal
- communication protocols with networked environments
- integration and management in networks

Performance improvement

In the context of the emergence of new protocols, it is now time for the smart card to enhance its communication capabilities, according to the state of the art in the world to which it is connected.

It is necessary to improve the interface in both the wired and wireless modes. As an example, the following targets should be considered:

- High speed protocols: from Kbit/s to 100Mbits/s data rate
- low power consumption
- full-duplex

Connectivity enhancement

From a communication and networking standpoint, the evolution towards open platform will be achieved when the smart card is the position of being smoothly integrated into the interconnected IT world. Following targets for research should be considered:

- TCP/IPv6
- Security of the link
- Wireless protocols

Support new communication model

True multi-applications smart cards require that different applications could simultaneously have access to resources available (communication stack, NVM memory, etc.). This will undoubtedly impact the underlying Operating System. In this context, following topics seem to be relevant:

- Multi-tasking OS
- faster NVM access
- enhanced RAM capacity

5.3.2 SYSTEMS AND S/W

5.3.2.1 Operating Systems and High Level Languages

Flexible, multi-application smart card environments should be supported by appropriate operating systems with standard operating system (OS) features, such as multi-threading and high-level memory management, and new OS features required by smart cards, such as resource control management (deadlock prevention/detection, optimised resource usage), or enhanced transactions (in particular with respect to multi-threading). A medium to long-term objective is to address real-time issues, which will be more and more critical in future applications. Such issues include in particular mastering the execution time of the OS primitives, predicting execution time of application codes, and scheduling real-time tasks in accordance to their respective deadlines.

Longer term R&D topics should target micro-kernels that support different smart card platforms, and open source OS with expected benefits of portability, flexibility and interoperability. They could help smart cards to evolve towards full-fledged, secure autonomous computers and could make the smart card a full partner on the network, for example by allowing to connect to a smart cards like to an ordinary web server, from web browsers via IP address or network name, by using XML protocol to enable XML based card applications, and by supporting a variety of application frameworks (Java,.NET, HTML, XML) in a single card.

5.3.2.2 Development Tools

Programming languages for smart card applications should be made more expressive by integrating features present in general-purpose programming languages, for example garbage-collection and threads that exist in Java, or type abstraction and genericity that exist in Modula 3 and generic Java. Additionally, there is a need to provide appropriate support for smart-card specific idioms such as byte-level manipulations, including APDU-based communication protocols, transactions and atomic memory updates, or event-based programming. Such idioms are often difficult to express in general purpose programming languages, and would benefit from the use of suitable domain-specific languages (DSL) that reflect by design the characteristics of the intended application domain, and hence provide maximal clarity, safety and conciseness for programming within this domain. Finally, existing compilers should be improved to produce better executable code.

In the longer term modelling and specification languages should be considered in the design of the programming languages themselves, rather than considering formal methods as an afterthought with significant fallbacks in the quality of smart card software. For instance, emphasis on program proofs favours declarative language constructs over imperative ones; and emphasis on model checking and formal testing favours programming via finite-state machines.

Validation should be facilitated through the development of compositional methods and of appropriate mechanisms for reusing validation proofs when changing/updating parts of a system. Furthermore clear validation strategies are required to determine where provability and testability could collaborate or supersede each other; in particular, it would be highly desirable to device methods to decide when a test is pertinent enough to substitute for a proof. As a further step to adapting development tools for smart cards, a range of dedicated development tools should emerge, that are cost-effective and accessible to non-experts,

5.3.2.3 Systems Integration and Card Application Management

An increased use of formal modelling and formal verification needs to be supported. On the other hand, development tools should be tailored to the perceived needs of the smart card industry, in particular with respect to certification and to the development of secure, trustworthy and optimized smart card systems. There is a strong need to develop environments that support, in a cost-effective manner, all aspects of certification: risk analysis, edition of security targets, system design and development via checked refinements, testing, formal modelling and verification. The security and optimization of the smart card systems should be addressed both at the level of the platform and at the level of applications. Concerning smart card platforms, there is a strong demand to derive efficient implementations and high-quality test suites from formal models, and to design specialized tools that reduce the cost of producing /maintaining formal models. Concerning applications, there is a need to develop integrated environments that provide an adequate interface between programming languages such as JavaCard, modelling languages such as JML, and verification tools based on testing, static-checking, model-checking or formal verification. Smart card applications would also benefit from precise program analyses that address smart card specificities such as persistence, atomicity, or specific run-time environments, and that focus on sensitive properties that are highly relevant to smart cards, including confidentiality, atomicity of updates, or exception raising.

System Integration should be improved through integrated tools that permit the development of applications in a global framework. These tools should fit in different usage scenarios: 3G Mobile Networks, TCP/ IP based networks, etc. Enabling middleware technologies should be developed or improved, such as RMI or MIDP.

In the medium-term, design models and design methodologies should be sought. In particular there is a need for a design methodology for identifying the right application model to be used by on-card software when an application is delegating parts of its functionality to a smart card, and for design models related to the management of the smart card.

In the long term system Integration should be facilitated by a framework that supports advanced smart card programmability and usage: extensible and scalable on-card and off-card framework, dynamic management of card framework services, etc. To achieve such goals, it is mandatory that adequate OS are used.

5.3.3 SMART CARD ACCEPTING DEVICES, INTERFACES AND BIOMETRY

The current smart card is to a large extent a slave of the reader. The main challenge is to make the relation between card and terminal more balanced, and to optimise the connection between card, reader and network in terms of security and cost-effectiveness.

To achieve this balance, the distribution of functionality between the smart card, the reader and the network must be changed. Currently the smart card is mainly a secure key storage device with limited processing capability, albeit adequate for current applications. Interfaces from the card to the user and the network are completely mediated by the reader. Depending on the application area, there are two scenarios of change possible:

a) The card takes on more responsibility, for instance by integrating a key pad, display, biometric sensor, and/or network interface. Such cards would be more expensive than current cards, but in the extreme, the reader could be made redundant, thus redistributing costs as well as functionality. The main advantage of such a concentration of functionality in the card would be that the user interacts with a device that she carries around all the time, and that she is more likely to trust her own devices than the reader owned by someone else.

b) The terminal takes on more functionality, leading to a PDA that can be used in ATMs, for building access etc. In the extreme, the PDA is the secure key store with processing and interfacing capabilities, and there is no need for a separate smart card. Again user trust would be increased, and thus also the business opportunities.

Both scenarios, whether taken to the extreme or not, will have huge implications. Both are driven to some extent by technology push (the increasing ability to integrate functionality on card or device) and by market pull (the increased need of the citizen for trust in access to the electronic world).

Clearly the above has a huge influence on the interfaces defined between smart card and reader on the one hand and the reader and the network on the other.

This has lead to the definition of the following challenges:

1. Terminals should support new formats in addition to the well accepted ID1 format, including various contact-less cards as defined in ISO/IEC 14443.
2. Cards with other form factors should become possible, such as thinner ID1 cards (<0.4 mm). New form factors will impact the read/write interface.
3. The die size of the smart card is limited by reliability requirements, which in turn limits the functionality. However, smaller feature sizes will increase the capabilities of the chips, and in the longer term the "system on card" with embedded peripherals will increase functionality further. Appropriate use of increased functionality and the ensuing interfacing (and standardisation) will require further work.
4. In the context of standard architectures, such as STIP, FinRead and Global Platform, the implementation of common test suites and of security certification procedures is a major requirement of the smart card industry as a whole.
5. High speed protocols: The reader needs to support new protocols that will allow for higher data rates
6. It will be necessary to add new physical interfaces to ease integration in existing infrastructure, e.g. a PC interface via USB, and a PDA interface via Blue-tooth.
7. The 5 Volt power supply is the de facto standard for POS terminals, whereas mobile phones operate at 3 Volt. These voltages will be reduced to lessen the energy demands of (mainly battery powered) devices. This requires redesign of terminals and revision of standards.
8. There are many ways in which biometrics can be deployed to capture some distinguishing element of the biological makeup of a person. Some of these (face recognition, hand geometry) are perhaps less easy to include in smart card based systems. Others would seem ideally suited to improve the security of smart cards. These include finger prints, voice recognitions and behavioural biometrics. The challenge is in the (on-card or off-card) integration, deployment, management and user acceptance.

9. How can a user gain trust in the card and the terminal? Designers must know what the effect of a security exception could be, and how systems and users will cope with these exceptions. This has significant influence on the design of the interfacing.
10. Allow for interface devices that can either be incorporated into normal everyday objects, for example into a watch or ring with contact less capabilities etc. On the other end of the spectrum, allow for the possibility of incorporating an interface for a removable device onto a hard disk to allow for removable data security.

5.3.4 CARD EMBEDDED PERIPHERALS, SUBSYSTEMS AND MICROSYSTEMS

5.3.4.1 Standard Card Hardware Architecture

- I2C or SPI bus (6 wires maximum)
- Interface between main chip and bus: managed by a separate interface chip (the interface should not be included in the main chip).
- Interface between bus and display: managed by an "already mounted on the display" chip.
- Interface between the separate interface chip and the knobs: direct connection, no need to be driven by the bus.
- Interface between the separate interface chip and the battery: direct connection, no need to be driven by the bus.
- Display: mono or bi-stable, segmented or pixel.
- ISO 14443 (13.56MHz) optional RF interface included in the separate interface chip: the antenna is connected to this chip and not to the main chip.
- Same as above with a fingertip sensor and a keyboard both managed by the bus and supplied with their interface chips "already mounted on".
- Extented range of peripherals (biometric sensors, MEMs), all supplied with their interfaces "already mounted on".
- Increased on card memory: up to 512K on the smart card controller, over 1Mb on addition silicon (e.g.FRAM, SRAM)

5.3.4.2 Power Supplies

- Primary and secundery batteries
- Voltage: from 3 / 4 Volts to 1,8 Volts
- Capacity: in the range of 25 mAh, depending on application profile.

Primary and secondary batteries: in a short term, secondary batteries will be loaded by contacts or power cells with control unit included into the interface chip through or reset function. In a longer term, flash loading feature and adapted power management unit should be added.

5.3.4.3 Packaging technologies

- Thinner (below 100µm) wafers handling, with required equipment, and improved chip packaging technologies for thinner and more reliable modules (<300µm).
- Co-design of packaging and card manufacturing technologies

5.3.4.4 Interconnections technologies.

- Flip chip technology for contactless and tags
- Lead-free components
- Cost effectiveness through
  - very thin (below 100µm), pads plated with stainless metal
  - pads layout with a minimum pitch (300µm)

5.3.4.5 Embedding technologies

- Integrated technologies: flexible handling equipment for the mounting of various additional card components at different stages of the production chain
- Low temperature pressure sensitive adhesives (<80°c), ideally room temperature

5.3.4.6 Material and material transformation.

Evolution towards biodegradable materials for card body

5.3.5 CRYPTOGRAPHY, TAMPER-PROOF AND SECURITY TECHNOLOGIES

5.3.5.1 Design of secure smart card chips

In this category the most important issue is to develop means to eliminate information leakage through side channels. The research and development work must comprise both elaborate chip design and the software running on the smart card chip.

Secondly, physical security protection techniques for the smart card chips must be developed. The chips must become tamper-resistant and tamper protection and detection mechanisms on the chip must be devised. This should include secure logic cells which destroy secret data when being manipulated or probed.

Furthermore, secure reprogrammable smart card chips must be developed to be able to re-configure processors during the usage life-cycle in a highly secure manner.

Also, more powerful and automated evaluation tools are necessary.

5.3.5.2 Investigation and prevention of attacks

Existing invasive and non-invasive attacks have to be investigated and developed further and countermeasures have to be conceived. Here especially active non-invasive attacks (e.g. by exposing the smart card chip to (electromagnetic) radiation or light pulses) and their countermeasures have to be investigated.

Besides that, attacks on smart card must be modelled to provide higher security of the smart card software.

5.3.5.3 Development and implementation of high-end cryptology

In this area, the highest priority is assigned to the enhancement of the security of smart cards in the PC and internet environment. Novel cryptographic security schemes for smart cards in the internet will become necessary.

Powerful cryptographic algorithms which enable on-the-fly encryption and decryption must be developed.

It is also important to develop efficient and secure implementations of asymmetric cryptographic procedures.

Besides that, new public-key algorithms with high security level and high speed for smart cards without crypto processor are of great importance.

Furthermore, secure on-chip key generation must be achieved.

The development of dedicated on-chip random number generator tests is important to guarantee high security for future smart card applications.

Finally, the security and the speed of the contactless interface must be enhanced.

5.3.5.4 Development of secure smart card software and protocols

The whole area of "secure software updating" on smart cards is highly important and security concepts for these procedures must be developed.

Besides that, the security for cards with a built-in user interface is very important in future smart cards (e. g. super smart cards with display and keypad).

In addition to that, achieving highest security and trust in smart card applications without a user interface is of importance.

Furthermore, compilers which produce safe code must be developed.

Simpler protocols to manage PKI (public key infrastructure) applications are necessary.

5.3.6 MICRO-ELECTRONICS

5.3.6.1 Javacard standard evolution (V2.2, V3.0)

On a short/medium term:	**Impact on chip technology**
Stronger interoperability	Silicon independent card O/S
Use of RMI (remote method invocation)	Comm, I/Os / CPU performances
Logical channels to access memories	NVM technology
Garbage collection	Memory Protection/Management Unit
New cryptographic API (RSA 2048, AES, Elliptic Curves)	Dedicated H/W or ISA
Biometric API	
Embedding card manager (for install / uninstall of applets)	Memory Protection/Management Unit
Javacard O/S will reach 200 / 300 KB	Memory size
On a medium/long term:	**Impact on chip technology**
Evolution toward J2ME	Size of ROM / RAM
Javacard O/S may reach 512 KB	Size of ROM
Migration of Toolkit (STK) toward Javacard Applet	
Distributed Javacard applications becoming a de facto model	Computing power / I/O communication speed /MMU
Card will run in a client / server environment	Memory Protection/Management Unit
Addressable memory size will reach 1 Mbyte	CPU architecture / memory techno.
Average size of applets will be above 32 KB	NVM memory technologies
Enhanced interoperability	Open architectures for CPU
Enhanced garbage collector / No persistent heap	MMU
Multithreading / Multitasking operations	Logical memory access
Performances will request all Java Object in RAM	RAM size or technology
O/S will be optimised for 32 bit chip architectures	32 bit CPU - ISA
Biometry API / Full Java compliance	Specific H/W, FPU

5.3.6.2 Improved security levels

On a short/medium term (EAL 5+, 6, 7)	**Impact on chip technology**
Resistance to fault attacks	Chip architecture or design methods
Tamper resistance	H/W sensors
Applets verifiers	
New algorithms and appropriate countermeasures	Specific ISA
Memory protection and partitioning	Memory Protection/Management Unit
Better resistance to non invasive attacks	Design methodology
On a medium/long term (above EAL 7)	**Impact on chip technology**
On Card applet verifiers	Dedicated hardware
Embedded Security audit systems	
Improved tamper resistance	
Improved fault tolerant architectures	Chip architecture / design methodology.
New algorithms	Specific H/W or ISA

5.3.6.3 Card interface with networks & systems

On a short / medium term	**Impact on chip technology**
High speed communications protocols	Comm. I/Os
Distributed applications architectures	Comm, I/Os, CPU speed
Client / server architectures	
Increasing need for computing power	CPU architecture
Contactless / contact communication capability	Multiple I/Os / UART
Multiple browsers on board	Memory size / NVM technologies
Dynamic memory management	Memory Protection/Management Unit
Low power compliance (GSM / 3G)	Chip architecture / PM
On a medium / long term	**Impact on chip technology**
Distributed Javacard applications	Fire wall / comm I/Os/ MMU/CPU
Integration of cards in frameworks for back offices, handset terminals	Comm,I/Os,chip architecture/CPU
Operated services	NVM technology and MM
High speed communications protocols	Comm. I/Os
Low power compliance	Chip architecture / PM / Chip Technology

5.3.6.4 Card manufacturing process / management requirements

On a short / medium term	**Impact on chip technology**
Low cost manufacturing	Chip size / Auto test features
Performant personalisation process	NVM technology, Comm, I/Os
OTA management	NVM technology, MM, Comm, I/Os
On a medium / long term	**Impact on chip technology**
Low cost manufacturing	Chip size / Auto test features
Performing personalisation process	NVM technology, Comm, I/Os
OTA management	NVM technology, MM, Comm,

5.3.6.5 Global technology improvement

Memory management unit/memory partitioning unit

High speed communication interface

Standard communication protocol support with card acceptor and network servers

High performance Non-volatile Memory (size and type)

Power consumption optimisation

Improved tamper-resistance

Fault tolerant design

H/W device re-configurability

Easy manufactured & cost effective camouflage technology

Single memory technology to replace RAM and NVM with same performances

Multiple IP integration, intensive IP re-use for both hardware and software with proven security and IP protection.

6 OPPORTUNITIES FOR COLLABORATIVE RESEARCH

6.1 OPPORTUNITIES FOR COLLABORATION - OTHER RTD PROGRAMMES IN EUROPE

6.1.1 THE MEDEA+ PROGRAMME

MEDEA+ is the new 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.

In the MEDEA+ projects running more than 2,600 scientists and engineers from almost 220 partners are working on the most advanced research challenges in microelectronics applications and their enabling technologies. MEDEA+ partners include major microelectronics manufacturers, systems houses, SME’s, universities and institutes from 17 European countries. In the projects, 36% of the partners are small companies, 32% are large companies, 32% are research institutes and universities.

6.1.1.1 MEDEA+ Projects

Since beginning of January 2003, there are 34 projects running in the MEDEA+ Programme: 17 in Applications and 17 in Technologies.

In the Applications, a line is given specially for the smart cards research, 2 projects are running:

- A302 - EsPass-IS: Enhanced Smartcard Platform for Accessing Securely Services of the Information Society

  The main goal of this project is to deliver HW and SW open Smart-Card platforms aimed at supporting value added electronic and mobile commerce services as required by most operators from the mobile telecommunication, banking or Pay-TV sectors. It targets SW or service companies aiming at developing or promoting such services.

- A304 - CRYPTOSOC: Cryptographic System On a Chip

  The main goal of this project is the protection of critical information systems (IS) infrastructures for business, communication, finance, distribution, energy and transportation. The high vulnerability of commercial software requires that it be associated with cryptographic hardware to provide an adequate security level in the field of smart card, Internet services etc.

  Partners: AMTEC, Bull, CEA-LIST, I2E, Politechnico di Milano, Politechnico di Torino, Sagem, STMicroelectronics

  Project Leader: Alain Filée, Bull

  Start date: April 2002 - End date: December 2004

Other Application targeted projects:

– A104 - SCUBA: System-on-Chip Solutions for Advanced UMTS Basestations

  Industry sources expect universal mobile telecommunication system (UMTS) based mobile communications to be used by up to a billion customers within the next five years. Providing wireless access to all types of information - including multimedia and other data - the "third generation" UMTS system is likely to create a turnover of 80 billion/year over the same period.

  The goal of the MEDEA+ SCUBA project (A104) is to boost the application of this new technology by developing innovative, inexpensive functional elements for base stations and their linkage to the worldwide communications network. As these demand a level of quality that cannot be provided simply by increasing the processing power and bandwidth of conventional chips, the partners are developing new processing architectures to deal with the complex high-speed signal/data processing and routing requirements.

  Partners: Alcatel, ATMEL, CEA LETI, ChipIdea, Italtel

  Project Leader: Klaus Wuenstel, Alcatel

  Start date: September 2001 - End date: February 2004

– A202 - FUST: Future Storage

  The exponential growth in communications - especially mobile devices -, the convergence of PC and consumer electronic products, the quest for static and portable digital video capability, and the emergence of home servers (residential gateways) are creating a continuously increasing need for mass data storage.

  The MEDEA+ FUST project (A202) seeks to strengthen Europes ability to deliver innovative system-on-chip (SoC) devices operating with both optical and magnetic storage media. As well as devising common system architectures, the partners are developing prototypes of key components, creating tools for testing and validation, and contributing to the format standardisation debate. Know-how acquired as a result of this initiative will stimulate growth in the professional and consumer electronics sectors. It could even lead to the emergence of completely new product types.

  Partners: CiaoLab Technologies, OnStream Data, Philips, STMicroelectronics, Thomson multimedia

  Project Leader: Jef Pijenburg, Philips Electronics

  Start date: January 2001 - End date: December 2002

The Technologies part of MEDEA+ program contains other smartcard related projects:

- T123 - CRESCENDO: Expanding Non-Volatile Memory and Analogue Functionalities for System-on-Chip

  Embedded non-volatile memory, low-cost custom programmability and built-in analogue functionality will be essential requirements in future deep-submicron system-on-chip technology for many applications. Process technology advances being explored in the MEDEA+ CRESCENDO project (T123) will lead to realisation of the advanced SoC solutions needed in fast-growing sectors such as microcontrollers, cellular communications, smart cards, multimedia, automotive electronics and data storage for audio/video. A consortium including Europe's top three semiconductor manufacturers is developing high density electrically erasable programmable read-only (EEPROM) and flash memory - as well as low-cost, low-density programming elements, in 0.18 and 0.12 µm generation CMOS technologies.

  Partners: IMEC, Infineon, Philips Research, Philips Semiconductors, STMicroelectronics

  Project Leader: Frans List, Philips Semiconductors

  Start date: January 2001 - End date: December 2004

- T124 - HOTCAR: High Operating Temperature Systems on Chip, Assembly and Reliability

  Electronics capable of functioning under severe environmental conditions are increasingly required for in-car systems and other demanding applications, where semiconductor chips must operate at temperatures up to 200°C and beyond. At the same time, European car-makers are seeking to cut costs by building and testing engine and transmission assemblies with all the electronic control devices in place. That can only be achieved if the components are mounted directly on the unit, where they will be subjected to long-term extremes of vibration and humidity, as well as elevated temperature. The primary technical goal of the MEDEA+ HOTCAR project (T124) is to achieve and demonstrate robust system-level solutions to meet such needs. It is pushing the results achieved by earlier projects to a new level of exploitation by focusing on system-on-chip (SoC) solutions, state-of-the-art microchips and other increasingly complex integrated circuits (ICs).

  Partners: AT&S, Atmel, C-MAC, Conti-Temic, CRF, DaimlerChrysler, EPS, HARTING, IMOMEC, Infineon, Isola, Schlumberger, SERMA, Siemens, Siemens VDO, STMicroelectronics, Valeo

  Project Leader: Günter Lugert, Siemens VDO Automotive

  Start date: December 2001 - End date: November 2004

- 301 - 0.1 µm Fab: 0.1 µm Fabrication Engineering

  The growing complexity of integrated circuits and the trend to build complete system-on-chip (SoC) architectures are placing demands on semiconductor manufacturers to provide ever tighter incremental gate spacing. As device dimensions decrease, however, the sensitivity to small defects and impurities caused by the production process increases. The MEDEA+ 0.1 µm Fab project (T301) brings together leading European semiconductor manufacturers and their equipment and material suppliers to develop fabrication technologies for the reliable production of silicon chips with feature sizes down to 100 nm and below. The project is split into two parts, one covering the improvement of material purity for the next two generations of IC technology, and the other the development of relevant hardware to be used with the new production materials.

  Partners: 40-30, Air Liquide, Alcatel Vacuum Technology, ALES, ALTIS, Faure Ingénierie, GRECA-Uni.Grenoble, INCAM, LETI, Mondia Quartz, Philips, RECIF, SEPAREX, SOPRA, STMicroelectronics

  Project Leader: Jacques Trilhe, STMicroelectronics

  Start date: January 2001 - End date: December 2004

- T503 - HI-MICRO Novel Packaging Technologies for Highly Integrated MICROmodules for next generation Telecom and Automotive Products

  Goals of the project are to develop novel design methods, production concepts and qualification tools for next generation of micro-modules and micro-components using highly integrated ICs and multi-layer substrates. This will be accomplished by using advanced high-density packaging technologies to enable new platforms for low-cost mass products to be used in next generation telecom and automotive applications.

  Partners: Robert Bosch, Chalmers University of Technology, EPCOS, Ericsson, STMicroelectronics

  Project Leader: Thomas Lewin, Ericsson

  Start date: April 2001 - End date: June 2004

6.1.1.2 MEDEA + Roadmap - EDA (Electronic Design Automation)

Electronic design automation (EDA) is a critical tool in reducing the length of the design cycle and thus speeding the marketing of new products. Even a small delay can result in lost market share - and hence reduced profitability. The MEDEA+ roadmap is therefore an important knowledge management tool, enabling EDA resources in Europe to focus on key developments to the benefit of manufacturers and consumers.

The current third release of the roadmap focuses on specific needs, at particular points in time, and with a specific time frame 2002 to 2007, as of the beginning of 2002. It is a living document and it has to grow. It is therefore subject to regular updates and contributions by the experts via a dedicated discussion forum set up by MEDEA+.

Key objectives of the roadmap include:

- Accelerating process maturity for time to volume production of new chips by increased automation in library production and early product design;
- Formalising the dialogue between system houses and semiconductor manufacturers to speed up high quality system-on-chip (SoC) design; and
- Allowing better use of the intrinsic capabilities of silicon, even very deep sub-micron (VDSM) silicon technology, which makes it possible to design complex SoC that might have tens of millions of transistors on a single chip and run at 200 MHz or more.

By supporting early development of processes and new products and enabling an exchange of real-time information, the roadmap will have a strategic impact on the time to market for new SoC products. As a result of this MEDEA+ initiative, the European electronics industry can achieve progress by pushing in a concerted way, ensuring major savings in resources while at the same time improving training and information exchange.

More information: www.medeaplus.org

Or mail to: edaroadmap@medeaplus.org

6.1.2 NATIONAL RESEARCH PROGRAMMES

Programme name	Projects / RTD domains	Comments
ACI Sécurité Informatique	http://acisi.loria.fr/	French national Research program
"Sicherheit in der Informations- und Kommunikationstechnik	"http://www.iig.uni-freiburg.de/telematik/spps/	German national Research program
A research program on computer security and secure networks	http://www.sentinels.nl	Dutch national Research program

6.2 RESEARCH ACTORS IN EUROPE AND WORLD-WIDE

The numbers in the list below are pertaining to the following domains:

1. Communication and networks protocols
2. Systems and software
3. Smart card accepting devices (CAD), interfaces and biometry
4. Embedded peripherals, subsystems and microsystems
5. High-end cryptography, tamper-proof and security technologies
6. Micro-electronics

		RTD activity in domain					
Name	**URL**	**1**	**2**	**3**	**4**	**5**	**6**
Chess embedded technology B.V.	http://www.chess.nl	X	X	X	X	X	X
Fujitsu	http://www.fujitsu.com	X	X	X	X	X	X
Gemplus	http://www.gemplus.com	X	X	X	X	X	X
Giesecke & Devrient	http://www.gi-de.com	X	X	X		X	
Infineon	http://www.infineon.com	X		X	X	X	X
Ingenico	http://www.ingenico.com		X	X			
Inria	http://www.inria.fr	X	X	X		X	
NDS	http://www.nds.com	X	X	X	X	X	X
Nedap N.V.	http://www.nedap.com	X	X	X	X		X
Oberthur Card Systems	http://www.oberthurcs.com	X	X		X	X	
Orga	http://www.orga.com	X	X	X	X	X	X
Philips Semiconductor	http://www.philips.com	X	X	X	X		X
Schlumberger	http://www.schlumberger.com	X	X	X	X	X	X
STMicroelectronics	http://www.st.com	X		X	X	X	X
TNO-TPD	http://www.tpd.tno.nl/smartsite41.html	X	X	X		X	
Trusted Logic	http://www.trusted-logic.fr		X			X	
University of Nijmegen	http://www.cs.kun.nl	X	X				
University of Twente	http://www.cs.utwente.nl	X	X	X			

7 CONCLUSIONS: SMART CARD RELATED RTD PRIORITIES

Domains for SC technology R&D	Core technologies for R&D	Timeframe to carry out RTD			Business opportunities
		Short (< 2005)	Medium (2005-2007)	Long (> 2007)	
1. SW & Systems	Open multi-tasking OS	▨	▨		Wider application/developer/customer base Flexible application management Reduced time to market Increased product reliability
	Real time OS		▨	▨	
	OTA platforms for wireless applications	▨	▨		
	High-level programming languages and tools	▨	▨		
	Technologies for integration, test, compliance	▨	▨	▨	
2. System on chip / system on card	NVM (FeRAM, Flash, MRAM)	▨	▨		Cost optimisation Increased product flexibility, reliability, security More cost effective security maintenance Enhanced HSI, card autonomy, card holder ownership Compliance to environmental regulations (reduced waste, energy consumption, etc.)
	Single memory technology		▨	▨	
	Memory management/protection unit	▨	▨		
	Assembly / embedding technologies	▨	▨		
	On card peripherals	▨	▨		
	On card power supply	▨	▨		
	Power management	▨	▨		
	Proprietary design integration		▨	▨	
3. Integration in networked systems and environments	High performance communication protocols (Full duplex, High speed, Wireless)	▨	▨		Ubiquitous and seamless access to e-services (total access) Interoperability of products, systems and services Wider developer base and reduced time to market
	New on-card interfaces (USB, Bluetooth, WLAN)	▨	▨	▨	
	Multiple communication channels		▨	▨	
	Middleware & browser components	▨	▨		
	Distributed systems (client/server vs. peer to peer)			▨	

Domains for SC technology R&D	**Core technologies for R&D**	**Timeframe to carry out RTD**			**Business opportunities**
		Short (< 2005)	**Medium (2005-2007)**	**Long (> 2007)**	
4. Security & trust	**Secure chip design:**	■	■		Better user confidence / acceptance Privacy protection Protection against fraud and counterfeiting Protection against identity theft-Digital Rights Management Cost-effectiveness and time-to-market Flexible product design (platform approach) Scalable implementation of security Digital signature applications Security of Internet identification and payment
	– Tamper resistance / anti-intrusion mechanisms	■	■		
	– Secure logic cells development	■	■		
	– Fault resistant design	■	■		
	– Information leakage elimination	■	■		
	– Biometrics chipset development	■	■		
	– Crypto-processors	■	■		
	– Asynchronous chips	■	■		
	– Chip reconfigurability	■	■		
	Investigation/prevention of invasive and non-invasive attacks:	■	■		
	– Fraud detection	■	■		
	– Simulation/modelling of attacks	■	■		
	– prevention of side-channel effects	■	■		
	High-end cryptography:	■	■	■	
	– Security in PC & Internet environment	■	■	■	
	– On the fly encryption/decryption	■	■		
	– New crypto algorithms for Internet security (PK)	■	■		
	– On-chip key generation	■	■		
	– On-chip random number generation-	■	■		
	– Fast & secure crypto for contactless	■	■		
	Secure SW and protocols:		■	■	
	– Compilers for safe code production		■	■	
	– Automated evaluation tools		■	■	
	– Formal methods for SW development		■	■	
	– Trusted Card Accepting Devices		■	■	

8 SCENARIOS FOR AN RTD IMPLEMENTATION

According to the Description of Work, the RESET Roadmap should also indicate potential implementation mechanisms for the required RTD activities. This section contains a tentative approach for RTD project organisation based on two possible scenarios:

- the first one is organised around a set of major technology challenges addressing needs which go beyond the specific scope of smart card requirements (e.g. secure chip design, real-time operating systems, etc.) but are directly connected to technologies worked out and required by the smart card industry,
- the second one is structured around a fully integrated approach from concept and technology development, to demonstration of the viability / benefits / potential, targeting the technological requirements identified by the RESET stakeholders, and addressing a global RTD challenge under the federating theme of the "next generation smart card / smart device".

8.1 IMPLEMENTATION WITH TECHNOLOGY FOCUSED RTD PROJECTS

The technology developments introduced hereafter refer to the specific objectives and focus of the main RTD domains introduced in Chapter 7. This scenario is presented as a set of topics which define the objectives and scope of projects addressing the RTD requirements according to these technology domains. In terms of implementation, this would mean that each of these topics (e.g. secure chip design) would correspond to one or several RTD projects focussing on this technology development. The topics mentioned only cover the direct RTD activities to be addressed. They would need to be completed by application development and demonstration projects and by accompanying measures addressing standardisation, information dissemination and technology transfer, etc. to ensure fastest possible take-up of the new technology developments.

8.1.1 TECHNOLOGIES FOR SECURITY AND TRUST

SECURE CHIP DESIGN

- specify means to eliminate information leakage through side channels
- develop physical security protection techniques: on-chip tamper-resistant and anti-intrusion mechanisms, including secure logic cells which delete secret data when being manipulated or probed.
- define and implement tools for fault tolerant chip design
- develop chipsets fitting requirements for high-end cryptography (public key, biometry,…)
- develop asynchronous chips for optimised power consumption and improved resistance to physical attacks

INVESTIGATION/MODELLING OF PHYSICAL/LOGICAL ATTACKS

- investigate invasive and non-invasive attacks and develop countermeasures
- conduct in-depth analysis of active non-invasive attacks, e.g. by exposing the chip to electromagnetic radiation or light pulses
- build a model of attacks on smart card components to provide higher security of the embedded software.

HIGH-END CRYPTOGRAPHY

- enhance the security of smart cards in the PC and iternet environment
- design cryptographic algorithms enabling "on-the-fly" encryption and decryption
- adapt new public-key algorithms with high security and speed features, enabled without dedicated HW crypto-processor
- enhance "on-chip" key generation mechanisms
- develop "on-chip" random number generator and tests
- enhance security and speed of the contactless interface

SECURE SW DEVELOPMENT TOOLS AND LANGUAGES

- design high level programming languages
- develop means for secure software updates
- design security concepts for cards with built-in user interfaces
- optimise SW compilers for safe code issuing
- develop software engineering of efficient, secure, certified applets
- apply formal method at the SW development phase
- develop methodology for automatic test case generation

8.1.2 TECHNOLOGIES FOR NETWORKING AND NEW COMMUNICATION MODELS

- enhance physical link between card and environment through full duplex ,high speed and wireless communication protocols
- implement multi communication protocols (USB, Bluetooth, WLan)
- adapt smart card systems to IT and consumer protocols (IPv6)
- investigate peer-to-peer exchanges

8.1.3 TECHNOLOGIES FOR SW PLATFORMS AND OS

OPERATING SYSTEMS

- develop multi tasking/multi-threading OS
- enhance file system management/memory management models
- implement modularity through multi layered OS
- develop real time OS technology
- enhance I/O speed
- develop open source model

SYSTEM INTEGRATION AND DEVICE MANAGEMENT

- specify integrated tools for application development and management
- optimize middleware components (RMI, Corba, MIDP,…)
- design methodology for right application model to on-card SW
- develop new application protocols
- develop extensible and scalable on-card and off-card framework: dynamic management of services and code distribution taking into account features such as security, performance, ease of use, dynamic behaviour, off-line operating mode

8.1.4 TECHNOLOGIES FOR HW CHIP PLATFORMS

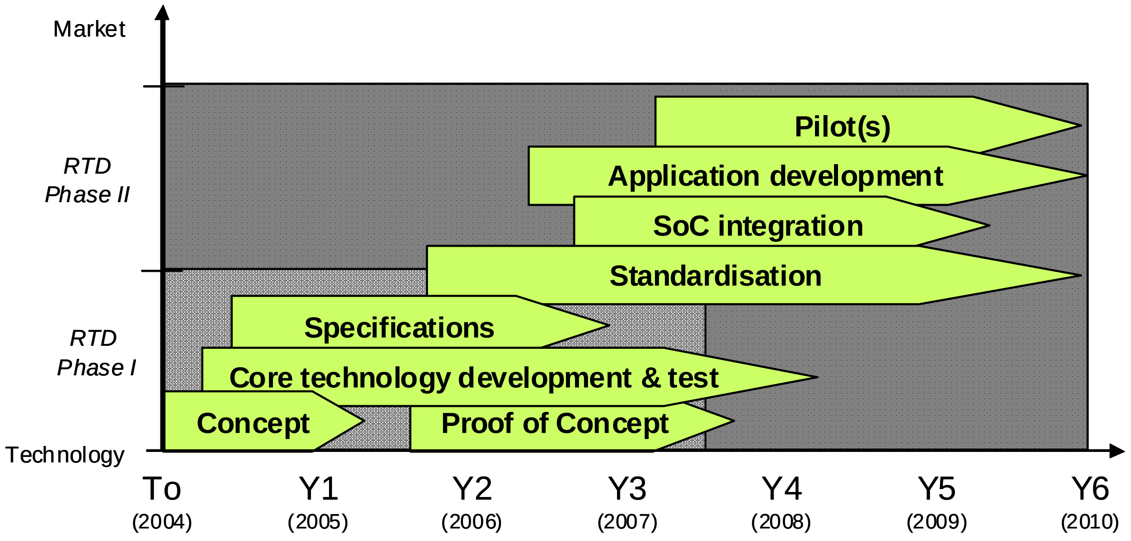
- enhance die size optimisation in smart card chips
- integrate high performance Non Volatile Memory Technologies
- enhance low power chip technology for contact-less interface
- specify and organise easy third party IP integration and re-use
- investigate evolution towards dynamically re-configurable chip devices

8.2 IMPLEMENTATION IN AN INTEGRATED APPROACH: DEVELOPMENT OF THE NEXT GENERATION SMART CARD DEVICE

The second scenario is based on the assumption that the RTD needs identified in the RESET Roadmap Report can be addressed in an integrated way, i.e. a collaboration gathering a significant part of the RTD forces in Europe, federating and structuring them around a common global research topic. This scenario is more favourable than the first on in the sense that the resulting concentration of RTD resources enables a faster development, higher impact and larger backing from the industry.

The conditions for its implementation are more demanding, requiring that 1. the leading players of the smart card industry agree on joining their RTD resources in a common RTD initiative and that 2. the necessary resources can be obtained to support a large RTD initiative for the development of the next generation smart device technology. In view of the size of such a project and its inherent European level impact, only FP6 Integrated Projects and MEDEA+ projects would represent potential opportunities to provide support.

Figure 8.



Integrated Roadmap - towards the next generation SC devices

It starts from the assumption that a new architecture needs to be defined and the corresponding technology developments need to be carried out. It could be divided in two main phases (short-mid term and long term) with the following objectives and key issues to be handled:

8.2.1 PHASE I: NEXT GENERATION SC DEVICE TECHNOLOGY DEVELOPMENT

To objective is to develop next generation secure smart device technology building blocks.

Key issues: Research and development of architecture and basic technology of next generation secure devices. Consistent overall security approach. Openness of the architecture to facilitate standardisation, multi-vendor solutions, extendibility and optimal integration in networked systems. Integrated and comprehensive approach involving all relevant stakeholders of the value chain and support from a significant part of the European smart card and security industry. Validation of the concept and technology bricks, in particular validation of their potential to break through current limitations of smart card technology regarding performance and functionality. Validation of its capability to address requirements of future ambient intelligence and complex ubiquitous computing and e-service environments. The first phase will focus on concepts and core technology which enables close cooperation between the industry players, who might be competitors.

8.2.2 PHASE II: DEVELOPMENT AND DEMONSTRATION OF NEXT GENERATION SC DEVICE COMPONENTS AND APPLICATIONS

To objective is to integrate and demonstrate the potential of next generation smart device technologies to real world application environment.

Key issues: Development of different application specific components (typically SoC implementations). Demonstrate that the technology meets requirements and constraints of different form factors through the design of different smart device prototypes. Integration of various applications on these devices corresponding to anticipated key e-service market segments. Demonstrate that the security concept enables secure downloading of applications in the field, secure multi-application capabilities and high tamper resistance to various forms of attacks.

Demonstration of the enhanced capabilities of the next generation secure devices in networking (IPv6), increased functionality, flexibility and performance (e.g. on the fly encryption/decryption of multimedia information) and enhanced user friendliness thanks to direct user interactivity, on device sensors and more intuitive user interfaces.

The second phase allows for differentiation in application targeted developments to the benefit of the user and the competitiveness of the European industry.

9 ANNEX

9.1 LIST OF ACTIVE CONTRIBUTORS

Note: WG leaders are indicated in bold characters

WG1: COMMUNICATION AND NETWORKS PROTOCOLS

Name:	Organisation:
Michel Leduc	**Gemplus**
David Simplot	**LIFL**
Christoph Schiller	Giesecke & Devrient
Eric Deschamps	Gemplus
Jürgen Tacken	Orga
Pascal Urien	Schlumberger
David Samyde	UCL

WG2: SYSTEMS AND SOFTWARE

Name:	Organisation:
Ulrich Bueker	**Orga**
Gilles Barthe	**INRIA**
A.Saibi	Oberthur
Boutheina Chetali	Schlumberger
Gilles Grimaud	LIFL
Jean-Jacques Vandewalle	Gemplus
Jean-Louis Lanet	Gemplus
Renaud Marlet	Trusted Logic
Michael Butler	University of Southampton,
Xavier Leroy	LIFL
Fabio Martinelli	CNR
Thomas Jensen	CNRS
Javier Contreras	Oberthur Card Systems
Christophe Louis	Oberthur Card Systems
Daniel Le Métayer	Trusted Logic

WG3: SMART CARD ACCEPTING DEVICES (CAD), INTERFACES AND BIOMETRY

Name:	Organisation:
Bruno Michaud	**GIE Cartes Bancaires**
Pieter Hartel	**University of Twente**
Arieh Moller	NDS
Eduard de Jong	SUN
Francois Brion	GIE Cartes Bancaires
Klaus Sickert	Philips
William Vanobberghen	GIE Cartes Bancaires
Stefano Bistarelli	CNR
Stefano Frassi	CNR
Dirk Scheuermann	Fraunhofer Institut
Christophe Colas	Ingenico

WG4: EMBEDDED PERIPHERALS, SUBSYSTEMS AND MICROSYSTEMS

Name:	Organisation:
Benoit Thevenot	**Schlumberger**
Christian Zenz	Philips
F.Launay	Oberthur
Henri Boccia	Gemplus
Philippe Patrice	Gemplus
Thies Janczek	Orga

WG5: HIGH-END CRYPTOGRAPHY, TAMPER-PROOF AND SECURITY TECHNOLOGIES

Name:	Organisation:
Albert Moedl **Jean-Jacques Quisquater** Antoni Martínez-Ballesté Arieh Moller David Samyde Francesc Sebé Jean-Bernard Fischer Josep Domingo-Ferrer Jean-Francois Dhem Renaud Marlet Thomas Hübner Thomas Jensen Jaap-Henk Hoepman Louis Goubin Peter Roelse Yaron Sella	**Giesecke & Devrient** **UCL** ETSE NDS UCL ETSE Oberthur ETSE Gemplus Trusted Logic Orga IRISA KUN Schlumberger Philips NDS

WG6: MICRO-ELECTRONICS

Name:	Organisation:
Jean-Paul Thomasson	**STMicroelectronics**
Enrique Canto	**ETSE**
Christoph Schiller	Giesecke & Devrient
Jean-Luc Ledys	Gemplus
Alain Fermy	Gemplus
Kai Grassie	Philips
Ritsuko Nakano	Fujitsu
David Samyde	UCL
Stefan Rueping	Infineon
Volker Timm	Philips
Yvon Gressus	Schlumberger

FACILITATORS AND EDITORS:

Name:	Organisation:
Florence Gras	EUROSMART
Bruno Le Dantec	ERCIM
Olivier Trébucq	ERCIM
Bruno Cucinelli	ARTTIC

9.2 GLOSSARY OF SPECIFIC TERMS AND ACRONYMS

Term / acronym / abbreviation	Description
ACA	Anisotropic conductive adhesives
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CAD	Card Accepting Device
CC	Common Criteria
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DPA	Differential Power Analysis
DRAM	Dynamic Random Access Memory
DRM	Digital rights management
DSA	Digital Signature Algorithm
DSL	Domain specific languages
DSS	Digital Signature Standard
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EEPROM	Electric Erasable Programmable Read-Only Memory
EMV	Europay Mastercard Visa
FeRAM	Ferro electric Random Access Memory
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
FPU	Floating Point Unit
GPRS	General Packet Radio Services
HSI	Human-System Interface
ISO	International Standardisation Organisation
ITRS	International Technology Roadmap for Semiconductors
JCP	Java Community Process
MCU	Micro-Controller Unit
MID, MIDP	Mobile Information Device, Mobile Information Device Profile
MMC	Multi Media Cards
MPU	Micro-Processor Unit
MRAM	Magnetoresistive Random Access Memory
nm	Nano-meters
NTRS	National Technology Roadmap for Semiconductors
NVM	Non Volatile Memory
OS	Operating System
OTA	Over The Air
PCM	Phase Change Memory
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
QoS	Quality of Service
RF	Radio Frequency
RMI	Remote Method Invocation
RNG	Random Number Generator
RRAM	Non-Volatile Resistor Random Access Memory
RSA	Rivest-Shamir-Adleman algorithm
RTD	Research and Technology Development
SD	Secure Devices

Term / acronym / abbreviation	Description
SeSoC	Secure System on Chip
SIA	Semiconductor Industry Association
SIM	Subscriber Identification Module
SOC	System-On-Chip
SPA	Simple Power Analysis
SRAM	Static RAM
SSCD	Secure Signature Creation Devices
STIP	Small Terminal Interoperability Platform
UART	Universal Asynchronous Receiver-Transmitter
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
WAN	Wireless Area Network
WiFi	Wireless Fidelity
XML	Extensible Mark up Language