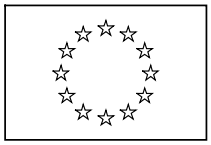
European Commission
Information Society Directorate-General

Research *for* the Smart Card *of* 2010

Report of the Consultation Meeting
held in Brussels on 23 May 2001
in preparation of the
6th Framework Programme



EUROPEAN COMMISSION
Directorate-General Information Society

Information Society Technologies: New Methods of Work and Electronic Commerce
Information security and confidentiality, intellectual property

Research for the Smart Card of 2010

Report of the Consultation Meeting held in Brussels on 23 May 2001 in preparation of the 6th Framework Programme

Version 5.1, 20 July 2001

Inquiries: infso-c4@cec.eu.int

This report is available on http://www.cordis.lu/ist/ka2/smartcards.html

Table of contents

1 EXECUTIVE SUMMARY 3

2 CONTEXT AND OBJECTIVES 4

3 CONTRIBUTIONS TO THIS REPORT 4

4 MAIN SOCIO-ECONOMIC DRIVERS 5

4.1 THE INTERNET 5
4.2 USER NEEDS 5
4.3 FRAUD 6
4.4 ENVIRONMENTAL FACTORS 6

5 MARKET TRENDS 6

5.1 MARKET SEGMENTS 6
5.2 INTEROPERABILITY 7

6 HARD TECHNOLOGICAL ISSUES 7

6.1 SMART CARD CHIP TECHNOLOGY 7
6.2 OPERATING SYSTEMS 8
6.3 SYSTEM INTEGRATION 9
6.4 DEVELOPMENT TOOLS 9
6.5 SECURITY 10
6.6 COMPONENTS AND MOUNTING 10
6.7 MATERIALS 11

7 HOW TO ORGANISE RTD COOPERATION 11

ANNEX: OVERVIEW OF THE TECHNOLOGICAL ISSUES 12

1 Executive summary

In preparation for the activities to be launched under the 6th Framework Programme for Research, Technological Development and Demonstration Activities (FP6[1]), the European Commission's Information Society Directorate-General organised a meeting to consult the industrial and academic research community on current and future RTD needs in the domain of smart card technology.

Those attending this meeting, which was held in Brussels on 23 May 2001, all agreed that the European smart card industry has major needs in R&D in various technology domains in the short and the long term. They identified the priority topics and related requirements. A lot of effort needs to be invested in RTD to ensure that Europe can maintain its current technology and industrial leadership in smart card technology domains such as chip and card design, secure embedded software, manufacturing technology and in smart card application developments.

Research and development needs are still dominated by hardware related topics (smart card chips, assembly and interconnection technology, materials, production techniques), but they also involve different types of development tools (to optimise effort, time, quality for HW and SW developments), advanced security technology solutions (cryptography, security protocols, tamper resistant design, etc.) and extended features of smart card operating systems (e.g. modular architectures, open source OS). The trend, however, will be to invest more effort on SW than on HW design in future in the development of complete smart card solutions.

The list of RTD priority topics to be addressed is long and the required effort and expertise to address all these issues is far beyond the possibilities of a single company or country. To cover these RTD needs a joint effort is required as well as the support of European programmes and its favourable framework for European cooperation in RTD . Cooperation is also needed to optimise resources spent on the development of new smart card products and their deployment, through the achievement of consensus of common design data formats, preparation of standards, unification of certification procedures, etc.

The present report also contains written contributions received from the participants following the meeting. In these contributions the participants were asked to answer, after discussion in their own organisation, a number of additional questions:

- on which topics would your organisation agree to RTD cooperation with other companies / research institutes?
- what would be the estimated required effort for RTD?
- what would be the specific (measurable) objectives in this area?
- what would be a suitable time frame ?
- how could the RTD cooperation be organised?

All organisations confirmed their interest in cooperating on a selection of RTD targets in consortia composed of industrial and academic partners. Going by these responses, the total investment needed in Smart Card priority RTD areas (as identified in the present report) is put at 320 M€, corresponding to approximately 74 projects to be initiated over a time frame of 5 to 8 years starting from 2002.

The consultation on smart cards will be further elaborated in 2001 and 2002. Parties interested to contribute are invited to contact the European Commission, Directorate-General Information Society, Unit C4 (infso-c4@cec.eu.int).

[1] http://www.cordis.lu/ist/fp6/fp6consult.htm

2 Context and objectives

The European Commission announced its proposal for the 6th Framework Programme for Research, Technological Development and Demonstration Activities (FP6) on 21.2.2001[2]. Information Society Technologies (IST) is one of the main thematic priorities of this proposal. In preparation for the activities to be launched in this field, the Commission is organising a series of meetings to consult the industrial and academic research community on the content and implementation instruments of IST in FP6[3]. These consultations are seen as a continuous process starting in March 2001 and ending in October 2002.

A key feature of FP6 is the further concentration of efforts to build critical masses and to increase the impact as well as providing for closer interlinking with Member States efforts.

The aims of the consultation are to:

- clarify and expand the strategic guidelines of FP6.
- identify the means of creating the FP6 instruments best suited to the IST constituency.
- provide input for the 2002 IST Work Programme as a bridge towards FP6.
- mobilise the industrial and academic RTD community for activities in FP6 in 2002 and contribute to the development of partnerships.

In this context, the Commission organised a consultation on Smart Card Technology to answer the question: *What research is necessary to prepare the smart card of the year 2010?* The discussion addresses technological and programme issues related to smart cards.

3 Contributions to this report

The Consultation Meeting organised by the Information Society Directorate-General on 23 May 2001 brought together nine experts from industry and research and a rapporteur. The Vice-Chairman of Eurosmart chaired the meeting. Some experts had presented their views in position papers distributed beforehand.

Mr Hans Brandl (Infineon Technologies), Mr Bruno Cucinelli (rapporteur) (Arttic), Ms Susanna Friis-Hansen (Ericson), Prof. Pieter Hartel (University of Twente), Mr Graham Higgins (Datacard Group), Mr Xavier Luck (Schlumberger Systems), Dr Reinhard Meindl (Philips Semiconductors), Mr Yves Moulart (Proton World), Dr Jürgen Moll (Giesecke & Devrient and vice-chair of Eurosmart), Mr Pierre Paradinas (Gemplus), and Mr Antonio Sanz Pulido (Sema Spain) took part in the consultation.

Following a short introduction made by the European Commission on the 6th Framework Programme, each expert presented his vision of current and future needs for research and development in smart cards.

These presentations were followed by an open discussion, which resulted in a list of topics agreed upon as priority RTD areas. The present report has been structured along the lines of this list of topics. The participants also compiled a list of complementary questions to be addressed after the meeting. The summary of this additional written input is presented in the annex.

[2] COM (2001) 94 of 21.2.2001, ftp://ftp.cordis.lu/pub/ist/docs/fp6finalversion.pdf
[3] http://www.cordis.lu/ist/fp6/fp6consult.htm

4 Main socio-economic drivers

4.1 The Internet

The Internet is evolving into a global network that connects various users to on-line services for business, leisure, travel, shopping, banking, etc. Electronic transactions are also used more and more to pay for goods and services in the physical world. Electronic transactions must be based on sound security solutions to give confidence to business and consumers. The smart card is currently the only single solution that can provide personalised and safe access to on-line services and electronic transactions in the virtual world as well as in the physical world.

Whilst already well established and proven as a secure medium for payment transactions in the real world, the smart card is an opportunity for Europe to take a slice of the Internet market. Smart cards will efficiently address society's needs in protecting data privacy in electronic transactions whilst addressing commercial needs by providing companies with the required information on the customer to facilitate and protect their business.

Smart cards can be compared to personal keys that control access to the virtual world, whilst card readers in various devices (PCs, mobile phones, set-top boxes, etc.) can be compared to the locks on the network entry points.

4.2 User needs

In the development of new smart cards and card technologies, end user needs will come more and more to the forefront. User convenience is the key word. Smart cards are evolving from an advanced technology to more interactive secure personal devices.

The main requirement of business and consumers in e- and m-commerce applications is to provide trust and confidence in electronic transactions in the physical and the virtual world. The user wants to have control on his personal data that is stored or transmitted during a transaction. This assumes however a direct interaction between the cardholder and the smart card.

Smart cards should be easy to use and should have enough flexibility to adapt their functions, interfaces, formats and shapes to the most suitable (convenient) ones for a given application. This should also improve the capability of smart cart for a “deeper” integration with global information systems along with their capability to exchange information with their environment. The communication capabilities of smart cards and transaction speed are important issues in the aim to reach maximum user convenience.

In the context of an ambient intelligence environment, for example, the card should be well integrated in the information system of a home or an office. The smart card should become the personal key of the user to all services provided by the whole system. To achieve this, the card should be able to communicate with this environment, exchange information on the services that are supported by the card itself and by the environment, present them 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.

Advanced user interfaces hence mean that support for interactivity between the user and the card are needed, directly with the cards, not only by the means of a terminal. For some current applications (e.g. electronic purse) the cardholder should be able to check the card content at any time thanks to displays or sensors, in order to see, for example, the balance of his e-purse.

Improved user interfaces will also help to provide the user with confidence concerning data privacy. The user should be able to scan the card application data, giving him the control over the personal data stored on his card.

Cost reduction is another area to be addressed for improved user acceptance. Smart cards are usually not sold as such to the end-user, but in a package providing the physical support for access to a service (e.g. the SIM card in a mobile phone), and the end-user has no direct idea of the card’s

cost. However, at the end of the day the user has to pay for it; the card price is part of the total product or service cost and should not exceed a small fraction of the total service or product cost. This is one of the road stoppers for the large deployment of certain new smart card technology applications. The difficulty in achieving these low cost targets, for example, is currently blocking the more general use of electronic tags for ID and tracking of basic consumer products (e.g. milk bottles), a market potential of several tens of billions of units per year.

4.3 Fraud

The general knowledge on smart cards, information systems and security techniques is on the increase and the general access to more sophisticated technology means more computing power and high-speed access to networks. Hackers are often the prime users of this knowledge and these techniques, which increases the level of sophistication of attacks into security systems. Consequently, there is a constant need to tighten security techniques in order to make it more difficult to hack into a system and to limit the means that are required to have a chance of succeeding. Improving security technology involves cryptography, OS and HW security design, as described in more detail below.

4.4 Environmental factors

Manufacturing processes for smart cards must take account of environmental factors, which are becoming an important socio-economic issue. With products manufactured in billions of units, there is a need to optimise the use of materials and the chemical characteristics of those materials and to reduce waste by addressing not only cost targets but also environmental protection aspects.

This is particularly the case for cards with complete on-card computer systems, because of the embedded power source, and for disposable products produced in large quantities, such as disposable transport tickets. Alternate materials and re-usability of silicon are RTD fields to be explored.

5 Market trends

5.1 Market segments

The future market demand can be segmented into:

1. high-end cards
   - cards with a high processing capacity or/and a large memory
   - cards with a complete system on card, including peripheral functions such as display, buttons, sensors, etc. Such cards are supposed to support direct user interaction and an on-card power source
2. low-end cards
   - cards with architectures similar to existing ones, with small to medium processing and memory capacity, as used for “traditional” applications such as banking, loyalty
3. electronic tags
   - electronic tags will be used in various formats for various applications: smart tags, dongles, tokens, disposable tickets. They will provide a secure solution for products, electronic ID and tracking of goods, access control, etc.

The smart card market is marked by strong pressure on unit cost, for low-end cards margins are becoming very small. The cost of electronic tags must also be extremely low for them to be used on a large scale.

Smart card technology advance in European companies will enable them to dominate market segments for high-end cards, where margins are more comfortable.

High market potential is also seen in the transfer of smart card technology to other application domains, such as secure embedded controllers for automotive applications. RTD cooperation in this field would be beneficial not only for the smart card industry but also for the industrial segments in which Europe also has a leading position.

5.2 Interoperability

There is a major trend towards interoperability. Technology and standards are needed to ease interoperability of smart card applications in order to overcome their compartmentalisation in specific sectors. Interoperability is needed to address user convenience, but also to reduce cost for development and certification (a smart card certification procedure typically takes about 6 months), and to accelerate time to market. Standards such as EMV and CEPS illustrate this trend, as do open platform systems, multi-application cards and 3G.

6 Hard technological issues

Current and future RTD needs of the smart card industry can be structured along the lines of the following topics:

1. Smart card chip technology
2. Operating systems
3. System integration techniques
4. Development tools
5. Security
6. Components and mounting
7. Materials

6.1 Smart card chip technology

A lot of specific needs in RTD are related to the required features of future smart card chips. The smart card industry does generally not have access to the latest silicon technology. Because of the specific needs of smart card chips (mixed technology, etc.), it typically takes two years to adapt a new silicon technology to the specific needs of smart card chip production.

The main topics for RTD in this domain are:

6.1.1 Low power consumption chips

In many smart card applications power consumption is a critical issue:

- smart cards are used in mobile phones,
- contactless cards are powered through RF fields, whilst higher computing power is needed to extend contactless card features,
- for battery powered cards, the life time is a function of the capacity of the on-card power source and the consumption in the chip.

More powerful chips consuming less power must be developed to address current and future requirements.

6.1.2 Alternative non-volatile memory technologies

Many performance limitations of the currently available smart cards are related to the constraints of non-volatile (NV) memory used. Smart cards use NV memory to store information (system data, application data and code). NV memory technologies such as EEPROM have quite long access times, in particular for the erase and write cycles, which significantly limits the overall performance of a smart card. Furthermore, the silicon area needed for such NV memories is high, and there is hence a serious trade-off between silicon area used for NV memory and the other on-chip functions, knowing that the physical size of the chip cannot be extended beyond a given dimension in order to comply with robustness requirements to physical stress. Another problem is the limitation for storing data reliably because of the endurance (limited number of write cycles) and retention time.

The smart card industry needs NV memory technologies with faster access times, smaller cell size (to make for higher memory and higher capacity), lower power consumption (to address the requirements mentioned above) and higher endurance and retention times to increase reliability.

6.1.3 Stronger HW security

Smart card security is not only dependent on cryptography and secure embedded software design, but also on tamper resistant HW design. The increasing volume of transactions and value of data protected by smart card applications encourages organised crime to invest more effort and resources into fraud and attacks on the security of the smart card system.

RTD effort needs to be invested in the development of tamper resistant chip designs, new security sensors, techniques for secure HW and SW design, etc.

There is a particular need for more powerful HW based security. This would simplify the software needed to manage current HW security limitations, which can be estimated at about 25% of the total smart card code and hence ease new smart card application developments.

6.1.4 Additional interfaces and protocols / multiple interfaces

The capability of smart cards to communicate with the environment needs to be improved. Smart cards should be easier to integrate in a complete information system. Smart cards need more and faster I/O channels. They should also support standards interfaces and protocols used in general information systems, such as USB, Bluetooth and IPv6.

6.1.5 More powerful chip architectures

Smart card chip architectures need to evolve into more powerful and complex micro-computer systems in the future. They must in particular support features such as:

- interfacing and management of peripheral functions on the chip / on the card (display, buttons, sensors, etc.);
- integration of Memory Management Units to increase security;
- interfacing and management of high capacity memory;
- more powerful crypto functions;
- power management functions;

An important direction for RTD is the development of modular chip architectures, which would facilitate the development of specific smart card applications based on a number of selected HW and SW functions.

There is also a specific need to develop chips for contactless cards supporting asymmetric cryptography.

6.2 Operating systems

Two major areas of research were identified and discussed.

6.2.1 Operating systems features

As a means of reducing time and effort for new developments, the smart card industry would benefit from operating systems with modular, configurable architectures. Libraries and tools should be developed to support extensibility as well as flexible, programmable, multi-application environments. Even low-end cards are expected to provide a minimum of multi-application support in the future. Future card operating systems should ease validation of new configurations regarding their functionality, but also the integrity of security.

6.2.2 Open source OS

The second main direction for research on card operating systems concerns the development of an open source OS. Whilst there were different opinions about the role that such a system can play, about who should develop and control the code, etc., it was unanimously agreed that this is an important RTD topic for the longer term.

The expected benefits are cost reduction (license fees), improved processing capacity and interoperability. The OS code should be under public control, following the LINUX model. One of the main discussion topics was the impact of such open source OS concerning security aspects: will public availability of the code improve the security of the system, or on the contrary create an even higher risk given that hackers can find security holes faster than researchers in universities and the industry?

One expected benefit of such a system would be the capability to adapt the operating system design to specific smart card requirements, such as built-in auditing mechanisms (Java Card does not provide this feature).

6.3 System integration

Smart cards should be looked at as part of global information systems. They should, for example, be an integrated component of “ambient intelligence” environments as mentioned above. The smart card would be the personal key for personalising and controlling such environments. There is a need to develop methods to export services supported by the card and to deal with services offered by the external system. Also, to address the complexity of such systems, high-level development tools should be available to facilitate the integration of smart cards in global IT systems and ensure interoperability.

6.4 Development tools

Industry needs more powerful development tools adapted to the specificity of smart cards. High level development tools already used in other IT industry sectors are not yet available for smart card environments. The smart card industry must optimise development costs, speed, reliability, etc., but also deal with limited availability of human resources, in particular hardware and software design engineers. Furthermore, the complexity of smart card systems is steadily increasing, whilst development time needs to be reduced.

Future development tools should in particular enable:

- formal modelling of SW and HW to improve security, cost, development speed / time to market, product / application performance and to deal with increasing smart card system complexity;
- automatic code generation (for the same reasons);
- testing and verification (100% code verification) to ensure reliability and security of the complete smart card system. These testing and verification tools should be scalable and cover the verification of combined HW and SW based functions.

Another important topic is the standardisation and/or integration of notations to facilitate the interchange of design data during the development cycles.

6.5 Security

Security features will continue to be one of the key areas for research and development. In order to fight attacks, security aspects must be constantly strengthened at different levels:

6.5.1 Card level features

Biometrics sensors should replace or come in addition to PIN codes. At the card level, it should become possible to directly integrate biometrics sensors on a card. This will heighten security by direct control of the sensors by the card system, and by the fact that the secret information remains inside the card.

Currently an HW attack on a card would typically be carried out with the card powered-off, when the security sensors are not operational. The availability of cards with on-card power sources would allow the development of tamper responsive cards, i.e. cards that can continuously scan security sensors and, if an attack is detected, take counter-measures such as erasing the secret information on the card.

Global security concepts are needed for multi-application cards with post-issuance, covering the various systems components, including the operating system, protection of the execution of applications against each other, design of applets and secure loading of applications after personalisation and issuing of smart cards.

6.5.2 Smart card design

As mentioned above, more efficient development and verification tools adapted to smart card specificity are needed. Development tools for new smart cards should support the production of combined HW and SW designs which are optimised for testability of chips/cards on functionality and security. Tools and techniques should be developed to facilitate verification of security protocols.

Furthermore, with the development of complete cards which integrate a complete system on a card (i.e. with several components), new security issues will appear related to the risk that communication between these system components can be scanned by hackers. Methods need to be developed for the secure design of individual components and the secure design of a complete assembly.

6.5.3 Cryptography

Research and development on crypto algorithms and security protocols is needed to strengthen security, enable faster and smaller codes, and support powerful security with smaller keys. New algorithms should also help to reduce power consumption, supporting more efficient power management and addressing low-power needs for many smart card applications as mentioned above.

6.5.4 Infrastructure

RTD effort should also be invested in the development of anti-fraud infrastructure. Security classification should also be developed.

6.6 Components and mounting

The smart card industry will need new components and mounting technologies if it is to manufacture the smart card products for future smart card markets.

New component technologies are needed to assemble several components on a card, and to allow flexibility of these components, such as thin chip, thin film and thin display. Mounting technologies for integration of thin and flexible components must be developed, as well as the machines that implement these new production technologies (thin component assembly).

Current smart cards mainly consist of a chip on a module, or a chip and an antenna, embedded in a plastic body. There are only very few interconnections. For the integration of several components on a card (display, button(s), biometrics sensor, battery, etc.), new assembly and interconnection technologies are needed. There is a technical challenge to developing the technology that will support both low-cost mass production and durable and reliable operation in the context of the usual physical stress endured by smart cards (bending, etc.).

Suitable manufacturing techniques for very low-cost, very high-volume mass production need to be developed for the production of electronic tags in billions of units.

Manufacturing techniques should become more flexible to allow the production of tags and smart cards in various formats and shapes to meet application constraints and user convenience.

Production processes also have to be designed for stronger security requirements. In an environment where smart cards are composed of several parts, techniques to ensure physical security during the manufacturing process will be needed.

6.7 Materials

New materials are needed for new smart card products. Materials and manufacturing technologies for flexible and thin components (chips, battery, display, etc.) need to be developed, along with suitable materials for the interconnection of the components. Alternative substrates/carriers are needed for disposable tokens while addressing the need for very low cost, flexibility to manufacture them in different shapes, and robustness in various environmental stress conditions.

The smart card industry should also be considered as a future massive user of chips made of Polymer materials as a replacement for Silicon. Polymer components might be able to address many of the requirements described above, including issues such as unit cost, environmental constraints (in particular for disposable products), and physical component flexibility, etc.

7 How to organise RTD cooperation

There was a broad consensus among the participants at the meeting that RTD cooperation between European organisations is essential. The 320 M€ estimated to be required to address the above-mentioned technology needs over the next years is far beyond the possibilities of a single organisation or country (see the table below). A collaborative effort is required as well as support through European RTD programmes. A favourable framework for cooperation is also needed in order to make progress on further European and international standardisation and improvement of interoperability of smart card applications, consensus on common protection profiles and mutual recognition of certificates.

For all RTD domains, the participants highlighted consortia of industrial and academic partners as the best structure for pursuing the work. The RTD programmes should facilitate cooperation with SMEs which are the prime movers for new ideas in technology.

Cooperation with Central and Eastern European countries with strong development capacity is also sought.

The European smart card industry is also open to cooperation with third countries (US, Japan, etc.), and this should be given support wherever it can be of benefit to RTD projects led by European companies or improve their competitive position on international smart card markets.

.

A number of indicators concerning the organisation of RTD cooperation, effort and time frame have emerged from the feedback provided by the participants:

Domain	Number of projects	Effort (M€)	Duration (years)
Chip technology	7.0	30.6	3.3
Operating systems	5.3	58.0	3.5
System integration	6.3	17.3	3.0
Strong security	5.6	31.9	3.6
Development tools	6.5	23.8	3.5
Components and mounting	8.0	25.2	2.2
Materials	6.0	24.0	3.0
Security for non-trusted platforms (*)	8.0	24.0	3.0
Card readers (*)	6.0	63.0	3.0
Knowledge transfer (*)	15.0	22.5	1.5
Total	**73.7**	**320.3**	**3.0**

The total effort required is approximately 320 M€ for some 74 projects over a time-frame of about 5 to 8 years starting from 2002.

Project duration depends on the RTD domain as shown in the table, ranging from 1.5 to 3.6 years. An average project would have a duration of 3 years and a cost of 4.3 M€ (total effort divided by the total number of projects). The average project cost is 5.0 M€ if the values are weighted per RTD domain.

Annex: Overview of the technological issues

The first table below provides a summary of the technological issues raised above. The second table summarises additional issues raised after the workshop.

Indeed, the participants in the workshop on 23 May 2001 decided to provide additional written contributions as follow-up action to answer complementary questions requiring additional thoughts and discussion within their organisations. This also allowed other Eurosmart members to be informed of the topics discussed on 23 May and responses with feedback from more smart card experts to be compiled.

The following questions were asked:

- on which RTD topics would your organisation agree to cooperate with other companies / research institutes?
- what would be the estimated required effort for RTD?
- what would be the specific (measurable) objectives in this area?
- what would be the suitable time frame?
- how could RTD cooperation be organised?

The responses are presented in a standard tabular format. Some contributions provided additional RTD topics, either by extending topics with more specific RTD targets, or by providing new RTD topics that were thus not discussed during the workshop on 23 May. The latter have been included in this report, but are clearly indicated in a separate table.

(*) Additional RTD topic provided after the workshop. It is reported, but to indicate that it was not discussed during the meeting with the other participants, it is written in italics.

Overview of the technological issues

Topic	Number of EU-wide projects	Objectives and deliverables	Time Frame	Total effort [M€]	Organisation
Chip Technology	7.0		3.3 years per project covering 2002-2010	31 M€	Industry led consortia, including universities
Interfaces Architecture Low power consumption Alternative memory Stronger security		Multiple interfaces New architectures Prototype Prototype Prototype			
Operating systems	5.3		3.5 years per project covering 2002-2010	58 M€	Industrial associations and bodies, including universities
Open source Modularity Verification Modular architectures Virtual engines		Common OS Prototypes Library standard Methods and tools Prototypes Interface and adaptation standards			
System integration	6.3		3.0 years per project covering 2002-2010	17 M€	University or industry led consortia Industry led consortia including academic bodies
Services Tools Integration Background, support and carrier systems, ubiquitous computing, world wide interaction		New demonstration services Ambient intelligence demo Distributed intelligence and security, fast and secure interaction			
Development tools	6.5	Development and certification tools	3.5 years per project covering 2002-2010	24 M€	Industry led consortia including universities
Formal modelling Code generation Testing tools Verification tools		Prototype card description tool Prototype code generation tool Prototype test tool Prototype verification tool			

Topic	Number of EU-wide projects	Objectives and deliverables	Time Frame	Total effort [M€]	Organisation
Strong security	5.6		3.6 years per project covering 2002-2010	32 M€	Industry led consortia including universities
HW SW Tests Cryptology Design Integrated biometrics Security classification & infrastructures Anti-fraud infrastructures		Secure card protocols Certification tools New algorithms and protocols			
Components and mounting	8.0		2.2 years per project covering 2002-2010	25 M€	Industry led consortia including universities
Thin components Tokens Mounting technology, assembly machines		 Prototype components New assembly machines			
Materials	6.0		3.0 years per project covering 2002-2010	24 M€	Industry led consortia including universities
Interconnection Carriers Assembly Machines		Demo materials and processes Prototype machines			

Additional RTD themes proposed after the workshop

Topic	Number of EU-wide projects	Objectives and deliverables	Time Frame	Total effort [M€]	Organisation
Increasing the security of SC systems which have to use non trusted platforms (e.g. Windows)	8		typically 3 years per project covering 2002-2006	24 M€	Industry led consortia including universities
Interfaces Distributed security concepts Adding or hardening anti-tamper structures to de facto platform systems		Security increase concepts SW / HW security interaction schemes Integrated protection and attack detection protocols, algorithms and concepts Protecting SW structures by add-on HW			

Topic	Number of EU-wide projects	Objectives and deliverables	Time Frame	Total effort [M€]	Organisation
Secure, inexpensive, intelligent smart card accepting devices	6	Standardised card acceptance device, OS and toolkits	2-4 years per project covering 2002-2008	63 M€	Industrial associations and bodies, including universities
Integrated tamper protection concepts		Open source concepts			
New adaptable and trusted OS + application toolkits		Common OS			
All in one chip solutions		Secure mounting technology			
Trusted integration and mounting technologies		Methods and tools			
Fast and efficient certification and evaluation standards and procedures		Interface, library and adaptation standards			
New form factors and interfaces	10		2-3 years per project short runtime, fast results required - covering 2002-2010,	30 M€	Industry led consortia including universities
Tokens		Prototype components			
New interfaces		New assembly machines			
Integration of wireless interfaces, biometrics, displays		Tests and trials			
Mounting technology, assembly machines		Test deployment			
Personalisation					
Distribution of smart card know-how, empowerment of SMEs, improvement of smart card technology knowledge in Candidate Countries	15	Training and know-how dissemination	1.5 years per project covering 2002-2010	22,5 M€	Industry led consortia including universities, especially SMEs
System technology		Deployment			
New applications		Cross fertilisation			
Networking		Cooperation concepts			

Further information is available from:

Phone: +32 2 295 34 13

Fax: +32 2 296 83 64

e-mail: infso-c4@cec.eu.int

European Commission
Information Society Directorate-General
New Method of Work and Electronic Commerce
Information Security and Confidentiality, Intellectual Property