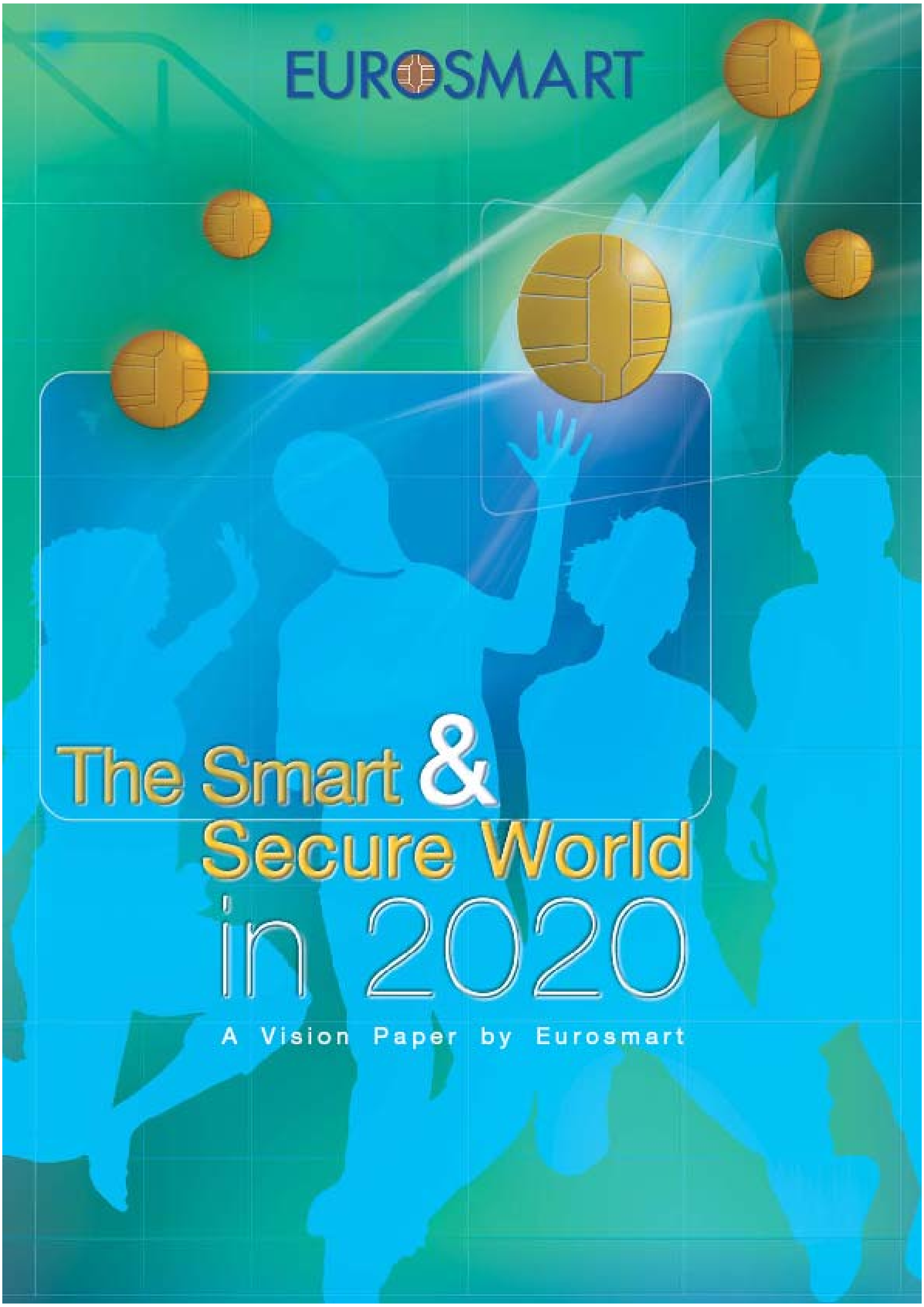

EUROSMART

The Smart & Secure World in 2020

A Vision Paper by Eurosmart

INDEX

PREFACE

By Jacques Seneca, Chairman, Eurosmart

There are 13 years to go till 2020. It can be tempting, when predicting the future, to veer to the extremes, to foresee either maximum change or none at all. After all, 13 years ago was boom time for prepaid phone cards (300 million sold in 1994), but that market has now been completely taken over by SIM cards. While these cards were launched initially for the same purpose - to make a phone call – SIM cards now provide many more services. Remember, in 1994 the worldwide deliveries of SIM cards were ten million units. This year they are going to be about 2.4 billion: 240 times more! Think about contactless today, think about ID, think about Internet security, USB tokens, convergence between telecoms, payment and Internet services… Some people say that very little may happen, others think almost anything can happen.

However the purpose of this Vision Paper is to take a realistic look into the future as it impacts the smart card industry and to offer guidance to its members about that future. To do that, Eurosmart has widely canvassed opinion and conducted formal research about the future of smart cards. One thing has become quite clear – the future is unrolling at different speeds, depending on who you talk to, consumers, vendors and issuers.

But first, does the use of the term «smart card» in itself show a specific bias? Eurosmart thinks so and for this reason, throughout this paper we will be referring to smart security technologies and objects, in addition to smart cards.

During our research, we found a high level of expectation from consumers, from citizens. They demand more secure and personalised tools to protect their interactions with the digital world. At the same time, technology vendors are promoting aggressive technology road maps capable of delivering many more features, more security and more convenience than some issuers are willing to deploy today.

There is therefore clearly a need for better alignment between consumer expectations, the capabilities of the technology and the relatively slow adoption by some issuers.

One difficulty so far has come from integrating smart security technologies into conventional IT structures. Some IT vendors may be reluctant to endorse them because of the logistics issues involved with issuing hardware devices to consumers. Some may simply be unaware of their capabilities, thanks to a lack of communication from our industry, some may just be waiting for issuers and service providers to produce requirements. While this is as true for mobile phone architecture evolution, network access control systems, PC vendors and back end systems as it is for other parts of the network, it also offers a rich array of opportunities for our industry.

Therefore there is a tremendous opportunity for leading issuers to leverage this level of expectation from users to demonstrate their customer-centric approach and to differentiate themselves from their peers.

On the other hand, there are also significant factors at play that could give our industry a fast track to growth and give end users many more services. These include the endorsement of smart security technologies by governments for national security schemes such as e-Passports, national e-ID cards and online e-Government services. There is also backing from major IT players such as Microsoft, and from some leading PC and consumer appliance providers (smart card reader slots in PCs, set-top boxes, pre-loaded smart security firmware and more). There is also the convergence of IT communication interfaces and traditional smart card interfaces such as USB onto new smart technology products.

So what will the situation be in 2020? One thing is for sure - with about 4 billion chip cards to be delivered this year, the growth of this market and the deployment of smart technologies, cards and more, into new applications mean that opportunity for our industry is by no means yet at maturity.

This paper is the result of both Eurosmart's research and the thinking of industry experts within Eurosmart. I would like to thank everyone who worked so hard on translating that thinking into this paper. Please read on to find out our vision for smart security technologies in 2020.

Jacques Seneca
16th April 2007

1.0 EXECUTIVE SUMMARY

Starting from a base in the telecoms sector, smart cards have been in use for over 30 years as secure, portable, personal objects. Today, smart cards are volume trusted computing products. Where and what will they be in 2020?

Experience since they first appeared suggests that standardisation will prevail, that new applications and technological developments will occur in the next 13 years and that the pace of change will differ from sector to sector. The purpose of this vision paper is to examine in more detail what smart cards will become by 2020.

Smart card applications fall into three areas of use today – human to human, human to machine and machine to machine. Their legacy is in bringing authentication and personalisation to transactions. In the future, that legacy will become ever more important but in addition, smart objects will add decision making capabilities too.

A typical day in 2020 will see smart objects being used by consumers and citizens to access and enjoy personalised educational and entertainment experiences, for civil and online identification purposes, to protect and monitor their health against unexpected threats, for access, for transit, for payments, for faster and more convenient shopping experiences and for much more. They will make life easier for all of us, not just the rich, but developing nations and the digitally excluded too. And around us, smart objects embedded in M2M applications will use heuristics to make our technological life simpler and better than ever before.

By 2020 human to human use, today primarily GSM, will have expanded, fuelled by the growth in Web 2.0. Human to machine, mainly accounted for by traditional applications such as banking, will develop along two axes – using smart objects for storage or for access.

These two paradigms account for the history of our industry to date. However machine to machine is another area with equally great potential, but the challenge is to develop enough intelligence to ensure that every situation can be handled by the smart card or, to be more accurate, smart security object. By 2020 machine to machine will be a dominant application of trusted hardware technology. Alternative low-end technologies in this area will not be a threat – instead they will help our industry to grow.

While smart object technology will continue to develop in the years up to 2020 and communications will become faster and more efficient, there are some issues to consider including power consumption and manufacturing business cases for small die sizes. There will be a far wider range of form factors than today with short range wireless communication technology prevailing.

Other prevalent technologies in 2020 that will relate to and complement smart security technologies will include RFID, secure networks, trusted software platforms, biometrics, memory cards and nanotechnologies.

The security/risk/privacy balance will continue to be an issue, in the face of growing threats. However, this is a duality that will not go away. It is our job to demonstrate that the benefits of the digital life and the simplicity and convenience brought to it by smart objects outweigh the possible negatives. There are two ways to deal with this – appropriate legislation and education. There are already a considerable number of legislative and research activities underway worldwide. However the industry has a major role to play in consumer education.

What this means is that smart objects will become totally integrated into everyday life as our digital proxies, bringing added simplicity and convenience to users and tighter relationships with issuers. By giving the user ownership of complexity and security and by simply making our lives easier, smart objects will be undisputed in 2020.

2.0 INTRODUCTION

It is now nearly 40 years since the first patents were filed for plastic cards with chips on board and 30 years since real interest started to build around chip cards. During that time, the telecoms sector has been crucial to the smart security technology industry. There was the introduction of low-end memory phone cards by France Telecom in the late 1980s and the roll out of (U)SIM cards to what are now over 2.2 billion 2G/3G GSM subscribers worldwide, a number that continues to grow daily[1]. Now there is the evolution of the UICC with gigabytes of memory and a full set of applications covering far more than just telecommunications.

Smart cards are also increasingly used in banking, for government applications, for transit ticketing, for access control. Smart cards, or rather, smart security technologies are now about far more than just memory on plastic cards.

Eurosmart first started monitoring smart card shipments in 1999. In that year, 1429 million units of microprocessor and memory cards were shipped, with banking and telecoms as the highest volume sectors. In 2003, 1898 units shipped: again telecoms and banking were at the top of the list. In 2007 we forecast that total units shipped will hit 4 billion, with the volume of microprocessor cards growing by over 20% from 2005, and with the greatest growth occurring in government and healthcare applications.

That's an amazing change in 8 years, let alone 40. There are now 13 years to go till 2020. What can we expect to see happen to the smart security technologies industry, both in terms of technologies and markets by that date?

We are in the business of volume trusted computing products and services

Today Eurosmart members are in the business of volume trusted computing products and services. This is most notably a subset of trusted computing, which itself encompasses three domains:

Human to human communication

[1] In Q2 2006. Source: GSM Association

Peer to peer transactions are rapidly gaining traction thanks to the success of Web 2.0 services, such as Skype™ telephony, entertainment services like YouTube™ and social networks like MySpace™. Humans are carrying out many more transactions with other humans and that creates a need for new schemes for managing identities, managing assets and securing transactions.

In addition to these new rising Web stars, H2H applications also include all the long-term, traditional SIM markets where the key role of the smart object is to ensure you are who «you say you are» and where the issuer needs a way of protecting against «repudiation of service».

Human to machine communication

H2M uses of smart cards, such as banking, concern electronic transactions involving a service issuer and its customers. The customer interacts using his/her card with a terminal to perform a set of pre-defined transactions. The smart card enables online and offline risk management to perform standalone decisions on behalf of the issuer.

The big success of smart cards in this area is to build service interoperability and to lower the costs of risk management.

Machine to machine communication

This is an area with considerable potential for the future of smart cards and smart objects. However in human to human and human to machine interactions, the presence of at least one human solves any unforeseen situations that were not pre-defined in the transaction. The challenge of M2M is to develop enough intelligence in the heuristics so that every possible situation can be handled. In a M2M transaction, each machine computes the deliverables of the transaction. The smart object's role is to set the rule and corrective actions in case of deviation to the rule. The intelligence is in the smart object.

> **By 2020 we can expect machine to machine communication to be a dominant application of trusted hardware technology.**

Traditionally the smart card industry has addressed human to human communication (in the form of telephony, banking, and most recently, identity applications), and in a limited way human to machine communication (banking terminals). With the exception of its semiconductor industry members, it has not yet addressed machine to machine communication. We anticipate that by 2020, that will change.

Radio Frequency Identity (RFID) tags and Trusted Platform Module (TPM) are two technologies in that market today. By 2020 we can expect machine to machine communication to be a dominant application of trusted hardware technology. In most applications, M2M will re-use existing smart security devices technologies and form factors. For new technologies, like the infinitely small nanotechnology devices that will emerge for medical applications for example, there will be a need to re-think of smart card shapes and implementations to scale with the challenges of small hardware machines. The term «smart dust» is often used in the literature: meaning a network of tiny wireless, microelectromechanical systems or sensors, it reflects the concept of software and rules embedded into nanotechnology machines and represents the ultimate reduction in scale of smart security objects. Already by 2007 there have been considerable advances made in terms of the hardware impact of nanotechnology machines. The remaining challenge is to bring intelligence, heuristics and security to those devices. For smart dust that means a complete set of new smart objects. Typical M2M applications might include monitoring hospital conditions or military tracking of enemies. It remains unclear how much of a reality this will be for the smart security industry by 2020 however.

In 2020 human to machine communication may have developed along two axes. One is the usage of personal secure objects of various shapes, depending on the application context. These will be an evolution of the memory tokens that we use today, but with far superior security protection and far more application rules embedded. The other is the protection of computing’s man machine interface - the next PC revolution is anticipated to be the replacement of the mouse and the keyboard with new interfaces like voice and touch. Smart objects will clearly be a key element of the way biometrics are imported into the system, as well as how all transactions will be secured.

In 2020 human to human communication will be structured vertically depending on security needs.

In 2020 human to human communication will be structured vertically depending on security needs. The top tier will still be dominated by smart card technology, secure in its technology and processes: i.e. vaults made individual for each customer with the highest level of secure personalisation. The middle tier will be a battlefield between various trusted technologies with trade-offs to provide «just enough security» to meet the application's demands. The bottom tier will be software based and will depend more on commercial terms and conditions and legal frameworks than on technology to solve deviations of usage.

Going forward from 2007, one potential challenge for the smart security technologies industry is the increasing presence of alternative, basic or medium security level technologies mentioned above in the field of trusted computing hardware. Those technologies will come from a basic position in the trust hierarchy but will necessarily try to move up in that scale, just like smart cards did from their invention to the present. Those technologies will pull a lot of new applications into the field of security and our industry will ultimately benefit from that. As soon as a service introduces a secure, more robust solution, trade-offs are made and that gives our industry an opportunity to propose an improved implementation and to demonstrate its merits.

The best image to visualise that is that for most of us, our first car in college is not a Porsche: it is the best value we can get for the little money we have. Once on the road, we get a taste for better cars! Equally, while peer to peer payments today use usernames and passwords for security, we need only to demonstrate the added value of a more secure authentication mechanism. Once we have achieved that, we can continuously propose security and convenience improvements, in a cost effective and user-friendly manner. The net outcome will drive this application to adopt smart security technologies.

For many reasons security has sometimes been treated as an «option». We can claim with certainty that it will no longer be the case in 2020.

As a result by 2020, what we call basic or medium security level technologies today will become members of the smart security technologies family, benefiting all of us. For many reasons security has sometimes been treated as an «option». We can claim with certainty that it will no longer be the case in 2020.

The purpose of this paper therefore is to consider likely scenarios for the evolution of the smart security technologies industry and a strategy for keeping their value proposition while presenting it as part of the overall way forward for trusted computing hardware at large.

To achieve that, we will review the situation today before presenting the likely features of the situation in 2020 and the ways that the three paradigms presented above will adapt. We will then present ways in which the smart security technologies industry can meet these challenges and stay ahead in 2020.

3.0 WHERE ARE WE TODAY?

3.1 Smart cards in 2007

In the 30 years since serious interest was first shown in smart cards, they have grown from being an esoteric technology to being ubiquitous items, in use worldwide.

Today, a smart card is an individual and personal object, involving hardware and software, ideal for securely interfacing individuals or individual items to the digital world. It is capable of representing its issuer's and user's best interests by performing offline risk management decisions. It simplifies the way services are delivered and often the way partnerships are implemented – the best example is the roaming management performed by the (U)SIM card for 2G/3G GSM networks.

Situations involving smart security technologies break down into three major paradigms: human to human, human to machine and machine to machine.

These three paradigms reflect the three different possible situations when performing a transaction.

Human to human

H2H appears to be the simplest of the paradigms but the reality is the exact opposite. The challenge is tremendous. Two individuals, non-trusted entities, often physically distant and who may not know each other must conduct a transaction according to a set of rules. They also have to settle whenever a deviation occurs. The benefits of smart cards today have addressed that very complex need. The scope of the definition of the service is protected in a «vault». Only the authorised user of that vault owns the credentials to activate the transaction. The second peer can confidently accept the transaction without any fear because the service issuer is «present» by the means of the smart device that represents his authority for the given transaction.

One of the biggest H2H areas today is telecoms. Today the smart card is an authentication device. By 2020, it will be a convergence and settlement device too.

In addition by 2020, the number of situations that will require such mediation between two humans will explode thanks to Web 2.0 «collaborative» services. For example, at the current pace of usage of MySpace™ or YouTube™, a significant portion of multimedia content will be user generated. People will buy music from other people, and not only from trusted, well-established retail stores or content providers. People are going to do more and more business with people. They will need trust, security and convenience, without adding complexity. In addition, the smart object will act as a proxy in this environment. H2H is hence a brilliant showcase for smart security objects.

Human to machine

Human to machine interactions fall into two camps – using smart security technologies for data storage and security protection and using them to manage and protect human interactions with the network. Applications include digital rights management, location based services and ID and access management. H2M transactions have a lot of common ground with H2H transactions, but in addition, there is a need to enforce rules that are contractually accepted by the customers when entering the transaction. In that respect, by 2020, the main evolution will be the ability to install and update in real time a set of very sophisticated heuristics. In that area the smart object is distinct from the microprocessor that runs the machines or applications. The microprocessor's job is to execute a large volume of data analysis and parameters settings, in brute force mode. The smart object's role will be to execute defined rules and decisions tailored for each particular client.

Here is a simple example. A vending machine delivers a pack of cigarettes whenever a payment transaction is validated. But by 2020, it will not do so if you are 12 years old, something that has already been realised in Germany. Additional rules will double check your biometry or/and your personalised data using a personal smart object (thus protecting your privacy) and will report to a decision engine to enable the particular transaction.

Machine to machine

This is the least developed of the three paradigms today but one where smart objects have equally great potential. A typical communication might be a settlement or a transaction, involving automated reference to a table of rules. Examples include vending machines requesting replenishment. In the telecoms sector, the smart security technology object can act as a communication module connecting several machines. In this scenario the UICC is a connectivity bridge able to communicate the working data flows of applications and machine processes in a secure manner. Of course, automatic interactions of this nature depend ultimately on human intervention or design.

However the biggest challenge for M2M transactions is that no human intervention will be available on the spot to solve deviations to the set of rules. Therefore M2M transactions involve the integration of smart objects, smart sensors and real-time software technologies to deliver a virtual H2H transaction, i.e. a transaction that always completes successfully with as many corrections of deviations as needed, again ultimately creating simplicity in our digital future.

3.2 With the benefit of hindsight

It might be instructive at this point to consider how we expected our industry and technology to develop in the early days. Did we foresee today's situation?

Back in 1987, when smart cards were an interesting idea, primarily used only in small volumes for computer access and security or as memory cards in the telecoms sector, one of the founders of the industry had this to say about smart cards in 2000[2]:

> *«There is no doubt that this small piece of plastic with an embedded chip will invade our everyday life in the coming years».*

Then, that was an optimistic prediction but it shows that the industry has the power to make optimism reality.

In 1987, card software was proprietary to individual manufacturers who were working towards compatibility within product ranges. By 2000, Java Card™ was well established. As in other areas of IT, there is a trend towards industry standardisation, although proprietary systems still exist.

The SuperSmart Card, with its keyboard and screen, was promoted as the way forward in 1987. Contactless cards were only just at development stage in 1987 – a few years later many people had written them off as failures. By 2000, cards were widely available with keyboards and screens – it was just that the keyboard and screen were to be found on the mobile phone into which the card was inserted.

[2] Ugon, Michel, Smart Card - Present and Future, Smart Card 2000, the future of IC cards, ed. Chaum, D and Schaumuller-Bichl, I, North Holland, 1989.

Contactless and dual interface cards were already being viewed as the future. Just because something doesn’t work today, that doesn’t mean it will not work in 2020. Equally, what looks promising could be a false dawn.

We could carry on, but the point is made – looking ahead 13 years is difficult. Much of the progress made - more processing power, more memory, more security, increasing communication speed – has mimicked earlier developments in mainstream computing. The time lag is a factor of physical constraints on the device.

There has been one big attitudinal change since the early days. Consumers may still think of smart cards or smart security technology objects as independent devices. They are nonetheless elements in a system, just as computers are becoming nodes on a network. Developers no longer plan systems around the wish to use smart cards. Instead they choose smart cards for their systems because they are the best choice for the simplest, most useful outcome. There is no reason to suppose that that will change again by 2020.

3.3 Pace of change

What then will be the likely pace of change over the next 13 years? After all, some changes in our industry (EMV for example) have taken many years to mature. And with a multiplicity of choice in some application areas, will society suffer from the menu syndrome, where there are just too many choices to pick from? On the other hand, when innovations make sense, they can be rapidly adopted – for example the (U)SIM card.

In reality, some areas will change quickly and others won’t, just as has happened over the past 13 years. In the following chapters we look at some of the factors, social and technological which will drive those changes, big and small.

4.0 THE TECHNOLOGY LANDSCAPE

4.1. Semiconductor technology - anticipated developments

Will semiconductor technology for smart objects continue to develop? Data from International Technology Roadmap for Semiconductors[3] seems to suggest that the answer is yes for more function integration and cost reduction for large systems on chip. However overall pricing levels are likely to remain constant, although there will be more functionality per euro.

The following table compares current state of the art for smart security technology chips to the predicted situation in 2020.

2007	**2020**
Production: 130/100nm EEPROM (< 256kbyte) 8/16b CPU	14nm for large System on Chip (CPUs +Flash) Most probable for smart security technologies and Trusted Personal Devices: 45-35nm in volume production, 35-25nm in development.
Introduction: 90nm Embedded NOR Flash (1Gb) Memory on Single Package	SoC Embedded Flash (NOR or PCM) > 64-128 Gb
16/32B CPU with 1 or several DPEs (Dedicated Processing Engine) for Cryptography & fast encryption	Multiple CPU (32b CPU + several DPEs)
multiple I/Os protocols support (ISO7816, USB FS , C-Less, SWP)	Multiple I/Os protocols support (ISO7816, USB FS, C-Less or UWB, SWP, ISO 14443).
Production wafer size: 300 mm	Production wafer size: 450 mm

Looking forward, there are some major hardware related issues to consider for 2020.

- Power consumption: complex HW/SW power management will be necessary with multiple CPUs and DPEs.

[3] International Technology Roadmap for Semiconductors - http://www.itrs.net/

- Time to volume and production lead-times will be shorter with maskless techniques and Flash technology.

- The usage of advanced lithography for small die size (<5mm^2) traditional smart card ICs with small volume production batches, using 450mm wafers, may become uneconomical and could put in doubt the business case for single application and service cards, because of the cost of manufacturing and testing. Will 300mm wafer fabs with 90 / 65 nm capability survive until 2020? Given smart security technology ICs volume demand and cost requirements, some products might be uneconomical to move to 450mm advanced fabs.

- How will we integrate ever-changing security requirements into the design of the whole chain from specifications, design, manufacturing and personalisation, up to post issuance of HW/SW security mechanisms and trusted upgrades?

From the outset, the smart card industry has benefited from technology development and progress in the semiconductor industry in general. This progress has generated significant die size and cost reductions and has allowed the embedding of more computing power, more functions and more memory in faster devices. The power consumption of each IC has as a result gone up, producing complex SoCs (System on Chip) power management functions, which are becoming even more complex on short-range wireless products such as contactless microcontrollers.

Our research shows a clear trend towards and requirement for more memory and the use of contactless devices.

Of course semiconductor technology is not the only aspect of smart security technology that will change by 2020. On the packaging side, significant progress has been made based on wafer thickness reduction, die attach and wiring techniques and multi-chip packaging leading to reduced cost assembly processes. New R&D programs concentrate on heterogeneous material integration (sensors, polymer antennae) for improving the functionality and the reliability of the components used in both contact and contactless smart objects applications.

So how else will hardware develop by 2020? The research carried out by Eurosmart shows a clear trend towards and requirement for more memory and the use of contactless devices. Will that reflect the reality? Will smart security technologies still lag behind technology progress in general and will cost continue to be the number one issue? Or can we amortise costs with other more powerful technologies?

4.2 Communications

By 2020, standardisation should have eased interoperability issues. IP based solutions will enhance high speed, high bandwidth communications with greater security. Telecoms will bring ubiquity of service on the move. Convergence will mean communications, anytime, anywhere. Multiple communications methods will operate in parallel. The best case is that smart security technology objects will act seamlessly and independently in an IP environment.

However, real interoperability will be dependent not just on standardisation but on greater levels of collaboration.

Convergence will mean communications, anytime, anywhere.

The opportunity for smart objects to quickly become «convergence enablers» is a tremendous challenge that our industry needs to build on. By 2020, the only thing in common between a wide variety of appliances will be the smart module, carrying the user identities, preferences and credentials to interact with multiple networks and multiple business relationship with service providers.

- Engineers will put the smart object in the centre of their integration strategy to be modular, scalable and cost effective.
- Marketeers will put the smart object in the centre of their ease-of-use strategy to build trust with their customers, as well as at the heart of their CRM strategy to continuously bring tailored value to their clients.
- Users will put the smart object in the centre of their overall service experience to simplify their learning curves and to manage their rights.

4.3 Operating Systems and Software Development

It has been the significant effort made in developing operating systems tailored for niche markets like banking and the public sector that has shaped the success of smart cards today. One very interesting trend we anticipate for the next 13 years is growth in the number of developers using our technology platform to in turn create significant growth in new areas that do not use smart objects today. That new exposure will be done without compromising either the quality or the fundamental merits of smart objects. In fact it will accelerate innovations and hasten adoption in new services. With the increasing number of applications in IT systems, it is clear that a wide variety of software developers, applications developers and integrators will start leveraging smart objects and deliver many new innovative schemes. In order to encourage that, our industry must be cautious to always include a solid Software Development Kit (SDK) layer with all new operating systems and architectures when introduced.

The trend started with the SIM Tool KIT for the SIM card and exceeded all our expectations. More than 500 Java™ applets have been implemented and many more ideas have been tested. Moving forward, by leveraging successful frameworks like Java™, Ajax™ and .NET™, our industry will focus on delivering the APIs and the SDK environment to attract many more innovative ideas embracing smart objects for built-in security, ease of use and convenience.

In 2020, the most visible change will be the number of corporations and solution providers that will provide their application layer on highly standardised baseline platforms. Smart objects will gain in visibility and will become more widely used.

Our industry offers today all the building blocks necessary to solve e-Payment issues.

Starting from today's building block for user authentication, payment schemes and protection of assets, the next foreseeable steps for developers are e-Commerce schemes where payment on the Internet needs to be made as secure, as convenient and as easy as payment with banking cards. Our industry offers today all the building blocks necessary to solve e-Payment issues.

Consumer habits are always slow to change, but we can say for sure that by year 2020, all payments on the Internet will be made using personal smart objects that will deliver the same level (or stronger with mutual authentication) of security as banking cards in retail payments today.

4.4 Further hardware and software developments: Smart Embedded Systems Engineering

New contactless smart cards and future smart objects using short range wireless communications are typically Smart Embedded Systems, i.e. engineering artefacts involving computation that is subject to physical constraints. Those physical constraints arise through two kinds of interactions of computational processes with the physical world: reaction to the physical environment and execution on a physical platform. This becomes especially important when considering security issues.

Accordingly, the two types of physical constraints are reaction constraints (deadlines, throughput, jitter, physical attacks) and execution constraints (processor speed, memory size and characteristics, power, dissipation, hardware failure rate, back-doors, side channels…and overall cost). Up till now, reaction constraints have been studied in control theory and execution constraints in computer engineering. Gaining control of the interplay of computation with both kinds of constraints, so as to meet a given set of requirements, is the key to smart embedded systems design.

Recent trends have focused on combining both language-based design and synthesis-based design approaches (hardware/software code-design) and on gaining the maximum independence from specific platforms during the early design process. This approach is often referred as a model-based approach because it tends to separate the design level from the implementation level. Recent examples of model-based methodologies are System C by the hardware design community, which uses synchronous hardware semantics but also allows the introduction of asynchronous execution and interaction mechanisms from software (with C++). UML (Unified Modelling Language) or AADL (Architecture Analysis and Design Language) attempt to be more generic and independent from their choices of semantics. But there is still progress to be made for computational models to deal with physical constraints and to transform non-computational models into efficient computational ones. This should lead to the development of further extensions for the implementation of extra requirements such as real-time timing constraints, the separation of human–guided design decisions from automatic model transformations, heuristic, power consumption, fault tolerance, security etc.

Another area where Smart Embedded Systems design will develop is Critical versus Best-Effort Engineering. Critical Systems Engineering is based on worst-case analysis and on static resources reservation, including in some cases «massive» redundancy, maximum failure detection and recovery at any cost. Such an approach has several drawbacks, not only on cost, but complexity if not properly implemented could also bring additional vulnerabilities. In contrast Best Effort Engineering is based on average-case (rather than worst-case) analysis and on dynamic resource allocation (computation resources, power etc.). The obvious advantage is cost versus performance optimisation (which is an important factor for smart cards and smart objects), but the degradation or even temporary denial of services (QoS or Quality of Service) could be acceptable under certain conditions, for example compensation with appropriate policies.

The gap between the two approaches has been widening, including in the transaction domains considered in this document. However, based on its long experience in hardware and software co-development, especially for achieving security requirements, the smart card industry can bridge this gap and change the traditional dual vision and separation between critical and best-effort practices that is widely in use in the traditional hardware or software industries. For example we have implemented methods (including formal methods) for guaranteeing sufficiently strong, but not absolute separation of critical and non-critical components or applications on a single-chip microcomputer in a card, by taking advantage of how hardware and software resources complement each other and of their respective constraints.

Finally, the future of hardware (cards and/or objects) and software (including middle-ware) developments for the deployment of smart objects cannot happen separately. Heterogeneity (as a property of systems to be built from components with different characteristics) will be encompassed. Constructivity (the possibility of building complex systems that meet given requirements from building blocks with known properties) will be achieved for robustness, optimised Quality of Service and performance, using appropriate modelling techniques and methods.

4.5 Physical aspects

By 2020, the standard card shape will no longer be the only shape or form factor for smart security objects. The standard 7816 card will still exist, for example in the conquest of the 3rd and 4th billion GSM users in emerging countries and in areas where cards are the standard paradigm (for example drivers' licences). In general though, form will follow function and the object will take the form most suitable for the application and the user. There will be considerable variety in form factors, enabled by the widespread use of contactless technology. Machine to machine communication may not even need a form factor as it could be realised in software. In applications like supply chain management, objects will have an IP address and will be able to communicate through embedded software with the outside world.

Contactless technology is a clear enabler to unleash creativity about new shapes and new form factors. Until now, the contact position on cards constrained developers' creativity. With contactless, the smart objects become «smart touch» or «smart proximity» objects and that open the door to an immense opportunity to improve the user experience. In the world of payments and mass transit, contactless is already perceived as a solution for reducing queues, increasing transaction speeds and reducing the cost of maintenance for mechanical parts inside readers. It is also easier to use for customers who do not have to pay much attention to the accurate positioning of the smart card inside the reader. Most of all, it contributes to the feeling of fun, ease of use and modernity. It is all for the good if new smart object markets can spread a positive, modern image of their services.

Form will follow function and the object will take the form most suitable for the application and the user.

The momentum today for contactless is tremendous. Deployments are already broad in payments. By 2020, contactless could potentially become, if not the most dominant, certainly the most visible member of the smart security technology family.

4.6 Security and risks

Security relating to smart objects, as it is understood in 2007, is laid out in standards such as the Common Criteria[4], a standard that is meant to be used as the basis of evaluating the security properties of IT products. It does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. It addresses protection of assets from unauthorised disclosure, modification or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively.

[4] http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

For the consumer and for businesses, security risks translate to related fears about protecting their identity from identity theft, data from unauthorised use and theft and transactions from interruption and hijacking.

By 2020, the widespread use of machine to machine transactions will enforce a model where legal frameworks will be reinforced by a set of heuristics in hardware and software to handle every possible deviation from the generic paths of expected transactions. In addition to the traditional building blocks of electronic transactions, a solid layer of artificial intelligence will have to be implemented.

Before then, the growth in Web 2.0 will mean a gradual move from trusted providers of Internet content to an online world where we primarily interact with user generated content. This will provide new security challenges.

The growth in Web 2.0 will provide new security challenges.

Phishing, pharming and key-logging trojans will get worse, rendering single factor authentication (what you know - user name or password) less and less effective. By 2020, two-factor authentication (what you know and what you have or what you are), currently deploying very slowly, will be widespread, aided by increased use of biometrics in preference to hardware tokens. Three-factor authentication will also be in use (what you know, what you have and what you are).

Mutual authentication schemes will help reduce pharming. Electronic signature for e-Government will be widely used and trusted entities to deliver and manage certificates will become common.

In the mobile world the growing number of service providers such as Skype™ and PayPal™, and Mobile Network Virtual Operators will make security an increasingly important requirement. The winning player in the upcoming «IP communication» market must be able to guarantee at least the same security levels offered by traditional fixed/mobile operators over their traditional networks and infrastructures.

The growth of the mobile Internet will bring the need for federated authentication mechanisms and the question of who owns the final user will become paramount.

Perceived security threats will also be an issue, particularly in the area of contactless technology. While technology to counter these threats exist, for example Faraday Cages, new and widely promoted security features will be necessary to enhance perceived security.

On the other hand, we will also have introduced mechanisms to enforce start and expiry dates for contactless smart objects. This will reduce consumer fears about perceived privacy threats arising from the use of contactless devices in retail and will also protect these devices themselves against fraudulent attacks.

So by 2020, we will have to target technology to deliver according to the following priority list:

1. User and service issuer privacy, using the best available techniques and with a full documented, widely accepted, traceability threat analysis.
2. Protection of identity with best practices coming close to the privacy that physical cash affords.
3. Protection of assets.
4. Secure transactions, with all the trust of a physical signature.

4.7 What other technologies will be part of the landscape in 2020?

Of course, smart security technologies will not exist in a vacuum in 2020. Technologies that are in use today may still exist, both as complements and competitors to smart security technologies. Other technologies that we have not even thought of will come along.

There are many examples. RFID, in the strict ISO 15693 and ISO 18000-3 sense will compete with smart security technologies in the machine to machine sector. In the more general sense that encompasses Near Field Communications (NFC), it will be a valuable aspect of smart security technologies, particularly involving mobile phones. Already, mobile operators representing 40% of the GSM market are working together on NFC to turn phones into personal access devices, targeting mass transit and convenient and low value payment applications. One of the goals of the project is to build on the secure billing and identity relationship operators have with their customers through the UICC. NFC technology, integrated with the secure and well-trusted environment provided by the UICC, has the potential to marry the ubiquity of the mobile device with a range of consumer services that have global appeal. That 40% can only grow.

In fact, RFID is purely a communications method that serves both intelligent and non-intelligent devices. Whenever applications using such protocol require intelligence, personalisation and security, then the products will belong to the family of smart security technology objects. A secure contactless device is a portable, standalone agent representing the issuer's authority to deliver one set of services to one individual. Contactless is only a way of achieving more user convenience.

The smart object will become a unique access key for every IP Network.

Secure networks will become ubiquitous, fuelled by the move from standalone PC computing to computers acting as nodes on a network. A full IP Network will still require a physical device embodying the user's credentials for a secure identification/authentication process.

Memory cards have two potential futures in 2020. With added intelligence, they could become a form of smart security object. They could also grow in capacity and complement network storage solutions. Some critical data will remain better suited to a local, safe device with strict access control. Network storage will always be attractive for backup strategies and to store large multimedia files. It is the same philosophy that applies to the choice humans make when selecting what goes in the safe versus what stays on the shelves.

While the future of biometrics may seem to be assured by the e-Passport scheme mandated by IATA, it is worth remembering that the accuracy of biometric systems has not greatly improved since the late 1980s. By 2020, biometric systems will proliferate and we can anticipate that their accuracy will have improved considerably.

One new technology that could have a significant impact in 2020 is nanotechnology i.e. infinitely small systems tailored to access areas that are unreachable today. We have already mentioned the emergence of smart dust i.e. the intelligence embedded into those nano-machines. It will be vital to put a strong political framework in place to cover all the new ethical issues created by the new applications of nanotechnologies, especially in the field of medical and genetic applications.

In total, technological advances will work towards enhancing functionality and ease of use of smart security objects and users will come to understand that increased security in itself makes their lives better.

5.0 LIKELY FEATURES OF THE SITUATION IN 2020 – POLITICAL AND LEGISLATIVE

Smart security technology objects are individual and personal objects ideal for securely interfacing individuals and objects to the digital world. Over time this link will become even more secure, with progress moving from credentials and personal data, through biometrics, to smart objects closely linked to our everyday lives. New shapes and new objects will find a more and more intuitive place in our daily activities and will become an intimate part of ourselves, akin perhaps to the way people view their spectacles or hearing aids today.

New applications will continue to appear. For them to succeed, the technology and security evolution required for these new applications will also require changes in the cultural, societal and politico/legal environment. In particular, there is a need to ensure that consumers and citizens understand the benefits of smart security technologies as well as the risks.

In most critical applications, the smart security object will be adopted by its issuer as the best possible choice and trade-off in terms of risks and benefits. The point will be to demonstrate that all other possible alternatives show a worse balance on trade-offs. It is crucial that we do not fall into lengthy polemical debates: there is no solution to the risk benefit debate – all we can do is show that smart security objects offer the best outcome.

5.1 Two major drivers

As we have already seen this century, terrorism is becoming a growing threat, with a few individuals able to wreak high levels of death and destruction. This driver is responsible of the recent take-off of the electronic passport, driven by the US government, and will continue to be a major factor in smart security technology adoption to identify individuals. This application will be the first to see a global adoption of biometrics.

Health is one domain in which the use of smart security technologies will change considerably, both through improvements in health care procedures but also via the potential applications of sensors with contactless technologies. For example, a pacemaker could securely connect with an external reader to provide very useful data. The smart object's key role here would be to determine who may access the data in addition to manage the data transfer itself. This is another example where RFID is a tool, a communication protocol while the intelligence of the transaction resides in the smart object.

Healthcare could become a key market for GSM operators, bringing a personal screen and keyboard to medical data gathering, analysis and storage.

5.2 Legislation

Appropriate legislation and regulations are critical to help accelerate the acceptance of new applications and to avoid criminal use of smart security technologies. This is the role of government but there is much that our industry can do to help - for example standardising technical solutions.

5.3 Consumer attitudes to technology and privacy and the role of education

Consumers want more and more from technology and the next 13 years will see the IT industry do all it can to satisfy that desire. But at the same time consumers expect to leave no trace behind, or at least to know who is using this traceability data, when and what for. Some of the security issues highlighted in the previous chapter mean that in 2020 privacy will be a major concern for consumers and citizens.

Smart security technology objects can offer freedom and convenience of use and protect the privacy of their owners. And as technology improves towards 2020, convenience of use will grow. But at the same time, they can directly or indirectly be used by authorised or unauthorised bodies to track consumers and to acquire and read personal data. Once again, a smart security solution is a combination of one or several technologies with an accountable authority in charge to deploy it. Both need to meet the goal to perform a list of pre-defined operations in well-defined situations. The strength of the solution depends on the quality of the duality, technology plus accountable authority. When that duality works, smart security solutions are by far the best solutions.

What’s more, the freedom of use granted by the smart object is a factor of its ability to link its owner and the system of which it is a part with a strength and security level far greater than any other. This duality will be accepted by educated citizens aware of smart object features and benefits and is usually ignored by the others (even in developed countries) but in some other countries, the media sometimes provokes questions about the perceived negative aspect of this duality. Indeed this duality will continue to drive most of the attitudes towards smart security technologies in the future. Education and legislation are the two remedies to prevent panic and irrational reactions. Recall that when the automobile was introduced more than 100 years ago, some people developed sophisticated theories about the fact the human body would disintegrate itself if exceeding a speed of 50km/h. The digital revolution will improve many aspects of our lives and smart security technologies will help us to better understand it to make it profitable to us. Education, more education and education again is what we need to defeat such fears.

> **While it is the role of government to answer the sensitive question of finding the balance between security and privacy for society, it is our responsibility as an industry to help explain smart security technologies to the general public.**

A major part of our task will be to reassure and educate users about the trade-offs involved. To facilitate the digital revolution, we will have to show that the benefits of a connected life largely offset its downsides, for the good of most. However the scale of that educational requirement is likely to slow down technical innovation, especially in the e-Identity space. No-one will want to compromise innovation by launching an inadequate system into such a sensitive space and the market will wait for robust, proven, flawless deployment and an accepting public. The moral is that we need to proactively prioritise this educational process.

We can use examples of successful applications already in long term use and give insight into mechanisms used to protect user data. This should be an ongoing process and should complement the progress made in the legal and regulatory domain to help increase the trust of citizens in the technology and foster the adoption of new smart security technology solutions.

In addition we must ensure that smart security technologies remain easy to use. This will make sure they appeal to those isolated by the digital divide and to citizens of developing countries.

Given all these issues, what actually is happening now and in the near future at the legislative and regulatory level that will influence the situation for smart security technologies in 2020?

5.4 Recent and expected legislation/framework at the worldwide level

WSIS (World Summit on the Information Society) supports the development of ICT infrastructures and applications in developing countries, to be implemented by 2015. Around 10 United Nations Agencies are cooperating, including UNESCO, UNDP, WHO, UPU, ILO and WTO.

ICAO (International Civil Aviation Organisation) took the initiative to improve the security of official travel documents in 2002. Today ICAO offers Member States the option to choose between various levels of control and is now working on common test guidelines. This organisation will continue to provide guidance and improve the e-Passports that all persons travelling on the planet will possess by 2020 as well as visas and all other necessary official travel documents.

In the U.S., Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on 27th August 2004, mandated the establishment of a standard for identification of Federal government employees and contractors. HSPD-12 requires the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems.

The Visa Entry Reform Act of 2001 was introduced to create a centralised database of visitors in the U.S. and develop a new biometric visa card that the INS and State Department will issue to foreign nationals.

The American Association of Motor Vehicle Administrators (AAMVA) has created a Special Task Force on Identification Security. This task force is working on a plan to strengthen the security of the driver's licence, which has, according to the group, «become the *de facto* national identification card used by law enforcement, retailers, banks and other establishments requiring proof of identification». By providing a uniform approach and set of standards, States would be able to issue a more secure driver's licence that could be used, in many instances, as a common secure personal ID for individuals.

The US Department of Defense (DoD) has initiated a program to issue a smart card based «common access card» to all military and civilian employees and contractors. DoD employees will use these cards to digitally sign and encrypt documents and to have secure access to buildings and networks. The US Department of State is in the process of implementing a new automated access control system for employees and visitors using a smart ID card.

All these measures will contribute to the widespread use of smart security objects globally by 2020.

5.5 Recent and expected legislation/framework at the EU level

Legal initiatives at EU level are at present focused on setting up a coherent framework for ICT developments and common identity management for 2010. The emphasis is on seizing the opportunities of the digital economy and underlying the importance and benefits of convergence. This will provide a basis for tools used to shape the lives of European citizens in 2020. Once again, smart objects will have a significant part to play in attaining these objectives.

i2020, an umbrella initiative, was launched by the Commission on 1st June 2005 as a framework for addressing the main challenges and developments in the information society and media sectors up to 2010. It promotes an open and competitive digital economy and emphasises ICT as a driver of inclusion and quality of life. The initiative contains a range of EU policy instruments to encourage the development of the digital economy such as regulatory instruments, research (9 billion € support for projects until 2013) and partnerships with stakeholders (Joint Technology Initiatives such as ARTEMIS).

EU decision makers are now preparing the second generation of e-Passport, a coherent agenda for e-ID development and have finalised the future EU driving licence Directive. These initiatives will be implemented from 2010 to be fully operational in 2020.

The BIG Group, Brussels Interoperability Expert Group, a subgroup of the «Article 6» Committee (EU Visa), is presently working on the annex of the European Passport (second generation of document including fingerprints). The first draft of the specifications was presented in June 2006 and is being finalised at the beginning of 2007 with the aim of producing the first prototype in March 2007 and implementing a pilot project in September 2007 leading to the finalisation in March 2008. 2013 will see the dissemination of new e-Passports. The same group is setting technical requirements for future electronic residence permit.

The European e-ID Roadmap Working Group is coordinating e-Government developments towards a common understanding of the concept, a coherent roadmap and adequate standards for 2010. The group has to face many «barriers», as identities might not be the same when looking across borders. A European model of e-ID management would have to cope with many variances, probably the biggest challenge in the area of e-ID. The combination of e-ID management and e-Documents are the next possible steps.

For local governments, the main goals are clearly to facilitate and optimise transactions between their administrative functions and citizens. Smart security technology allows the public sector to be more open and more transparent, and to reduce significantly the costs linked to business and administrations activities. In order to offer all possible solutions to the Member States, our industry has contributed to the CEN group on the European Citizen Card. A standard for a common European Citizen Card was completed in June 2006 and comments were delivered at the end of October 2006, with the final document from committee TC224 made public at the end of 2006. The third part relating to middleware will be delivered in less than a year and the fourth part that proposes use cases to government in one year. Pilots and implementations may follow in future years.

Smart security technology allows the public sector to be more open and more transparent.

A new Directive harmonising driving licences throughout Europe was approved at the end of 2006 to be implemented by 2012 in all EU Member States. Under the scheme, the EU driving licence would be phased in over 20 years, gradually replacing the 110 existing formats in the EU. However, the electronic format is optional. Similarly, a Directive adopted in 2003 leaves Member States the same choice regarding electronic car registration documents.

Healthcare

The deployment of interoperable e-Healthcare infrastructures is likely to be the next step after e-Passport and e-ID. e-Healthcare cards are already deployed in many European countries albeit at differing rates, with France and Germany already deploying the second generation of cards.

There is a European standardisation process under way within CEN TC251 that is working on common requirements for a health information structure to support clinical and administrative procedures, technical methods to support interoperable systems and requirements regarding safety, security and quality. In addition, the European Commission is supporting the i2010 subgroup on e-Health, which aims to develop a European e-Health service and information space to improve quality access to care and enabling cost effectiveness of e-Health systems and services while ensuring European patient mobility. The subgroup published a compilation of all the available Member States' plans and roadmaps on e-Health and the good practices and will present on this basis a set of guidelines to implement e-Health interoperability by 2010.

From 2004, the European Health Insurance Card replaced all national paper forms in Member States, to improve coordination between national social security services for health treatment during a temporary stay in another Member State. By 2020, this is likely to be fully implemented in smart card form.

The Health Professional Card is used by health care professionals to assign access rights to data on the patient card. It is also a tool that aids the mutual recognition of professional qualifications, a solution that could be encouraged by the European Commission to foster mobility in Europe.

Payments

The implementation of the Single European Payment Area (SEPA) by 2008 (for the first phase and 2010 for the second phase) should encourage electronic payments in Europe and also worldwide. The European Commission proposed to establish a new legal framework for payment services (NLF) which will replace the national rules with common rules for the European internal market. The NLF should spell out the obligations and rights of payment institutions and of consumers and provide a framework for the developments of common technical and commercial standards.

Shaping R&D developments at EU level for 2020

To aid future R&D programmes, the European Commission has decided to link industries and research centres with a common research objective. These forums, now called «Technology Platforms», were informal at first, but restructured themselves at the beginning of 2005 and are now producing roadmaps for 2030 and recommendations to shape the content of the future European research. Many of these «Technology Platforms» are closely linked to mobile and smart security technology:

ARTEMIS («Advanced Research and Technologies for Embedded Intelligence and Systems») is led by Thales. Europe currently leads the world in embedded technologies for aerospace, automotive, industrial, communications and consumer electronics. This leading position is, however, threatened by global competition, fragmentation and lack of coordination across these industries. It is therefore necessary to mobilise and coordinate the private and public resources needed to meet business, technical and structural challenges and to ensure that systems developed by different vendors can communicate and work with each other using industry standards.

ENIAC («European Nanoelectronics Initiative Advisory Council») for mastering the revolutionary transition from microelectronics to nanoelectronics. The Steering Committee brings together the main semiconductors manufacturers and research centres such as IMEC (Belgium) and CEA-LETI (France). Although Europe has already succeeded in establishing itself as a world leader in microelectronics, it faces formidable challenges in achieving the same world-class position in nanoelectronics. The cost of the research, development and manufacturing infrastructures required will be extremely high and competition from the U.S. and the Far East will be fierce.

On 7th June 2005, the European Commission proposed a specific **Action Plan on Nanotechnologies** (2005-2009). This aims to boost funding for nanotechnology in the future 7th Framework Programme (FP7), including specific support for research into the impact on human health and the environment, and to foster technology platforms in certain key nanotechnology sectors such as nanoelectronics.

Mobile telecommunications have had a positive impact on economic and social activities comparable to the effect of the Internet. This evolution is not yet complete. Europe's position is being challenged by developments in Asia and the U.S. Therefore action needs to be taken to ensure that Europe participates fully in the coming wave of innovation. In its mid term report in January 2005, the **eMobile** Technology Platform identified challenges that still need to be overcome - network rollout, interoperability, appropriate regulatory environment, research, security, content, m-payment and spectrum management.

EPoSS («European Technology Platform on Smart Systems Integration»). Smart systems integration addresses the trend toward miniaturised multifunctional devices and specialised connected and interacting solutions. EPoSS proposes a multilevel approach incorporating various technologies, functionalities and methodologies to support the development of new visionary products. The visionary goal is smart systems able to take over complex human perceptive and cognitive functions, devices which frequently act unnoticeably in the background of human capabilities. The technological priorities of EpoSS are technologies for micro/nano-scale integration, packaging (wafer-level packaging), 2,5/3D integration, integration of heterogeneous materials (Si (Silicium), SiC (Silicium Carbon), SiGe (Silicium Germanium), non-Si-semiconductor, ceramics, polymer, glass, textiles, etc.) . In addition EPoSS focuses on common functionalities research for sensing (nano-sensors and MOS-detection devices), human-machine interface and visualization, security (low-power cryptography, multisensor, technologies etc.), privacy protection, robustness, quality and reliability.

The final platform is the **Networked and Electronic Media** (NEM) Initiative, created in July 2005. It focuses on an innovative mix of various media forms, delivered seamlessly over technologically transparent networks, to improve the quality, enjoyment and value of life. NEM represents the convergence of existing and new technologies, including broadband, mobile and new media across all ICT sectors, to create a new and exciting era of advanced personalised services.

There are also relevant research projects taking place. A pan-European consortium of companies, universities and user groups has been created to develop an open architecture for the development, deployment and use of NFC-enabled applications in mobile handsets. Co-funded by the European Commission, Information Society Technologies (IST) program, the «Store Logistics and Payment with NFC» (StoLPaN) project aims to define open commercial and technical frameworks for NFC-enabled services on mobile devices. These frameworks will facilitate the deployment of NFC-enabled mobile applications across a wide range of vertical markets, regardless of the phone type and the nature of the services required.

In order to accurately address the interoperability issues currently affecting the technology, various usage cases are to be defined within the StoLPaN framework and tested throughout Europe. These use cases will contribute to the identification of a common set of business rules, which will define the roles and responsibilities of every player in the NFC ecosystem. The results will then be submitted for approval to the relevant industry bodies for standardisation of payments, mobile, transit and ticketing.

Many industry-led initiatives are gaining the support of European institutions and will boost coherent and strong European research. Of course, our industry will also be helped if large scale projects can be deployed that move the technology from research to everyday life applications by 2020.

6.0 THE THREE PARADIGMS IN 2020

6.1 A day in 2020 with smart security technologies

The world in 2020 will not be only the world of smart cards, or RFID tokens but the world of many powerful personal, smart and secure devices with full Internet access. These devices will allow direct communications and fast exchange of data with remote servers. The five following examples will give an idea about how helpful these devices will be for the future everyday user's life. It is worth noting that each example employs aspects of several of the three paradigms.

There are many other possible examples but we have chosen only those which might support a real mass market. We should also bear in mind that systems of this scale can take a long time to deploy and that the smart card or object aspect of the system is just one part – smart security objects are not standalone items and the rest of the system must be developed too. In addition, what looks simple may be tremendously complex to implement. However many aspects of the following systems already exist today.

Culture and multimedia

In the future, a large part of video-on-demand will be done through mobile telephony. The mobile phone will be used as a set-top box, very easily and everywhere. The following story explores these possibilities.

Mr and Mrs Smith and their two children Jane and Bill have just arrived in Europe. They are planning to visit different cities, museums and places of interest but they don't want to miss their favourite TV shows or movies either.

The first stop is Paris. Everyone is tired, so they stay at the hotel and watch a good movie. They choose Star Wars, season XXVI. Mr Smith takes his mobile phone containing a new multimedia UICC. He starts the Internet browser from his handset and connects himself to his operator's server.

Authentication is done automatically between the new multimedia UICC and the server. Mr Smith selects the movie and starts the streaming. The mobile phone automatically establishes a connection with the TV using the new wireless USB port, and the movie starts.

However Bill has seen this movie a thousand times, so he decides to start his favourite game. He takes his mobile phone and his 3D glasses and connects himself to the proxy server of World of Warcraft. His multimedia UICC authenticates itself automatically to the server. His 3D glasses connect through wireless USB4 to his mobile phone. Bill is immediately plunged into his fantasy world.

After the movie,. Mr and Mrs Smith start planning the next day. Jane wants to go to the Louvre museum. Mrs Smith agrees and decides to prepare the visit. She takes her mobile phone and contacts the museum's server over the Internet. She asks for a three hour tour covering things that all the family wants to see. She gives out the IP addresses of everyone's multimedia UICCs to the server, and pays using her multimedia UICC.

The next day, the whole family arrives at the museum. They avoid the queues thanks to the electronic ticket provided by their multimedia UICCs. On entering the museum, each member of the family puts on Bluetooth headphones connected to their own mobile phone. The visit starts. Each member hears a commentary appropriate to his age and interests.

The multimedia UICC card has a very fast processor, enough onboard memory, a crypto-coprocessor, and some hardware accelerator for video rendering. There is a real https IP stack available onboard, and most services are available as web services.

Shopping in 2020

Many companies are working on the concept of the smart shopping trolley. They focus on gathering the ID code of the products put in the trolley, using their RFID tag. With proper privacy protection, the mixed usage of RFID tags and powerful smart security objects could attract consumers.

Suzanne and Pierre Desmoulins, who live in a small village close to Paris, are driving to the big mall, which opened recently near their village, to buy groceries They both work and don't have time to spend hours shopping. Shopping for Suzanne and Pierre must be fast and efficient.

Before leaving home they prepared their shopping list. All week they collected the RFID tags of the products they finished and wished to replace. Preparing the *shopping list consists of «reading» the RFID tags using the smart object provided by the mall inserted in their mobile phone. They also download a list of fresh items from their fridge. The phone also records their habits when they are shopping.*

They arrive at the big mall, collect a trolley and synchronise the trolley and the smart object in the mobile phone. On the trolley, they select the «fast shopping» option - somebody who wants to wander about in the mall looking for new products could select «complete shopping».

The trolley, after a dialogue with the smart object, establishes a «route» in the mall, linking in the fastest way the various products listed in the shopping list. Each time a product is picked up from the shelf and put into the smart shopping trolley, the receipt is updated. At the end of the shopping activity, if Suzanne and Pierre agree to the total submitted, the payment is made automatically by the smart object to the trolley.

Several tests have been done on smart shopping trolleys: in Tsukuba in the 80s, and more recently in real big malls in Japan. Automatic payment testing is in progress also at several large malls in Europe.

Healthcare in 2020

Today, healthcare applications only use the smart card as portable secure storage for a little data. Powerful smart security technologies with full Internet communication capabilities can provide some very useful services in the healthcare domain.

Mr Herbert Schmidt is a German citizen travelling in Bordeaux on business. Previously he has had two heart alerts and had to visit a physician to check his heart. The physician has decided to maintain a constant recording of Herbert's heart. Herbert now has to wear sensors to record heart beats all the time. Fortunately, these sensors are wireless, very light and can be removed and reinstalled very easily. They are permanently connected to Herbert's mobile phone in which a powerful smart token with a specific application has been installed.

Herbert is wandering around Bordeaux, admiring the architecture. During his walk, the sensors detect an abnormal heart rhythm. Nothing very serious but abnormal. The sensors send the abnormal signal to the mobile phone, which sends back this signal to the smart token, which compares this signal to previously recorded signals and decides to raise an alarm.

The smart token connects to the closest emergency centre. A physician is called to consider the situation. He establishes contact with Herbert's smart token to review the previous records and the record received and decides that Herbert’s situation is an emergency. The emergency centre obtains Herbert’s position from his smart token and sends an ambulance to Herbert, who is driven quickly to the hospital, before the heart attack starts.

Most of this technology exists today, but not so small and not so smart. The situation described above is just an extrapolation of what happens in a hospital today, extended to the wider world outside, again assuming the provision of proper privacy protection.

The connected home life in 2020

Paulo wakes up bright and early. It is another working day and he can smell the coffee that his kitchen management system has started to brew for him. As a delivery driver, he has to wear a uniform so after showering he puts on his jacket and smart trousers. The trousers contain RFID tags that variously pay for his commute to work, give him access to his work premises, verify his identity as the authorised driver of his work vehicle and confirm that he is driving his assigned route.

Before he leaves, he realises that he left his mobile phone at his mother’s the previous evening. No worries. He immediately goes online to temporarily deactivate the (U)SIM and to transfer its credentials and contents to his backup PDA. When he gets the phone back, he’ll reverse the process.

Before leaving for work, he authorises his fridge to place an order for groceries with a delivery service. These will be delivered and stored in the refrigerated delivery box outside his apartment building. After placing the order, the fridge automatically and remotely opens the box, ready for the delivery man, who closes it after placing the order inside.

It is a mundane day at work. While Paulo is out on a delivery, a teenager attempts to steal his van but without Paulo’s smart uniform trousers, is unable to bypass the van’s security system.

When Paulo gets home, he collects the groceries, using his smart apartment key for access. There is a message waiting for him from his elderly mother's home management system. It's nothing urgent, which is why his home did not automatically transfer it to him at work – she simply needs some help with a little housework. He's planning to go back tonight to pick up his phone anyhow, so he changes and heads back out. It's a leisure trip so this time he'll be paying his bus fare with his apartment key rather than his smart trousers. He'll use his PDA to access his own home network while he's travelling so he can catch up on some television viewing he's been planning for a while.

In Hong Kong, the Octopus system is already combining transit ticketing and door access on one token.

Sport in 2020

Some sports may change as technology develops but others, such as football, don't. Recently, a proposal to let referees use video replays was rejected. However by 2020 it's likely that this will have changed.

Herbert Schmidt, back home in Munich and feeling much better, decides to attend the big game between his favourite team, Bayern, and the Grasshopper from Switzerland. He connects his mobile phone to the web server of the stadium and buys a ticket for a seat with a good view, using the stadium seating plan displayed by his mobile phone. He also buys the replay access offered by the stadium web server. Ticket and access rights are stored in his multimedia smart object.

After entering the stadium, he is guided to his seat by the mobile phone, which gets information from the stadium web server. Herbert wears his new 3D glasses connected to his mobile phone using the new wireless USB4 technology.

After the two teams run onto the pitch, the referee's whistle marks the beginning of the game. The quality of play is good due to the high standard of the two teams. Herbert enjoys the game and cheers on his team.

Bayern exert consistent pressure and after some confusion, score against the Grasshopper. The stadium erupts with the cheers of the Bayern fans. Unfortunately, the referee disallows the goal. Immediately, Herbert starts the replay and discovers that the player from Bayern responsible for the goal was offside. He has exactly the same images that the referee has and can agree with the referee.

Many sports could benefit from this type of feature, including athletics.

Developing markets and the digitally excluded

While the examples above show the potential of smart security technologies in the prosperous first world, they also have considerable potential in 2020 to help bridge the digital divide in less developed parts of the world and amongst poorer Europeans too.

The M-Pesa™ initiative run by Vodafone™ and Safaricom™ in Kenya currently uses mobile phones to transfer money between prepaid electronic money accounts, bypassing the need for a banking network. We expect this type of initiative to spread in Africa over the next 13 years. Indeed research by the GSM Association[5] has shown that developing nations can enhance tax revenues and even GDP by encouraging the spread of mobile phones. The M-Pesa™ example itself shows the benefits of not ignoring developing economies – what started as a corporate social responsibility exercise for Vodafone™ is about to turn into a potentially lucrative remittances business.

Initiatives to sell basic technologies into developing markets, such as low end mobile phones and PCs/laptops and associated software will mean that there will be a need for higher end smart security technology objects to help operate them.

Other areas where smart security technologies could help include monitoring the health and well-being of the elderly, encouraging participation in democratic processes through e-Government and enhancing access to facilities and benefits for the economically disadvantaged.

Multi-applications in 2020

In 2020 there will certainly be no technical reasons why multiple applications and services could not exist on the smart security object. Indeed, some of the scenarios above incorporate multi-applications. That however is largely true today. Will the multitude of other reasons, including branding and ownership of the customer that have held back multi-application cards still apply? Will commercial protectionism still be an issue? Multiple services are not always easily visible to the consumer. Different

[5] http://www.gsmworld.com/digitaldivide/index.shtml

applications may have different lifecycles, making card or object lifecycle management difficult. Inter-domain security may be an issue. There is the challenge of having a unique ID and a unique identification process.

It is easier to implement multiple services from a single issuer than multiple services from several issuers. Nonetheless, by 2020, if there is a need for multi-application devices, the commercial issues above will have been resolved.

Some have suggested that a device could be purchased in a store. This would be either as a smart object (blank card), a mobile phone or equivalent (blank module) or a mobile phone with a (U)SIM. Services could be loaded from aggregators or from individual service providers at the initiative of the consumer. This raises the issue of multi-domain security (which technically is already solved), but also the issue of a certified and universally accepted and recognised level of security for the device. In addition, the issue of the acceptance of a common key/certificate must be dealt with (to achieve a unique identification process) or the hosting of multiple security tools under the same and accepted umbrella.

It has also been suggested that a main issuer could sell/rent memory and other resources to other organisations willing to be hosted in a given device. In this case, the psychological obstacle that must be overcome is more than trust and confidence, it is the willingness to be hosted by another organisation which would have control at the highest level. Other obstacles are the economics of this operation, the sharing of costs and revenues, in other words the business case for the arrangement.

There are however alternative scenarios. New actors could exploit the smart object as a secure module (in hardware or software) for trusted identification processes. In this case a high memory object would be useless; players would require just a few KB of memory to manage all access procedures to all services. Another scenario would keep the smart security object as a secure bridge to all new peripherals; in this case the module will identify the user and will manage the secure access to all these external devices for content management, storing processes, identification and multi-applications management.

6.2 A day in 2020 without smart security technologies

In contrast, what would a day in 2020 be like without smart security technologies, if society takes the decision to choose minimum security and convenience rather than maximum security and convenience? Leaving aside the sad example of Herbert Schmidt's premature death from heart failure in Bordeaux, it would probably be remarkably similar to a day in the late 1970s or early 1980s, except with some of the following features:

- more fraud, both physical and online,
- constant security surveillance by the state to prevent and monitor crime and terrorism,
- massive centralised, online databases of biometric and other personal data,
- a lack of privacy in both the private and professional spheres,
- password proliferation.

The world has changed in many ways over the past 30 years, the life cycle so far of smart security technologies. Without these smart objects, we will not return to simpler times, we will simply find it harder to maintain privacy, security and convenience in an ever-changing world. Consumers and citizens would lose out from the absence of smart security technologies – dealing with the everyday digital world would be far less simple. In fact, given where we are today in 2007, a world in 2020 without smart security technologies simply will not exist. But there are things that we as an industry can do to ensure that people in 2020 benefit from smart security even more than they do today.

7.0 CONCLUSION

Today, smart security objects (i.e. smart cards) are standalone risk management devices, linked securely and conveniently to an individual, bringing authentication and personalisation to transactions. Over the next 13 years, their convenience and security will continue to evolve, but there will be wider changes too with a strong emphasis on making life simple for citizens and consumers. To authentication and personalisation we will be able to add decision making and enforcement of heuristics too.

That's because one of the key themes of our industry's evolution will be a growth in the importance of machine to machine applications for smart objects, although this will add to rather than displace human to human and human to machine usage. In addition, transparency and simplicity of use will be key and smart objects will become vital enablers of convergence.

Smart object technology will continue to develop, with greater semiconductor functionality so hardware capabilities will not limit the potential of the smart security industry. Wireless communication protocols will become the norm and multiple communications methods will operate in parallel. We need have no fear of new and competing technologies – RFID will be classified with secure contactless devices, rapidly becoming part of the smart security technologies industry. Aided by the growth in the use of contactless devices, there will be a far wider range of form factors than there are today. The mobile phone will continue to grow in importance as a personal device, hosting smart security devices.

To meet the needs of the growing number of applications developers, operating systems will become increasingly standardised. The convergence of markets and their applications will enlarge the market for smart objects and will add value to our sector.

For smart objects in telecoms, the best is yet to come.

Citizen and government applications for smart security objects will become the main application area, ahead of GSM. However the (U)SIM card will not disappear – it will rebound as a convergence device. For smart objects in telecoms, the best is yet to come. In banking, smart objects will be the norm, everywhere. For P2P payments on the Internet, by 2020, services using smart objects to provide security far greater than that afforded by user name and password will become the intelligent choice. Multi-application objects will finally become common, with the branding and administrative issues of today resolved.

With citizen applications for smart objects becoming prevalent, our dependence on the telecoms sector will lessen, making pricing easier. We can also build less price dependency on the GSM sector by building services – the UICC becomes a service platform.

Overall we can expect market growth of around 20% a year up till 2020 in volume.

There are a number of actions that should be taken and attitudes that should be held to make this vision a reality in 2020.

We cannot expect a definitive solution to the privacy versus functionality issue – this is the fundamental duality of our technology and society will learn to accept trade-offs. However we will be helped in this by the fact that smart devices will be more and more personal, creating an intimate relationship with their users in the same way that personal music players and mobile phones are doing today.

As a result, the smart security technology industry has a valuable educational role to play in helping consumers to accept this duality. In 2020, our customers and end users will be today's young. That educational effort can and should start now.

Indeed our industry will have to decide soon if it wants to adopt a B2C profile. If so, it should consider creating an overarching brand for smart security technologies, perhaps based around the following qualities: discrete, secure, personal, close to you, low profile, unbreakable, easy to use. However, that is of course a matter for Eurosmart's individual members to decide for themselves.

Citizens will want to be able to choose between a range of functionalities and complexity in their device, again as they do today with phones. Producers should therefore develop a range of devices that are simple and user friendly as possible, issuers should provide basic information on functionality and guarantee assistance and after-sale service and should define clearly who is responsible in the end in the case of fraud.

By making life more secure we are making it easier.

Security and hence smart security technology can no longer be viewed either as an option or as a hygiene factor. We need to get the message across that by making life more secure we are making it easier and more desirable.

As an industry, we do not fear rival technologies. To compete, they continue to evolve and as they evolve they become smarter and once that happens, by default, they become part of our industry.

By 2020, smart objects will not be optional. So service providers must put smart objects at the centre of their design now as the convergence device for their service or product.

In fact smart security technologies drive inclusion, convergence and increased quality of life, themselves key aims of the European Commission in its ICT programs.

By 2020, smart objects will not be optional.

In conclusion, what this vision translates to is that smart objects will become totally integrated into everyday life as our digital proxies, bringing added simplicity and convenience to users and tighter relationships with issuers. By giving the user ownership of complexity and security and turning them into ease and convenience, smart objects will be undisputed in 2020. Simply put, people will use smart objects in 2020 because they make their lives simpler.

APPENDICES

EDITORIAL COMMITTEE

Chairman: Jacques Seneca
Project managers: Jane Adams and Xavier Larduinat

In alphabetical order:
Edmond Alyanakian
Bertrand du Castel
Sergio Cozzolino
Florence Gras
Michel Koenig
Thomas Kraft
Coline Lavorel
Lutz Martiny
Clotilde Servajean
Jean-Paul Thomasson
Hubert Vigneron

And with the contributions of: Jacques Patarin, Pierre Paradinas, André-Jacques Selezneff.

Contacts:

Eurosmart Secretariat
Rue du Luxembourg 19-21
B - 1000 Brussels
Tel: + 32 2 506 88 38
Fax : + 32 2 506 88 25

florence.gras@eurosmart.com
coline.lavorel@eurosmart.com

PRESENTATION OF EUROSMART

Created in 1995, Eurosmart gathers representatives of the whole industrial chain, from the chip manufacturers to the terminal and equipment manufacturers.
Very early, the security of the whole smart card chain became the priority of the Association whatever applications: banking, identity, access, telecommunication, transport, pay-TV…

Around 15 billion cards have been shipped over the past 10 years. The European industry represents 80% of the worldwide shipment of cards today. More than 20 000 jobs have been created worldwide and 60% of the employees are working in the EU.

Priorities of the Association

- Promote smart cards and smart card-secured transaction systems
- Promote smart card applications regarding identity documents for secure and data protection advantages: identification, authentication, privacy, convenient and ubiquitous access
- Define a consistent range of quality standards and security levels that improve the industry efficiency, growth and sustainability
- Provide a forum for the consolidation of industry marketing and technical statistics
- Advance public awareness through international and national bodies

Participation to the European legal agenda

In coherence with the priorities of the industry, many proposals were and are still followed by the Association at the European level, for instance:

⇒ Recommendation on the New Legal Framework on Payment in the internal market, December 2003
⇒ Payment fraud prevention expert group active member
⇒ Recommendation on e-Visa and e-Passport regulation proposals, September 2004
⇒ Position paper on EU Health card, November 2005
⇒ Position paper on EU Driving licence, March 2006
⇒ Member of the e-ID roadmap workshop (since January 2006)
⇒ White paper on security into e-Passports, February 2007

Eurosmart expects EU governments to lead the way with e-Government applications and e-ID implementations and promotes common standards to achieve digital convergence.

More information: www.eurosmart.com

FIGURES

EUROSMART - WORLDWIDE SMART CARD SHIPMENTS 2006
Cards (Millions of units - Mu)

	Memory	**Microprocessor**
Telecom	480	2040
Financial Services - Retail - Loyalty	30	410
Government - Healthcare	250[1]	90
Transport	140	20
Pay TV	-	65
Corporate Security*	15	15
Others	10	15
TOTAL	925	2655
	3580	

[1] Including Chinese ID at 200 Mu

*Cards with logical access or multi-application feature (does not include single function access control cards)

EUROSMART - WORLDWIDE SMART CARD SHIPMENTS
FORECAST 2007 (March 2007)
Cards (Millions of units - Mu)

Forecast 2007			
	Memory	**Microprocessor**	
Telecom	440	2400	18%
Financial Services Retail - Loyalty	30	490	20%
Government - Healthcare	350[2]	140	56%
Transport	160	30	-
Pay TV	-	70	-
Corporate Security*	20	20	-
Others	10	15	-
TOTAL	**1010**	**3165**	**20%**
	4175		

[2] Including 300 Mu forecasted for Chinese ID Card

GLOSSARY

A

AADL: Architecture Analysis and Design Language
AAMVA: American Association of Motor Vehicle Administrators
API: Application Programming Interface
ARTEMIS: Advanced Research and Technologies for Embedded Intelligence and Systems

B

BIG Group: Brussels Interoperability Expert Group
B2B: Business to Business
B2C: Business to Consumer

C

CC: Common Criteria: a standard meant to be used as the basis of evaluating the security properties of IT products.
CEN: European Committee for Standardization
Convergence: multiple networks or services integration
CPU: Central Processing Unit
CRM: Customer Relationship Management

D

DoD: US Department of Defense
DPE: Dedicated Processing Engine

E

ECC: European Citizen Card
EEPROM: Electrically- Erasable Programmable Read-only Memory
EMV: Europay MasterCard Visa
ENIAC: European Technology Platform for Nanoelectronics
EPoSS: European Technology Platform on Smart Systems Integration

F

Faraday Cage: Shield protection to prevent over-the-air access to a Secure Object. Such as shield often consist of a Metallic cage/grid

G

GSM: Global System for Mobile Communication
2G/3G: second and third generation of GSM

H

Heuristics: Set of rules and pre-determined decisions to be enforced whenever given situations occurs. The equivalent of the Civil Code, applied to computing.
HSPD 12: Homeland Security Presidential Directive 12
H2H: Human to Human communication
H2M: Human to Machine communication

I

IATA: International Air Transport Association
IC: Integrated circuit
ICAO: International Civil Aviation Organisation
ICT: Information & Communication Technologies
INS: Immigration and Naturalization Service
I/Os: inputs/outputs
IP: Internet Protocol
ISO: International Organisation for Standardisation
IST: Information Society Technologies
IT systems: Information Technology systems

J

JTI: Joint Technology Initiative

M

M2M: Machine to Machine communication

N

Nanotechnology: infinitely small systems tailored to access areas that are unreachable today.

NEM: Networked and Electronic Media Initiative

NFC: Near Field Communication

NLF: New Legal Framework for Payment services

NOR (Negative Or) Flash: flash memory technology based on NOR cells

O

OS: Operating system

P

PCM Flash: Phase Change Memories

PDA: Personal Digital Assistant

POS: Point of Sale

Q

QoS: Quality of services

R

RFID: Radio Frequency Identity

ROI: Return on Investment

S

SD Card: Secure Digital Card

SDK: Software Development Kit

Secure contactless device: a portable, standalone agent representing the issuer’s authority to deliver one set of services to one individual.

SEPA: Single European Payment Area

Si: Silicium

SiC: Silicium Carbon

SiGe: Silicium Germanium

(U) SIM: Subscriber Identity Module

Smart dust: meaning a network of tiny wireless, microelectromechanical systems or sensors, it reflects to the concept of software and heuristics embedded into nanotechnologies machines.

Smart Embedded Device: engineering artefacts involving computation that is subject to physical constraints.

Smart Security Technology Objects: individual and personal objects ideal for securely interfacing individuals and objects to the digital world.

SoC: System on Chip

StoLPaN: Store Logistics and Payment with NFC project

SWP: Single Wire Protocol

T

TDP: Trusted Download Programmes

TPM: Trusted Platform Module

U

UICC: Universal Integrated Circuit Card

UML: Unified Modelling Language

USB FS: Universal Serial Bus Full Speed

UWB: Ultra wideband

W

WSIS: World Summit on the Information Society

POINT OUT TO OTHER DOCUMENTS

Manchester e-Government Ministerial Declaration, 24 November 2005.
http://www.egov-goodpractice.org/download.php?PHPSESSID=af06ba085534ed8c1ad47dc2a482cf00&fileid=246

«Signposts towards e-Goverment 2010», European Commission, November 2005.
http://ec.europa.eu/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

«i2010 - A European Information Society for growth and employment», European Commission, June 2005.
http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/com_229_i2010_310505_fv_en.pdf

«A roadmap for e-ID for the implementation of the e-Government Action Plan», European Commission, January 2007.
http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_table.pdf

«A Roadmap for a pan-European e-IDM Framework by 2010», European Commission, January 2007.
http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

«New working environments. A decade of achievements. A strategy for the next decade», European Commission, October 2006.
http://ec.europa.eu/information_society/activities/atwork/work_paradigms/advisory_group/documents/2006_11_nwe_achievements_strategyforfuture.pdf

UE ICT Task Force Report, November 2006.
http://ec.europa.eu/enterprise/ict/policy/doc/icttf_report.pdf

FP7 Cooperation Programme 2007-2013.
http://cordis.europa.eu/documents/documentlibrary/2753EN.pdf

«Interactive content and convergence: implications for the Information Society», a study for the European Commission, Screen Digest Ltd, CMS Hasche Sigle, Goldmedia Gmbh, Rightscom Ltd, October 2006.
http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/interactive_content_ec2006_final_report.pdf

EPOSS Strategic Research Agenda, February 2007.
http://www.smart-systems-integration.org/public/documents/070306_EPoSS_SRA_v1.02.pdf

ENIAC Strategic Research Agenda, November 2006.
http://www.eniac.eu/web/SRA/SRA2006.pdf

ARTEMIS Strategic Research Agenda, March 2006.
http://www.artemis-office.org/DotNetNuke/Portals/0/Press%20documents/SRA%20MARS%202006.pdf

NEM Strategic Research Agenda, Version 4, August 2006.

http://www.nem-initiative.org/Documents/NEM-SRA-040.pdf

e- Mobility Strategic Research Agenda, August 2006.
http://www.emobility.eu.org/documents/SRA/eMobility_SRA_05_060907.pdf

«Digital.Life », International Telecommunications Union Internet Report 2006, December 2006.
http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf

«Towards an inclusive Information Society. ICT industry White Paper on Inclusion», EICTA, December 2006.
http://www.eicta.org/fileadmin/user_upload/document/document1166540368.pdf

«Information Security Programmes in the UE – and Guidance for Member States», September 2006.
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf