Smart-Card Technology: Business & Consumer Aspects within a European Perspective

Dr. Debbie I Keeling

September 2002

Contents

Executive Summary

- Smart cards are set to revolutionise transactional systems over the next few years. Offering secure, trustworthy systems for European citizens that will boost electronic and mobile commerce.
- The eEurope vision is to make a true information society a reality and the eEurope Smart Cards initiative has a major role to play in realising this vision. This report describes the European activity that seeks to promote smart card development, structured around five key issues: legislation, interoperability/standardisation/certification, electronic/mobile-commerce, consumer issues and enhancing public services.
- There has been a concerted effort to develop legislation to govern the development and management of smart card schemes. The relevant EU regulatory framework consists of the E-Signatures Directive, the E-Commerce Directive, the Copyright Directive, the E-Money Directive, the Data Protection Directive, Jurisdiction and Applicable Law, Indirect Taxation considerations and Financial Services issues.
- An impressive body of research development and consultation has been undertaken within Europe that will facilitate smart card standardisation, interoperability and certification processes. Within this movement the main foci of smart card development are identification processes, multifunction smart cards, the development of a generic card reader to be used by all systems and contactless technology. The main activity revolves around the eEurope Smart Card trailblazers (TB).
- Public Identity (TB1), Identification and Authentication (TB2), Protection Profiles and Security Certification (TB3) and Advanced Electronic Signature (TB12) are concerned with developing solutions for identification, authentication, e-signatures and certification. The activity of these trailblazers is linked to the European Electronic Signature Standardisation Initiative (EESSI). A major European project linked to these trailblazers is the EUROSMART led SMART.IS project that is developing an authentication module NAME.ES. a number of standards have been produced to date. Of principal interest is the CWA 141172, which provides guidance on how to facilitate standardisation of e-signatures. Public Key Infrastructure has a key role to play in future generation identification and certification procedures.
- Generalised Card Reader (TB4) is concerned with the development, standardisation and implementation of a generic, interoperable smart card reader. The principle project linked to this trailblazer is the FINREAD project, which is developing the specifications for a multi-channel FINREAD secure smart card reader. The three key parts of this project are Embedded FINREAD, Trusted FINREAD and FINREAD showcase. FINREAD is well-developed and a CWA 14174 has been developed that defines the key features of a generic smart card reader covering user requirements, compatibility, standardisation and cost.
- Contactless Smart Cards (TB6) is concerned with the development and interoperability of contactless smart card technology. The EUROSMART led SINCE project aims to facilitate the widespread implementation of contactless smart cards. CLUB (the Contactless Users Board) acts as an important forum fostering the adoption of contactless technology. Many of the public transport

projects view contactless smart cards as the key enabler of such services. A number of standards have been produced by the ISO/IEC JTC SC17 regarding contactless technology (ISO/IEC 14443, 15693, 10536, 10373).

- Multi-Application Systems (TB7) is an extremely important trailblazer investigating the technical, business and consumer issues related to the deployment of multi-application smart cards, representing the next generation of smart card innovations. The ETSI Smart Card Platform, the Java Card Forum, Global Platform, MULTOS, EMV Co. and the PC/SC workshop are major players in the development and interoperability of multi-application smart cards (and have developed their own standards). The SmartCities project represents a key pilot implementation of a multi-function smart card designed to improve quality of service for citizens and utilise the data collection capabilities of smart cards to modernise and improve existing services shaped to the needs of users.
- Smart cards can give Europe the edge in e/m-commerce development. However, there are a number of challenges that face organisations that wish to make e/m-commerce a reality.
- The search for a successful business model has indicated the need for a proactive approach that embraces technology at a strategic level rather than a reactionary one. A successful model will be built on a good understanding of the consumer, provision of a complete service, careful attention to image and branding, development of the user-system interface, consumer education and development of technology to meet consumer needs.
- There is a need to assess the receptiveness of the market to smart card technology, in terms of both consumer receptiveness and the state of existing technology and infrastructure to support new innovations. An iterative approach is indicated, for example, the introduction of e-purse in order to smooth the transition to multi-function cards.
- Within e/m-commerce banks face major competition from other service providers, the so-called non-banks, who may utilise a go-it-alone strategy providing not only telecommunications but also payment services. However, successful business models are likely to be based on strategic alliances between non-banks and banks – utilising the strengths of each. However, careful consideration needs to be given to card management issues in such alliances.
- Alongside these issues, there is a need to promote interoperability amongst e/m-commerce systems; otherwise they are not likely to meet consumer expectations and needs.
- e-Payments and m-Payments (TB5) is a major initiative working towards the promotion of e/m-commerce. The Mobey Forum, Mobile Electronic Transactions (MET) and the ETSI Smart Card Platform are major players working towards a specification for standardisation within e/m-commerce and the development of related business models.
- There is a need to gain a good understanding of the major consumer issues (individuals and merchants) that play a role in the adoption of smart card innovations, developing a model of based on multi-group perspectives.
- Smart card innovations need to add value to the transactional process, including convenience, economical benefits and customisation options. Further there is a need to understand the money management philosophies of consumers and how these might affect their adoption of smart cards. An understanding of such

issues can be utilised by marketing to enhance the image of smart cards to diverse groups. Classic innovation theory can help us to understand the smart card adoption process. In particular, issues such as relative advantage, compatibility, image and voluntariness may be influential in early adopters of smart cards (both individual and merchants). Late adopters may be more complex and base adoption on a demonstration of smart card utility. However, amongst merchants late adopters may be primarily concerned with relative advantage.

- Characteristics of smart card implementation require careful consideration as they can affect critical mass. Implementers may wish to utilise social learning aspects in order to help achieve critical mass. An understanding of the prevalent payment cultures will also be useful in understanding what obstacles may be met in smart card implementation programmes.
- Several barriers to usage have been identified including 'perceived barriers' relating to power and privacy, security and trust. 'Real barriers' may relate to transactional costs, service quality and the user requirements of the user-system interface.
- User Requirements (TB8) focuses on the user requirements of the user-system interface. It has identified a user behaviour model in an attempt to understand how the consumer interacts with the smart card system. SATURN, the CEN/ISS workshop on User Related Information (URI) and the ETSI Human Factors Committee (ETSI TC/HF) are major projects within this trailblazer. SATURN has identified the users requirements of elderly and disabled groups in order to inform smart card design and enable such groups to utilise smart card technology. Indeed, smart card technology is likely to have the most impact on the quality of life of these groups as it empowers the user. The URI project is working on the development of standards for multi-application smarts cards in relation to user related information. The ETSI TC/HF is concerned with keeping handling abilities in line with emergent technology and is currently developing five standards (STF 180-184). A main thrust of these groups is the promotion of the 'Design for All' concept, where smart cards systems must be designed in order to accommodate as many citizens as possible.
- eEurope ultimately seeks to utilise smart cards to enhance public services for all European citizens. The major focus to date has been on the development of smart card applications within public transport (TB9), which is viewed as a key spawning ground for smart card technology development. The CALYPSO, TRIANGLE, FASTEST and SIROCCO projects are the key areas of development within this trailblazer. e-Government (TB10) aims to modernise local and national government services fostering links between member states. In particular, Health (TB11) aims to develop administration services and health ID cards.
- 2003 will be an exciting time for smart card development, when major developments from the eEurope Smart Cards Initiative will be developed. The challenge will be to combine the results into a coherent whole that will inform the next generation of smart card applications.

Introduction

Technological advances in smart card development have the potential to change the face of modern society, not least in the banking environment. Such advances can radically change the way that consumers and service providers interact and exchange services, offering the development of new channels of distribution (Plouffe et al 2001a). Thus, smart cards are seen as critical to the modernisation of the economy and the development of the Information Society (ICTSB Project Team 2000, eEurope Smart Cards 2002).

Smart cards are set to experience a boost in the marketplace over the next few years, with the potential to be in common use within the next 5 years (CEN 2000, Wrathall 2002b). Europe is a leader in the smart card industry; the main innovations for smart card techniques and applications have been made in Europe since the 1970s and there is a concentration of expertise in all smart card related areas (Ankri 1999, Longo and Stapleton 2002). Indeed, Europeans use smart cards on a regular basis for a diverse range of applications, including stored value cards (e.g. payphone cards), health data storage and e-purse (Longo and Stapleton 2002). In 1998 approximately 90% of worldwide smart card production was in Europe, and, during 2000, 2390 million smart cards were produced by European manufacturers (CEN 2000).

The key catalysts in advancing smart card development over the next few years are the:

- Development of Internet and Global open networks;
- Increase in cross border transactions and the need for interoperability;
- Development of multi-application smart cards;
- Development of contactless technology (CEN 2000, Bohle and Krueger 2002).

The successful development of smart cards will depend on:

- Economic Factors – Europe holding a significant position in the smart card market, Europe important in e-commerce development, EURO reinforcing need for harmonisation of payment systems;
- Social Factors – Consumer confidence as a key factor for successful development;
- Technical Factors – Convergence between industries, grouping of companies and formation of alliances of operators instigated by the development of multi-application cards;
- Legal Factors – National and European regulations;
- International Trade and Standardisation Aspects (CEN 2000).

Security & Trust

Security and trust are a key priority in Europe as Communication and Information Technology have developed as critical factors underpinning both societal and economic development, supporting vital infrastructures within modern day society (European Commission 2001). More specifically, security and trust have been placed at the top of the EU policy agenda through:

- Recognition of the extent to which society depends on efficacious communication and information systems;

- The global interconnectivity afforded by the Internet greatly increases the potential for problems such as cybercrime;
- Viruses have caused widespread disruption to the Internet and have destroyed vital information and denied access to the Internet.

In particular, the growth of the Internet and e-commerce has sharpened the focus on security and trust. The Internet is viewed as a prime 'driver' in the growth and productivity of EU economies (European Commission 2001). The most recent surveys by the European Commission demonstrate the growth in the use of the Internet by consumers and businesses alike; where 50% of UK households and 90% of EU organisations (10+ employees) are connected to the Internet, 60% of these organisations also have established company websites (European Commission 2002).

For companies and consumers alike security and trust are at the top of the agenda in relation to e-commerce (Lareau 2002). For companies business models are driving the development of security models to support the development of trustworthy systems (Lareau 2002). Electronic and mobile commerce are the only way forward for growth in many companies and security and trust are proposed as a fundamental pre-requisite for the growth of e-commerce and the economy in general (European Commission 2001, Lareau 2002). For consumers the lack of trustworthy security systems is a major barrier to their use of information technology and e/m-commerce services.

The main threats to the security of transactional systems are interception of communication, unauthorised access, network disruption, malicious software, malicious misrepresentation, environmental and unintentional events (European Commission 2001). One of the main benefits of smart cards is their ability to improve security throughout transactions and hence to engender trust in users. However, ensuring security is a challenge given the rate of technological developments. The European Commission (2001) have detailed the basic, generic security requirements of any trustworthy network or communication system:

- Availability – data remains accessible and services operational despite disruptive events;
- Authentication – appropriate authentication procedures are employed;
- Integrity – data can be sent, received and stored as complete and unchanged over the transmission;
- Confidentiality – identities and information are protected from unauthorised sources.

Smart cards are well placed to fulfil these requirements for secure and trustworthy systems, and thus, are seen as the key to the development of e/m-commerce and beyond.

Although smart cards are viewed as a promising and enabling technology, they have not fulfilled their potential (Van Arkel et al 2000). Despite the wide usage of smart cards within Europe the current market has been described as 'fragmented', which, coupled with user acceptance issues, is a main obstacle to successful adoption of such technology (Van Arkel 2000). This report aims to explore the current trends in Europe with regards to smart card development, the consequent business issues and the consumer perspectives of smart cards and smart card adoption.

The Way Forward: A European Perspective

The promotion of the information society has a high priority within the European Union, underpinned by the establishment of the eEurope framework in December 1999. There is a vision for Europe to become the most *'competitive and dynamic economy in the world'* driven by the development of Communication and Information Technology (European Commission 2000). This will involve:

- The development of a cheaper, faster and secure Internet;
- Investing in people and skills;
- Stimulating use of the Internet.

Smart card technology is allotted a key role in the development of this vision. At a top level, smart card technology can underpin the development of a competitive and dynamic economy. From a consumer perspective, smart card technology offers a convenient and secure way to conduct everyday transactions. From a retail perspective, smart card technology, not only offers convenience and security, but also the ability to offer a wider range of services and access to a wider market. E-commerce transactions need to offer convenience, universality and security in one and smart cards can offer such a solution (FINREAD 2002).

Further, consumer confidence is seen as a key element in the development of e-commerce. Secure access through the use of smart cards is vital in building consumer trust in e-commerce (European Commission 2000). The issues most important to the development of communication and information systems and associated security are (European Commission (2001):

- Legislation – appropriate, strong legislation to safeguard security and build on current foundation of telecommunications and data protection legislation;
- Interoperability, Standardisation and Certification - Co-operation amongst major players to increase inter-operability of security systems and support market-oriented standardisation and certification;
- Awareness – raise public awareness to encourage use and prevent inappropriate behaviour leading to compromising of systems;
- Warning systems – European warning systems to alert to new threats;
- Investment in network and information security (security included in 5th and 6th framework programmes).

eEurope Smart Cards

Of particular relevance to this report is the establishment within the eEurope framework of the eEurope Smart Cards (eESC) initiative, which brings together all the major players in the European finance and smart card field. The eEurope Smart Cards Initiative demonstrates the need for a collective and co-operative effort to develop smart card technology to its fullest potential. The initiative aims to identify and address the key issues that have to be resolved before smart cards can be fully exploited (eEurope Smart Cards 2001). This industry-led initiative was established to empower the individual using smart cards, enabling access to resources (physical and virtual) at anytime and anywhere, whilst

protecting both privacy and security. It addresses both business and consumer needs in relation to multifunctionality, interoperability and trust, with a significant focus on producing recommendations for standards.

During a Smart Card Summit (Lisbon 2000) it was agreed that in order to promote the development of the digital economy:

- A high level task force should be established to facilitate smart card development throughout the EU;
- There was a need for greater interoperability of smart card based systems to promote widespread usage of smart cards and to realise the full potential of smart cards for the e-Economy.

Furthermore, a Smart Card Charter was established that indicates the activities that the task force will undertake in order to ensure that smart cards fulfil their potential within the EU (eEurope 2001). There are four key areas of activity: building trust; enhancing usability; improving access; deploying application and services. An Action Plan to address these issues was also implemented (initial stages of work are to be completed by December 2002). There are twelve key development strands, called trailblazers, described below (Van Arkel & Papaspyrou 2000, eEurope Smart Cards 2001). These twelve strands are important in highlighting the way forward for the promotion of smart cards across Europe, identifying key development issues:

- TB1 – Public Identity
- TB2 – Identification and Authentication
- TB3 – Protection Profiles, Security Certification
- TB4 – Generalised Card Reader
- TB5 – e-Payment and m-Payment
- TB6 – Contactless Smart Cards
- TB7 – Multi-Application Cards
- TB8 – User Requirements
- TB9 – Public Transport
- TB10 – e-Government
- TB11 – Health
- TB12 – Advanced Electronic Signature

Each trailblazer has produced a two-year action plan and work on these trailblazers will be completed December 2002. Where information regarding progress is available it will be provided within this report.

The Smart Card Charter is illustrated below and associated trailblazer streams are identified.

Building Trust	Enhancing Usability
• Develop common set of security requirements for hardware devices • Define common security certification procedures and infrastructures (products and devices) • Develop common specifications for electronic identification and authentication • Promote free use of cryptographic products • Ensure transport and fair cost conditions of smart card infrastructures • Ensure citizen trust in protection and use of personal data *Related to TB2, TB3, TB8, TB12*	• Ensuring easy access by applying design for all principles • Coherent use of contact and contactless technology • Road map for multi-application cards and terminals *Related to TB6, TB7, TB8*
Improving Access	**Deploying Application and Services**
• Framework for interoperability between terminals in different countries • Smart cards as easy and secure means of access to digital applications from a range of terminals using standard protocols • Reducing risk of fragmentation by having an open dialogue between telecom industry and the finance sector • Ensure efficient electronic payments and best use of existing infrastructure *Related to TB4, TB5, TB8, TB12*	• Support development of public sector applications • Define common requirements for public services, including public transport and health care • Exchange experiences and define common requirements for an electronic national and cross border identification function *Related to TB1, TB9, TB10, TB11*

The Smart Card Charter and associated trailblazer streams (eEurope 2000)

Smart CORD

This project (launched September 2001) plays a supportive role in the eEurope Smart Cards Initiative by creating an infrastructure (expert leadership, Secretariat and website facilities) to co-ordinate the trailblazer deliverables and facilitate the production of common guidelines and specifications (with reference to European standards organisations).

The remainder of this report will consider European activity in relation to the main issues relevant to smart card development based around the eEurope Smart Cards trailblazers:

- Legislation;
- Interoperability;
- Electronic and Mobile Commerce;
- Consumer Issues;
- Enhancing Public Services.

Legislation

Providing appropriate legislation for communication and information technologies is a complex task as:

- Communication and information services are now operated by many private operators and service providers;
- Networks support an enormous variety and number of services, that are becoming increasingly interconnected;
- Operators and service providers partly use the same infrastructure (European Commission 2001).

It has been suggested that a minimum level of security is provided by current legislation at both a National and EU level. A substantial body of legislation exists that covers telecommunications and another significant body of legislation covers data protection. The EU Regulatory Framework for e-commerce consists of:

- E-Signatures Directive (adopted 11/1999) – e-signatures have the same legal status as hand-written signatures across EU Internal Market.
- E-Commerce Directive (adopted 5/2000) – establishes the 'country of origin' principle, limits liability of ISPs and telecom operators (caching, hosting, temporary copies), and recommends 'opt-out' schemes for unsolicited e-mails and legal recognition of electronic contracts.
- Copyright Directive (adopted 4/2001) – makes cross-border trade in copyright protected goods and services easier, gives greater protection for right-holders in protecting private copying of digital content.
- E-Money Directive (adopted 6/2001) – lays down conditions under which banks and other financial institutions can issue e-money.
- Data Protection Directive (entered force 10/1998, implemented by 10 Member states) – ensures a high degree of privacy protection for individuals and free movement of personal data within EU. This led to the Safe Harbour Arrangement with the USA (11/2000), where authorised EU companies can transmit data with no extra safeguards.
- Jurisdiction/Applicable Law
- Brussels's Convention (12/2000) – addresses jurisdiction including disputes arising from online transactions.
- Rome Convention – under review and consultation to address non-contractual obligations.
- Indirect Taxation (VAT) – proposal under discussion to modify rules for applying VAT to e-services as well as subscription based and pay-per-view broadcasts. Agreed definition of transactions, territoriality rules and rates of taxation, but has not yet agreed on how to deal with non-EU businesses.
- Financial Services – development of policy for e-commerce financial services to establish Internal Market within EU.

A real challenge faces policy makers to develop and maintain legislation in the light of a rapidly changing technology environment. Government have an important role to play in ensuring that the underpinning legislation protects consumers and businesses alike, addressing the known imperfections in the marketplace, as well as protecting National Security as information systems are increasingly employed (European Commission 2001).

Interoperability, Standardisation and Certification

The widespread usage of smart cards and the associated security benefits will only be realised when solutions are commonly implemented and based on an open, interoperable system, founded on international standards (ICTSB Project Team 2000, European Commission 2001). Interoperability has been defined as:

> *The ability for one application to communicate seamlessly with another. Other aspects of interoperability include the ability to mix and match various .. components from one vendor with those of another. Interoperability can also refer to the interaction between one enterprise domain and another*
>
> ***(Lloyd 2002, page 1)***

Interoperability supports transactions between different companies and different users that do not use the same technology, offering more flexibility and freedom of choice in the marketplace (Lloyd 2001). At the highest level interoperability covers not only technology but business procedures and relevant legal issues (Lloyd 2002). Further protocols for communication between smart cards, transponders and readers should be standardised so that users can utilise their own personal equipment when using smart card systems (ICTSB Project Team 2000).

At the end of the 1990's the market was fragmented and standardisation and certification activities needed better co-ordination, as the abundance of standards was a hindrance to smart card development (Borman 1996). Harmonisation of specifications leads to increased interoperability and swift implementation of security solutions (European Commission 2001). Although, it should be recognised that standards must keep up with technological advancements. ISO 7816 Information Technology, Identification Cards and Integrated Circuit Cards with Contacts is a multipart international standard defining smart card specifications (in terms of physical and electrical characteristics). Whilst this standard is not a perfect solution to interoperability, it represents a key foundation from which companies can operate to enable interoperability, particularly when combined with certain specifications (Longo and Stapleton 2002). Some commonly utilised specifications are shown below.

Specification	Primary Sponsoring Organisation/Company	Purpose
PC/SC	Microsoft	Smart Card Reader Architecture - specification for PCs
OCF	Sun Microsystems	Smart Card Reader/Card Access Device specification
EMV	Europay/Mastercard/Visa Consortium	Industry-wide chip specifications to enable interoperability of smart cards and card terminals for finance sector
JavaCard 2.1	Sun Microsystems	Java-based smart card specification
PKCS	RSA	API specifications (PKCS 11 & 15 apply to cryptographic smart card functions)
Global Platform	Visa	Comprehensive smart card and terminal specifications for application loading and management
GSA Interoperability Specification	General Services Administration	Interoperability specification

Commonly accepted specifications for smart card systems (after Longo and Stapleton 2002).

This table serves to illustrate the number of specifications in operation. To date the primary smart card technology platforms have been provided by Microsoft (Smart Card for Windows), Sun Microsystems (JavaCard Platform) and Mondex (Multos OS Platform).

There is a current trend to dissociate applications from the underlying operating system so that applications can be loaded and modified after the card has been issued (Ankri 1999). The benefits of this will be:

- To extend the life cycle of the card and produce a higher return on the initial investment;
- To allow multi-applications on a single card;
- To promote faster development times though the use of higher level programming languages (Ankri 1999).

The achievement of this goal depends on interoperability and the production of clear-cut standards. However, it should be recognised that providing clear cut standards for smart cards will be a complex task given the vast array of potential uses of smart cards and associated forms (ICTSB Project Team 2000). There are a number eEurope Smart Cards Trailblazers that attempt to harmonise smart card development, facilitating interoperability, standardisation and certification processes.

Public Identity (TB1)

This trailblazer aims to establish the minimum requirements for a European multipurpose citizen's identity token (European Citizen Digital ID, European Driving Licence) including the creation of a qualified signature and development of biometrics for cardholder authentication. Pilot work will be carried out in at least three countries. Rather than replacing current documentation, this token be an additional tool that will mainly operate within the electronic environment. This stream will work closely with Identification and Authentication (TB2).

Link to Initiatives

TB1 is linked to the following initiatives.

European Initiative for a Citizen Digital ID solution (EUCLID)

EUCLID aims to facilitate the implementation of citizen digital identification in Europe and subsequently support the introduction of e-government and e-commerce applications. The main objective of EUCLID is to provide a forum for reaching a consensus on the issues relating to digital identification, through a series of working groups, meetings and a EUCLID network.

CEN TC 224 Machine Readable Cards, Related Device Interfaces and Operations

This initiative is concerned with the development of standards for cards, related devices and operations with a special emphasis on smart cards and inter-industry standardisation in order to promote a high level of commercial interoperability (CEN 2000). Working Group 11 – Surface Transport Applications has links with this trailblazer.

ISO/IEC Joint Technical Committee Sub-Committee 17 Cards and Personal Identification

Formed in 1988 this sub-committee has responsibility for developing standards for identification cards and personal identification, and operates through a series of working groups. Working Group 3 – Machine Readable Travel Documents has relevance to TB1. This working group aims to revise IOS 7501 and to

monitor and develop standards for machine-readable travel documents and related machine-readable cards.

Identification and Authentication (TB2)

A primary business concern in e-commerce is a breach in security within commercial transactions that lead to loss of assets (Lareau 2002). Identification and authentication are key developments within smart card technology that can aid businesses.

This trailblazer aims to:

- Firstly, offer practical, operational security solutions for electronic transactions that require authentication and identification for the promotion of access within eEurope, working closely with the other streams to establish functional requirements.
- Secondly, develop secure smart cards with a view to promoting e-commerce, standard specifications for inter-operability and secure smart card acceptance systems (e-business and internet transactions).

Token technologies are becoming increasingly important as the need for authentication and identify verification grows in the marketplace (Longo and Stapleton 2002). Several options are available:

- Hardware security modules and PC Cards – offer the highest security but entail the highest cost and have bulky form factors that make them generally unsuitable for personal use;
- USB Tokens – have moderate costs and security, are ubiquitous in that most desktops and laptops have USB ports, but are prone to physical wear on the plug-in interface. USB tokens are only supported by Microsoft operating systems and they are not able to include a multifunction capability;
- Magnetic Strips Cards and Software Tokens – offer the least security and lowest costs but read only tokens are susceptible to replay attacks and rely on application software that is vulnerable to viruses and Trojan attacks (Longo and Stapleton 2002).

In recognition of these issues the smart card is proposed as the best option for use as an authentication token as it:

- Is the only option that provides a multi-application capability alongside multi-function form factor. The smart card can combine a magnetic strip, bar code, contact/less chip and photo on one form factor, which is perhaps its greatest benefit;
- Is more technologically advanced than USB tokens (Longo and Stapleton 2002).

Link to Initiatives

Trailblazer 2 is linked to a number of initiatives within the EU.

European Electronic Signature Standardisation Initiative (EESSI)

The European Directive on Electronic Signatures describes the minimum requirements for certificates, certification service providers and signature creation/verification devices. Although there are several standardisation initiatives in this area they lack the consistency and coherence necessary for valid electronic signatures (ICT Standards Board 2002). In recognition of the need for a complete set of agreed industry standards and technical

specifications for the use of authentication products that provide a common level of security, the European ICT Standards Board established the EESSI initiative, which aims to identify a universal set of standards that will facilitate the implementation of the European Directive on Electronic Signatures. Three key areas will be focused on:

- Quality and Functional Standards for Certification Service Providers (CSPs);
- Quality and Functional Standards for Signature Creation and Verification Products;
- Interoperable Standardisation Requirements for Electronic Signatures.

This initiative will focus on Public Key Infrastructure (PKI) in order to support electronic signatures (ICT Standards Board 2002). EESSI will focus on:

- Security requirements for trustworthy systems and products;
- Security requirements for secure signature creation devices;
- Signature creation environment;
- Signature verification processes and environment;
- Confirmatory assessment of products and services for e-signatures.

The CEN/ISSS E-Sign workshop addresses the quality and functional standards for Certification Service Providers (CSPs) and quality and functional standards for Signature Creation and Verification Products. It has identified a number of core areas within which it is establishing a set of standardisation requirements. To date the E-sign workshop has completed/nearly completed a number of CWAs:

- CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures;
- CWA 14168: Secure Signature-Creation Devices, version EAL 4;
- CWA 14169: Secure Signature-Creation Devices, version EAL 4+;
- CWA 14170: Security Requirements for Signature Creation Systems;
- CWA 14171: Procedures for Electronic signature Verifications.
- CWA 14172: EESSI Conformity Assessment Guidance (in five parts);

CWA 141172 aims to provide guidance to certification of service providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories in order to facilitate the standardisation of e-signatures. It aims to provide guidance on conformity with the other CWAs 14167 to 14171 produced by the E-Sign workshop and thus its main role is as a management facilitator. The CWA is in five parts:

- Part 1: General;
- Part 2: Certification Authority Services and Processes;
- Part 3: Trustworthy Systems Managing Certificates for Electronic Signatures
- Part 4: Signature Creation Applications and Procedures for Electronic signature Verification;
- Part 5: Secure Signature Creation Devices (CEN/ISSS 2001).

During 2002 the E-sign workshop will also focus on:

- Security requirements for trustworthy systems and products – this will involve the definition of requirements for cryptographic modules for trustworthy systems run by CSP issuing qualified certificates. The resultant CWA will be a protection profile based on the Common Criteria (ISO 15408), and will be entitled 'Security Requirements for a Cryptographic Module Usable in Trustworthy Systems'.
- Extension of Secure Signature Creation Device (SSCD) requirements towards specific applications/environments and towards e-commerce applications (Art 5.2) – this will include guidance on the implementation of SSCD protection profile for specific implementations and the operation of specific environments. A standard will be produced to specifically address the requirements of electronic commerce.

The ETSI SEC Electronic Signatures and Infrastructures initiative address the interoperable standardisation requirements for e-signatures. In particular this group focuses on:

- The use of X.509 PK certificates as qualified certificates;
- Security management and certification policy for CSPs issuing qualified certificates;
- E-signature syntax and encoding formats and technical aspects of signature policies;
- Protocol to interoperate with a Time Stamping Authority (ICT Standards Board 2002).

PKI Forum

This alliance of end-users and vendors, established in 1999, aims to accelerate the adoption of Public Key Infrastructure (PKI) and promote a standards-based, interoperable PKI as a foundation for secure transmissions in e-business (PKI Forum 2002a). Public Key Cryptology enables a private key to have a public counterpart, whilst the private key remains secret the public key is disseminated for all to use when conducting business (Lareau 2002). PKI addresses several key business needs in terms of securing business services:

- Entity Authentication – the basic need to confirm an identity uses digital signatures, which is very important as it binds a digital signature to an individual's request;
- Data Confidentiality – sensitive information must be safeguarded, PKI utilises encryption to secure confidentiality;
- Data Integrity – the need to ensure that data is not altered is secured using digital signatures to assure receiving parties that the data has not changed since it left the sender;
- Non-repudiation – data integrity and entity authentication are vital elements of non-repudiation and can be used to ensure that the sender cannot deny having authorised/signed/originated the document. Digital signatures enable non-repudiation;
- Privilege Management – Digital certificates can be used to bind an identity to a set of privileges and thus manage access to sensitive data (Lareau 2002).

Using PKI, businesses need to consider:

- Certification Authorities – responsible for creating certificates that bind identify to public key;
- Registration Authorities – used to support certificate authorities, for example a large geographically dispersed organisations may have several registration authorities;
- PKI Policies – a certificate management statement (practices employed in issuing and managing certificates) and a certification policy (set of rules that govern applicability of certificates to community/application) (Lareau 2002).

It is proposed that PKI is a 'cohesive framework' within which company transactions can be conducted with the required level of confidence and trust in the system (Lareau 2002). In particular PKI enabled smart cards can be utilised as an effective authentication tool (Longo and Stapleton 2002) that offer:

- Easy to use, familiar mobile unit to securely store an individual's private signature key;
- A tamper resistant security module in which to generate keys, securely store keys and generate digital signatures;
- A multi-functioning capacity that means that digital signatures can be easily enabled for a diverse range of applications;

The PKI Forum has published their PKI Interoperability model. This model has three major levels (Lloyd 2001):

- Component level interoperability – concerning the interaction between systems directly supporting and/or consuming PKI related services, e.g. certificate formats, methods of storage and retrieval of certificates, certificate status information;
- Application level interoperability – concerning the interoperability between two applications even when the application software is supplied by two different manufacturers;
- Inter-domain interoperability – the most complex level concerned with the interoperability between two isolated PKI domains, involving the co-operation of multiple administrative domains.

European Forum for Electronic Business (EEMA)

This International organisation formed in 1987 provides an independent forum for all e-business participants (EEMA 2002). A number of projects concerning identification and authentication are being conducted under EEMA leadership.

The PKI Challenge Project

The PKI Challenge is a two-year project (Jan 2001 to Dec 2002) that aims to:

- Provide a solution for interoperability between PKI related products;
- Develop specifications and best practice for PKI interoperability facilitating faster, secure global e-commerce.

This project was initiated in response to the slow uptake of PKI products and services worldwide, which has inhibited the growth of e-commerce (EEMA 2002). This situation has mainly arisen because:

- PKI products do not interoperate successfully;
- Choice of products and services is not based on a clear set of specifications;
- There is an astonishing range of different levels of security, which has resulted in an atmosphere of uncertainty amongst users (EEMA 2002).

European Electronic Signature Directive Project

The European Electronic Signature Directive aims to give e-signatures the same legal standing as handwritten signatures. However, this directive has not been implemented consistently across Europe, mainly because of a plethora of different interpretations of the directive (EEMA 2002). In response to this EEMA has set up this initiative that aims to:

- Compare and contrast different interpretations of the directive within Europe;
- Disseminate this information to enable users to understand the business implications of the directive.

Global CA Project

There are around 100 Certification Authority Service Providers (CAs) operating as managers of organisational PKIs. However, there is confusion amongst users of the choice of CAs available (EEMA 2002). This project aims to:

- Provide a matrix of CA services offered aimed, giving users an indication of the range and type of services offered, information sources and how to initiate the PKI process within their organisation;
- Provide an overview of the inter-working CA initiatives (Identus, Bridge CA etc.), indicating 'who they are' and 'what they do';
- Provide an overview of PKI usage amongst users, specifically establishing the importance of PKI within organisations, the use of PKI and the business/technological elements of PKI implementation;
- Develop best practice in terms of PKI implementation and management (EEMA 2002).

WAP Forum/Open Mobile Alliance

An industry alliance that aims to facilitate the development of Wireless Application Protocol (WAP) technology, which is an open, global specification that enables mobile users with wireless devices to contact to and access the Internet (Open Mobile Alliance 2002). The proposed benefits of WAP are the increased mobility of Internet usage, broadening the spectrum of usage, and fast delivery of information and services to users.

This technology is being used within a number of handheld devices including mobile phones, pagers and smart phones.

Protection Profiles, Security Certification (TB3)

This trailblazer aims to:

- Promote trust and confidence in smart card usage through offering practical solutions to protection profiles and certificates applied within 'real' products.

- Facilitate adoption of Common Criteria (ISO/IEC 15408) standard for the evaluation and certification of products/systems/services.
- To define and support educational processes for operators and users.

ISO/IEC 15408, entitled Information Technology - Security Techniques - Evaluative Criteria for IT Security, is composed of these parts:

- Part 1: Information and General Model;
- Part 2 – Security Functional Requirements;
- Part 3 – Security Functional Requirements.

Trailblazer 3 is linked to several national and international certification bodies (eEurope Smart Cards 2001). It is also of interest to note the parallel activity in the USA in relation to this issue.

The Smart Card Security Users Group

The US-Based SCSUG was formed in 1999, and members include many of the major players in financial payment systems (e.g. American Express, Mastercard) (SCSUG 2002). This group aims to:

- Develop and promote the use of standardised security requirements;
- Ensure that the device security and data protection of users are met by smart card products (SCSUG 2002).

Its main areas of activity are focused on:

- Developing an issuer/user-oriented smart card protection profile;
- Developing smart card lab accreditation criteria;
- Developing smart card lab test methods and tests.

The SCSUG have released their smart card protection profile, which identifies the IT security requirements for smart card that is to be used within sensitive scenarios, for example, on-line banking. Whilst the requirements cover the integrated circuit (contact and contactless smart cards) and operating software, it does not cover specific applications or the security requirements for car terminals or networks interfacing with them. This protection profile has been adopted by the US Government's General Services Administration to describe security requirements for its 'Smart Access Common ID Card RFP. The major difference between the European protection profiles (PP/9806 Smart Card Integrated Circuit Protection Profile v2.0, PP9810 Smart Card Embedded Software Protection Profile v1.2 and CPP/911 Smart Card Integrated Circuit with Embedded Software v2.0) and the SCSUG protection profile is that it focuses on threats and organisational security policies from a card issuer and end-user perspective, whereas European protection profiles have a tendency to focus on the manufacturing process (SCSUG 2002).

Generalised Card Reader (TB4)

This trailblazer aims to develop the architecture and technical specifications for a multi-channel FINREAD secure card reader that can be used in e-commerce and other card-based systems.

CEN/ISS FINREAD Workshop

The European Commission funded (Information Society Technologies) FINREAD project has developed a smart card reader that can be connected to

the Internet via an individual's PC, either as an external peripheral or embedded within the keyboard (FINREAD 2002). This reader aims to offer a high degree of security for transactions over the Internet. This initiative is connected to the eEurope Smart Cards trailblazer 4 – the development of a generic card reader. It has also been developed in accordance with the European directive on electronic signatures. Its prime objectives are:

- To address the needs of today's modern consumer, providing a flexible and portable data support that allows the card holder to conduct e-purchases and use online services within a secure environment;
- To promote interoperability, reducing costs for the consumer and retailer alike and allowing access to an enlarged European and International market place;
- To provide at least the same user-friendliness and security of today's POS transactions for both consumer and retailer.

The FINREAD Consortium is made up of seven central players: Banksys, Europay International, SIZ, Groupement des Cartes Bancaires, VISA EU, Ingenico, Interpay Nederland.

Currently, there are three major developments within the FINREAD project.

Embedded FINREAD - Aims to extend the current concept of FINREAD to a larger base of mass-market 'acceptance devices', including mobile phones and TV set top boxes. Additional members within this project are France Telecom, Canal Plus Technologies, Sagem and Orga.

Trusted FINREAD - Aims to promote the implementation and evaluation of FINREAD readers in order to demonstrate and validate its interoperability. This process will involve the creation of a certification infrastructure and extensive pilot testing. Additional members within this project are: OMNIKEY, GTS and SCM Microsystems.

FINREAD Showcase - Aims to promote worldwide dissemination of the FINREAD and Embedded FINREAD technical specifications. Additional members within this project are France Telecom, Canal Plus Technologies, Sagem and Orga.

To date the CEN/ISSS FINREAD Workshop has published a multi-part CWA, number 14174 (parts 1 to 8). This agreement establishes the key features of FINREAD, it should be:

- Cost efficient and easy to distribute;
- Compatible with standards and interoperable;
- Adaptable to future requirements;
- Easy to use;
- Support a wide range of card types;
- Be secure.

Contactless Smart Cards (TB6)

Contactless smart cards are a fast, reliable and easy to use system that can be better protected against vandalism and has reduced maintenance in comparison to contact smart cards (eEurope Smart Cards 2002).

This trailblazer aims to:

- Address the problems of lack of standards and interoperability for contactless smart cards. .
- Promote the use of contactless smart cards in e/m-payments and public transport systems.

To date this trailblazer has identified that problems with the interoperability of contactless cards arise from:

- Communication distance;
- Execution speed;
- Compliance with ISO standards;
- Packaging type;
- Reader technology (Massot 2002).

Consequently, TB6 aims to find ways of overcoming such problems.

Links to Initiatives

Along with links to the ETSI Smart Card Platform, this trailblazer has links to a number of specific initiatives within Europe.

Smart MEIJI

An initiative launched in September 2001 involving both European and Japanese smart card industry representatives, supported by the EC under the IST funding programme and managed by EUROSMART. This project involves the exchange of knowledge and expertise in order to 'pool' resources on smart card development, focusing on security and contactless smart cards. This project not only strengths the links between European and Japanese industries but also facilitates interoperability of smart card technology and will act as a catalyst for smart card usage across the regions.

Smart Meiji is now in its mid-term, and after 10 months has fulfilled its objectives (EUROMART 2002). The European and Japanese smart card community have achieved a common position on interoperability, a major step towards worldwide interoperability. Smart Meiji workshops have led to a better understanding of security requirements between Japan and Europe. The Japanese smart card industry has recognised the EUROSMART protection profiles and Japanese protection profiles have been translated into English and comments from the European smart card industry have been incorporated (EUROSMART 202). Then final results of this initiative can be expected early in 2003.

SINCE

A EUROSMART project to promote, harmonise and stimulate uptake of contactless smart card technology across Europe. SINCE (Secure and Interoperable Networking for Contactless in Europe), launched in October 2001, aims to identify and find solutions to the factors hindering the uptake and development of contactless technology (EUROSMART 2002). In particular it will focus on:

- Interoperability issues relating to current technology and systems;
- Security aspects of contactless technology;
- Certification;
- Education and promotion of contactless technology.

This project aims to produce a 'foundation report' that identifies the current strengths and weakness of contactless smart card technology as a means of centralising existing knowledge and expertise in this area. The majority of SINCE deliverables can be expected by the end of 2002.

Contactless Users Board (CLUB)

CLUB, established in 1995, acts as an 'information exchange platform' for transport operators. It aims to:

- Foster adoption of contactless technology worldwide;
- Provide an information exchange platform for its members about contactless technology;
- Offer diverse views and feedback in order to inform the development and implementation of contactless smart cards (CLUB 2002).

CLUB focuses on the use of contactless cards in the transport industry, suggesting that such cards offer an all-in-one travel card solution. This card would offer a quick service that can handle heavy volumes of traffic (and aid the compilation of accompanying statistics), alongside an e-purse facility and the ability to offer bonuses such as loyalty schemes (CLUB 2002).

ISO/IEC Joint Technical Committee Sub-Committee 17 Cards and Personal Identification

Formed in 1988 this sub-committee has responsibility for developing standards for identification cards and personal identification, and operates through a series of working groups. Working Group 8 – Contactless Integrated Circuit Cards, Related Devices and Interfaces has relevance to TB6. This working group aims to develop standards for contactless chip cards. It has developed standards in the following areas:

- ISO/IEC 14443 (2001) Identification Cards – Contactless Integrated Circuit Cards – Proximity Cards;
- ISO/IEC 15693 (2000) Identification Cards – Contactless Integrated Circuit Cards - Vicinity Cards;
- ISO/IEC 10536 (2000) Identification Cards – Contactless Integrated Circuit Cards – Close-Coupled Cards.
- ISO/IEC 10373 – 6/7 – Test Methods for Contactless Integrated Circuit Cards.

Multi-Application Systems (TB7)

To date special-use smart cards have been deployed and studied to a greater extent than multifunction (all-in-one) cards (Truman et al 2002). Svigals (2000) suggests that multi-application cards offer several advantages:

- Communication catalyst – using mobile phones to access services;
- Co-operation development – multifunction cards lead to multi-alliances between organisations;
- Security catalyst – the Internet and other communication services need such security solutions (public encryption keys, digital signatures, certificates).

However, as multi-function cards necessarily involve a number of parties there are a number of key business issues that need to be resolved in order to fully exploit multi-function cards:

- Who owns how much of the card, for example in a finance and loyalty companies card partnership;
- Who has a say in how the card is managed;
- Who pays for the development and test marketing of the card;
- Who pays for the marketing and promotion of the card;
- The need to avoid brand erosion and confusion over branding in combination cards requires that special consideration be given to branding and logos (Plouffe et al 2000).

Trailblazer 7 aims to:

- Widen consumer choice in the selection and management of communication and information technology services through the use of a 'generic access token' (smart cards).
- Compare the strengths of three active platforms: Global Platform (Proton World); ETSI EP Smart Card Platform; ISOP Project of ISOP Consortium.
- Use this analysis as a basis for defining the way forward for open interoperable multi-application smart card platforms, encouraging more transparency for card users and sustaining an open platform.

Link to Initiatives

This trailblazer is linked to a number of initiatives.

ETSI Smart Card Platform (ETSI SCP)

The ETSI SCP, having replaced the SMG Technical Sub Committee (SMG9), aims to develop and maintain:

- A common Integrated Circuit (IC) card platform for all mobile telecommunications systems;
- Application independent specifications for IC cards/mobile equipment interface of these telecommunications systems under the ETSI;
- IC card standards for general telecommunication purposes;
- IC card standards for employing advanced security methods for telecommunication applications for m-commerce (ETSI SCP 2002).

The 'backbone' the smart card platform, dealing with the physical and logical characteristics of the smart card interface, has been approved. There are three working groups within the ETSI SCP:

- SCPWG1 – to maintain and evolve interface specifications for an interoperable multi-application IC card platform (UICC) and to develop the appropriate supporting documentation and models;
- SCPWG2 – to develop and maintain specifications and develop supporting documentation for advanced security methods for applications on UICC platforms such as m-commerce;
- SCPWG3 – To develop, maintain and support a Card Application Toolkit and the Application Programming Interface Specifications of a

UICC platform. The Card Application Toolkit (CAT) is a generalisation of the SIM Application Toolkit.

The major achievements of this group to date are the publication of three specifications:

- TS102 224 Security Mechanisms for UICC based applications;
- TS102 225 Security Packet Structure for UICC based applications;
- TS102 226 Remote APDU Structure for UICC based applications.

The next major publication will be an architectural model of smart cards and usage of PINs for UICC (ETSI SCP 2002).

Java Card Forum

This forum, established in 1997, aims to:

- Promote Java (Sun Microsystems 1995) as the standard programming language for multi-application smart cards;
- Promote Java Card API specification as standard;
- Prepare technical documents;
- Exchange information about implementation;
- Foster dialogue amongst the main players in the field (Java Card Forum 2002).

Java Card is proposed as providing:

- A security model that enables multi-applications to coexist on one card;
- The ability for applications to be developed and validated more quickly with Java, hence reducing the time to market for new smart card applications (Java Card Forum 2002).

The forum invites interested parties to join and participate in the definition of Java Card requirements. In order to achieve this, two fora, which meet on a regular basis, have been established: The Business Committee and the Technical Committee. These fora then prepare recommendations to Sun Microsystems for new JavaCard API specifications. JavaCard Management Specifications v1.0b and v.2.2 are currently available. The current work on these fora is focusing on vertical market extensions to the core specifications for GSM, Banking and IT.

Global Platform

A co-operative (launched in 1999) of organisations interested in issuing multiple application smart cards to their customers, which aims to define specifications and infrastructure for the development of multi-application smart cards (Global Platform 2002). Global Platform manages, promotes and evolves the Open Platform card specifications and terminal framework developed by VISA International. Open Platform (established 1996) is a collection of specifications and technologies allowing financial institutions to develop multi-application smart cards. Principally it enables applications and keys to be securely loaded onto smart cards after the card has been issued to the cardholder. Open Platform technology can be implemented with Java Card (Sum Microsystems) and Microsoft Windows for Smart Cards. Open Platform is to be implemented by a number of key players (Global Platform 2002).

Bankernas Kontantkort Cash Association - This consortium of banks that operate the Proton-based CASH smart card scheme in Sweden (Nordea, SE Banken, Svenska Handelsbanken and Swedbank) upgraded their existing Proton host system to support smart cards based on Proton Prisma technology, a new multi-application smart card technology (utilising the Open Platform standard) designed to enable e-payments in several domains (Internet, Television, GSMs). Specifically, the smart cards incorporate CALC (Card Application & Life Cycle Manager), a spearhead implementation of Open Platform 2.1, that provides a framework for easily managing multi-applications on a single card, provides the ability to download smart card applications and allows users to access multi-applications through a single PIN.

American Express - American Express is to adopt the Proton Prisma Dynamic Profile product for future issuances of American Express's Java-Card based smart cards, incorporating CALC. This technology has been described by American Express as *'a cost-effective, competitive delivery mechanism'* for the delivery of smart card solutions.

French Bank Alliance - A French bank alliance (BNP, Banques Populaires, Caissess d'Epargne, CCF, Crédit Lyonnais, La Poste and Sociétié Générale) work closely with smart card systems utilising Open Platform, including loyalty cards, e-purse and e-ticketing solutions combined with credit/debit/cash withdrawal functions. Using Open Platform allows this alliance to utilise any Java compatible operating system, any chip manufacturer and application developer, maximising choice and flexibility and facilitating market place innovation.

European GSM Mobile Phones - The telecommunications industry are adapting Open Platform to enable smart cards to be loaded with applications via GSM mobile phones. The specifications for GSM (including the Subscriber Identity Module) have been developed by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

Asia Mobile Electronic Services Alliance (AMESA) - This alliance consists of Standard Chartered PLC, Microsoft Corp., Motorola Inc., LM Ericsson Telefon AB & Nokia Corp. amongst others. The aim is to provide a multi-application smart card that can access a wide range of e-services combining smart card technology and mobile phones. Hong Kong University of Science and Technology, the Open University of Hong Kong and the National University of Singapore provided research and development expertise, including market surveys and pilot tests. Standard Chartered PLC provided the regional financial infrastructure. The mobile and Internet networks of SingTel Mobile, SingNet and SmarTone were utilised by the Alliance. Electronic Identification services are provided by Hong Kong Post and Singapore Post. Gemplus and Microsoft provided the multi-application smart card technology based on Open Platform.

SmartCities

This project aims to:

- Design a dynamic smart card and multi-application management architecture;
- Evaluate the technical and commercial feasibility of exploiting the data sources gathered from use of the smart card scheme to inform the development of future services (SmartCities 2002).

Southampton is the first 'smart city' (2000), introducing a single multi-application card. The card will give access to a range of services in the areas of transport, leisure, retail and education. During 2001 over 3000 cards were issued to residents (Jennings and Holzer 2001). In order to underpin trust in the system, Southampton City Council has:

- Notified the Office of the Information Commissioner of the intended use of the processed data;
- Allowed people to choose whether to have a card;
- Ensured that registration only uses information that is already available on other databases (e.g. driving licences and passports);
- Undertaken a risk analysis of the consequences of misappropriation of an identity and have set the registration processes at an appropriate security level;
- Ensured that no sensitive data (as defined by the Data Protection Act) is collected;
- Ensured that personal information is kept in a secure card management system, where transaction information is anonymous (kept in a secure data warehouse needing a high level of authentication to access) and personal information and transaction information are not stored in the same place on the card (Jennings and Holzer 2001).

Data from these sources will then be used to inform the development of future services within Southampton for the benefit of citizens, better quality information under effective management will produce better services for all (SmartCities 2002). The partners in the SmartCities project are: Southampton City Council, Schlumberger, University of Southampton, Europay International Technolutions CRID, University of Namur (Belgium).

MULTOS

Multi-application cards are a more cost-effective way of delivering smart card services than single use cards. In recognition of this MULTOS was developed as a complete scheme for managing multi-application smart card applications. The MULTOS Consortium (MAOSCO Ltd) actively promotes and develops the MULTOS specification as an open industry standard. The MULTOS specification was originally developed by MONDEX International, who decided to offer the specification on an open (under licence) option in order to promote MULTOS as the preferred industry standard. The specification defines a secure, efficient and cost-effective process for application management for multi-application cards, and is compliant with the relevant standards including ISO 7816 and EMV. The support infrastructure allows for the secure loading and deleting of applications on a card, and relies on PKI (MULTOS 2002).

MULTOS is described as the 'complete business solution' as it offers:

- A new business case for multi-application smart card issuers;
- A platform for interoperability;
- Open, royalty free standard;
- Complete scheme for managing smart card applications (MULTOS 2002).

Indeed, MULTOS has been endorsed by Europay International as offering the best combination of security, performance and value for customers in an open, non-proprietary platform; offering a full operating system supported by proven by certification authority infrastructure; being available for easy implementation (Dutrieux 1999). MULTOS has received support from a number of organisations. Pocketcard Company Ltd., invested 40 million dollars in upgrading their system to MULTOS, because it would allow them to expand their service easily, it has the ability to load and delete multiple applications, its high level of security and has the support of the global industry. The SNORAS bank has based on new smart card solutions on MULTOS. Hitachi has based their employee ID system on MULTOS, which also allows employees to use the Mondex e-purse system. This system thus, not only offers both employees and employer a secure and efficient accessing and ID management system, but also offers employees a cash free environment in the building and speeds up administration processes. The National Irish Bank has based their CITRUS smart card for use in a Dublin Shopping Mall on MULTOS. This represents the first multi-application card released to the public in Ireland. The card combines the Mondex e-purse with a loyalty scheme. Cardholders can load value from bank accounts, over the telephone, at ATMs or on home-load devices. The database being developed through use of the card is being used for modelling purposes in order to improve services and service delivery.

PC/SC Workgroup

The PC/SC workgroup sets standards for integrating smart cards and smart card readers and aims to:

- Promote standard specifications to ensure that smart cards, smart card readers and computers made by a range of manufacturers will be interoperable;
- Facilitate the development of smart card applications for the PC and other computing platforms (PC/SC Workgroup 2002).

PC/SC specification v1.0 (1997) is available, the PC/SC Workgroup are currently working on version 2 of this specification to accommodate contactless technology.

EMV Co.

This organisation, established in 1999, aims to manage, maintain and enhance the Europay Mastercard Visa (EMV) Integrated Circuit Card Specification for Payment Systems, utilising the classic working group system. The EMV (2000) v4.0 specification is now available, in four books:

- Book 1 – Application independent integrated circuit cards to terminal interface requirements;
- Book 2 – Security and key management;
- Book 3 – Application selection;
- Book 4 – Cardholder, attendant and acquirer interface requirements (EMV 2002).

Small Terminal Interoperability Platform (STIP)

Established in 2000, STIP aims to define and promote a specification for a small terminal (e.g. mobile phones, payphones) interoperability platform, which is

complete and royalty free (STIP 2002). STIP's mission is to specify a software platform that:

- Supports multiple secure transaction applications on a terminal;
- Provides interoperability such that applications may run on a wide range of device types;
- Provides platform and application lifecycle management;
- Implemented small devices with limited resources typical of the card-accepting environment today (STIP 2002).

The STIP v.2.1.1 specification is now available.

CEN Information Society Standardisation System Workshop on User Related Information (CEN/ISS WS URI)

Building on the remit of CEN/ISSS to develop standardisation to promote the success of the information society, this initiative focuses on the user related information held on smart cards. This project is an extension of CWA 13987:2000 Smart Card Systems: Interoperable Citizen Services: User Related Information (based on DISTINCT), focusing on standards for multi-application smart cards (such as JavaCard and MULTOS) and the associated management systems (such as Global Card Platform) for which there are currently no mutually compatible standards (CEN/ISSS 2002). Further information on this initiative is given in the next chapter on consumer issues.

CEN TC 224 Machine Readable Cards, Related Device Interfaces and Operations

This initiative is concerned with the development of standards for cards, related devices and operations with a special emphasis on smart cards and inter-industry standardisation in order to promote a high level of commercial interoperability (CEN 2000). A number of specific working groups operate within this initiative, each with some relevance to TB7:

- WG6 – Man-machine interface;
- WG8 – Thin flexible cards;
- WG9 – Telecommunication applications;
- WG10 – Inter-sector electronic purse;
- WG11 – Surface Transport Applications;
- WG12 – Health Applications.

ISO/IEC Joint Technical Committee Sub-Committee 17 Cards and Personal Identification

Formed in 1988 this sub-committee has responsibility for developing standards for identification cards and personal identification, and operates through a series of working groups. Working Group 4 – Integrated Circuit Cards with Contacts has relevance to TB7. This working group aims to define specifications related to Integrated Circuit Cards with contacts. They have published the ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards with Contacts –standard (in ten parts).

Internet Engineering Task Force (IETF)

This task force is draws on the international community of network designers, operators, vendors and researchers concerned with the development of Internet architecture (IETF 2002). There are a number of working groups within each of the following area: Applications; General; Internet; Operations and Management; Routing; Security; Sub-IP; Transport. A number of these working groups focus on a number of issues relevant to smart cards. For example, SACRED – Securely Available Credentials, in the Security Area, amongst other technological advancements proposes that PKI-enabled smart cards are a viable secure solution for portable identity cards.

Advanced Electronic Signature (TB12)

This trailblazer aims to develop a smart card based Internet system allowing consumers use of an Advanced Electronic Signature, identifying minimum requirements for such a system, defining system architecture and evaluation of pilot schemes for implementation.

Links to Initiatives This trailblazer is linked to the following initiatives.

Smart.IS AM

This EUROSMART project (officially launched June 2000) aims to accelerate e-commerce through the promotion of the interoperability and security of smart card systems, to define an authentication module (NAME - Network Access Module for Internet Users) within a smart card, to define user requirements for such systems to facilitate e-business and e-commerce and to identify major barriers to the development of smart card applications. The original action programme was structured around three major components:

- Research and Design – To demonstrate and validate the interoperability of an open platform (e.g. Java, MULTOS, Smart Card for Windows) within an e-business framework. The two core projects are ISOP (Interoperability and Security of Open Platform – defining an architecture for interoperability and security requirements within the GSM, Banking and Pay TV markets) and ECC (Elliptic Curves Cryptosystems) concerned with the new technologies combining contactless and contact cards and biometrics.
- Interoperable smart card framework for e-business – to develop a smart card security framework to support e-business, focusing on PKI and a standardised API for e-commerce payment (CEPS, EMV);
- New applications – to develop a new generation of transaction systems to facilitate and enhance consumer access to services and quality of service (Ankri 1999).

In November 2001 the project was re-defined to include the specification of a standard smart card solution used in the implementation of the European Directive on electronic signatures (NAME.ES). Thus a final outcome of Smart.IS AM is to produce a standard smart card solution for the authentication of end users and provide a usable electronic signature function. The project is conducted in a climate of co-operation with other interested bodies both in Europe and worldwide.

Smart.IS operates through a series of working groups:

- WG1 – Definition of a common cardholder authentication module – NAME. NAME version 1 was revised based on comments collected and a final NAME version has been produced;

- WG2 – Telecom Operator requirements and business model. A security solutions document has been released detailing existing security solutions currently implemented to authenticate end users and identifies additional benefits of NAME and NAME.ES. A telecom requirements and business model document has been released defining business requirements for telecom operators for authentication and e-signatures on smart cards (including banking industry needs);
- WG3 – Requirements of terminal manufacturers and convergence model for multi-platform access to services. A terminal manufacturers requirements document has been released defining business and technical requirements for enabling cardholder authentication and e-signatures to work with any type of Internet terminal.
- WG4 – Liaison with standardisation committees. This working group holds a series of meetings with interested parties, such as the ETSI/ISSS and ETSI/EESSI.
- WG5 – Specifications of a common cardholder electronic signature module (NAME.ES). A NAME.ES consultative document has been released, which extends the work done on NAME and adopts recent standards, and specifies how NAME.ES will be prepared for e-commerce and e-government (Smart.IS 2002).

MEDEA+

MEDEA+, established in 2001, is supported by EUREKA (pan-European Network for Market Orientated Industrial R & D) and is concerned with advancing microelectronics to ensure that Europe remains a leading force in the technological field. MEADEA+ focuses on enabling technologies for the Information Society and e-economy. MEDEA+ currently has a large number of projects underway. Of particular interest to this report are the EsPass-IS and CRYPTOSOC projects.

- EsPass-IS – Enhanced Smart Card Platform for Accessing Securely Services in the Information Society. This aims to evolve hardware and software for an open smart card platform that supports e and m-commerce services.
- CRYPTOSOC – Aims to address a key issue in e-business – maintaining confidence in a system. The project will develop an interoperable validated architecture from which cryptographic components can be produced to meet specific market requirements (MEDEA+ 2002).

Together these trailblazers and the associated initiatives form an impressive body of research, development and consultation that aims to promote interoperability, standardisation and certification for smart card development.

Electronic & Mobile Commerce

Smart cards can revolutionise the electronic commerce industry, forming a solid foundation upon which to develop this important concept. They are the building blocks of e-commerce giving Europe a leading edge in providing secure payments over the Internet (Ankri 1999, APACS 2002). They offer the means of embracing both the physical and virtual world in a 'seamless' manner, providing a common link between the two worlds (Lefebvre 1999). Furthermore, smart cards offer a cost-effective solution to e-business deployment through securing access and payments (e.g. PIN authentication advocated by the UK Chip and Pin System), strengthening user authentication and non-repudiation and increasing mobility and portability of user profiles. Chip technology is difficult to copy and could drastically reduce card counterfeiting (Dutrieux 1999). They also offer versatility with the ability to support 'add-on' services such as loyalty schemes and e-purse, and, in the future, the introduction of biometrics (APACS 2002). Smart cards are a key channel for the distribution of a wide range of financial services. They offer the consumer, beyond the basic payment function, the ability to manage their financial affairs more effectively; smart cards provide secure home banking, facilitate the transfer of funds and offer more secure home shopping (Worthington 1998).

The ultimate goal of smart card development is to achieve real flexibility in electronic commerce and to make mobile commerce a reality. Mobile commerce affords the service provider with the opportunity to, not only provide traditional services over a mobile channel, but also to offer new types of services and reinforce their position in the value chain (Mobey Forum 2000). All interested groups agree that with the introduction of WAP the mobile handset is the 'natural choice' as a device for making daily payments, particularly as the mobile phone does not have to rely on a card reader plus PC plus modem or POS terminal (Krueger 2001). Indeed, mobile phones are evolving beyond a mere telephone to become a Personal Trusted Device (PTD) offering a vast range of services (MET 2001a). The m-commerce industry is becoming an increasingly important area of development and research, as there are likely to be 1 billion mobile phone users, 500 million of which will be Internet-enabled, by 2003 and industry analysts predict that m-commerce will be a multi-billion dollar business by 2005 (Krueger 2001, MET 2001a). It is estimated that by 2004, 350 million people will use mobile ticket purchasing and retail ordering, around 350 million will utilise mobile banking services and more than 50 million will use mobile financial trading services (Krueger 2001).

E/M-Commerce Business Challenges

There is still a divided opinion, however, as to whether there is a solid business case for committing entirely to 'digital money' (Dutrieux 1999, Lefebvre 1999). The concept has not 'taken off' as expected, with a number of smart card related projects falling below expectations (Bohle and Krueger 2001). For example, it was found that in established card schemes only 9% of Proton card customers use the card everyday, and only 1% of Geldkarte customers use the card more than once a month (and the average load and transaction sizes were falling) (Lefebvre 1999). Further, the picture is not clear as to whether some smart card schemes are more successful than others. For example, loyalty schemes have had more success than e-purse schemes (Worthington 1998). However, a number of researchers have suggested that many of the projects are not as

successful as initially expected due to characteristics of the way that they have been implemented rather than the function of the card itself (Plouffe et al 2000). In order to ensure that future schemes are successful players face a number of business challenges.

A Successful Business Model

In order to fully exploit e/m-commerce market players need to adopt an aggressive business model. Many businesses have relied on a reactive model, utilising on-line marketing at its most basic level and viewing the Internet as merely another communication device rather than realising its full power. A successful business model needs to embrace technology at a strategic level (Kolasker & Payne 2002). For example, using technology to collate information about consumer habits (as in the SmartCities project) and utilising modelling procedures to inform future practice, reinforcing consumer satisfaction. A successful business model will also be built on:

- A good understanding of consumer reactions to e and m-commerce, including on-line trust, security and accountability of payment card services;
- Completeness of service – where it is possible to conduct the entire transaction over a mobile channel from negotiation through ordering to payment;
- Multi-channelling approach – where a user should have the opportunity to choose the preferred channel for each step of a transaction. For example, user authentication can be conducted over a mobile channel whilst the rest of the transaction could be performed over the Internet;
- A solid set of image dimensions for the virtual store (where relevant) whilst maintaining the physical product and consumer related services;
- Focusing on the consumer-virtual store interface (where relevant) and boosting the consumer experience; for the consumer the service becomes a key focus in e/m-commerce (Buck 1996, Mobey Forum 2000, Kolsaker and Payne 2002).

It has been suggested that we are moving towards a ‘card centric’ culture where there is more reliance on plastic and a virtual relationship with the consumer will be the norm (Worthington 1998, Dutrieux 1999). In essence the smart card may become the ‘primary channel’ for the relationship between banks and consumers (Dutrieux 1999), highlighting the need to gain an understanding of consumer needs and reactions to cards and technology.

In order to achieve this successful business model, organisational strategy will need to address the following issues:

- Technology – where developers need to anticipate mobile operators needs dependent on consumer needs and expectations;
- User experience – where there is a need to ensure consistent user experience across transactions;
- Service and customer management – where there is a need to pay careful attention to the maintenance of the Customer Relationship Management to ensure that this is not neglected in favour of technological innovation;

- Interoperability – where there is a need for standardisation of the mobile infrastructure;
- Security, Trust and a User-Friendly Interface – where systems are based on a user-friendly interface that provides strong security and engenders trust in the user, which is particularly important in financial applications;
- Payments – where there is a need for a demonstrably secure and widely accepted method of payment;
- User Education – where users need to be adequately informed as to the benefits and use of new technology and transactional systems;
- Step-by-Step Approach – where the ultimate goal is a global open architecture, but an iterative approach can be utilised building on local and national solutions evaluated against global standards (Mobey Forum 2000).

The main requirements of consumers, merchants and financial institutions in mobile commerce are summarised in the following table.

Consumer Requirements	Merchant Requirements	Financial Institutions Requirements
Ease of use	Availability with different payment instruments	Service and relationship management with consumer, including the ability to fund purchases with branded products
High security (including transaction tracking and prevention of fraud)	Guarantee of payment and/or non-repudiation	Control of transaction risk and security
Free selection of payment instrument	Minimal integration and management costs	Independence of the financial services from the operator services
Broad acceptance by merchants	Broad acceptance by consumer	Interoperability
Financial services accessible via all mobile equipment and operators	Financial service accessible via all mobile equipment and operators	High security
	Universality and openness	Integration with existing infrastructure
	Fast efficient payment completion	Universality and openness, including no proprietary solutions

Functional Requirements in Mobile Commerce (from Mobey Forum 2000, page 7)

The Mobey Forum (2000) suggests that in order to meet these requirements a dual chip or dual slot phone approach is desirable.

Market Conditions

Banks need to assess the receptiveness of the market to new technology based on the current situation. Further they need to concentrate on an appropriate distribution strategy, using the right mix of channels with the appropriate allocation of resources (Worthington 1998).

In terms of consumer receptiveness, an iterative approach may be appropriate where new technology is introduced in small steps, for example, the introduction of e-purse for small value transactions may precede the introduction of a full multi-functional card smoothing the transition from use of one technology to another (Puri 1997, Dutrieux 1999). Further, the e-purse should be implemented

in 'high value-added: high volume' situations such as for vending machines, payphones and public transport. Public transport is seen as a key application for smart cards (Lefebrvre 1999); meeting the need to obtain a critical mass in terms of high volume use, whilst providing consumers with a high value-added card that will improve service quality and provide an impetus to maintain usage over time. Closed communities, such as Universities and holiday villages may also prove fruitful grounds for launching smart card products; indeed such applications have been seen to be more successful than generic use cards in the past (Lefebvre 1999). Further, combining an e-purse with an already popular function such as a credit/debit card is also likely to increase acceptance and provide a useful foundation upon which to release multi-function smart cards (Lefebvre 1999). Players need to ensure that the economic rationale for switching to smart card technology is transparent in order to counteract public distrust in new schemes (Lefebvre 1999). For example, with e-purse schemes, the high handling costs of cash (which are often hidden from consumers) and the subsequent savings gained through use of the e-purse should be made clear to potential users (Lefebvre 1999).

In terms of technical receptiveness, the technical infrastructure needs to be in place before systems can be introduced to avoid problems arising from poor support structures that can erode the image of smart cards (Puri 1997). Completely overhauling existing infrastructures is likely to be costly, especially as such infrastructure must be ubiquitous if the scheme is to be successful. For example, e-purse will not successfully replace cash (if this is ever possible) if it is not as flexible as cash or cannot be utilised in the same diversity of situations (Lefebvre 1999). Players need to make the most of any opportunity to update existing infrastructure by introducing card readers. For example, if parking metres and vending machines have to be updated to accommodate the Euro in the future, smart card readers could be included at the same time (Dutrieux 1999). In terms of mobile commerce, consideration needs to be given to the position of mobile payment capability for proximity transactions. For example, considering if mobile payment systems will complement or substitute existing POS systems for proximity payments (Mobey Forum 2000).

Changing Nature of Competition

M-Commerce does not just involve the traditional banks, a number of service providers (e.g. GSM operators, telcos, software companies) are now interested in m-commerce and the emergence of non-banks is a reality (Puri 1997, Dutrieux 1999, Schule et al 2002). Indeed, many of these 'non-banks' are already either introducing or planning their strategy for utilising chip technology (Dutrieux 1999). The popularity of mobile phones coupled with the emerging WAP technology make telecommunication operators (telcos) 'natural' m-payment service providers (Krueger 2001). Telcos will be prime market players in the m-commerce industry. As such they need to pursue a sound business model, whether they act as a carrier for data transportation or use a 'go-it-alone' strategy (Krueger 2001). In the more traditional 'Bank-Dominated' model, banks issue smart cards enabling m-payments on mobile phones (and other mobile devices) and telcos only play a data transport role. Newer models of m-commerce might involve telcos taking a more independent stand, offering payment services and taking control of the payment process themselves (Kruger 2001). Equally banks can adopt a similar 'go-it-alone' strategy. Two examples following a successful 'go-it-alone' strategy can be found:

- i-mode - NTT DoCoMo's i-mode is a successful packet-switched mobile service. This service has its own portal and offers billing services to merchants using that portal.
- Merita Nordbanken – have also moved into hosting and building portals and developing technology could easily expand into mobile telephony.

'Non-Banks' are a major growth area that can provide alternative secure billing channels to handle on-line transactions (especially micropayments) and, whilst banks will be involved in the final accounting, they will loose direct customer access and transaction processing business (Ankri 1999, Dutrieux 1999). However, many banks have been proactive towards this potential threat, for example:

- Mondex International teamed up with banks such as Wells Fargo to design the MULTOS based card for Internet banking;
- Barclays released the Endorse card to manage digital signatures for authentication purposes;
- In France most banks and financials players (Groupement des Cartes Bancaires, VISA, France Telecom, Europay France) have been involved in the launching of CyberComm (1998) aimed at designing and developing a French bankcard for SET transactions (Ankri 1999).

However, a successful business model is likely to rely on strategic alliances being formed between groups of players from different sectors, each bringing their own strengths in complementary areas (Krueger 2001). Banks contribute a trusted brand and risk-management 'know-how'; telcos contribute mobile capabilities and expertise in mobile technology. Indeed, current models of m-payments indicate that a variety of business models are in use in today's pilot schemes, including stand-alone and bank/telco alliances (Krueger 2001).

Alongside these issues the success of multi-function smart cards will depend on the resolution of a number of problems, as indicated in the previous chapter:

- Who will issue the multi-function cards;
- Who will manage these cards;
- Who will control the relationship with the cardholder and will the cardholder want just one relationship tied to a multifunction card or will they still want multi-relationships with several card issuers;
- The resolution of multi-branding issues (Worthington 1998).

Indeed, the CALYPSO project, described in later chapters, faced these very problems when introducing a multi-function card.

Increased Risks & Interoperability

Whist technology expands the market and offers greater opportunities for e/m-commerce, there are a number of associated security risks, not least data protection and privacy issues (Krueger 2001, Centeno 2002). These issues will need to be addressed alongside interoperability (and associated standardisation), open access and improving the efficiency of cross-border retail systems demanded by consumers utilising e/m-commerce systems. Alliances and outsourcing will be the key to providing an interoperable service, but also require efficient management of inter-member relationships and contracting (Krueger 2001). We need to move from a situation of competition to a situation of 'co-competition' between market players, allowing the basic infrastructure to

be implemented within acceptable costs to all (Lefebvre 1999, Schule et al 2002). Further, we can already see the need for new legislation to protect and control the emerging e/m-commerce industry.

The emergence of multi-function cards necessitates smooth cross-industry communication (Puri 1997). The e/m-commerce industry suffers from an abundance of non-interoperable approaches and concepts, delaying the development of this industry (MET 2002). Major market players are working together to develop a convenient, secure and trustworthy infrastructure to underpin mobile commerce services in a number of initiatives. There is a genuine desire amongst market players to develop and promote standards in e/m commerce as a means towards commercial success (Schule et al 2002). The major initiatives are bound together under the eEurope Smart Cards trailblazer number 5.

e-Payments and m-Payments (TB5)

Trailblazer 5 aims to:

- Identify current barriers to the implementation of e/m-payments and develop appropriate solutions that facilitate the adoption of smart cards;
- Develop payment systems for mobile commerce, payment terminal infrastructure for smart cards, payment systems for Internet and small payment systems in euro across borders (CEPS e-purse).

The Common Electronic Purse Specification (CEPS) has been hailed as a key blueprint for e-purse schemes throughout Europe, having the advantage of being compatible with the EMV standard (Dutrieux 1999).

Link to Initiatives

Trailblazer 5 is linked to a number of major initiatives.

Radicchio

Established in 1999, Radicchio is a 'Global Initiative for Wireless E-Commerce' (Radicchio 2002). This forum aims to:

- Establish a common foundation for secure m-commerce based on the promotion of interoperability.
- Promote and facilitate the implementation of the resultant solutions.

The rationale behind the establishment of this group is that with the increasing number of 'mobile devices' in use today users will be looking for 'value-added' services from these mobile devices. If this is to be realised then a trusted infrastructure (addressing authentication, confidentiality, non-repudiation and integrity issues) needs to be established so that such value-added services can be offered on a large scale. Radicchio (2002) highlights PKI as an important solution to the delivery of such services, as it addresses the four key security issues. Their research indicates that the ideal device, that is both physically and logically secure, utilised within e/m-commerce is the Integrated Chip Card (ICC) or smart card that is PKI enabled (Lannerstrom et al 2000). Radicchio suggest that PKI smart cards, equipped with cryptographic processors for asymmetric encryption such as RSA, are the only cards that can provide the necessary level of security requisite for m-commerce (authentication, confidentiality, non-repudiation and integrity) (Lannerstrom et al 2000).

Radicchio formally merged its international activities with the Mobile Electronic Signature Consortium (established to develop a secure cross-application infrastructure for mobile digital signatures) late 2001.

Mobey Forum

Established in 2000, this global forum brings together those sectors of the finance industry interested in the promotion of e and m commerce. Its mission is to 'encourage the use of mobile technology in financial services' (Mobey Forum 2002). This forum focuses on the business and technical aspects of providing user-friendly and secure mobile banking and payment systems. In order to do this a number of workgroups have been set up:

- Business Workgroup – To investigate and develop business models and business requirements for m-commerce applications;
- Requirements and Technology Workgroup – To investigate interoperability of technical and security requirements of the financial industry for mobile services and technology;
- Rules and Regulations Workgroup – Acts as a legal advisory board for the Mobey Forum and its workgroups;
- Marketing Workgroup – To build awareness of the forum and its goals within the financial services and m-commerce industries.

The Mobey Forum has announced their 'Preferred Payment Architecture' to underpin the development and growth of m-commerce, which is based on dual-chip technology. This architecture:

- Provides consumer choice as consumers are not forced to select a specific operator or bank to use the m-commerce services, which;
- Is achieved by placing financial applications on a smart card placed in the mobile device alongside the SIM card.
- This smart card communicates with tills over a local communication method or with remote merchants and bank-operated server wallets over GSM or other cellular connections (Mobey Forum 2002).

In terms of value for the groups involved, this service offers:

- Consumers convenience, trust and security;
- Banks an open, non-proprietary, independent and cost efficient service that offers an easy access mechanism for offering m-commerce services. They also gain convenience, trust and security;
- Mobile operators a cost-efficient standards-based solution for the provision of m-commerce that will allow m-commerce to gain market acceptance (Mobey Forum 2002).

Mobile Electronic Transactions (MET)

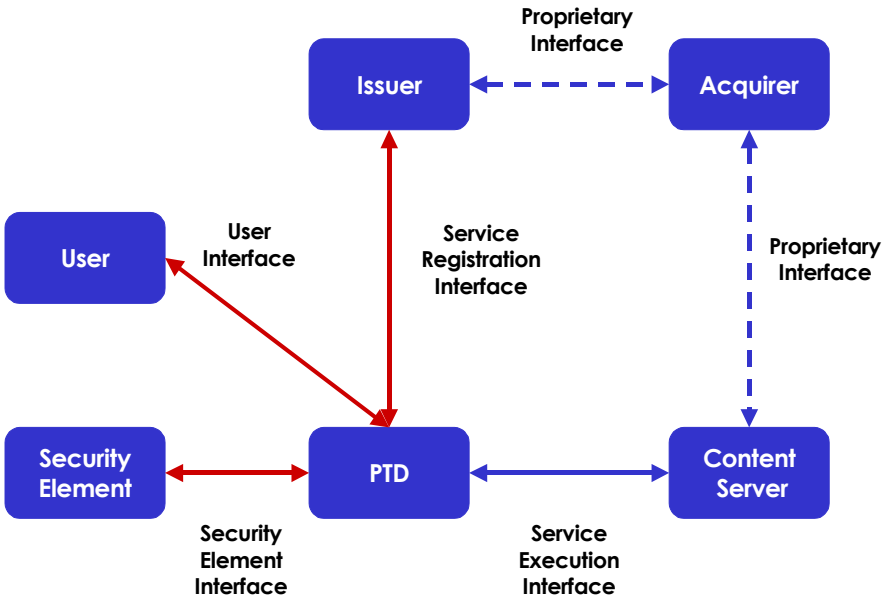
MET Ltd. was established by Ericsson, Motorola and Nokia to develop a framework for secure mobile transactions that also ensured a consistent user experience (MET 2002). This initiative recognises that the mobile phone will play a key role in m-commerce and that the concept of a PTD places consumers at the centre of the m-commerce world, but fragmentation of the market is a real threat unless approaches and applications are brought together under the interoperability umbrella (MET 2001a).

MET aims to:

- Define a common framework enabling the development of m-commerce, which describes how secure mobile electronic transactions are performed by the mobile device based on MET standards;
- Ensure a consistent user experience across devices and services;
- Adopt and extend existing industry standards and technologies where relevant (including WAP, WIM –Wireless Identity Module, wireless PKI and Bluetooth wireless technology) (MET 2001a).

The MET Specification

The MET specification documents the core functions and feature used in m-commerce. The following diagram illustrates the system reference diagram.



System Reference Diagram (after MET 2001b)

MET defines four core interfaces:

- Service execution interface – used for conducting secure transactions with content server;
- Service registration interface – used for loading service certificates onto PTD;
- User interface – used to perform transactions through presentation of information to user; prompting for input; accepting input and forwarding to relevant recipient within a consistent user experience;
- Security Element interface - used to ensure secure transactions (MET 2001b).

MET transactions are built on a common set of core functions (MET 2001b). These include:

- Initialisation – public/private keys for authentication and signing;

- Registration – an online request by PTD to a PKI portal forwards request to a CA, the CA generates the certificate, which is sent back to the PTD, the certificate is entered by CA in its public key database;
- Establishment of secure access – WTLS used to establish secure services;
- Authentication – Utilising WTLS to perform user authentication, client authentication unlocked via PIN (in the future biometrics may be utilised);
- Authorisation by user – signature key to create digital signature (provided by SignText function in WAP) (MET 2001a, 2001b).

MET also provides a security technology specification in its Core Specification document version 1.0 (MET 2001b).

The following security issues will be addressed through MET:

- Confidentiality – using WTLS (Wireless Transport Layer Security;
- Authentication – using WIM (holding encryption keys for mobile devices);
- Integrity of data – using WTLS;
- Authorisation – WIM enabled digital signing (MET 2001a);
- Removable security element – MET security element stored as WIM functionality on SIM card or as a separate smart card with WIM;
- Non-removable security element – using custom hardware and software (MET 2001a).

The following elements have been identified as contributing to the consistent user experience:

- Flexible service selection (multiple services on PTD);
- Awareness of used services/brands;
- Awareness of security environment;
- User verification (e.g. through PIN);
- Awareness of digital signing;
- Access to digitally signed contracts;
- Access to delivered objects (MET 2001a).

MET also provide a number of usage scenarios related to the MET framework. For example in the banking scenario MET define the following elements as prerequisites for WAP banking services.

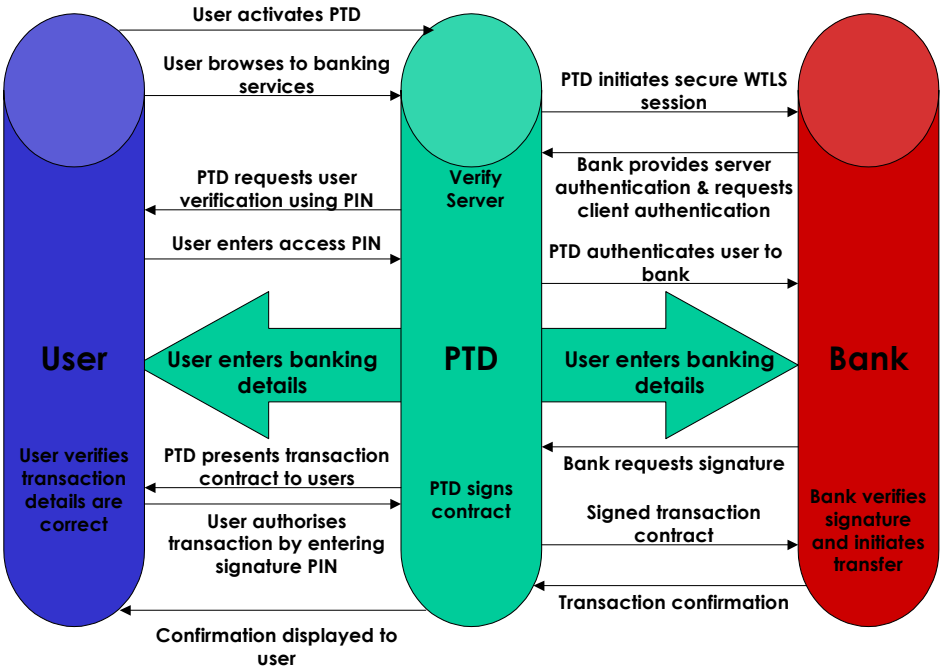
The bank must:

- Offer WAP access to banking services through a secure gateway;
- Establish a sign-up mechanism for users to register for account access over WAP;
- Issue a service certificate to the user enabling identification of the bank's WAP service and authentication of the user to the bank.

The user must:

- Hold an account with the bank providing a WAP service;
- Possess a PTD that can perform authentication, establish secure sessions, create digital signatures and store certificates;
- Initialise the PTD;
- Register with the WAP banking service and receive a service certificate from that bank (MET 2001c).

The following diagram illustrates a successful banking transaction using a PTD.



A successful banking transaction (after MET 2001c)

ETSI Smart Card Platform (ETSI SCP)

The ETSI SCP, having replaced the SMG Technical Sub Committee (SMG9), aims to develop and maintain:

- A common Integrated Circuit (IC) card platform for all mobile telecommunications systems;
- Application independent specifications for IC cards/mobile equipment interface of these telecommunications systems under the ETSI;
- IC card standards for general telecommunication purposes;
- IC card standards for employing advanced security methods for telecommunication applications for e/m-commerce (ETSI SCP 2002).

The 'backbone' the smart card platform, dealing with the physical and logical characteristics of the smart card interface, has been approved. There are three working groups within the ETSI SCP:

- SCPWG1 – to maintain and evolve interface specifications for an interoperable multi-application IC card platform (UICC) and develop and to develop the appropriate supporting documentation and models;

- SCPWG2 – to develop and maintain specifications and develop supporting documentation for advanced security methods for applications on UICC platforms such as m-commerce;
- SCPWG3 – To develop, maintain and support a Card Application Toolkit and the Application Programming Interface Specifications of a UICC platform. The Card Application Toolkit (CAT) is a generalisation of the SIM Application Toolkit.

The major achievements of this group to date are the publication of three specifications:

- TS102 224 Security Mechanisms for UICC based applications;
- TS102 225 Security Packet Structure for UICC based applications;
- TS102 226 Remote APDU Structure for UICC based applications.

The next major publication will be am architectural model of smart cards and usage of PINs for UICC (ETSI SCP 2002).

ETSI M-Commerce

This initiative focuses on defining the requirements for e-signatures and e-payments for m-commerce (ETSI M-Comm 2002). ETSI M-Comm combines the views of the telecommunications industry with finance industries. ETSI M-Comm aims to focus on:

- Devices including wireless PKI and security environments for m-commerce and digital identities;
- Interoperable requirements;
- Technical, political and user requirements for standardisation of a generic environment and procedures for allowing users to control more privacy in m-commerce.

M-Comm activity in 2002 will focus on publishing requirements for users and content providers for mobile payments and mobile signatures, and starting standardisation activities in the Third Generation Partnership Project.

ISO JTC1 Business Team on Electronic Commerce

This initiative focused on the current status of standardisation in e-commerce. The key recommendations of this group were for the establishment of a:

- Quality standard – providing guidelines for the behaviour of parties during the various stages of a transaction;
- Electronic Transactions Protocol – providing web site developers with standardised methods for describing to the consumer the sequence of e-commerce transactions, defining merchant's presentation of transactions ensuring good understanding amongst consumers and including typical sequences (profiles) to reflect codes of conduct (ICTSB Project Team 2000).

Global Mobile Commerce Interoperability Group (GMCIG)

Formed in 2000, this forum for key players in the m-commerce industry aims to establish a global framework for secure wireless purchases (GMCIG 2002). To date it has produced a number of specifications, including:

- Digital Mobile Payments Over Open Networks;

- Remote EMV Payments Using A Mobile Device;
- Remote Wallet Server Architecture;
- Remote EMV/SET Payments Using A Mobile Device.

In support of this initiative Mastercard have launched the Mobile Payment Forum, that is a global cross-industry forum established to create a framework for standardised, secure, authenticated mobile payments based on payment card accounts (Mobile Payment Forum 2002).

In addition, Mastercard have teamed up with Motorola Inc. to conduct research to ensure interoperability between Mastercard e-payment systems and Motorola wireless Internet devices and platforms. This represents the next generation of m-commerce technologies based on the GMCIG initiatives.

E-payment Systems Observatory (ePSO)

The ePSO, set up by the Institute for Prospective Technological Studies, aims to:

- Enhance information exchange in the e-payments arena and thus facilitate the promotion of e-payments in Europe;
- Monitor and analyse the strategic views of key market players and experts in the field;
- Enhance inter-group communication amongst interested parties;
- Enable standardisation and regulatory bodies to keep pace with advances in technology (ePSO 2002).

The ePSO have established a number of forums in order to achieve its objectives.

In addition to a number of published papers (including ones on payment culture and the future of m-payments) EPSO has developed the ePSO Database, which offers access to a wide database on e-payment systems, related projects and initiatives and is a valuable source of information on smart card developments (http://epso.jrc.es/paysys.html).

Smart Card Schemes

The following table describes some of the current smart card schemes introduced across Europe.

Country	Product	Description
Austria	Banko.max	WAP-based m-commerce service
	Quick (2001)	e-purse, requires card readers (about 65€)
Belgium	Bancontact/Mister Cash	Debit card payments over the Internet using smart card and reader for identification
	Proton e-purse	Chip mounted on debit card, used since 1997 for payments over the Internet, loading of e-purse over the Internet possible since 1998
Denmark	Danmont	e-purse, technology used for VisaCash trial during Atlanta Olympics
	Orange Mobile Betaling (formerly Mobilix Open Mobile)	m-payment scheme, using PIN to access services via SIM, payments accepted from Dankort, Visa, Eurocard, Mastercard
	Sonofon	M-payment scheme, using PIN to access services via SIM
Finland	EMPS	m-payment scheme, dual chip phone used (SIM and WIM) using credit card payments
	Avant	e-purse, can be loaded via the Internet
France	Cyber-Comm	Debit card with chip, smart cards and readers, relying on SET
	Moneo, Modeus, Mondex	e-purse
	Paiement CB sur mobile	M-payment based on dual slot mobile phones (slot for inserting cards)
	Payline GSM	m-payment, via GSM dual-slot mobile phones
Germany	GeldKarte	e-purse, requiring smart card reader
	PayCard	e-purse
	Paybox	m-payment scheme
	Payitmobile	m-payment scheme
	Mobilbank	m-payment scheme
Greece	BALCARD	Prepaid smart card for secure cross border Internet transactions
Italy	Movercard	Virtual wallet combined with smart card and reader for security, non-bank service, credit card payments
	Minipay (PayOnWeb)	e-purse
	Omnipay Onphone	m-payment scheme
	Blu/EMPS	m-payment scheme
	We@TIM	m-payment and banking scheme
Netherlands	Chipper	e-purse (taken off market)
	Chipknip	e-purse
	VASCO Digipass 800 (Rabobank)	Smart card and reader access to on-line banking
Portugal	Porta Moedas Multibanco	e-purse
Sweden	Cash	e-purse, based on Proton technology, can be loaded via Internet since 1998
Spain	Monedero 4B	e-purse
	Euro 6000	e-purse
	VisaCash	e-purse, 'clic and cash' service allows loading via Internet
United Kingdom	Mondex	e-purse
	VisaCash	e-purse (new to UK)

Smart Card Schemes

Mondex

Nat West, Midland Bank and British Telecom established Mondex UK and the Mondex card (based on MULTOS) was launched on an experimental basis in a Natwest computing centre (UK) in 1992 and Swindon (UK) in 1996. It is a stored value card that allows value to move directly one card to another without third party (e.g. Banks) intervention. The Mondex card acts like cash, it passes from one person to another without an expensive clearing and settlement process (Puri 1997). However, it offers the advantage of being more secure than cash as it can be electronically secured, utilising the secure functions of smart cards (PKI) it allows access to the genuine cardholder only (Puri 1997). The Mondex card is the first 'real' alternative to cash for low value payments (Worthington 1998).

Value is loaded onto the card either from an ATM, specially adapted public payphones or a handheld 'wallet' (Buck 1996, Worthington 1998). The value is stored on the card and not in an account. The card allows up to five different currencies to be stored on the card at one time (Mondex International 2002). The card can be used in a number of situations, including restaurants, public transport and cafes and enables pay-as-you-view TV and mobile commerce. The Mondex card has now been launched in Japan (Mondex International 2002).

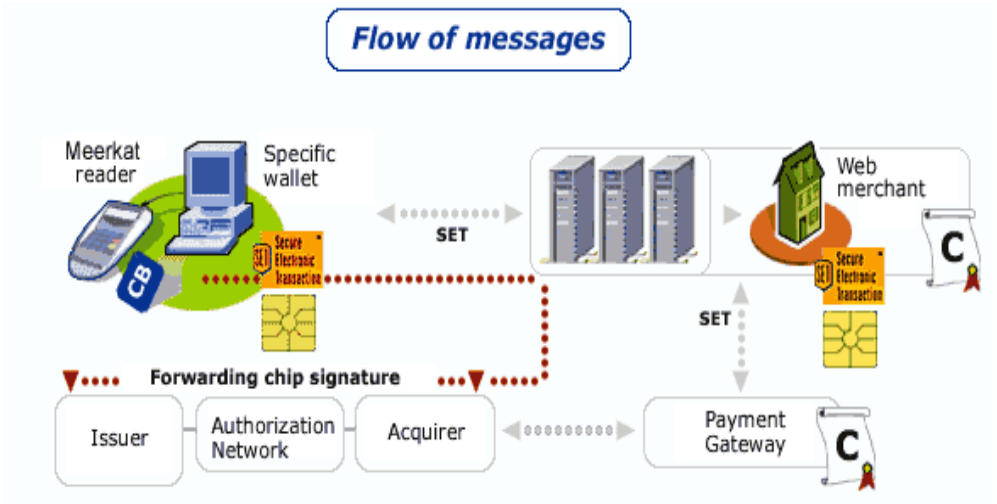
Multibanco Electronic Purse (PMB)

The PMB was launched in 1995 by SIBS (Sociedade Interbancaria Deservicos) and aims at replacing small cash transactions in vending machines, restaurants, kiosks, parking metres and cafés amongst others. The card can be issued by a bank as an independent e-purse or as a combined debit/credit card. The cards can be loaded at ATMs and banks. To date 13000 PMB cards are in use, with an average monthly volume of 30,000 operations (SIBS 2002).

Cyber-Comm

Cyber-Comm is a bank-controlled organisation that has developed a smart card-based means of secure Internet shopping. Cyber-Comm is the first commercially available chip card-based solution (Card Technology Today 2001).

This solution is based on SET and utilises a smart card and reader system, providing strong identification and authentication that guarantees non-repudiation (Ctt 2000). The diagram below illustrates the Cyber-Comm transaction process.



The Cyber-Comm transaction process (from Cyber-Comm.com 2002)

Once the user has been identified through use of a PIN (verified by the card itself), they enter their payment details using the reader and the smart card signs the transaction. The 'Meerkat' reader encrypts the information and signs the transaction again, this information is then sent to the 'Meerkat' wallet (payment software loaded from a CD onto the user's PC). The wallet conducts a 'payments dialogue' with the gateways and host computers of the relevant banks and merchants (using SET). The transaction is processed using the Carte Bleu and Europay France networks within France and the Visa and Eurocard-Mastercard networks internationally.

This system was initially developed for the French market and the infrastructure to read these cards has already been installed by French merchants and banks. Cyber-Comm has devised solutions to overcome the problems inherent in non-French transactions. For consumers within France who wish to buy goods from non-French sites, an SET certificate is generated to replace the chip signature. For consumers outside France wishing to buy goods from French sites using magnetic strip cards they use their normal SET certificate that can be processed by French merchants and banks. It should be noted that Cyber-Comm meets the standards set by the European Directive on Electronic Signatures (Ctt 2000).

Cyber-Comm is working with the FINREAD project to create a common standard for security in card readers. It is also developing an infrastructure to accommodate dual slot mobile phones, where the bank card is held in one slot and the phone pad is used to enter the PIN and transaction details, encryption is performed by a Cyber-Comm card in the second slot. Cyber-Comm has adopted the EMV standard and the first EMV cards will be issued throughout 2002. France is the only country in the EU faced with the problem of moving from one chip system to new one (CB 2002). There are currently 27 operational merchants set up for the Cyber-Comm scheme with over 40 more to come (Cyber-Comm 2002).

Conditional Access For Europe (CAFÉ)

CAFÉ (1992-1995) is part of the EC's ESPRIT programme and has developed a secure electronic payment system (or e-wallet) designed to protect the privacy of users on an open network (CAFÉ 2002). CAFÉ focused on payments in retail outlets on the high street, which faced two major challenges: the portability of the system and the lack of Internet connections in all outlets (CAFÉ 2002). CAFÉ relies on a pocket-sized e-wallet, with an infrared interface. The smart cards are used as the money storage facility.

Rabobank

Rabobank view smart cards as a key strategy in its development, but launching the card involved more than adding a chip to existing cards they need to consider the card reader as well. Rather than a merchant terminal or a device for attaching to a PC, Rabobank have opted for a portable, standalone device that in combination with the smart card acts as a limited PDA – the VASCO Digipass 800 reader (Schneider 2001). This reader has been distributed to Radobank's entire Internet banking customer base (300,000 readers for 2001, with a further 500,000 ordered for 2002). The reader is a calculator type device with a slot for a smart card; using a PIN the user accesses a time-stamped code, which is then entered with a user ID and password when using the Internet banking site. No connection between the reader and PC is required making the reader a highly portable device (Schneider 2001).

Consumer Issues

Technological advances such as smart cards can facilitate 'connectivity', the integration of computers and networks into everyday lives (Choi & Whinston 1998, Petri 2002). The opportunities offered by the information society may change the lives of nearly all consumers (ANEC 2002). However, we need to ensure that there is access for all consumers and we also need to recognise their current fears regarding information technology (ANEC 2002, eEurope 2000). The establishment of Trailblazer 8 to examine user requirements within the eEurope Smart Cards initiative underlines the importance of the consumer perspective, recognising the need to understand and incorporate the consumer perspective within smart card system design.

User Acceptance

Svigals (2000) describes the following stages as necessary to move from consumer acceptance of smart cards through to consumer preference of smart cards:

- New technologies replace existing old functions (smart cards replaces magnetic strip cards);
- New technologies introduce new functions (smart cards become multi-functional);
- New functioning impacts on society and consumer lifestyles (smart cards reduce fraud and bad debt losses, facilitate convenience and reduce system costs)

Within this model Svigals (2000) suggests that the current state of smart card development falls into phase one. For example, there is a widespread acceptance of memory only (stored value) smart cards. However, smart cards have not yet replaced existing technologies in the majority of service areas. Thus we need to understand what would facilitate consumer acceptance and ultimately consumer preference for a smart card.

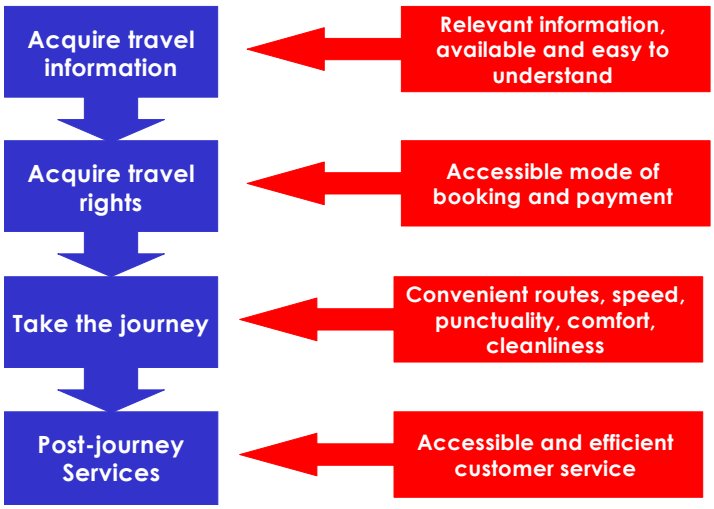
However, when understanding smart card adoption we should not focus exclusively on the consumer. Smart card technology can radically change the whole service exchange procedure and as such requires multiple groups to adopt them in order to ensure their success: the consumer must use the cards AND merchants must install the transaction processing hardware (Plouffe et al 2001, Truman 2002). Thus there is a need to understand adoption of smart cards from a multi-group perspective – we need to examine the 'value-added' element for both consumers and merchants alike.

The Value-Added Factor

Trailblazer 8 (eEurope Smart Cards 2002) emphasises that system design needs to consider more than the 'card' itself; previous designs focusing only on the 'card' have led to imperfect designs. For users the 'card' is a small component of a broader service or set of services; the technology itself is often not the primary focus (Wrathall 2002c). We must not forget that the user is the final purchaser of systems and as such they have certain expectations, not least to be able to easily understand and operate systems and to be able to interface with systems without being overburdened (No 2002). For the consumer, 'value-added' indicates the degree to which the smart card improves the utility gained

from the consumption experience. For the merchant, 'value-added' indicates the degree to which the smart card systems will boost profit (both the cost and revenue sides) – (Plouffe 2001).

Wrathall (2002c) offers the example of a consumer wishing to travel as an example of the broad range of issues inherent within a relatively simple action.



What is important to the user is the service rather than the technology used to deliver that service. The technology is only of value in that it is instrumental in performing the task. Thus, we need to ask the question *'what do customers want from a smart card?'* Product development must fully understand their final users needs for a smart card if it is to be adopted on a wide scale (Plouffe et al 2000, Truman et al 2002).

Card News (1999), in a US Survey, identified that the ideal smart card for a consumer would be:

> ***'one that can do many things as well as a current card does, not a card that can do one thing better than anything else can'***

Consumers have expressed a wish to use the smart card in a variety of diverse contexts, including: as a substitute for money, including cash for small purchases; as a key or access token; to hold medical records (Card News 1999). Several important generic value-added aspects of smart cards have been identified (Clarke 1997, ETF 1999, Card News 1999, Walsh and Berger 2000, FINREAD 2002, Petri 2002, Truman et al 2002), including:

Convenience:

- The production of ID cards that serve multiple functions in one card;
- Ease of use of a multi-function card;
- Cutting down on processing and speeding up transactions;
- On the internet – acts as a payment card and a remote identification system;

- In the case of stored-value cards (SVC) reduced 'wallet bulge', less cash handling and change counting.

Economics:

- Streamlining of transactions can lead to a reduction in costs.
- Fewer transaction errors.

Customisation:

- Customised web pages, e-mail etc from any terminal using smart card as identification;
- Storing information, e.g. phone numbers, on smart cards rather than the appliance allows easy transition between appliances.
- Enhanced privacy;
- Enhanced security.

These proposed value-added aspects of smart cards give us a good understanding of the value that smart cards can offer consumers. We should further examine consumer money management philosophies and issues influencing their adoption of technological innovations.

Money Management

It has been suggested that those people most likely to be interested in smart cards are:

- 18-25 years old;
- Mobile phone or PC users;
- Those with a college education (Card News 1999).

Indeed, intention to use a smart card has been found to be highest amongst those in younger age groups, low-moderate household incomes and college students (Plouffe et al 2000). However, this relationship may be governed by the way that such groups manage their everyday budgets. Thus a focus on demographics can be misleading; instead we should focus on classifying consumers according to their money management philosophy and how this affects the use of innovations within the banking environment (Barczak et al 1997). Indeed, surveys have found a prevailing positive attitude towards smart cards amongst a diverse range of users (e.g. Simpson 2002). Thus, an understanding of consumer needs that goes beyond demographics is needed to understand usage and non-usage of smart cards.

As indicated above, consumers use a product such as smart cards as a means to an end, that is, the consequences of using a product are more important (or self-relevant) to a consumer than characteristics of the product itself. Products must be instrumental in achieving consumer goals (Mulvey et al 1994). Barczak et al (1997) have developed a typology of consumer money management philosophies for using technologically based banking services, which are particularly relevant to the current report. The four categories within this typology are:

- Security Conscious – To users in this group money equals security, they have a tendency to delay purchases and will save for a purchase rather than utilising credit schemes (which they are wary of). This

group is the least likely to enjoy spending money and are the least interested in instant gratification.

- Maximisers – Members of this group try to use money to the best advantage, they will see credit as a way of maximising money (as they pay of balances and do not incur credit), they have a tendency to save, are not interested in instant gratification and monitor the performance of their money closely.
- Instant Gratification – This group enjoy instant gratification and use money to 'feather their nests', they are more convenience orientated and they enjoy spending money.
- Hassle Avoiders – This group also enjoy instant gratification and enjoy spending money, however, they try to avoid 'hassles' such as lengthy paperwork in their banking.

Not surprisingly, 'security conscious' and 'maximisers' tend to be in older age groups than the 'instant gratification' and 'hassle avoiders' groups. Importantly, these money management philosophies will have a significant impact on banking behaviour (Barczak et al 1997). For example it has been found that the highest use of ATMs is amongst the 'instant gratification' and 'hassle avoiders' groups (80% and 78% respectively). For these groups ATMs save time and, as ATMs make money more readily available, they can spend more money. Furthermore 'hassle avoiders' are more likely than the other groups to use automatic withdrawal mechanisms (Barczak et al 1997). The differences between these groups are most striking when applied to telephone-banking behaviour.

	Security Conscious	Maximisers	Instant Gratification	Hassle Avoiders
Verifying account balance	35%	24%	51%	35%
Verifying deposits	28%	19%	45%	30%
Verifying withdrawals	26%	14%	42%	28%
Verifying cheques have been cleared	30%	17%	41%	31%

Percentage of users utilising telephone-banking services (Barczak et al 1997)

Clearly, 'instant gratification' groups utilise telephone-banking services most heavily, whilst maximisers utilise telephone banking services the least. 'Maximisers' are less likely to use automatic banking services, preferring a more 'hands on' approach.

What this research indicates is that a bias towards different money management philosophies can influence banking behaviour. This is likely to have important implications for smart card adoption. For example, 'instant gratification' and 'hassle avoiders' groups are likely to welcome any technological advancement that means smoother, quicker access to money, particularly if it aids such things as on-line shopping. The 'security conscious' group might welcome the advanced security aspects of smart card technology. 'Maximisers' might welcome cards that are multifunctional and that offer incentives for use, such as loyalty points. Understanding the implications of this typology for smart card use

can be used as a powerful marketing tool, where marketing material can be targeted to underline the different features attractive to each group.

Adopting Innovations

Smart cards technology is still relatively novel to many consumers and merchants (Truman et al 2002), and innovation theory can aid our understanding of how to facilitate smart card adoption. Wide scale adoption of smart cards may be a challenge given that it will rely on multiple groups adopting and using the end product (Clemons et al 1997).

The innovation theory of Rogers (1995), the Technology Acceptance Model of Davis (1989) and the Perceived Characteristics of Innovations (Moore and Benbasat 1991) have been utilised in a great many diverse situations and has recently been utilised to explain smart card adoption. The basic tenet of these theories is that the adoption of an innovation will be heavily influenced by consumer perspectives of a series of characteristics of the innovation itself.

Relative Advantage/Perceived Usefulness - Rogers (1995) suggested that an innovation must be perceived as better than its predecessor. Similarly, Davis (1989) proposed that users must perceive a technological innovation as useful; a technological innovation is expected to improve the user's performance by achieving a goal, if it is to be adopted. This fits with our previous discussion on the value-added components of smart card schemes and the achievement of an end-goal being ultimately how service users will evaluate innovations.

Compatibility - Rogers (1995) suggested that an innovation must be perceived as consistent with existing values and past experiences. Similarly, Hagerstand proposes that social resistance to an innovation may result from a perception that their values are not consistent with the adoption of the innovation. Compatibility is important in that it eases the incorporation of the innovation into user behaviour by building on existing values (Plouffe et al 2001a).

Complexity/Ease of Use - An innovation must be perceived as being easy to use and understand (Davis 1989, Moore and Benbasat 1991, Rogers 1995).

Trialability - Trialability represents the degree to which a potential user believes that the innovation can be adequately tested prior to deciding to adopt the product (Rogers 1995).

Observability - Rogers (1995) original concept of observability can be split into two categories (Moore and Benbasat 1991). The visibility construct, where users perceive the innovation to be widely diffused. The result demonstrability construct, the unique features and benefits of the innovation can be readily recognised by potential users.

Image - Image was originally included in 'relative advantage', however, Moore and Benbasat (1991) suggest that this concept should form a separate category in the list of innovation characteristics. They propose that social approval is associated with the adoption of innovations and that the perceived added prestige and status to be gained by using an innovation will have an important impact on its adoption.

Voluntariness - Moore and Benbasat (1991) also propose that the concept of voluntariness, where an individual perceives the adoption of the innovation to be under their volitional control, is an important issue in innovation adoption.

Environmental conditions are also important to consider in promoting the adoption of an innovation, principally participative safety and support.

Participative Safety - West (1990) suggested that a key element for users to adopt innovation was a feeling of 'participative safety', where users must feel secure in using a product. Such a feeling of 'safety' can be engendered by openness in communication and interaction between designer and user, enabling the end user to gain a holistic view of the product and a broader awareness of the consequences and implications of using the product. Such an approach will facilitate the process of adoption (Monge et al 1992). The various characteristics of innovation described above may well enhance the feeling of participative safety, particularly, compatibility, complexity, trialability, image, voluntariness and observability.

Support - West (1990) posits that for an innovation to be adopted the necessary supports must be in place to sort out 'teething problems' and create a resilience to the inevitable early problems encountered by the introduction of an innovation. A lack of appropriate support systems can lead to non-adoption of the innovation.

The Consumer and Adoption

The perception of innovation characteristics is closely and consistently related to the adoption of an innovation. In particular, high perceived relative advantage, low perceived complexity and high-perceived compatibility are the most consistently related to the successful adoption and use of innovations (Tornatzky and Klein 1982). In terms of these three main innovation characteristics, the consumer may therefore be looking for the following (Plouffe et al 2001a, Truman et al 2002):

- In terms of relative advantage the smart card is better than cash because:
    - Consumers only need to handle one item;
    - No counting of money is involved;
    - Smart cards reduce the chances of errors being made;
    - They increase the ease of the transaction;
    - They reduce the time taken to transact;
    - They provide greater convenience to the customer.
- In terms of complexity, consumers may be concerned about the processes involved in maintaining a card; for example, replenishment of stored-value cards must be viewed as uncomplicated.
- In terms of compatibility, consumers will utilise their past experiences to evaluate the cards compatibility. Thus those who use credit/debit cards are more likely to perceive smart cards as compatible with their current values.

Research examining the mass adoption of smart cards has found that some of these innovation characteristics do have an impact on adoption. In terms of consumer adoption, relative advantage and complexity were found to have a significant impact on adoption and use of smart cards (Truman et al 2002). Indeed, users have specified that a smart card has perceived relative advantage over current methods, particularly the convenience of having one multifunctional card instead of many cards in their wallet (Card News 1999). Multifunctional smart cards are seen as a key development in order to reduce 'card overload' and facilitate successful adoption (Truman et al 2002). Indeed, Van Schaik

(1999) found that multifunctionality was the most important predictor of positive attitudes towards smart cards, which consequently impacted on intention to use.

A US survey also found that users would like a card that fitted with their past experiences (compatibility), in that the card should look and feel like current credit/debit cards (Card News 1999). Indeed, when users are asked what they want from a smart card they have a tendency to relate their needs to there own past and current experiences, for example that the card needs to offer at least the same level of security and ease of use as traditional commerce (Card News 1999). Plouffe et al (2001) also found that compatibility had an impact on the adoption of smart cards. A key theme is that familiarity breeds acceptance (FINREAD 2002). No (2002) also suggests that consistency across user interfaces will encourage a higher acceptance of smart card products amongst users, that is familiarity with one type of smart card system will aid adoption of other smart card systems that offer similar interfaces. However, the user interface is seen as a key area of competition amongst service providers and there has been some resistance to standardisation in this area (ICTSB Project Team 2000). The financial and telecommunication sectors have been the most active in the standardisation field in recent years (ITCSB Project Team 2000). In addition, Plouffe et al (2001a) found that image and voluntariness had a significant impact on the adoption of smart cards, although to a lesser degree than relative advantage or compatibility.

In a 12 month study of the Exact smart card, including over 400 businesses and over 5000 card users, Plouffe et al (2001a) contrasted the influential innovation characteristics amongst those users that intended to adopt smart cards and those that did not, the results can be seen in the following table.

Adopting User	Non-Adopting User
Relative Advantage (38.2%) Compatibility (28.9%) Image (10.9%) Voluntariness (13.3%)	Relative Advantage (40.5%) Compatibility (16.4%) Image (4.7%) Voluntariness (0.9%) Visibility (13.2%) Trialability (12.5%) Result Demonstrability (4.0%)

Significant innovation characteristics in intention to adopt smart cards (% of variance explained) (after Plouffe et al 2001)

Amongst the two groups, relative advantage, compatibility, image and voluntariness are important to both groups. However, the non-participating group are more complex and show a more wary attitude towards smart cards. For them it is also important to that the product can be tested before a decision to adopt is made, that the product is widely diffused and that the benefits of the card can be easily discerned. Such a group are likely to be late adopters, if at all, of a smart card, as they wish to 'see it in action' first before that take a risk in adopting the product themselves. It is also interesting to note that complexity/ease of use did not have a significant role to play in intention to adopt. It may be that this issue is important at later stages of the adoption process such as in the maintenance of use.

The Merchant and Adoption

In terms of smart card characteristics, the merchant might be looking for the following (Plouffe et al 2001a, Truman et al 2002):

- In terms of relative advantage, that the card enhances operational efficiency by reducing the average transaction time, reducing cash handling thus reducing errors and overall making cost savings. In particular the smart card should enhance the attractiveness of the merchant's services to the consumer.
- In terms of complexity, the smart card procedures need to be viewed as easy and reliable.
- In terms of compatibility, where merchants utilise debit/credit cards then they may find smart cards easier to adopt.
- In terms of observability, merchants must see that smart cards are successfully applied by others and are seen by the consumer as attractive.

In terms of merchant adoption, relative advantage was found to have a significant impact on adoption and use of smart cards (Plouffe et al 2001a, Truman et al 2002). Perceived low relative advantage led to failure of adoption of a trial smart card, despite the fact that the smart cards were seen as simple to use (complexity). Plouffe et al (2001b) also found that compatibility, image, visibility, trialability and voluntariness had an impact on intention to adopt smart cards amongst merchants. Furthermore, in line with West's (1990) suggestion that appropriate support needs to be in place for successful adoption, merchant adoption also failed as there were a number of technical hitches, which were not supported by the appropriate back-up systems from the design companies and there was also a lack of adequate training in the proper procedures (Truman et al 2002). Thus support systems must be in place from the beginning so that they can rapidly respond to any problems that occur and rectify these to facilitate innovation adoption (Truman e al 2002).

Plouffe et al (2001a) contrasted innovation characteristics that were important amongst those intending to adopt smart cards and those not intending to adopt. The results can be seen in the table below.

Adopting Merchant	Non-Adopting Merchant
Relative Advantage (29.7%) Compatibility (17.3%) Image (17.0%) Visibility (13.1%)	Relative Advantage (32.3%)

Significant innovation characteristics in intention to adopt smart cards (% of variance explained) (after Plouffe et al 2001)

Whilst a number of factors are influential in the intention to adopt smart cards amongst the adopting merchant group, the non-adopting merchant group are influenced by one key variable, relative advantage. This suggests that if merchants do not see the relative advantage of smart cards then they are unlikely to see beyond this issue and are not likely to evaluate the smart card against any other criteria. This underlines the importance of establishing the relative advantage of smart cards amongst user groups.

Furthermore, intention to adopt a smart card system may be dependent on market sector amongst merchants. For example, so-called 'tip-based' restaurants and speciality retailers (e.g. clothiers) were found to be less enthusiastic about smart cards as they felt poorly suited to a smart card system (Plouffe et al 2000). Smart card innovation in this area will need to consider how to tailor smart card functions to suit these sectors.

It is also important to note that those users intending to adopt smart cards and those merchants intending to adopt smart cards shared three factors in common as influential in their intention to adopt: relative advantage, compatibility and image. Marketing and education programmes are needed that help users to understand the utility of the smart card in terms of the innovation characteristics discussed above (Plouffe et al 2001a, Truman et al 2002). In particular, the differences between current credit/debit cards and smart cards should be expounded to enable users to see the relative advantage of smart cards. Compatibility should be facilitated by developing means of integrating POS equipment so that it can be used to process all electronic payment systems, e.g. credit/debit and smart cards (Plouffe et al 2001a). An image building campaign can utilise promotional campaigns and build a strong smart card logo in order to make smart card usage attractive to potential adopters.

Critical Mass

In order for an innovation to achieve widespread adoption it needs to reach a critical mass – a certain number of adopters need to use the product before it can be sustained. This is because the inherent benefits of the smart card for the consumer and merchant are dependent on mass adoption; benefits derived from the smart card are based on the size of the participating community (Truman et al 2002). In other words, the benefits derived from the use of a smart card are directly proportional to the number of adopters utilising the smart card; as usage increases so the benefits of the card increases (Shurmer 1993). These benefits are also enhanced by the number of complementary products produced (Shurmer 1993). The eEurope initiative recognises the need for smart card adoption to reach a critical mass and the accompanying need for a new infrastructure across Europe to support the widespread usage of smart cards (eEurope 2000c).

Recent research has found that failure to adopt a trial smart card was partly as a result of a failure to reach critical mass in terms of usage. Two key factors were identified as restricting the mass adoption of the card. Firstly, geographical constraints, where the trial card could only be operated within a specific geographical area. Thus users could not effectively exploit the smart card within their everyday lives, which included much travel. Secondly, merchant sector constraints, where many of the key merchant sectors were not involved in the trial, including transport, payphones and vending machines, thus restricting the utility of the card (Truman et al 2002). These two factors, geographical and merchant sector constraints, have been found to affect the achievement of critical mass by others (Deogun 1996, Beckett 1998). This has important implications for future smart card trials, where the scope of the cards usage must be carefully considered in the design of any pilot. Subsidies might be considered as a means to promote early adoption of smart cards and hence accelerate reaching critical mass (Truman et al 2002).

Social Learning & Payment Cultures

Social learning is an important mechanism towards achieving a critical mass (Antonides et al 1999). For example, the abundance of credit card usage has informed social learning about the benefits, uses and processes involved in card transactions. Such learning is invaluable in the successful adoption of smart cards, the usage of which relies on many of the processes learnt through credit card adoption (Antonides et al 1999). For example, the introduction of smart cards in such places as the Netherlands (Chipper & Chipknip cards) and France (Cybercard) has been found to be much swifter than other countries, such as

Italy, because of the abundance of card usage in France and the Netherlands (Antonides et al 1999). Market players can boost social learning about smart cards by introducing simple, high volume cards, such as library cards, parking metre cards and cards for use on public transport. Such high visibility stimulates social learning through word of mouth and affecting social norms, which will smooth the path for the introduction of more complex smart cards, such as multi-function cards (Antonides et al 1999).

On a related note, Bohle and Krueger (2001) suggest that payment culture should be taken into account in order to understand that factors that impact on the adoption and diffusion of innovations in payment systems. They define payment culture along three dimensions:

- The political, economical and regulatory background;
- The range of payment methods available;
- The usage patterns of those payment methods.

The dominant payment culture may act as both a 'filter' and a 'catalyst' for the introduction and assimilation of new payment systems, similar to the social learning mechanism suggested by Antonides et al (1999). Whilst the EU is seen as one payment area with regard to the Internet, in reality cross-border transactions may be complicated by diverse payment cultures between countries (Bohle and Krueger 2001). Thus, whilst there is a strong smart card orientation in Europe, this is not equal across the member states, which may delay full integration of smart card payment systems across Europe.

Barriers to Usage

From an implementation perspective the lack of standard smart card readers, the prevalence of infrastructure for and acceptability of magnetic strip cards and cost (including re-equipping cardholders and merchants with cards and readers) have been viewed as significant barriers to the widespread introduction of smart cards (Clarke 1997, Petri 2002). Similarly, cost is seen as a significant barrier to the use of biometrics in banking security (Bruno 2001).

However, there are several potential barriers resulting from the user perspective of these cards. These can include real and perceived barriers to participation. Real barriers to participation focus on transaction costs, processing speed, special needs and marketing and promotional support (Plouffe et al 2000, eEurope Smart Cards 2001). Many of the perceived barriers to participation revolve around fear of technology and user confidence, and its constituents of security, trust and awareness of the power of smart cards. These issues have been repeatedly reported as key factors hindering the development of e-commerce (Centero 2002). eEurope Smart Cards (2001) propose that the removal of these real and perceived barriers will enable the mass deployment and availability of smart card services, fulfilling many consumer needs and enhancing quality of life.

Power & Privacy

It has been suggested that consumers may only have a narrow perception of the scope of smart cards, seeing them merely as an alternative electronic payment system, rather than understanding the potential scope of such systems. In consequence, resistance may be met from consumers who do not see the need for the introduction of new systems (Choi and Whinston 1998). Consumers need to be aware of the benefits to be gained from smart card systems if they are to consider using them.

Conversely, some consumers may fear that the smart card is overly powerful. Consumer concerns over the potential power of a smart card include data security, consumer rights and privacy issues (Clarke 1997). For example, the introduction of ID cards in Hong Kong has met widespread concerns regarding issues of privacy, civil liberties and security (the very issue that smart cards were meant to improve); consumer concerns have led to pressure being put on the government to minimise the amount of data held on the card (Hermida 2002). In Australia 'Big Brother' fears amongst consumers are a major obstacle to the widespread acceptance of smart cards (Vandore 1999). Jennings and Holzer (2001) note that although big brother fears exist about the smart card, it is in fact a superb device for securing information. Data is secure through the encryption processes adopted and storing information on one card reduces the need for multiple databases storing personal information (which subsequently reduces the risk of data being exposed). Further, Plouffe et al (2000) found that users were concerned about the voluntary nature of smart cards; they felt that they were going to be introduced regardless of their feelings towards such technology as a means of reducing service levels available to consumers.

Furthermore, some users are wary of the 'electronic paper trails' left by using electronic means to make payments. Users resented that there may in the future be no means to go about their financial affairs in a purely untraceable manner. On a related note, users were concerned that their consuming histories would be captured by smart cards and sold to marketing companies, which they felt was an intrusion of their privacy (Plouffe et al 2000).

Consumer acceptance of the use of biometrics may be a big obstacle, particularly to the use of retinal scans. Consumers are typically suspicious of such technology, through a lack of information and a 'fear of being scanned' (Bruno 2001).

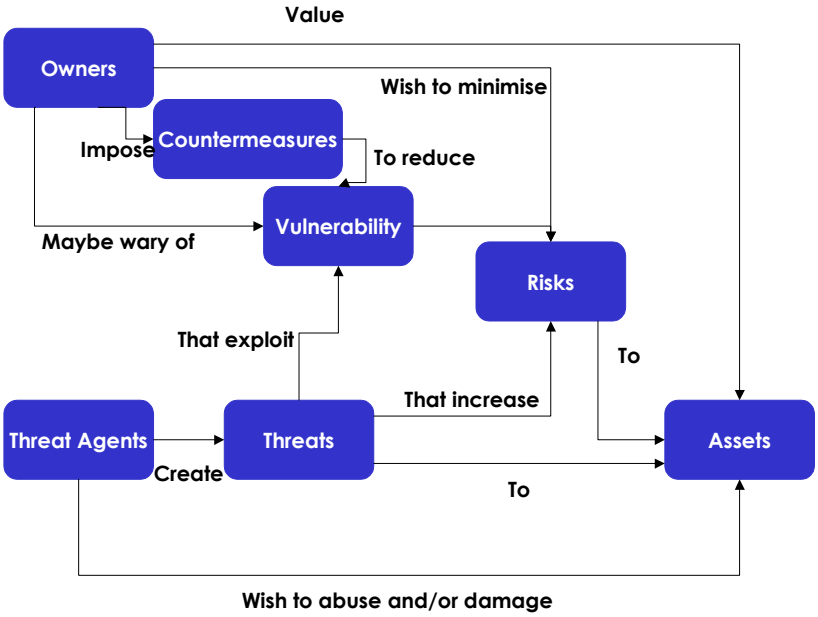
Security

Security is an important facet of consumer confidence (eEurope 2000b). We have stressed that for the user the service and end product are important rather than the underpinning technology; security can be viewed as an essential part of this process (Centeno 2002). Principle security concerns for consumers focus on: viruses; hacking; credit card fraud; lack of confidentiality and authentication (eEurope 2000a). For example, in terms of on-line purchasing:

- 75% of users were concerned about the potential of on-line fraud (Ipsos-Reid Group 2001);
- 95% of users were very/somewhat concerned about privacy and security using credit cards on the Internet (Gartner Group 2000).
- Merchants are afraid of selling on-line, and about 66% had reported serious cybercrime attacks (CBI 2001).

Whilst these figures do not relate specifically to smart cards, they do illustrate that a high percentage of users are concerned about using electronic services. Whilst smart cards can be marketed as a more secure device for utilising e-commerce services, these initial users fears are likely to generalise to all types of e-commerce.

eEurope Smart Cards (1999) offer the following model as a guide to the factors and relationships indicated in security.



Security factors and interrelationships (eEurope Smart Cards 1999)

There is obviously a role for 'hard' technological solutions to the issue of security. Indeed, a major benefit of smart cards is their positive impact on security, offering solutions to many of these key threats, including the following mechanisms:

- Public Key Infrastructure (PKI) is more secure than password based systems – there is the ability to keep the key private as there is no sharing of knowledge of the key;
- Increases security of password based systems by storage of passwords accessed through PINs;
- Enabling 2-factor authentication or greater – including biometrics such as thumbprint signatures;
- Auto-disabling PINs against dictionary attacks (Clarke 1997, Petri 2000).

However, there are also a number of 'soft' measures that can also be put in place to increase security and boost user perceptions of e-commerce security.

Humans are the weakest link in the security chain, often compromising their passwords and divulging information through conversation (Centeno 2002). Many customers remain ill informed about technology and the potential security risks of technological advances, which can lead to inappropriate behaviours and risk taking (European Commission 2001). Consumers lack knowledge about the lack of privacy of their e-transactions and the means available to protect themselves (eEurope 2000b, Kolsaker and Payne 2002). Indeed, there is a mismatch between consumers' heightened fears about security and the lower reality of security breaches (Centeno 2002, Kolsaker and Payne 2002). There is a need to raise public awareness of issues to prevent, at one extreme, user avoidance of e-commerce through poor understanding, and, at the other extreme, taking risks on e-commerce. Consumers need to be made aware of

the potential security risks, such as e-mail scams. Consumer education could focus on:

- Checking SSL protocols are used;
- Check privacy policies of merchants;
- Looking for insurance for buyers;
- Minimising data provided to merchant;
- Using pseudonyms where possible;
- Keeping a trace of all transactions and examining statements for any errors (Centeno 2002).

Merchants can also play an important role in increasing security:

- Utilising customer follow-ups (e.g. through e-mail or telephone);
- Utilising address validation and on-line authorisation systems;
- Building a consumer history database (Centeno 2002).

We also need to consider the education of service providers, making them aware of the potential risks of internal as well as external attacks, as this has been found to be lacking (Centeno 2002).

However, a significant hurdle in security seems to centre on cost issues; consumers and merchants alike are unwilling to pay for increased security, which leads to a reduced demand for more secure products (Centeno 2002).

Smart cards can play a key role in increasing security and engendering a positive consumer outlook of transaction security (eEurope 2000b). Thus in terms of smart cards, we should not only promote the security aspects of smart cards, but we should also be encouraging best practice amongst consumers and merchants alike. Through raising awareness and education programmes users can gain a realistic view of the security risks inherent in e-commerce and hence make an informed choice about utilising e-commerce and m-commerce services.

Trust

Trust is an important factor in the delivery of smart card services. We need to understand the overall concerns that consumers have in relation to trust in the key applications of smart cards, particularly e/m-commerce. Trust is a complicated issue involving the consideration of consumer rights, including security, identification, privacy and confidentiality issues (eEurope 2000).

Trust has been defined as:

> *A belief or expectation that the merchant's word or promise can be depended upon and the seller is not trying to take advantage of the consumer's vulnerability*
>
> **(Kolsaker and Payne 2002, p. 207)**

This definition emphasises that the consumer and the merchant rely on one another to maintain trust within their relationship. Trust is important as it is a prerequisite for commitment and motivation to stay in the consumer-merchant relationship (Morgan et al 1994). Driving factors of trust are perceived risk, the importance of the goal, willingness to accept risks and reliance (belief that although there are risks involved they can be fixed) (Pichler 2000, Centeno 2002). Trust can be divided into:

- Initial trust – encouraging first time users;
- Maintained trust – maintaining current users (Egger 2001).

Trust is a multifaceted issue and building consumer trust is likely to be a complex issue. This is reflected in the factors influential in building initial trust, which are summarised in the following table.

Pre-Interaction Factors	Brand reputation & awareness Previous Experience in off-line world Advice or experience of other trusted sources
User Interface Factors	Design, image & professionalism Usability, effective and easy navigation Native language
Site Information Factors	Transparency Company information (incl. address and contact details) Customer service contact numbers Link to trusted companies Data protection and data privacy statements Security policy statements
Purchase Interaction Factors	Contractual terms & conditions Clear pricing offers (incl. delivery, taxes etc.) Clearly stated return polices Ability to cancel transaction Security seals of approval (credit card logos and trust marks) Provision of alternative payment methods with different risk levels Use of up-to-date technology Detailed step-by-step payment procedures

Initial Trust Factors (after Centero 2002)

Thus consideration needs to be given to a whole host of factors in order to gain initial trust in smart card products.

Maintaining trust of users once gained hinges on providing them with a positive experience in their first usage of the service based on the application of good business practices (see EC Directive on Distance Selling and OECD Guidelines for Consumer Protection in E-commerce) and ensuring that tools are in place to solve any potential problems that might occur (Centeno 2002). Indeed, West (1990), as indicated above, has suggested that for innovation to become part of everyday practice then support for teething problems needs to be in place from the start.

Integrity in relation to returns and refunds can also maintain trust. Appropriate support services need to be in place to underpin after sales services ensuring that, especially in the absence of a physical store, employees can deal efficiently with returns and refunds (Kolsaker and Payne 2002). Being able to return items to a physical store can also boost consumer trust (Greenberg 2001) and virtual companies might give consideration to forming partnerships with offline stores in order to provide such a service. The importance of maintaining integrity is underlined by findings that 23% of consumers who have had poor experiences in returning goods have stopped shopping on-line (BCG 1999).

Consumer awareness and education can go some way towards enhancing consumer trust in e-commerce. Making consumers aware of the actual risk levels (rather than perceived risk that can be higher than reality) and awareness of risk reduction measures and protection mechanisms can play a key role in enhancing trust (Centeno 2002). Consumers need to be encouraged to check

certain details about the service that they are using, including information on cancelling orders, returning goods and complaints procedures. Marketing of the product and the provision of on-going support are repeatedly highlighted as essential in smart card studies. Marketing plays a key role in informing consumers and merchants alike of the relative benefits of smart cards and helps to establish a strong identity or image for the product stimulating interest and trust in the smart card. Good quality on-going support for product usage is also essential for maintaining initial interest and trust in a smart card. Poor on-going support has been shown to undermine consumer interest and trust and lead to reduced usage of cards, particularly where there has been no clear line of responsibility when errors have occurred (Plouffe et al 2000).

Within this dynamic context smart cards are seen as an important empowering tool, which facilitate secure access to a wide range of services and are an important basis upon which to build consumer trust and confidence (eEurope 2000). Smart cards represent a huge leap forward in the promotion of trust as they offer the opportunity for 'strong' identification, authentication and proof of transactions, as well as offering the means of delivering other security functions such as digital signatures (eEurope 2000). In addition, smart cards can engender trust within consumers as the security confirmation procedures are transparent to users, that is, they automatically confirm security access to users themselves (Svigals 2000).

Other mechanisms can also enhance consumer trust in services:

- Limiting consumer liability in case of fraud (EC Recommendations 97/489/EC e-Payment Instruments);
- Providing redress procedures (EC Recommendations 98/257/EC and 2001/310/EC);
- Repudiation systems – e-Bay have founded a feedback forum that is used to build trust successfully. Buyers and sellers rate and document their quality of experience with each other and these are made available for other users. This encourages sellers to be trustworthy and discourages disreputable service providers from using the service (Resnick and Zeckhauser 2001).
- Merchant trust marks (European Trust Mark Scheme aims to establish a single trust mark) can reinforce the bond of trust between consumer and merchant by establishing guidelines for consumer service and e-fraud issues (Centeno 2002, Kolsaker and Payne 2002).

Real barriers may focus on transaction costs, service quality and the user requirements of the user-system interface.

Transaction Costs

Merchants and consumers alike have raised the issue of transaction costs associated with smart cards as a significant barrier to participation. Thus card issuers need to ensure that sufficient value is offered by smart cards in comparison to other payment mechanisms (Plouffe et al 2000). This was a particularly significant factor in intention to adopt a smart card and led to emotive reactions amongst users (Plouffe et al 2000).

Service Quality

Service quality has been found to hinder use of e-commerce; indeed the importance of quality of experience has been highlighted above in relation to maintaining trust in a system. In the case of consumers, equipment missing from orders, products unsuited to needs and a lack of comprehension of e-commerce were all important in lack of use of e-commerce services over fraud fears (EcaTT 1999). Thus quality of service, as stressed earlier, and education about services are important aspects of e-commerce services.

From the merchant perspective, no need for on-line services, specific characteristics of their products, missing consumer demand, lack of know how and cost were all important factors in not offering on-line services to consumers. Security itself was not as important as these variables (EcaTT 1999).

User Requirements

Many of the real barriers to participation revolve around the actual use of the system itself – the user requirements.

CEN/ISSS Workshop Design for All and Assistive Technologies for ICT

The Design for All concept is particularly concerned with addressing the real barriers to participation inherent within the transaction design. Whilst there are a wide variety of smart card uses there is no overall holistic and consistent approach to the standardisation of smart cards in relation to Design for All (ICTSB Project Team 2000). This initiative, established 2001, has been set up to ensure the effective co-ordination between a number of ICT-related standardisation activities at a European level relating to the design for all concept and assistive technologies. User Requirements are defined by the following categories:

- Locating and Accessing Terminals;
- Physical Handling of Smart Cards and Controls;
- User Interface;
- Operation;
- Adaptation to User Profile;
- Security of Operation (ICTSB Project Team 2000).

Design for All is concerned with a number of issues within each of these categories that aims to promote social inclusion of all groups within smart card system services:

- General – including interoperability and all-in-one card reader;
- Home Environment – concerning the design of systems in the home;
- Public Environment – concerning the design of systems in the public domain and the provision of the appropriate tangible and informational support;
- Physical – physical requirements of the transaction;
- Auditory – auditory aids to the transaction;
- Visual – visual aids to the transaction;
- Cognitive – concerning the cognitive demands of the transaction, ensuring that it is easy to understand;

- Dexterity – the requirements of dexterity of the transaction (ICTSB Project Team 2000).

There has been a rolling programme of development for user requirement standards, promoting the Design for All concept.

User Requirements (TB8)

TB8 of eEurope Smart Cards aims to:

- Ensure that consumer needs are met by user interfaces and smart card based systems.
- Develop and promote systems that are both attractive to users and socially inclusive.
- Contribute to enhancing consumer trust and confidence in smart cards and facilitate usage.
- Liaise with external bodies (e.g. data protection bodies) and establish their concerns within the e-Europe Smart Card Initiative.

A principle outcome of this trailblazer will be a 'User Requirements Best Practice Manual' (to be produced at the end of 2002) that aims to inform the design of smart card solutions, enhancing the user-friendliness of interfaces and applications. This best practice manual aims to:

- Heighten awareness of user requirements;
- Promote European interoperability;
- Promote consistency between devices;
- Promote an intuitive interface;
- Facilitate compliance with relevant standards;
- Enhance compatibility;
- Enable the consumer.

User Behaviour Model

Smart card system design also needs to understand the practical issues of using a smart card in everyday life, and in recognition of this Trailblazer 8 (eEurope Smart Cards 2002) recommends that during system design the user is defined as a:

> ***human lazy learning machine, a non-rational signal processor orientated towards action.***

The non-rational element emphasises that when users interact with technology there may be aspects of fear, rejection, goodwill and desire that influence attitudes and behaviour towards that technology. Allowing for 'laziness' indicates the need for consistency in operation, reduction in information overload (promoting intuitive interfaces), familiarity, natural sequence and avoiding misleading users. Trailblazer 8 (eEurope Smart Cards 2002) also emphasises the need to:

- Provide short cuts for heavy users to prevent boredom;
- Allow for mistakes being made and provide recovery procedures;
- Attract attention of users when something important is going on;

- Ensure that during long delays in processing users are not led to believe that they have made a mistake.

Common actions and concerns for users when using a smart card need to be considered within system design (eEurope Smart Cards 2002):

- Getting started;
- Aborting a transaction;
- Repeating a transaction;
- Finding help;
- Dealing with a re-entry;
- Updating data in a system;
- Level of privacy;
- Short cuts for repeat users.

Links to Initiatives

Trailblazer 8 is linked to a number of European Initiatives.

SATURN

Technological advances in information and communication technologies can both help and hinder the elderly and disabled population. Whilst the needs of such groups have long been neglected, this is being redressed by projects such as SATURN (Gill 1996). The SATURN project studies the needs of disabled and elderly people in relation to smart card systems (Gill 1996). Its principle aims are to:

- Identify needs of disabled and elderly users in relation to smart cards;
- Examine technical possibilities and economic constraints;
- Design prototype adapted smart cards and terminals;
- Evaluate systems with a cross-section of disabled and elderly users;
- Prepare appropriate standards and legislation.

Whilst these user groups are positive towards the idea of smart cards, for example they could see the advantage of storing personal emergency medical information on smart cards, SATURN has also identified a number of requirements from smart card systems for this groups of users. Generic issues include:

- The need for a consistent method of operation (e.g. the same keyboard and numerical keys layout);
- The need for more effective instructions in using new technology.

Specific issues include:

- For the physically disabled – the need for contactless smart cards operating as keys for access;
- For the visually disabled – the need for a standard design of input devices, the ability to differentiate cards by touch, card readers to accept cards in the same orientation, keypads to provide tactile keys, contactless smart cards as keys for access, use of smart cards to increase crossing times are pedestrian crossings and increase audible warning signals;

- For the hearing disabled – all public telephones to have a text teleplay facility, where smart cards give access to the keyboard;
- For the intellectually disabled – menus using pictoral and spoken text instead of relying on the ability to read, identification by fingerprint as problems were found with remembering PINs.

Within the financial environment, it was felt that smart cards could revolutionise banking services, which many users within this group currently have problems with. Contactless smart cards that enabled audible location signals and changed the card insertion format were seen as particularly promising. Similarly, smart cards could aid this user groups in telecommunications (by storing user preferences for audio frequency and information display) and public transport (utilising contactless smart cards to change automated ticketing procedures, triggering wheelchair ramps and audio messages about bus destinations) (Gill 1996).

This project has been beneficial in highlighting the importance of the Design for All concept amongst key players in the area (ICTSB Project Team 2000). IT has produced a number of documents, including 'User Requirements for Smart Card Systems' (Balfour 1995).

CEN Information Society Standardisation System Workshop DISTINCT (CEN/ISSS DISTINCT)

Following on from SATURN, this initiative has produced a CWA on coding user requirements on cards to:

- Provide a mechanism for payment between parties providing services for the cardholder;
- Provide a register of requirements that are coded to ensure interoperability (ICTSB Project Team 2000).

CEN Information Society Standardisation System Workshop on User Related Information (CEN/ISS WS URI)

Building on the remit of CEN/ISSS to develop standardisation to promote the success of the information society, this initiative focuses on the user related information (URI) held within smart cards systems. This project is an extension of CWA 13987:2000 Smart Card Systems: Interoperable Citizen Services: User Related Information (based on DISTINCT) which is not sufficient for open, interoperable environments. This extension focuses on standards for multi-application smart cards and the associated management systems for which there are currently no mutually compatible standards (CEN/ISSS 2002). The focus of this workshop will necessarily be technical, but also partly political, attempting to bring interested parties together to promote interoperability.

Specifically, WS URI aims to:

- Promote the development of a smart card handling system that responds in a consistent manner to users whilst supporting specific user requirements;
- Facilitate smart card issuers, service and terminal providers to work together to optimise the use of smart card infrastructures whilst maximising business flexibility;
- Ensure that cardholders can use more terminals to access services.

The URI covered under the standard will include: Language preferences; Interface preferences; Description of mobility needs; Authentication and e-signature elements; Scheme related management information (e.g. card number). The standard will be composed of three parts:

- Part 1: Definition of URI – defines contents of URI to bridge gaps in existing standards and enable business relationships;
- Part 2: Implementation Guidelines – how URI may be created, changed and accessed;
- Part 3: Guidelines for Creating, Operating and Maintaining an Interoperable Network – describes how URI might be managed through an environment of collaboration amongst card issuers, service terminal providers and facilitating bodies.

The main focus of work on URI will focus on:

- Evaluation of multi-application smart card products – identifying details, operations and differences between multi-applications smart cards to enable a definition of extended URI;
- Evaluation of card management systems – analysing the capabilities, background, requirements, operations and differences between various smart card management schemes to enable a definition of extended URI.
- Development of the extended URI standard (parts 1, 2 and 3).

European Telecommunications Standards Institute Human Factors Committee (ETSI TC/HF)

Applications are becoming more complex and design of user interfaces is becoming increasingly important; human factors are viewed as the key to successful commercial communication networks. The usability gap in product application is growing through the increasing complexity of products, particularly as the user interface development lagged behind technology innovation (No 2002). This initiative aims to bridge the usability gap by keeping handling abilities in line with increasing system complexity through the evaluation of the capabilities and limitations of all users (including elderly and disabled) in order to make products, systems and services safe, efficient and easy to use. The Human Factors standard will aim to ensure that users familiar with one system can easily learn to use other systems as they are based on the same user-interface concept (No 2002). The User-interface can increase competitive advantage through the promotion of consistent UIs based on a recognised standard because consistency can lead to higher acceptance by users, and standardised functions and operations encourage the exchange of terminals and services and increase market opportunities (No 2002). In addition, UI standards simplify and improve the system design process.

Focusing on the man-machine interface, ease of use is seen as a key factor in the commercial of telecommunications products. TCHF standards aim to enhance ease of use by establishing

- Standards for basic components of user dialogue (e.g. command and keyboard layout);
- User guidance and presentation of instructions;
- Symbols, pictograms and other notations;

- Experimental evaluation of UI standards.

TCHF is concerned with:

- User Interfaces on the Internet;
- Mobile Communications (e.g. Universal Personal Telecommunications);
- Multimedia and Videotelephony;
- User Interfaces for Network Management;
- Numbering, Addressing and Service Codes.

TCHF produces standards, guidelines and reports detailing the requisite criteria for widespread accessibility for information technology access (ETSI 2002). Five standards are currently being developed within the telecommunications area:

- STF180 Standards for Universal Communication Identification Solutions
- STF 181 Requirements of Assistive Technology Devices in ICT
- STF182 Speech Recognition – Voice User Interfaces, Generic User Command, Control and Editing Vocabulary for ICT Products and Services: Main European Languages
- STF 183 Study on Multimodality of Icons, Symbols and Pictograms
- STF184 Design for All: Guidelines for ICT Products and Services.

The Human Factors initiative is concerned with promoting the 'Design for All' concept, making products and services usable by everybody. In cases where it is not possible to 'Design for All' through cost and pragmatic considerations then 'assistive technologies' need to be developed. The Design for All standard is of particular relevance to this section on consumer issues. The concept of this standard is that products are designed so that the widest range of people have access to them regardless of disabilities and can use such products in a safe and convenient way. The 'Guidelines to address the needs of older persons and people with disabilities when developing standards' (CEN/CENELEC Guide 6) document has already been produced.

ANEC ICT Working Group

The ANEC is the European Consumer Voice in Standardisation and through the Information and Communication Technologies (ICT) working group has identified consumer requirements that should be considered as standard in system design (ANEC 2002). Generic consumer requirements include: Ease of use; Functionality of Solution; Interoperability; Design for All.

Specific consumer requirements for smart cards include:

- Direct consumer involvement in smart card standardisation;
- Interworking between standards;
- Customisable smart cards;
- Security of confidential information;
- Consumer access to information stored on card/terminal or database and modification of information by users;
- Privacy;

- Security;
- Standard procedures for redress;
- Legal issues;
- Cost transparency;
- User interface standards;
- Information retrieval and identification.

CEN TC 224 Machine Readable Cards, Related Device Interfaces and Operations

This initiative is concerned with the development of standards for cards, related devices and operations with a special emphasis on smart cards and inter-industry standardisation in order to promote a high level of commercial interoperability (CEN 2000). CEN TC 224 is related to a number of trailblazers through specific working groups. Working Group 6 focusing on man-machine interfaces is relevant to TB8 as it is specifically focused on producing standards in relation to user requirements. It has produced a four-part standard – EN 1332 – which aims to increase the accessibility of services through achieving a high level of interoperability of smart cards within a user-friendly framework:

- Part 1 – User Interface dialogue design specifications;
- Part 2 – Tactile Identifier;
- Part 3 - Keypads;
- Part 4 – Coding of Special User Requirements (ICTSB Project Team 2000).

WG6 also addresses the:

- Physical access to card reading devices;
- Differentiating Plastic Cards by Touch;
- A supplement to EN 1332-1 concerning icons, symbols and pictograms (ICTSB Project Team 2000).

There seems to be a major problem with the issue of a tactile identifier on cards, principally the problem with lamination when using tactile identifiers and this issue needs to be resolved (ICTSB Project Team 2000).

DELTASENTERET (DELTA Centre)

Is a Norwegian initiative, composed of a National Resource Centre for Participation by and Accessibility for People with Disabilities. The main activity of this group is based around:

- Identifying how assistive technologies and facilitation of the environment can increase participation by the disabled;
- Promoting the Internet for All.

This project has produced ‘Self service for everyone? – Guidelines for the procurement and installation of self-service systems to meet a Design for All Approach’ (2000).

Enhancing Public Services

eEurope Smart Cards aim to enhance the quality of life of EU citizens through the modernisation of key public services, particularly, public transport, government services and health services. The smart card will play a key role in modernising services and three key trailblazers have been formed to accelerate the development of smart card services within public services.

Public Transport (TB9)

To promote access to public transport systems through the use of smart cards as an 'access token'. Consequently to promote the interoperability of European transport ticketing services, social inclusion, consistency of user experience and develop a best practice business model for operators.

Interoperable ticketing schemes have been addressed by 4th Framework and IT for mobility projects – CALYPSO and SIROCCO and by current IST projects – TRIANGLE and TELEPAY. A number of CEN workshops have been devised to develop standards for interoperable e-ticketing systems, namely CEN TC 224/WG11 (smart-card applications) and CEN TC 278/WG3 (back office and systemic aspects).

Link to Initiatives TB9 is linked to a number of initiatives.

Integrated Transport Smart Card Organisation (ITSO)

This UK-based forum, established in 1998, aims to facilitate members deliver integrated public transport and develop and manage technological specifications for interoperable multi-modal public transport (ITSO 2002).

In order to achieve this ITSO provides:

- A forum for members to create and improve interoperable smart card specifications;
- Public Transport Industry and suppliers with a certification process that ensures conformity with the specification;
- Support for promote the use of the specification;
- Passengers with a recognised trusted symbol to make interoperable products easily recognisable and usable by them (ITSO 2002);

The ITSO specification of 2000 provides a clear definition of the technology and operational issues involved in the use of smart cards in this field.

CALYPSO

CALYPSO (Contact and Contactless Environment Yielding a Citizen Pass Integration Urban Services and Financial Operations) was launched in 1998 and involves four cities – Constance, Lisbon, Paris & Venice. It builds on the ICARE project (Integration of Contactless Technology into Public Transport Environment) and works closely with CLUB (set up by ICARE partners). CALYPSO aims to efficiently integrate city services through the use of smart cards, simplifying access procedures whilst addressing the need for increasing access to information and services (De Maria 1999). The CALYPSO City Pass is a multi-function card that combines banking, ticket office, public transport, parking, library and museum services amongst others. CALYPSO is widely tested and validated multi-application card that complies with International

standards (FranceTech 2001). There are now 8 manufacturers that produce compatible equipment: ASCOM-MONETEL, ASK, DASSAULT, INTEC, SAGEM SCHLUMBERGER, ST Microelectronics and VERON.

CALPYSO had to solve a number of issues:

- The involvement of multiple players, not only introduced the problem of compliance with a diverse range of standards, but also each player brought their own 'level of resistance' relating to the problem of brand/image erosion that could result from a poor trial of the card;
- Consumer needs directed technical choices, but the diverse nature of needs meant that this was difficult to accommodate. The need to keep up-to-date with the latest technology had to be tempered against the growing costs;
- In planning the system the sharing of profits had to be addressed (De Maria 1999).

CALYPSO has designed and validated a range of compatible solutions now in use in 30 cities.

Constance - Transport Operators Landkreis Konstanz in partnership with DSGV (banking institution that issued Geld Karte – a German bank card and e-purse) developed and tested a combination bankcard with a case (Flexplus) that had an embedded antenna for contactless communication. The test indicated that a combined ticketing and banking card was a valid concept. The next step is to draw up specifications for a new bankcard used as an e-purse for public transport.

Lisbon - OTLIS (a transport operators federation) and SIBS bank (who introduced the Portuguese Multibanco e-Purse PMB) designed and tested a ticketing and e-payment card – URBI. The tests were deemed successful and the URBI card has been universally launched.

Paris - From 1997 to 1999 a number of tests were conducted in teleticketing in the Ile-de-France region, combining e-purse with ticketing and other services. In trials consumers were described as being impressed with the card and results indicated that the contactless debit concept was valid.

Venice - Transport and other service operators worked with the Italian bank TSP (who introduced the Minipay e-purse) to develop and test an Urban Pass – Carta Venezia – integrating transport, parking, museums, churches and universities. In addition, this project also created a service centre to manages the card and services on offer. The card was successful and is now in general circulation.

Brussels - In their role as observer, they guaranteed the project findings would be transferable. STIB also studied how to integrate the CALYPSO card with the e-purse card introduced by Belgium banks (PROTON Card).

The CALYPSO project also fostered the contactless standard ISO 14443/B. The CALYPSO partners have set up two streams of research to focus on multi-site interoperability: TRIANGLE and COSMIC.

- CEN/ISSS TRIANGLE Workshop - This workshop focuses on the issues of interoperability in multi-application smart cards schemes that relate to the mobility of users. For example, transport schemes that utilise contactless smart cards combining e-purse, credit and debit functions. The CEN/ISSS Workshop C-Ecom – Cluster for E-commerce - supports this project

- COSMIC - This is a working network set up to define a communication standard between contactless terminals and central systems.

FASTEST

FASTEST (Facilitating Smart Card Technology for Electronic Ticketing and Seamless Travel) is a CEN/ISSS Workshop designed to provide a channel for TB9 to identify and define common user requirements and the technical/business processes upon which an interoperable e-ticketing system can be built, as well as provide a platform for validating the emerging standards for such a system (FASTEST 2002). The aim of the workshop is to provide guidelines that encourage and facilitate ease of use of access tokens (smart cards) in public transport across Europe, in addition to producing guidelines to support public transport service providers to incorporate an interoperable transport system.

The FASTEST workshop established that customers and suppliers have different perspectives in relation to mobility services. Intermobility – the consumer requirement to have the ability to use different modes of transport run by different operators – needs to be supported by a mobility network on three levels (Wrathall 2002a):

- Home network – Interoperability between local, common fare area suppliers
- Unified Network – 2+ fare areas share a set of products or have a cross selling agreement
- Unified European Mobility Network – Several fare areas across Europe share a set of fare products or have a cross selling agreement.
- Interoperability – the service provider requirement for systems across providers to be interoperable – is supported by interoperable fare products/systems, requiring compatible medium and software, applications accepted by terminal and fare products valid across networks. Payment operability enhances such a system, where card readers must be able to read any smart card and write to specific tickets on smart cards (Wrathall 2002a). Interoperability between suppliers necessarily requires co-operation between these organisations as defined by appropriate contracts that give consideration to (Wrathall 200b):
- Ownership model (transport operator, service provider, joint)
- System architecture (fare payment system, distribution system, clearing house system)
- Administrative Functions
- Customer Service Functions
- Legal, finical and technical barriers.

Wrathall (2002c) also stresses that the customer focus is on the provision of good service, not whether that service is based on smart card technology; such a perspective is vital to understand in designing new services. The general requirements of mobility customers are (Wrathall 2002c):

- Uniformity of procedures
- Service management at interchange points

- Quality of transport infrastructures
- Quality of new ticketing systems
- Integrated approach to intermodality
- Customer service quality.

However, the smart card can underpin good service, in the transport scenario basic functions enhanced by smart cards include (Wrathall 2002c):

- Travel Information – can be contained on cards
- Acquiring Travel Rights – not only can tickets and travel 'values' be stored on cards but also details of booking in a single, convenient and secure card. Smart cards also extend access for diverse services
- Taking Trip – timetable details, connections and other related information can be made available on cards
- Customer Service – can be enhanced by retrieving information about customer from cards and using as a basis for service. Smart cards can enable better service management by suppliers through appropriate data collection.

SIROCCO

SIROCCO forms part of the EC's ESPRIT programme. Based in Spain the project has developed a new smart card that combines a travel pass for the public transport system and an e-purse facility. The cards could be used to purchase tickets, small quantities in kiosks, stores and cafes located in the stations, enter station parking lots, access travel information at ATMs and use public telephones located in the station. The card also utilised contactless technology enabling it to be used at a distance (passing card in front of receptor screen) and as such addresses some of the needs of people with disabilities. During this pilot scheme 10,000 cards were distributed.

The proposed benefits of the card are:

- For the user – a simplification of transactions, speeding up processing and thoroughfare, no need to carry cash and increased consumer satisfaction;
- For the merchant – the deliver of better service quality and a streamlining of services.

CEN TC 224 Machine Readable Cards, Related Device Interfaces and Operations

This initiative is concerned with the development of standards for cards, related devices and operations with a special emphasis on smart cards and inter-industry standardisation in order to promote a high level of commercial interoperability (CEN 2000). CEN TC 224 is related to a number of trailblazers through specific working groups. Working Group 11 focusing on surface transport applications is relevant to TB9.

e-Government (TB10)

This trailblazer aims to:

- Develop a European model for Public Administrators interface utilising smart card technology, in order to promote better access to and more effective use of government's services, simplifying on-line administrative procedures.
- Develop appropriate policy, define system architecture and requirements for such systems.

This trailblazer is linked to the PEALS project.

Piloting Electronic Access to Local Services (PEALS)

PEALS is a major initiative to modernise local government services. Under PEALS there are 20 micro projects evaluating the delivery of e-government services across 5 key themes: Democratic Connections; Strategic Information; ICT Services; Content Development; Local Community (PEALS 2002).

Amongst these 20 micro projects the PEALS Resident User Card Project is particularly relevant to this report. Smart cards are utilised to give residents access to services or facilities that they are entitled to or have made a prepayment for (PEALS 2002). There are two key piloting areas:

- Dalaston Community School – All students are issued with a smart card, upon which merit system points are recorded directly. Students can then redeem these points for rewards offered to them;
- Moxley and Dalaston Local Committee Areas – Cards are offered to all residents in these two areas to access local services. They gain reward points for using the cards, which can be redeemed in local facilities (e.g. leisure centres and libraries). A number of commercial organisations have also become involved in order to offer a broader range of rewards to users of the card.

Health (TB11)

This trailblazer aims to contribute to the development of a European wide interoperability of healthcare cards and associated Internet usage, incorporating an ID card, signature card and health card (potentially as a three-in-one card).

This project is trailblazer is linked to the TESS programme.

Telematics in Social Security (TESS) Programme

The TESS programme aims:

- To replace the conventional paper-based exchange of data by electronic transfer in order to improve service quality by accelerating the administration for access to rights and social security payments for migrant workers;
- To put in place a generic, secure and stable telecommunications network for the exchange of data between the administrations of member states.

Thus the TESS programme aims to utilise information systems to develop a more modern social security process.

Conclusion

Smart cards represent a core enabling technology for the advancement of transactional systems within Europe, with the ability to enhance transactional security, to underpin consumer confidence in such transactions, and, increase convenience and mobility for the consumer. This report discussed European trends in addressing the key elements in smart card development. The eEurope Smart Cards Initiative has focused on:

1) The need for a legislative framework ensuring the smooth operation and management of smart card schemes across Europe;
2) The development of standards and certification processes to promote interoperability amongst smart card schemes, working towards a consensus amongst interested parties about the key directions for smart card development. The main foci of which are identification processes, multi-application cards, a generic card reader and contactless technology;
3) The development of proactive business strategic plans to promote the success of electronic and mobile commerce, including the promotion of an atmosphere of 'co-competition';
4) Gaining a better understanding of the consumer issues that affect adoption of smart card innovations (including relative advantage, compatibility and user perceptions of power and privacy, security and trust) and the specific user requirements for the user-system interface;
5) Development of ways forward for enhancing public services utilising smart card technology.

The eEurope Smart Card Initiative will make a significant contribution to the advancement of smart card development, addressing many major barriers. 2003 will be an exciting year in smart card development, as it will mark the publication of the results from this two-year programme, representing a major step forward in the development of smart card technology. The challenge will be to combine the emergent research and development strands into a coherent whole that will inform the next generation of smart card innovations and facilitate electronic and mobile commerce. These exciting developments will take place within a dynamic environment characterised by increasing demands from consumers, merchants and financial institutions with regard to faster, more efficient services; where it is envisaged that interactive TV with chip card reader for set top boxes, PCs with chip card readers and dual-chip/two-slot mobile phones will be commonplace (Jones 1999).

Following the culmination of the eEurope Smart Cards two-year plan, EUROSMART RESET (September 2002) will act as a 'roadmap project' to investigate future research needs for smart card technology focusing on communication and network protocols, systems and software, interface technologies, peripherals, subsystems and microsystems, high end cryptography, tamper-proof and security technologies, microelectronics. This project will be a valuable source of information regarding smart card development over the next few years.

References

ANEC (2002) ANEC European Consumer Voice in Standardisation. http://www.anec.org

Ankri D (1999) Accelerating Smart Card System Developments in Europe: Smart-IS Action Program, Strategy Paper. http://europa.eu.int/ISOP/fiwg/archives/wg3/strategy_pape_ankri.htm

Antonides G, Amesz HB, Hulscher IC (1999) Adoption of Payment Systems in Ten Countries – A Case Study of Diffusion of Innovations, European Journal of Marketing, 33(11/12), 1123-1135

APACS (2002) APCAS. http://www.apacs.org.uk/

Barczak G, Ellen PS & Pilling BK (1997) Developing Typologies of Consumer Motives for Use of Technologically Based Banking Services

Beckett P (1998) Smart Card Still Needs More Answers Sponsors Conceded as Big Test Nears End, Wall Street Journal, 4 Nov, A4

Bohle K & Krueger M (2002) Payment Culture Matters: A Comparative EU-US Perspective on Internet Payments. JRC Institute for Prospective Technological Studies, Seville

Borman C (1996) Smarten Up your Act, Computer Weekly, October 3, 18-20

Boston Consulting Group (BCG) (1999) Winning the Online Consumer: Insights into Online Consumer Behaviour, BCG: Boston

Bruno M (2001) Biometrics are too hot to handle despite high hopes, bankers are still all talk when it comes to identification technology. Bank Technology News, 14, 9

Buck SP (1996) Electronic Commerce – Would, Could and Should you use Current Internet Payment Mechanisms? Internet Research: Electronic Networking Applications and Policy, 6(2/3), 5-18

CAFÉ (2002) CAFÉ – Conditional Access For Europe. http://www.semper.org/sirene/projects/café/

CB (2002) Press Releases: EMV: A New International Standard for Chip Cards. http://www.gie-cartes-bancaires.fr/GB/Pages/communique/Com070202.htm

CEN (2000) Market Environment Objectives of CEN/TC 224 Machine Readable Cards, Related Device Interfaces and Operations. CEN: Brussels

CEN/ISSS (2001) Workshop Agreement EESSI Conformity Assessment Guidance Part 1: General, CWA 14172-1. CEN: Brussels

CEN/ISSS (2002) CEN/ISSS User-Related Information. http://www.cenorm.be/isss/worshop/URI/default.htm

Centeno C (2002) Building Security and Consumer Trust in Internet Payments – The Potential of ''Soft'' Measures, Background Paper No. 7. ePSO: Spain

Choi S-Y & Whinston AB (1998) Smart Cards: Enabling Smart Commerce in the Digital Age. KPMG & University of Texas at Austin

Clarke R (1997) Smart cards in banking and finance. The Australian Banker 111, 2

Clemons EK, Croson DC & Weber BW (1997) Reengineering Money: the Mondex Stored-Value Card and Beyond, International Journal of Electronic Commerce, 1(2), 5-31

CLUB (2002) CLUB On-Line. http://www.contactless-club.com/

Ctt (2000) Cyber-Comm Set to Get consumers to Buy on the Web, Ctt, November/December

Commission of the European Communities (1989) Commerce and Distribution: New Technologies in Commerce: The Potential and the Cost, Final Report. Commission of the European Communities: Luxembourg

Cyber-Comm (2002) Cyber-Comm. http://www.cyber-comm.com/

Davis FD (1989) Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology, MIS Quarterly, 13(3), 319-340

Davies FD (1993) User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioural Impacts, International Journal of Man-Machine Studies, 38, 475-487

De Maria M (1999) CALYPSO – A Smart Card for Simplifying the City Life

Deogun N (1996) The Smart Money is on Smart Cards but Electronic Cash Seems Dumb to Some, Wall Street Journal, 5 Aug, B1

Dutrieux M (1999) The European Digital Money Picture: Europay's Role and Strategy in Developing the Market, European Business Review, 99(4), 222-227

EEMA (2002) The European Forum for Electronic Business. http://www.eema.org/

eEurope Smart Cards (1999) Common Criteria for IT Security Evaluation: Part 1 Introduction and General Model (version 2.1), eEurope Smart Cards

eEurope (2000a) An Information Society for All: Smart Cards for Secure Electronic Access: the Smart Card Charter. eEurope

eEurope (2000b) eEurope Action Plan. eEurope

eEurope (2000c) Communication on a Commission Initiative for the Special European Council of Lisbon. eEurope

eEurope Smart Cards (2001) Common Requirements. eEurope Smart Cards

eEurope Smart Cards (2002) Trailblazer 8 WP1: Input Specification of the TB8 User Requirements Best Practice Manual

EMV (2002) EMV CO. http://www.emvco.com/

ePSO (2002) e-Payment Systems Observatory. http://epso.jrc.eu/

ETF (1999) Privacy, Convenience Key to Smart Card Acceptance, ETF Report, June 16, 22, 2

ETSI (2002) ETSI Telecom Standards. http://www.etsi.org

ETSI M-Commerce (2002) ETSI M-Commerce. http://www.portal.etsi.org/m-comm/summary.asp

ETSI SCP (2002) ETSI Smart Card Platform. http://www.portal.etsi.org/scp/summary.asp

European Community (2001) Network and Information Security: Proposal for a European Policy Approach. Commission of the European Community

European Commission (2002) eEurope Benchmarking Report 2002. Commission of the European Community

EUROSMART (2002) Eurosmart Current Events. http://www.eurosmart.com/D-Activities/D1-Current.htm

FASTEST (2002) Facilitating Smart Card Technology for Electronic Ticketing and Seamless Travel. http://www.nen.nl/wsfastest/

FINREAD (2002) Europe Unites to Provide e-Business Security. http://www.finread.com/index.php

Gill J (Ed) (1996) Smart Cards Interfaces for People with Disabilities. Royal National Institute for the Blind. http://trace.wisc.edu/docs/smartcards/schome.htm

Global Platform (2002) About Us. http://www.globalplatform.org/aboutus.asp

GMCIG (2002) Global Mobile Commerce Interoperability Group. http://www.gmcig.com/

Greenberg P (2001) Nasty Return Policies Damage e-Shopper Relationships, E-commerce Times, 24 April. http://www.ecommercetimes.com

Hermida A (2002) Smart Cards Head for Hong Kong, http://news.bbc.co.uk/1/hi/sci/tech/1919616.stm

Krueger M (2001) The Future of M-Payments: business Options and Policy Issues. Background Paper No.2. ePSO: EU. EUR 19934 EN

ICT Standards Board (2002) EESSI – European Electronic Signature Standardisation. http://www.ict.etsi.fr/eessi/eessi-homepage.htm

IETF (2002) Internet Engineering Task Force. http://www.ietf.org/home.html

ICTSB Project Team (2000) Smart Cards. Chapter 12 in Design for All Final Background Report

ITSO (2002) Integrated Transport Smart Card Organisation. http://www.itso.org.uk/index.asp

Java Card Forum (2002) The Java Card Forum. http://www.javacardforum.com/

Jennings P & Holzer M (2001) There's No Big Brother Here, the Source Public Management Journal. http://www.sourceuk.net/articles/a02085.html

Jones T (1999) The Future of Digital Money, European Business Review, 99(4), 261-264

Kolsaker A & Payne C (2002) Engendering Trust in E-Commerce: A Study of Gender-Based Concerns, Marketing Intelligence & Planning, 20(4), 206-214

Labady DG & Kinner TC (1981) Exploring the Consumer Decision Process in the Adoption of Solar Energy Systems, Journal of Consumer Research, 8(3), 271-278

Lareau P (2002) PKI Basics – A Business Perspective, PKI Note Series, PKI Forum

Lefebvre PJ (1999) Digital Money – A View from the European Commission, European Business Review, 99(4), 242-256

Lloyd S (Ed) (2001) PKI Interoperability, White Paper, PKI Forum

Longo E & Stapleton J (2002) PKI Note: Smart Cards, PKI Note Series, PKI Forum

Massot V (2002) TB6 Report: Interoperability, eEurope Smart Cards

MEDEA+ (2002) MEDEA+ System Innovation on Silicon. http://medeaplus.net/

MET (2001a) MET Overview White Paper, Version 2.0: The Met Initiative – Enabling Mobile E-Commerce. MET

MET (2001b) MET Core Specification, Version 1.0. MET

MET (2001c) MET WAP Banking, Version A: Usage Scenario. MET

MET (2002) Mobile Electronic Transactions. http://www.mobiletransactions.org/

Mobey Forum (2000) Mobile Financial Services Trust Infrastructure and Payment Services for Mobile Commerce: White Paper, The Mobey Forum

Mobey Forum (2002) The Mobey Forum. http://www.moberyforum.org/

Mondex International (2002) Mondex. http://www.mondex.com/

Monge PR, Cozzens MD & Contractor NS (1992) Communication and motivational predictors of the dynamics of organisational innovation, Organisational Science 3(2), pp. 250-276

Moore GC & Benbasat I (1991) Development of An Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, Information Systems Research, 2(3), 192-222

Mulvey MS, Olson JC, Celsi RL & Walker BA (1994) Exploring the Relationships Between Means-End Knowledge and Involvement, Advanced Consumer Research, 21, 51-57

MULTOS (2002) MULTOS. http://www.multos.com/

No W (2002) Human Factors Involvement in Standardisation of User Interface. http://www.etsi.org/literature/aa-oldtokeep/stateart/noe.htm

Open Mobile Alliance (2002) The Open Mobile Alliance http://www.wapforum.org/

PEALS (2002) Piloting Electronic Access to Local Services. http://www.walsall.gov.uk/peals/projects.asp

Petri S (2002) An Introduction to Smart Cards. http://www.sspsolutions.com/solutions/whitepapers/introduction_to_smartcards

PC/SC Workgroup (2002) PC/SC Workgroup. http://www.pcscworkgroup.com/

PKI Forum (2002) The Public Key Infrastructure Forum. http://www.pkiforum.org/

Plouffe CR, Vandenbosch M & Hulland J (2000) Why Smart Cards Failed: Looking to Consumer and Merchant Reactions to a New Payment Technology, International Journal of Bank Marketing, 18(3), 112-123

Plouffe CR, Vandenbosch M & Hulland J (2001a) Intermediating Technologies and Multi-Group Adoption: A Comparison of Consumer and Merchant Adoption Intentions Towards a New Electronic Payment System, Journal of Product Innovation Management, 18, 65-81

Plouffe CR, Hulland JS & Vandenbosch (2001b) Research Report: Richness Versus Parsimony in Modeling Technology Adoption Decisions – Understanding Merchant Adoption of a Smart Card-Based Payment System, Information Systems Research, 12(2), 208-222

Puri V (1997) Smart Cards – The Smart Way for the Banks to Go? International Journal of Bank Marketing, 15(4), 134-139

Card News (1999) Customers are willing to Pay for Smart Cards, Card News, May 5, 14, 9

Lannerstrom S, Bezuidenhoudt J & Claasen G (2000) Choosing a Smart Card for Secure Wireless E-commerce (Version 1.01). Radicchio White Paper

Radicchio (2002) Welcome to Radicchio. http://www.Radicchio.org/

Rogers EM (1995) Diffusion of Innovations (4th Edition). Free Press: New York

Schneider I (2001) Rabobank Makes Calculated Move to Smart Cards, Bank Tech, Dec 7. http://www/banktech.com/story/technologyLeaders/BNK20011207S0021

Schule U, Kulak T, Schmidt J & Kubo T (2002) Mobile Payment Business Requirements (version 2.0): Final Report, European Commission.

SCSUG (2002) Smart Cards and the CC. http://csrc.nist.gov/cc/sc/scllist.htm

Shurmer M (1993) An Investigation Into Sources of Network Externalities in the Packaged PC Software Market, Information Economics and Policy, 5, 231-251

SIBS (2002) SIBS. http://www.sibs.pt/en/sibs/sibs.html

Simpson B (2002) The Public Sector Takes the Lead, Credit Card Management, February 14, 12

SmartCities (2002) SmartCities. http://www.smartcities.co.uk/

SMART.IS (2002) SMART.IS AM Working Groups News, SMART.IS

STIP (2002) STIP. http://www.stip.org/

Svigals J (2000) Get Smart, Credit Union Management, January 23, 1

Tornatzky LG & Klein KY (1982) Innovation Characteristics and Innovation Adoption-Implementation: A Meta-Analysis of Findings, IEEE Transactions on Engineering Management, 29(1), 28-45

Truman GE, Sandoe K & Rifkin T (2002) An Empirical Study of Smart Card Technology, Information and Management 2004, 1-15

Van Arkel R J (2000) Report on the Smart Card Summit, 10-11 April, Lisbon

Van Arkel RJ & Papaspyrou S (2000) First Follow Up Meeting, Athens

Vandore S (1999) Fantastic Plastic, Australian Personal Computer, 20(9), 72-78

Van Schaik P (1999) Involving Users in the Specification of Functionality Using Scenarios and Model-Based Evaluation, Behaviour and Information Technology, 18(6), 455-466

Walsh G & Berger G (2000) Alternative Payment Methods: A White Paper, DCTI e-Payment Services

West MA (1990) The social psychology of innovation in groups. In West MA and Farr JL (Eds) Innovation and Creativity at Work Chapter 15. Wiley and Sons, Chichester, UK.

Worthington S (1998) The Card Centric Distribution of Financial Services: A Comparison of Japan and the UK, International Journal of Bank Marketing, 16(5), 211-220

Wrathall C (2002a) Implications of Levels of Interoperability on User Requirements. CEN/ISSS

Wrathall C (2002b) Catalogue of Technical and business Procedures. CEN/ISSS

Wrathall C (2002c) Europe Wide Essential User Requirements. CEN/ISSS