# E-Commerce Applications of Smart Cards

[Published in *Computer Nerworks* **36**(4):453–472, 2001.]

David M'Raïhi[1] and Moti Yung[2]

[1] Gemplus USA
3 Lagoon Drive, Suite 300, Redwood City, CA 94065-1566, USA
[2] CertCo Inc.
55 Broad Street, Suite 22, New York, NY 10004, USA

**Abstract.** Smart cards (also called chip cards or IC-cards) are portable modest computing devices with programmable data store and certain tamper-resistance capabilities. They are embedded in a plastic card that looks like a traditional magnetic stripe credit-card. We review the state of the art of e-commerce applications of smart cards.

## 1 Introduction

Smart cards typically provide a cryptographic token, and their design and development in the last few years have been influenced by development of e-commerce. On the other hand, developments in e-commerce and related technologies (e.g., the language Java) also affected trends in smart card design, assuring that card architectures are based on the growing demands and needs of e-commerce users.

Note that smart cards have the tremendous advantage, over their magnetic stripe ancestors, of being able to execute cryptographic algorithms locally in their internal circuitry. This means that the user's secrets (be these PIN codes or keys) never have to leave the boundaries of the tamper-resistant silicon chip, thus bringing maximum security to the overall system in which the cards participate.

Smart cards contain special-purpose micro-controllers with built-in self-programmable memory and tamper-resistant features intended to make the cost of a malevolent attack on them far superior to their benefits.

While smart cards have been around for about 20 years, over the last four years there has been an increasing demand for public-key smart cards from government administrations and large companies such as telephone operators, banks and insurance corporations. More recently, another market opened up with the increasing popularity of home networking and the usage of the Internet which implies increase of e-commerce amongst stationary parties. Finally, the mobile wireless infrastructure is rapidly growing enabling further applications and commercial activities even between roaming parties.

In this issue, other works cover the basic notion of smart cards and how it can provide security compared to existing alternatives. Also, various software and hardware developments, as well as various platforms (API's) are presented

in other works. In this work, we will concentrate on applications of smart card to basic Internet and mobile infrastructure and e-commerce applications. Since e-commerce has been and will be a major economic drive which motivates new applications for security, and since smart card is an essential tool for increased security, the area is very active, and promising. We concentrate on concrete existing applications to PKI, payments and telecommunication applications (necessary to support mobile commerce), as well as properties of card architectures and how they support e-commerce needs.

We note that we cover mainly the current state of the art together with some remarks on potential future developments. We do not present much of the current extensive cryptographic research activities. These activities are geared towards future applications of smart cards (typically presented in the conference series of CARDIS and that of Financial Cryptography). Nevertheless, we remark that these research activities together with future technology advances will be paramount to future development in the field. Finally, it is natural that we concentrate on issues and aspects that we are familiar with; though we try to give extensive coverage of some areas and recent issues of this fast-moving field. Familiarity with basic cryptographic functions (RSA, DSA, ECC, DES, SHA, etc.) is assumed (see [7]).

More specifically, in section 2 we describe PKI applications and introduce various products implementing public-key cryptography features. Section 3 is devoted to payment applications, including electronic purse applications and credit cards. Eventually, section 4 gives an overview of mobile applications, elaborating on different smart-card based solutions available today. A glossary can be found at the end of this work for further references and definitions of technical terms.

## 2 Public Key Infrastructure Applications

Over the past several years, global networks (the Internet in particular) have transformed from a way for scientists and researchers around the world to share ideas and information to an increasingly effective way for businesses, financial institutions and government organizations to communicate and engage in commercial activities. Today we stand at a dawn of a new era of electronic commerce, one that will enable these organizations to move from simply establishing a network presence into sharing sensitive information and conducting business transactions with customers, contractors and business partners. To assure this transformation, it is be necessary for all parties involved to reach the same level of trust in electronic transactions that they have built up over years of doing business face-to-face in the physical world.

Public Key Infrastructure (PKI) and Digital certificates were created to overcome the general lack of presence and entity anonymity which typify insecure networks like the Internet. Such certificates provide a reliable and trustworthy proof of identity in much the same way as passports and driver licenses. Used in conjunction with web browsers, email software and other applications, digital certificates (and the public key technology they are based on) possess the po-

tential for ensure secure electronic commerce and similar transactions over these networks.

Once PKI is available trusted digital signature is made possible as well as secure communications. A trusted electronic signature is critical as paper documents such as purchase orders, checks and contracts are increasingly replaced by their electronic counterparts. The digital signature is a vital component of many applications such as e-commerce, home-banking, intranet, identity, health care, physical access control services.

Software systems are sensitive to various attacks like Trojan horses and viruses which can be activated remotely. Thus, like a passport without a photograph attached, a digital certificate stored in the usual manner on a PC hard drive is susceptible to compromise and fraudulent use. Before certificates can be widely accepted as a highly trusted proof of identity, a way must be found to protect them. Smart cards offer this protection by securely locking the digital certificates in a secure, removable medium, and making them inaccessible to anyone but their rightful owner. Without knowledge of this critical information, would-be hackers and thieves are unable to usurp the rightful owner identity and use it to gain access to secure information or conduct transactions.

We will review the difficulties and the smart card solutions in this area.

### 2.1 Passwords Make Poor Identifiers

Simple retail transactions pose little threat and personal email communications entail little risk if intercepted (though, lost of privacy is a concern). More sensitive types of personal transactions and most business-to-business transactions pose a much greater risk, especially when conducted over an insecure channel like public networks, and require much greater assurances of authenticity, privacy, integrity and acceptance.

The risks can be huge as organizations face the potential loss of money, intellectual property or customers, as well as the potential for legal consequences. The March 1998 Computer Security Institute/FBI computer Crimes Survey found that 47 percent of the 563 organizations surveyed were attacked via the Internet, and the FBI believes as many as 95 percent of the attacks go undetected. Corporate America spent about $6 billion in 1997 on network security, and financial losses were estimated at $10 billion.

Whether an individual buys or sells stock, or Boeing submits a purchase order to a contractor in Japan, there is a big difference when conducting these transactions in person or using traditional paper documents and when conducting these transactions over networks. Today, the most popular way to establish identity is with a password. While passwords continue to be widely used to identify users, they cannot be relied upon for real proof of identity for many reasons.

Passwords are often sent over networks without any encryption, making them highly susceptible to interception and compromise. Users generally need to remember many passwords, and often end up using the same password for many systems, using easy-to-remember (and easy to crack) passwords, or writing the passwords where they are easily accessible. On the back end, all passwords must

be stored in a single file, and although encrypted, there are numerous cases of these files being stolen and unlocked. Further, these password files are expensive to support and maintain, with much of the expense resulting from users forgetting their passwords. The bottom line is, passwords offer no proof of who is actually using the password.

Passwords have proven to be poor vehicles for ensuring identity, and without firmly establishing who is really at the other end of the wire, it is impossible to control access to sensitive information, ensure the confidentiality of messages, ensure that communications have not been tampered with or provide undeniable proof that a transaction occurred. With passwords there is no way to authenticate documents in a way which is valid in court (namely, achieving non-repudiation), or to resolve disputes.

### 2.2 Digital Certificates to the Rescue

Public key cryptography uses two keys and a series of mathematical formulas to scramble and unscramble digital data of any kind. Whatever one of these keys scrambles, the other one can unscramble. In practice, the "public" key is made readily available while the "private" key is secured and accessible only by the rightful owner of the keys. Someone wishing to send a message that can only be read by the intended recipient will scramble the message using the recipient's public key. When received, only the intended recipient can unscramble the message using their corresponding private key. In addition, the sender can digitally "sign" the message scrambling it with their own private key, an operation which the recipient can confirm using the sender's public key. This proves that the message actually originated with the stated sender, while at the same time ensuring that the message has not been tampered with.

As good as public key cryptography is at securing/ authenticating messages, it alone cannot attest to who is actually presenting any particular public key. In theory, a criminal could present a public key and claim it belongs to the FBI, and lacking any other mechanism for ascertaining identity, there is no way the other party in the transaction can tell the difference. We need a way to associate keys with individuals/ entities.

Digital certificates as part of a Public Key Infrastructure (PKI) solve this problem by attesting to the binding of a public key to the identity of an individual or entity. They allow verification that a public key does, in fact, belong to a specific individual.

The digital certificate is a data file that contains an individual's public key along with other identifying information, including the owner's name, the certificate's serial number and expiration date and possibly other user-supplied information such as a postal address, email address or employer name and address. In addition, the digital certificate contains the name and digital signature of the certification authority (CA) that issued the certificate. The certification authority is a trusted third party, such as a bank, government agency or employer that verifies the identity of the certificate owner before issuing the certificate.

Namely, digital signature is assured by another more familiar digital signature as a rebooting methodology.

Similar to an international passport, most digital certificates today conform to an international standard – the ITU X.509 standard – so they may be used universally. The standard helps ensuring interoperability of digital certificates regardless of issuer, network or application by specifying what information must be contained in the digital certificate and how it is formatted.

Digital certificates are an important component of a larger PKI, which also includes the issuing certification authority, certificate revocation and key management functions. Organizations employ a PKI on their networks to support the use of public key cryptography and digital certificates for authentic (and at times also secure) transmission of sensitive non-repudiated information.

Already, a number of standard protocols, being widely adopted for digital signature (achieving non-repudiation) and public-key encryption (achieving secure communication) within electronic commerce, require the use of digital certificates. Currently the two most popular are the secure sockets layer (SSL) protocol and the secure multipurpose Internet mail extensions (S/MIME) protocol. SSL enables both servers and (potentially also) client browsers to authenticate each other and perform secure data transmission. It is implemented in browsers from Netscape, Microsoft, and others, as well as in most commercial servers. S/MIME ensures that email and EDI messages are kept private and not tampered with, as well as offering non-repudiation.

### 2.3 The Problem with Digital Certificates

With a digital certificate, anyone with access to the private key is assumed to have rightful ownership of the certificate. Thus, while digital certificates can associate an identity with a public key, the digital certificate alone cannot confirm that the individual presenting the certificate as proof of identity is actually the rightful owner.

Consequently, protecting the private key is the single most important aspect of using digital certificates because if the private key becomes known by others, it is possible for them to assume that identity and engage in fraudulent use of the certificate.

Most digital certificates today, and more importantly their associated private keys, are simply encrypted with a password (or a passphrase) and stored on the owner's PC hard disk drive where it may be vulnerable to attack either directly or through the network. The private key is vulnerable to many of the same password-related problems mentioned earlier, and several programs are available to either divert PC files or attack password mechanisms.

As a result, although digital certificates can provide digital authentication, they are not fully secure without strong user authentication. Without strong user authentication, a digital certificate is about as much good as a passport without a photograph of its owner attached. A passport may attest to its owner's identity and be an official document issued by a government agency; but without a photograph, it is impossible for anyone presented with the passport to confirm

whether or not the person presenting the passport is, in fact, the owner. We need to assure (unique) ownership.

### 2.4 The Smart Card Solution

The measures taken to protect the private key must be at least as strong as the security/ authenticity of the messages encrypted/ signed with the key.

Smart cards offer superior protection for private keys because they require not only a password/ PIN (which weaknesses were discussed above), but also "physical possession" of the card, in order to gain use of the private key. This kind of two-factor protection offers significantly stronger security than passwords encrypted software, and ensures that the digital certificate is used only by its rightful, intended owner.

With a smart card, the private key never leaves the card and is completely inaccessible from outside the card. All cryptographic functions requiring use of the private key for secure Internet browser and electronic mail transactions– digital signatures and decryption of the session keys– take place on the smart card by the onboard microprocessor, and only the results are passed back to the host PC.

The smart card itself is not only easy to use and portable but it is also unique and very hard be cloned. Its use is PIN protected, and it becomes completely unusable after a specified number of failed access attempts. The user has fewer passwords to remember and IT departments have fewer problems with lost or stolen passwords. In fact, more than 40 percent of all help desk calls involve resetting passwords for users, and a large organization could significantly reduce its help desk costs.

Some recent organizations like the Identrus bank consortium [5], requires in its rules to host private keys on smart cards. The model of operation is that users who are members of companies registered in a bank, will perform transaction with a representative of another company registered as client in another bank. The infrastructure of banks will mediate the transactions and will manage the exposed risk involved in the transaction to each party. The description of such an infrastructure as an abstract protocol was first given in [2].

Let us discuss security measures that are taken in constructing smart-cards.

Rule number one of security is to gather all the smart card elements into a single chip. If this is not done, the external wires, linking one chip to another, could represent a possible penetration route for illegal access (or use) of the card. ISO standards specify the ability of a card to withstand a given set of mechanical stresses. The size of the chip is consequently limited and imposes constraints (especially on memory and on cryptographic capabilities) which mainly follow from this stress resistance limitation.

Smart-card chips are reliable and most manufacturers guarantee the electrical properties of their chips for ten years or more. ISO standards specify how a card must be protected against mechanical, electrical or chemical threats, but for most existing applications, a card is far obsolete before it becomes damaged. A

known example is the French phone card where the failure rate is less than three per 10,000 pieces.

Nevertheless, as smart card usage extends its scope to more and more sensitive applications, improving the security of the hardware and software becomes critical to a large scale deployment. Most card operating systems standardize security. For instance, ISO 7816-4 standards suggest secure-messaging features for message integrity and authentication, GSM standards specify thoroughly authentication OS-security (A3-A8) and EMV introduced challenge-based authentication framework.

Some specific protections against various attacks are usually implemented, such as:

- Random statistics (s/w): software modules run tests (primitive statistics) on the output of the random-number generator to detect external biasing attempts.
- Filters (s/w): a part of the software is written in EEPROM, so as to "kill" the card in case of U.V. exposure (the executable code disappears with the security bits).
- Timer-polling (s/w): in some cases, response-time measurements allow to detect malevolent terminals.
- Memory matrices Security: matrices control and limit very precisely, which part of the code (RAM, ROM, EEPROM segments) can access which other part.
- Temperature detectors: Low temperature detector (against RAM charge leakage rate) and High temperature detector (against various phenomena).
- VCC Detectors: Low Vcc detectors are due to protect EEPROM writing and the random-number generator whereas High Vcc detectors offer protection against EEPROM erasure and random-number generator manipulations as well.
- Clock Detectors: Fast clock detectors avoid signal jamming and Slow clock detectors avoid step-by-step debug.

Smart card chips also include depassivation detectors, which physical locations are kept secret and changed periodically. Their design is usually hidden and scrambled. Witness cells also protect EEPROM against malevolent or accidental modifications. Eventually, all the buses are scrambled to avoid eavesdropping and filters are added to eliminate signals shorter than 100 ns from I/O, Reset and Clock.

In order to protect not only the smart card but the application as a whole, system designers must also consider additional prevention and detection mechanisms.

Possible prevention mechanisms are:

- Prevent Initial conditions from being valid (e.g. prevent perturbations from entering the IC: filter all signals, shield critical elements).
- Prevent attack requirement from being valid (e.g. limited number of attempts, impose relations between inputs and outputs of the secure token).

– Structure input and output information and limit the freedom of the attacker (e.g. internal counters).

Detection mechanisms can take place at the IC level or the system level:

– Detect an attack in the token such as abnormal modifications of the process (e.g. verify all calculations), the data (e.g. CRC), the environment (e.g. physical detectors).
– Detect an attack in the system including abnormal behavior of tokens (e.g. clones i.e. same identifier at different locations) and abnormal activity pattern (e.g. frequency pattern).

### 2.5 PK-enabled Smart Card Solutions

In this section we review different solutions for implementing public-key cryptography using smart cards. We start with a particular setting (namely, DSA coupons) which assumes no cryptographic capacity on the smart card side (this will be our example on how cryptographic operations, at times, need to be modified in a card environment). Then, some of the most recent products rom various smart card manufacturers are introduced (demonstrating that regular cryptography can now be applied by cards). We present details regarding processing, computational and storage– as well as temporary and permanent– resources.

**DSA Coupons** In [8], Naccache et al. proposed a method for delegating the computation of random values required to generate DSA [1] signatures by sharing a common secret with a trusted authority. From this secret, the trustee can pre-compute "coupons" ($r$'s) which can later be used to generate DSA signatures, saving time and effort. We assume familiarity with DSA signature (which structure is also made clear in the discussion below).

Next we describe various flavors of the DSA Couponing Scheme. We adapt the descriptions to the context of a three party payment system. The underlying idea is to propose various solutions enabling a low-cost device to sign on-line a transaction. We consider the following parties :

– Issuing Authority (IA): which defines the payment protocols and issues the low-cost devices
– Integrity Circuit Card (ICC): are the user's device, which able to pay at Point of Sales and generate on-line electronic signatures requiring limited computational power
– Points Of Sale (POS) : units which receive payments and are able to authenticate payment while relying on the IA for stronger security.

We consider three different protocol:

1. Use & throw coupons: the basic scheme where ICC signs a transaction spending a 20-byte coupon

2. Compressed coupons: the same protocol with 64-byte coupons (i.e., increased signature capacity)
3. Tiny coupon: an on-line scheme where the size of a coupon is drastically reduced (to 2–5 bytes)

*Use & Throw Coupons:* In order to generate a signature $(r, s)$ the signer and the authority engage in the following protocol, assuming they share the knowledge of a secret key $x$ :

1. Signer sends a random $J$
2. IA computes and sends a set of coupons $\{r_i\}$ where:

$$r_i = g^{k_i} \bmod p \bmod q \text{ and } k_i = 1/\mathsf{SHA}(x|J|i) \bmod q$$

   (in regular DSA $k_i$ is a random value).
3. when receiving a message $m$ the signer selects a coupon $(r_i, i)$ and generates:

$$s = (\mathsf{SHA}(m) + xr)\mathsf{SHA}(x|J|i) \bmod q$$

The signer performs only two SHA computations (SHA is a relatively efficient cryptographic hash function) and two modular multiplications.

*Compressed Coupons:* In this case, the commitment is computed in a different way. Rather than calculating $r = g^k \bmod p \bmod q$, we compute $r = \mathsf{Comp}(g^k \bmod p)$ replacing the operation $\bmod q$ by a different function to reduce $g^k \bmod p$ into a 64-bit string. This value is further replaced by SHA(r) to be expanded into a random number mod$q$. As an example, we may consider the Comp function: $\mathsf{Comp}(u) = u \bmod q \bmod 2^{64}$.

The generation of the signature consists in :

1. Prepare the $k_i$ corresponding to the current transaction index $i$
2. Compute $s = (\mathsf{SHA}(m) + x\mathsf{SHA}(\mathsf{Comp}(r))\mathsf{SHA}(x|J|i) \bmod q$

*Tiny Coupons:* The third protocol proposes the use of very short commitments, reduced to only a few bytes. This is done in order to increase the number of signatures the ICC can generate between reloading phases. The idea is to limit the time available to the signer in order to produce a correct signature. Namely, the verifier sends a challenge at the very last moment, to be appended to the message.

On-line authentication process for $m$ :

1. Prepare the $k_i$ corresponding to the current transaction index $i$ and sends the corresponding commitment $r$
2. Receive a challenge $a$ (at least 80 bits) chosen at random by the verifier
3. Compute $s = (\mathsf{SHA}(m|a) + x\mathsf{SHA}(r)\mathsf{SHA}(x|J|i) \bmod q$

*Three Party Protocol:* This version assumes a complete system where POS is the verifier and IA the issuer of ICCs and set of coupons is also present. The protocol is a sort of two-step protocols where a message authentication is performed at the POS level and then, a stronger verification of the signature is done at the IA level.

1. IA loads onto the ICC a set of coupons $r_i = \mathsf{Comp}(g^{k_i} \bmod p)$ where $k_i = 1/\mathsf{SHA}(x|J|i), \mathsf{Comp}(u) = u \bmod 2^{24}$
2. ICC commits by sending a coupon $(i, r_i)$ to the POS
3. POS chooses an 80-bit random $a$
4. ICC computes $s = (\mathsf{SHA}(m|i|a) + x\mathsf{SHA}(r))\mathsf{SHA}(x|J|i) \bmod q$
5. POS accepts the signature iff:
   - $s$ is returned within a certain time-out delay
   - $r == \mathsf{Comp}(y^{\mathsf{SHA}(r)/s} g^{\mathsf{SHA}(m|i|a)/s} \bmod p)$
6. POS sends the signed transaction $(i, r, a, s, m)$ to IA
7. IA checks that $s$ is properly formed :

$$s == (\mathsf{SHA}(m|i|a) + x\mathsf{SHA}(r))\mathsf{SHA}(x|J|i) \bmod q$$

**GPK8000 and GemSAFE** Next we review settings where the cards possess a more complete cryptographic capability. The basic RSA encryption and signature operations are assumed to be known.

GPK8000 from Gemplus [3] incorporates the following features : fast 512/ 768/ 1024 RSA operations (sign, verify, unwrap, encrypt, decrypt) including highly secure on-board key generation. It further possesses fine configuration of key pair usage, e-purse, proven banking security level, GPK2000 and GPK4000 upward compatibility and migration path towards new open platforms. GPK8000 benefits from the very latest hardware and software security mechanisms to achieve the highest possible level of security, including anti-DPA (Differential Power Analysis) mechanisms.
The GPK8000 SDK kit help users to learn about card functions, run scenarios an show program examples to interface with GPK8000 at card level (also called APDU level).

Another Gemplus realization, GemSAFE provides a personal network safeguard by using digital certificates stored on smart cards for accessing corporate intranets, extranets, websites and electronic mail systems. Designed for quick, easy, plug-and-play installation and set up, GemSAFE combines a smart card, smart card reader and software for integrating with Microsoft and Netscape software suites.

GemSAFE works seamlessly with Microsoft Internet Explorer 4.x, Outlook 98 and Outlook Express via Microsoft's Crypto API, as well as Netscape Navigator 4.x and Messenger via RSA PKCS#11. When using these applications, GemSAFE provides SSLv3 client authentication to requesting web servers and secure S/MIME email exchange via the user's digital certificate and private key stored on a smart card. The user's private key never leaves the smart card and is inaccessible from outside the card. All cryptographic functions requiring the

private key are handled on the card by the onboard microprocessor. GemSAFE also works out of the box with Microsoft Windows NT 5.0 logon, and GemSAFE is fully PC/SC compliant. No extra drivers are needed to get up and running. Further, GemSAFE smart cards can be used in any industry-standard PC/SC-compliant smart card reader, including readers from Gemplus.

GemSAFE is designed to work with all certifying authorities, whether an organization chooses to take on this task itself or to outsource it to an external trusted third party (such as VeriSign or Cybertrust). Organizations can also choose to personalize GemSAFE smart cards themselves using Gemsafe Enterprise, a complete solution for issuing and managing cards for employee IDs, etc. This makes it easy for security officers to generate, manage and recover smart card-based digital certificates and keys throughout the enterprise.

**AuthentIC** The Authentic range of smart cards from Oberthur Card Systems [9] offers varying levels of memory capacity and cryptographic algorithms, meeting the following market requirements:

- Security tokens based on RSA or ECC (Elliptic Curve Cryptography) technologies
- All digital signature protocols and standards
- Compliant with Public Key Infrastructure interfaces (e.g. PKCS)

Authentic is flexible enough to be adapted to different devices and to suit various customer requirements. During personalization, the secret keys and certificates are loaded onto the card. These security elements can then be used by card to perform cryptographic algorithms. The card issuer is then able to develop customized digital signature applications, using Java or Microsoft languages.

The Authentic family is derived from RSA or ECC cryptography and has different development platforms.

**Authentic RSA**

- CPU: 8 bits
- Co-processor: RSA 2048 bits DES, 3DES
- Memory Size: EEPROM 16K or 32K bits
- Characteristics: T = 0/T = 1, Java Virtual Machine (Microsoft Platform) and Common Criteria EAL4 (for 32K version only)
- Compliance with standard: ISO7816-4 EMV PC/SC
- Cryptographic algorithms: RSA 2048 bits/Key generation DES/3 DES SHA-1 MD5 Random number generation DSA
- Interface: PKCS # 11 - Microsoft CSP

**Authentic ECC**

- CPU: 8 bits
- Co-processor: no
- Memory Size: EEPROM 8K bits

- Characteristics: T = 0/T = 1, Java Virtual Machine (Microsoft Platform) and Common Criteria EAL5
- Compliance with standard: ISO7816-4 EMV PC/SC
- Cryptographic algorithms: DES/3DES SHA-1 MD5 ECDSA
- Interface: PKCS # 11 - Microsoft CSP

**Easyflex Corporate** Schlumberger [11] proposes a multi-application dual interface smart card for total access management, from building to network, as a PKI encryption-based ID badge. Designed for authenticating employees, customers, suppliers and partners, Easyflex Corporate also supports e-commerce and electronic payment. The card combines the speed and facility of contactless operation with the security inherent in PKI cryptography. It offers a highly portable ID badge for controlling and monitoring physical access to buildings and services, and logical access to computers and networks. The complete Easyflex Corporate solution includes Reflex readers, client software integration and installation, card management system support and consulting services. Schlumberger has selected Easyflex Corporate to be its worldwide company ID card. The card is in use in five of the company's international locations since early 2000. The locations include Austin, Texas, and Montrouge, France campuses, where it is being used to control access to its computer networks, as well as the campus perimeter, internal buildings and areas, car parks and restaurants.

**Contact Interface**

- ISO 7816 based, T=0 transmission protocol on-card
- 512, 768, 1024 RSA key generation
- on-card 56 and 112 bit DES key generation
- RSA 512, 768, 1024 signature calculation
- SHA-1 and MD5 hashing operations
- DES and Triple DES ECB and CBC modes (56, 112, 168 bit key length)
- Encrypted key loading (DES and RSA)
- EMV compliant
- integrates with PC/SC
- integrates with PKCS # 11
- usable memory: up to 7900 bytes
- selectable communication speed (9,600 - 153,000 baud)

**Contactless Interface**

- 8 Kbits EEPROM memory divided into 16 sectors
- operating frequency: 13.56 MHz (no battery)
- ISO 14443-Type A compliant
- ISO 7816 card dimensions
- more than 100,000 write cycles possible per sector
- typical transaction time: 100 milliseconds (transport standard)
- distance range: 10 cm with reference reader
- up to 16 separately-secured applications

– each sector has two 48-bit diversified keys and its own access conditions
– replay attack protection and mutual 3-pass authentication procedure
– unique fast-anticollision algorithm
– Mifare protocol

**Performance at 9600 bauds**

– hashing SHA-1: 110 ms for 64 bytes input
– DES external authentication: 77 ms for 56 bit key
– RSA signature: 564 ms for 1024 bit key on-card
– 1024 bit RSA key generation, average time: 30 sec.

We can therefore conclude this section that recent smart cards are equipped with impressive mechanisms to support PKI applications in reasonable performance and with high level of functionality.

## 3 Payment Applications

Electronic payments are a crucial component in the development of e-commerce. Smart cards naturally aid in this new area as well. In a typical payment application, one party (a client) transfers money (in one shape or another) to another party (a merchant, another person, etc.). Also involved in such systems are financial institutes, and perhaps governments and regulatory organizations. The transfer of "e-money" should not open the door to fraud and financial problems. Payments as basic control mechanism, underlies sound e-commerce.

### 3.1 Electronic Purse Scheme

An electronic purse scheme involves several participants which perform complementary functions. In any particular electronic purse scheme, a single entity, such as a commercial bank, may perform the function of one or more of the participants. Each of the participants, and their respective roles, are described below.

An electronic purse scheme typically involves five main participants:

1. The Purse Provider: the organization which provides and guarantees value throughout the electronic purse scheme. The Purse Provider defines the operating rules and is responsible for the global security of the scheme. The Purse Provider could be an organization representing a group of banks.
2. The Load Agent: a trusted agent of the Purse Provider who loads and reloads electronic funds into the Purse Holder's electronic purse. Often the Load Agent is the Purse Provider or the Purse issuing bank. Load Agents sometimes also perform the card personalization function when they may also include an initial value in the purse.

3. Service Providers: sell goods and services to Purse Holders who pay using electronic funds from Purse Holders' purses. Service providers use terminals in which they store individual transactions. A Service Provider is referred to as the merchant.
4. Acquirers: trusted agents of Purse Providers which collect transaction payments from Service Providers' terminals. They generally exchange the collected payments for other proceeds, such as a credit to the Service Provider's bank account.
5. Purse Holders: consumers possessing smart cards containing one or more electronic purses.

**Generic Processing of Transactions** Purse Provider processing is a batch processing computer system which performs several functions:

- Transaction Settlement: carries out a settlement in which Acquirers and Service Providers are given consideration (i.e., credit to their bank accounts) in exchange for electronic purse debit transactions collected from Service Providers' terminals.
- Audit and Reporting functions: offer the Purse Provider the means for auditing all transactions executed within the scheme. The audit enables detection of anomalies (such as a security breach) and resolution of questions raised by Purse Holders, Service Providers, Load Agents and Acquirers.
- Black List Management: enables the Purse Provider to disable lost, stolen, or cloned cards and to provide the required associated reports.
- Load Management functions: enable the Purse Provider (acting in the capacity of the Load Agent) to securely credit an electronic purse and to provide the associated reports.

**Processing a Transaction: MPCOS as a toy example.** The Multi-application Payment Chip Operating System-EMV (MPCOS-EMV) is an operating system designed for multi-purpose and payment applications. The MPCOS-EMV features and applicable standards include:

- ISO 7816-1, -2, -3 compliance: the default communication protocol is T = 0. MPCOS-EMV also supports protocols T = 1 and T = 14.
- ISO 7816-4 compliance: the compliant commands, data structures (multi-application) and return codes ensure a wide acceptance of the operating system by application issuers and terminal manufacturers.
- EMV compliance: this compliance allows implementation of VSDC Template 1 (magnetic stripe image in the smart card according to Visa specifications).
- I/O routines Up to 115,200 baud and fast cryptographic routines.
- Dedicated security features such as:
  - secret code/key management and verification
  - sensitive system data protection
  - 3DES algorithm for authentication, secure messaging and payment certification

  - Application-level countermeasures against DPA
- Enhanced administrative command set is available for easy card personalization.

A purchase transaction can be seen as an off-line process split into four different steps:

Step 1: mutual authentication (card and terminal)
Step 2: purse balance reading
Step 3: purse debiting
Step 4: debit signature

*Mutual Authentication:* The cryptographic protocols implemented in order to detect counterfeit cards and fake or emulated Secure Access Modules (SAMs) are challenge-response protocols, based on secret key cryptography. The algorithm implemented is the 3DES in EDE (Encrypt-Decrypt-Encrypt) mode with 16-byte keys. The Master Keys are stored in the SAM, which can compute from public data communicated during the protocol exchanges the card derived keys.

A terminal checks that a card is genuine as follows:

1. the Card Serial Number (CSN) is read and used by the SAM to derive the card secret key $K_{auth}$ from the Master Key $MK_{auth}$. The CSN is stored by the terminal and used throughout the transaction process to derive secret keys.
2. the SAM generates a random (TRND) number to be encrypted by the card
3. the card encrypts the random number using the authentication key $K_{auth}$
4. the cryptogram (IAC) computed by the card is returned to the terminal to be checked by the SAM against its own result.

If the authentication fails, the process is terminated and the card is rejected.

Remark: The Answer To Reset (ATR) should never be considered as a means of card identification since the ATR of a card can be configured or customized very easily.

In order to detect SAM emulators the card must also authenticate the purchase device's SAM. The same process described previously is repeated, with the card generating a random number and sending this random challenge to the terminal, the SAM computing a response (authentication cryptogram) to be checked by the card.

*Reading Purse Balance:* The purchase process can continue with the reading of the purse balance and the computation by the card of a Card Balance Certificate (CBC) using a different secret key, Kbal. The CBC can then be verified by the SAM.

- the SAM generates a random (TRND) number and the terminal sends TRND and a command *Select Purse and Key* to the card

- the card increments the Card Transaction Counter (CTC), generates a new payment transaction temporary key (SK) and computes the authentication cryptogram $Cr$
- the cryptogram computed by the card is returned to the terminal to be checked by the SAM
- If result is OK (ACK is returned), the command *Read Balance* and the terminal transaction counter value (TTC) are sent to the card
- the card computes the cryptogram (CBC) and sends the balance value $Bv$ and CBC to the terminal
- the SAM checks the CBC against its own (recomputed) result.

Purse balance reading is used for the terminal display and is, therefore, optional.

*Debiting Purse:* A Card Debit Certificate (CDC) is computed by the card using the card key Kpay. This certificate has to be checked by the SAM to ensure that the debit operation has been properly done. This verification can be done after the Kpay has been diversified (derived) from the Mother Key (Mkpay) and the Card Serial Number.

- the SAM generates a random (TRND) number to be sent together with SelPk command,
- the card increments the Card Transaction Counter (CTC), generates a new payment transaction temporary key (SK) and computes the authentication cryptogram $Cr$
- the cryptogram computed by the card is returned to the terminal to be checked by the SAM against its own result
- If result is OK (ACK is returned), the Debit command and the terminal transaction counter value (TTC) are sent to the card
- the card computes the debit cryptogram (CDC) and sends it to the terminal to be checked by the SAM

The terminal can then display the new purse balance value.

*Debit Transaction Signature:* The debit signature enables the detection of "false" transactions which may be generated by terminals (each transaction has to be signed electronically by the card), as well as fraudulent cards whenever a debit key has been exposed. The signature shall only be checked by the acquirer.

The signature is computed by the consumer's card from the transaction elements and the signature key Ksign. A new temporary key must be established before each step of the purchase processing.

The sign certificate (CSC) must be sent to the host with related card transaction counter value (CTC), transaction value (Tv), balance value (Bal), card serial number (CSN) and card sign certificate (CSC). Usually, the transaction collection is a batch process: transactions are sent in batch and the SAM computes a Message Authentication Code (MAC) so that the host can verify integrity and authenticity of the transaction batch.

This concludes the description of the purse example, we next view another type of payment architecture.

### 3.2 Credit Card Schemes

The most common type of payment used on-line are credit card payments. The main reasons for this is of course convenience, ease of use, and because they are omnipresent. However, they are insecure, offer no anonymity, and do not allow small payments.

- **High costs and inability to allow small payments.** Each credit card payment has a fixed cost of 20-40 cents, plus a variable cost depending on the method used and the negotiated contract.
  The fixed costs originate from the cost of performing a transaction, since transactions usually involve some type of paperwork, and the traversal of a proprietary network rented by Visa, Mastercard, or some other credit card provider. US banking regulations exist which mandate that users' accounts be maintained so as to enable a mechanism for disputing payments. This makes relatively high fixed costs unavoidable.
  The variable costs are a reflection of the security problems associated with credit cards. In other words, the credit card issuers recover their costs from fraud by charging the merchants a percentage on their customers' purchases. For this reason this fee is variable, and is much higher for, say, Internet or telephone purchases (non presence transactions) than it is for purchases where the physical card is presented (established presence transactions). It also varies by industry sector, with certain high-fraud businesses being penalized with higher fees. In short, the main reason for these high fees is the insecurity of the original credit card design, which allows merchants to view (and copy, and reuse) all of the customer's private information.
  As a result of these high fees, payments of less than $10 cannot be made with credit cards with a reasonable profit being made by the merchants (especially for on-line merchants, who incur higher charges). Aggregating small payments into one reasonably sized amount before charging one's credit card is the solution currently used, but this poses too many unnecessary restrictions on both users and merchants.
  When a merchant incurs too much fraudulent transactions, he is penalized as well, reducing the attractivity of credit card payments.
- **All purchases are traceable.** Despite the convenience of a full history of one's purchases, as well as the ability to dispute payments made with a credit card (especially in the US), the fact that credit card issuers have all the users' spending information available poses serious privacy concerns. This information is sold to advertisers, and is utilized internally by credit card issuers to target advertisements to their audience. From both an ethical as well as a practical perspective, giving someone the ability to conduct payments should not go hand-in-hand with knowing their whereabouts, their spending patterns, and their personal preferences.
- **Security problems for the customers.** One of the bigger problems with credit card payments is that all the user's private information is exposed to the merchants. This allows merchants to effectively steal and use their

customers' credit cards. Obviously, this is a much greater threat over the Internet, where the merchant can be located anywhere in the world.
This security problem is manifested in two different ways, depending on where the credit card has been issued:

- For credit cards issued outside the US, the end-customer is held liable for all purchases. Thus, a stolen credit card number has a direct impact on the consumer. Clearly, this is a serious security problem, especially since the customers have little or no control whatsoever over the merchants' handling of their credit card information.
- For US-issued credit cards, there is a regulatory limit of $50 on the consumer's liability in case of a lost or stolen card number. In addition, most credit cards will typically refund the whole amount from a fraudulent purchase, so more likely than not the customer's liability is nil. Credit card issuers often take advantage of the fact that consumers are afraid of losing their credit cards by offering them additional "security guard" features. In essence, this is an insurance against theft or loss of one's credit card; the problem is that the fee for this insurance is extremely high, typically 0.5 to 1% of all the customers' purchases.

Thus, in either case consumers are unfairly penalized for the credit cards' own inappropriate security design.

It is therefore expected that micropayment and e-cash schemes that are now at their second generation of commercialization, will play role in the payment area, in conjunction with credit card applications. New generation of such applications is also under development since we need more flexible, yet secure credit-card support technology, more flexible/ cost-effective than the existing schemes which we cover next.

*SET:* Visa and Mastercard's electronic counterpart of the credit-card setting which incorporates legally-binding signatures, implements digital signatures as a tool for authenticating users, merchants, and banks. This reduces the possibility of fraudulent transactions, thus bringing on-line transactions on par with physical-card solutions. Note however, that the complexity of SET has, so far, hampered its full-scale deployment.

It is, in fact, too expensive for most merchants to implement, and it also requires end-users to download specific software and to participate in a public key infrastructure –which is not yet firmly in place. (SSL, requiring only server public keys, is an alternative which is used in credit card payments.) Also, even SET (or SSL) do not raise credit cards to a sufficiently high security standard to completely overcome fraud. Hence, credit cards still charge merchant fees which makes micropayments prohibitive.

*Blue from American Express and Smart Visa* The first serious move by the financial industry to embrace smart card technology was Blue from American Express, addressing the issue of Internet fraud. The Blue card was also advertised

as a tool to improve user's experience when surfing on the web and purchasing on-line.

A recent initiative driven by Visa in the US is the Smart Visa program, aimed at providing member banks with a framework to smoothly operate the transition to smart card technology. The first issuers ready to deploy these new smart visa cards are First USA, Fleet and Providian. The marketing message is roughly the same as in Blue, proposing enhanced security and additional features to card holders.

Technically speaking, the fact that the infrastructure for using smart card in the US is not yet there means that the real usage of the chip will be restricted to the Internet. It will also require specific enhancements in order to interface the smart card with the applications running on top of the servers. Nevertheless, this new wave of e-payment instruments clearly indicates the smart card model is turning global, since the United States were the only region not yet contaminated by the, so called, "smart virus"!

The recent technological improvements in chip design combined with the new open architecture models such as Javacard, Multos and Windows for Smart Card will enable issuers to propose application management at the user's level. The Visa Open Platform (VOP) initiative for instance, can be seen as a framework for new developments in cards, applications and users management. More generally, the new deployments supported by advances in technology and standardization effort are paving the way to a new set of applications mixing the best of the breed of payment, security and communication media.

Remark: The inclusion of various payment mechanisms in smart cards is expected in the future. In addition smart card as a component aiding in control and securing software based payment (in a hybrid system where the hardware performs part of the transaction) is also expected. The development of efficient payment mechanisms for small values (micropayments) and secure mechanisms for high value transactions, and a right tradeoff in between, is still a very active area of research.

A related area, where payments and billing take place, is content protection and Digital Right Management (DRM) where smart cards can help in controlling usage, payments, and help impose access rights to content, in much the same way as it can aid in other access control and delegation of rights issues. This is due to the fact that in a protected token on a card (unlike in a pure software environment), much of the checking of access rights as well as transferring of rights can be done secretly. Motion of access rights which are unique is quite analogous to the transfer of payment instruments.

## 4 Telecom/Mobile Applications

This section is dedicated to sketching smart card products and solutions in the telecom and wireless application field. This will help in understanding the way new smart card architecture intend to support this emerging market.

Wireless devices which communicate over the air are highly exposed. Thus they require security and authenticity services for their operations, and as e-commerce applications increase, further sensitive services such as support for payments and billing will be needed soon as well. It seems therefore, that smart cards are crucial in allowing safe operation of mobile telecom applications which will enable much more availability of e-markets.

Here we consider selected products from three smart card vendors (without pretending to cover the entire spectrum of products, applications and solutions delivered by the industry). For further information on GSM and a clear description of most of the technical terms in this section, the reader can consult [12] for an overview (also useful is the GSM association web site at [4]).

### 4.1 Oberthur: ConnectIC and SIMphonIC products

Oberthur Card Systems introduces ConnectIC - a Java based, RSA enabled multi-application WAP Identity Module (WIM) allowing end users secure mobile and fixed Internet browsing.

ConnectIC acts by setting up a secure WTLS session (the equivalent of SSL / TLS) through which the subscriber can gain access to typical Internet facilities while on the move. Internet transactions can be secured through ConnectIC's ability to digitally sign the data, ensuring the integrity and authenticity of the transaction.

Oberthur Card Systems has developed ConnectIC according to the WIM specifications, as proposed by the WAP Forum. ConnectIC is based on Java Card 2.1 in the form of a Java applet. This allows the WIM functionality to be combined with other applications on a multi-application card, as well as acting as a stand alone application. ConnectIC is compliant with Open Platform 2.0 from Visa, which specifies a strict environment for the secure loading of keys and applications.

Not only can the ConnectIC applet be combined with other applets, but it is also network and terminal independent. This allows the card to be used in different environments - as a full sized card in a dual slot phone, or in a PC reader, or as a plug-in card in dual chip phones.

ConnectIC's functions include:

- Transport level security: WTLS session key generation.
- Application level security: performing digital signatures.
- Storage of Certificates: CA's and user's.

ConnectIC's ability to adapt to different environments means that the personal information stored on the card can be re-used in other devices.

The ConnectIC applet can be combined with a SIM or SIM Toolkit Card and is compatible with PKI standards PKCS #15 as well as the ISO7816 series of standards, part 8 in particular. Security being of prime importance, Oberthur Card Systems continues this pioneering work by the establishment of standards, offering solutions that are also compliant with ETSI and the Open Platform

protocol from Visa. Conformity to these standards ensures end–to–end security for the players using a SIM Toolkit scenario:

- End-to-end security for the service provider (application owner)
- Secure application and data download for the network operator and service provider

At a different level, the SIMphonIC solution allows the card issuer to modify the card profile either Over-The-Air whereby application updates, additions or removals are transferred by SMS to the card, or are done at a Point-Of-Sale terminal. Data transfer is carried out in complete security with key management being at the heart of this activity. In both scenarios, the card can be modified quickly, easily and cost effectively, avoiding lengthy and costly redevelopment. Card management becomes a key issue; no longer do operators need to be product focused, but they can rather be service focused - with the ability to create and adapt tailored solutions which best suit their customer base.

Oberthur Card Systems and Prosodie, one of the principal developers of services for mobile telephony, have joined forces to create Rapsodia. Designed to respond specifically to the needs of cellular operators and content providers wishing to maximize opportunities in mobile Value Added Services, Rapsodia specializes in offering interoperable, flexible and secure software modules that can be tailored to specific local operator needs. Working through a network of system integrators, Rapsodia's off-the-shelf server platform and applications offer the advantage of a fast route to market, while incorporating features that can be adapted to local requirements.

### 4.2 Gemplus: GemXplore Suite and Case

**GemXplore Suite** GemXplore Suite lets operators administrate SIM cards remotely and change their content after issuance. Applets can be securely downloaded over-the-air onto SIM cards and users can browse Internet sites on their mobile phones. The life cycle of a SIM card is thus expanded and targeted services can be offered to the right people at the right time.

Subscriber Service Monitoring GemXplore Suite lets users download new applets onto SIM cards and remotely add new functionalities after issuance. It lets them perform individual subscriber tracking to administer, bill and market multiple services on a single SIM card.

SMS, CSD, GPRS, WAP, 3G are just a few examples of mobile technologies that will deliver value-added services in the years to come. GemXplore Suite has been designed as an open framework that supports all major standards, smart card operating systems and communication protocols and technologies. Operators are free to select the technology that fits their value-added services best.

GemXplore Suite is upgradeable, protecting the operators' investment by providing a scalable distributed architecture and extensive use of open, platform-independent standards. GemXplore Suite was designed from the start to be an

industrial-strength platform. Thus, it can handle message throughput requirements of the fastest SMSC, 24 hours a day, 7 days a week from thousands to millions of subscribers.

GemXplore Suite is composed of a set of common administration tools and services.

Each product is independent. Operational and management functions are separated and connection to GemXplore Suite communications and management interfaces is supported. These products can therefore be purchased separately and installed on different sites. In turn, they communicate with one another using a common communication protocol. The functions include: access and license control, logging and audit trail, system configuration and operations, billing, time and scheduling services, SNMP services, performance monitoring, transactional services and management.

GemXplore Suite's functional offering includes four centrally administered products:

1. GemXplore Card Manager: offers over-the-air data management services for a portfolio of SIM cards. It automatically chooses the channel that is best fitted to deliver messages intended for the cards on the field. Other features which are included are request management and card-specific security.
2. GemXplore Channel Manager: operates message interchanges between applications and mobile phones over several types of channels: SMS, HTTP, CSD, GPRS, etc.
3. GemXplore Applet Manager: handles the downloading of applets onto cards and their life cycle. It supports security functions specific to the applets, as well as service monitoring and billing. GemXplore Applet Manager has been designed according to the latest standards: GSM OP download, ETSI 03.48, etc.
4. GemXplore On-Line Manager: allows mobile subscribers to browse web sites without upgrading their Phase 2+ mobile phones. GemXplore On-Line Manager is compatible with HTML- and WML-based web sites

**GemXplore Case** With GemXplore CASE V2.0, value added services (VAS) are easy to define and quick to design, thanks to the user-friendly graphical interface. There is no need to be an expert in complex development languages. GemXplore CASE V2.0 has been specifically designed to be plug and play and it targets two different cards : GemXplore 98 and GemXplore 'Xpresso for Java Card Technology.

GemXplore CASE V2.0 is composed of several modules that share the same user-friendly development environment:

– The GemXplorer is a tool for card management. With GemXplorer SIM card files can be edited, modified and tested using a fully graphical interface. SIM card profiles can be saved as PC files, profiles can be dragged and dropped from PCs to SIM Cards and vice versa.

- The Menu Editor enables simple point and click design of SIM Toolkit applications: application architecture, menu displays, command sequences and more. A SIM Toolkit application can be developed in minutes with the Menu Editor and immediately downloaded onto GemXplore TM 98 SIM cards, ready for field testing (or onto GemXplore TM 'Xpresso with the Object Designer plug-in).
- The Script Editor has been designed for advanced application development. Scripts are written in a simple, yet powerful GemXplore macro language. A wizard menu guides the user through each GemXplore macro command to optimize their use.
- The remote processing module helps designing and testing remote management applications. It formats applications into ESMS and downloads them onto the target SIM Card simulating the Over-The-Air process. For users who already have a GemMobile Remote Manager gateway, a GemMobile Remote Manager connection kit will be supplied in order to perform real life SIM Toolkit Remote SIM Card administration.
- The Database Manager is dedicated to profile management. It enables GemXplore CASE users to keep track of batches of test SIM Cards, used, for example in Remote SIM Management or SIM Toolkit field tests.

Advanced Development Tools comprises several prototyping and debugging tools: the handset simulatore, the network simulator, the protocol analyzer and the object designer.

- The Handset Simulator will assist the user in qualifying his application for a selection of SIM Toolkit compatible handsets;
- The Network Simulator will enable the user to prototype his application as if it were in real life;
- The Protocol Analyzer will elp the user debug hus SIM Toolkit application;
- The Object Designer is a Java Card applet development tool for SIM Cards. Object Designer has integrated state-of-the-art Java development methods and tools to offer the perfect basis for SIM Toolkit application development on GemXplore 'Xpresso cards. It also offers a set of debugging tool.

### 4.3 Schlumberger: USIMERA and Simera Solutions

USIMERA is a universal Java SIM card, giving mobile operators enormous flexibility today as well as a proven platform for the coming new generation services. It supports traditional 2G Phase2+ SIM Tool Kit-based value added services (VAS) and is ready for CDMA and TDMA network roaming support.

Its main characteristics are that it:

1. meets latest Java and 3GPP standards
2. designed to fit 3G mobile system evolution
3. ensures security, value added services and roaming WIM, CDMA and TDMA ready

4. has Smooth path to 3G

Simera Designer Studio allows a value-added service specialists to use STK[1] functions to develop applets for new services, without the need for any programming skills, or the requirement to brief programming personnel. This obviously shorten the development cycle. With Simera Designer Studio, the experts use Windows software with familiar graphical icons to access all the powerful Simera features. They drag and drop the functions they need for the creation of the applet script and for setting up the screen menus subscribers will use. the full SIM Tool Kit plus a range of conditional test, file access and validation features. The entire Java code required to build the applet is generated automatically, as automatic background validation ensures the logical consistency of the application.

When the script created on the screen is ready for operation, it is loaded onto a live Simera card for testing in a real Phase 2+ handset. If any changes are needed, it is simple to modify the script, and load the new version onto the SIM. Once the final version is ready, it takes a single keystroke for Simera Designer Studio to generate the complete specification package that Schlumberger technical specialists need to put the prototype into production.

Simera Designer Studio technical features the complete set of STK functions (GSM 11.14 release 98), i.e.:

- Conditional and loop functions
- Arithmetic, logic and string functions
- UCS2 compatibility
- Customized functions libraries
- Application graphical validation
- Internal Java code generator (GSM 03.19 release 98 compliant)
- Internal application builder
- Internal application loader
- Internal application documentation generator (Rich Text Format including menus and flowcharts)

The Beta version of this product should have been available from September, 2000.

The above selection of products demonstrates that the latest products for the mobile market are gaining in sophistication and are typically multi-faceted. They will enable global web access and global e-commerce, being useful over the air or at stationary locations.

## 5 Conclusions

We have presented e-commerce applications of smart cards. Smart cards are important for security of operation as well as for other aspects (flexibility, client

[1] SIM Tool Kit (STK), a standard set of powerful functions for creating client application programs - applets - that reside on the SIM

loyalty, service availability). The area is very active and growing. Our presentation reflects the state of the art (based on our knowledge). We reviewed smart card contributions in the areas of PKI, payments and telecom/mobile, which are all technologies serving growing markets. We believe that future developments of smart cards (which will include numerous elements which are now under research consideration) will be influenced by the increasing demand for web and mobile commerce. The increased demand in such a high level application area will, in turn, influence the changes in smart card technologies. For example, it will necessarily transform smart card design into a more higher level (CAD like) design as semantically-richer application are interfaced with the cards and increase the complexity of applications. The integration of smart card technologies with emerging technologies (mobile computing, the bluetooth protocol, flash memory, etc.) will also influence the advancements in the field. The emerging inter-dependencies and synergies between advances in e-commerce and advances in smart card technology are expected to grow and to get more involved and interesting.

## References


1. FIPS PUB 186, February 1, 1993, Digital Signature Standard.
2. Y. Frankel, D. Kravitz, P. Montgomerry and M. Yung, "Beyond Identity: Warranty-Based Digital Signature Transactions", Financial Cryptography '98, LNCS **1465**, pp. 241-253.
3. Gemplus, `http://www.gemplus.com`.
4. GSM Association, `http://www.gsmworld.com/index1.html`.
5. Identrus, `http://www.identrus.com`.
6. J. de Langavant, The Multos System and Architecture, Gemplus Developer Conference, Paris, 1999.
7. A. Menezes, P. Von Oorschut and S. Vanstone, The Handbook of Applied Cryptography, CRC Press, 1997.
8. D. Naccache, D. M'Raïhi, S. Vaudenay and D. Raphaeli, "Can DSA be improved ? - Complexity trade-offs with the Digital Signature Standard", Advances in Cryptology - EUROCRYPT '94, LNCS **950**, pp. 77-85.
9. Oberthur Card Systems, `http://www.oberthur.com`.
10. R. Rivest, A. Shamir and L. Adleman, "A method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. **21**, n. 2, Feb 1978, pp. 120-126.
11. Schlumberger Smart Cards & Terminals, `http://www.slb.com/smartcards`.
12. J. Scourias, "Overview of the Global System for Mobile Communications", `http://ccnga.uwaterloo.ca/ jscouria/GSM/gsmreport.html`.
13. Smart Card for Windows Help File. Smart Card for Windows Kit Documentation.
14. Sun Microsystems: Java Card 2.1 Application Programming Interface Specification, 1999. Available from `http://java.sun.com`.
15. Sun Microsystems: Java Card 2.1 Runtime Environment Specification, 1999. Available from `http://java.sun.com`.
16. Sun Microsystems: Java Card 2.1 Virtual Machine Specification, 1999. Available from `http://java.sun.com`.

17. L. Talvard, Smart Card for Windows Overview, Gemplus Developer Conference, Paris, 1999.
18. E. Vetillard: Java Card 2.1 General Presentation, Gemplus Developer Conference, Paris, 1999.
19. Visa International: Open Platform specification, 1999. Available from `http://www.visa.com`.

## A Glossary

ADC Application Delete Certificate. The ADC includes the Application ID (AID) and the Issuer ID to be checked by the multos card before authorizing the application to be removed.

ALC Application Load Certificate. The ALC includes the Application ID (AID) and the Issuer ID to be checked by the multos card before authorizing the application to be loaded.

ALU Application Loading Unit. An ALU contains the application code and data to be loaded on multos cards.

API Application Programming Interface. An API usually provides building blocks used by applications written for a specific operating system. Using an API, the programmer can provide an application with a GUI, manage system objects and processes, etc. For instance, the Java Card Application Programming Interface specification describes the set of core and extension Java Card packages and classes for programming smart card applications.

CDMA Code Division Multiple Access. CDMA is a "spread spectrum" technology, which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal.
For further information, connect to `http://www.cdg.org/index.asp`.

DPA Differential Power Analysis. DPA describes a new class of attacks against smart cards and secure cryptographic tokens. The attacks are performed by monitoring the electrical activity of a device, then using advanced statistical methods to determine secret information in the device.

EMV Europay/Mastercard/VISA. Europay, MasterCard and Visa worked jointly over the last few years to develop specifications that define a set of requirements to ensure interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used.

GSM Global System for Mobile Telecommunications. GSM is an open, non-proprietary system that provide international roaming in more than 159 countries. GSM satellite roaming has extended service access to areas where terrestrial coverage is not available.

ICC Integrated Circuit Card. A smart card is essentially an electronic microchip, embedded in plastic in the form of a credit card, with limited storage and processing capability. The chip stores electronic data and programs that are protected by various security features. The circuitry in a smart card derives power from a smart card reader (IFD or Interface Device) after the card is inserted into the reader. Smart card readers are available in a variety of form-factors and can be connected to a computer using an RS-232, PCMCIA or USB interface.

JCRE Java Card Runtime Environment. The Java Card Runtime Environment specification describes Java Card runtime environment behavior. This includes memory management, application management, security enforcement, and other runtime features.

JCVM Java Card Virtual Machine. The Java Card Virtual Machine specification defines a subset of the Java programming language and virtual machine specification suitable for smart card applications.

KTU Key Transport Unit. The applets stored in a Multos ALU can be protected according to three security profiles: Unprotected (only integrity checking), Protected (signature verification) and Confidential (encryption of parts of the applet). The encryption is performed using a block encryption algorithm and the key is transported within a specific block of data, the Key Transport Unit. The KTU is encrypted with the Applet Transportation public key specific to the card issuer.

RPC Remote Procedure Call. In the context of Smart Card for Windows (see SCW for further information), RPCs provide the programmer with a transparent communication channel directly to the On-Card API of the Smart Card for Windows.

SCW Smart Card for Windows. Smart Card for Windows (SCW) is highly integrated in the Windows world, supports the PKCS #11 interface for cryptographic tokens and respects PC/SC recommendations for application interoperability. SCW integrates several features such as Multi-application capabilities, On-Card API, MS-DOS.-type file system, Authentication Mechanisms with Entities Naming, Access Rules defined by Logical Expressions and Remote Procedure Calls (RPC).

SMS Short Message Service. SMS is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice mail systems.

TDMA Time Division Multiple Access. Since radio spectrum is a limited resource shared by all users, a method must be devised to divide up the bandwidth among as many users as possible. The method chosen by GSM is a combination of Time and Frequency-Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier

frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a burst period and it lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a TDMA frame (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame. For further information, go to `http://www.iec.org/tutorials/tdma/`.

TLS Transport Layer Security. TLS, more commonly known as SSL, is a popular mechanism for enhancing TCP communications with privacy and authentication. TLS is in wide use with the HTTP protocol, and is also being used for adding security to many other common protocols that run over TCP. WTLS is a lightweight and efficient wireless version of the protocol, with respect to the bandwith, memory and computational power limitations related to wireless usage.

VOP Visa Open Platform. The Open Platform, originally developed by Visa and now managed by GLOBAL PLATFORM, is an architecture and associated standards for the definition and management of dynamic, multi-application smart cards. The Open Platform focuses on the entire smart card system, rather than just the card.

WAP Wireless Application Protocol. WAP is a technology designed to provide users of mobile terminals with access to the Internet. WAP integrates telephony services with microbrowsing and enables interactive Internet access from the mobile handset. Typical WAP applications include over-the-air e-commerce transactions and online banking. For further information, go to `www.wapforum.org`.

## B Short Biographies

**David M'Raïhi** David M'Raïhi is currently Senior Scientist with Gemplus, working in smart card application design, security and cryptographic technologies evaluation. Dr. M'Raïhi, a former member of Gemplus Crypto Group in Paris, France moved to Gemplus USA in 1998. He recentlty extended his scope to mobile commerce and PKI applications integrating smart cards and secure tokens. He has authored and co-authored over 30 scientific papers and patents, mainly related to smart card applications, including fast encryption, public-key authentication and digital signature techniques.

**Moti Yung** Moti Yung is currently the Chief Scientist and Vice President of CertCo Inc. (formerly Bankers Trust Electronic Commerce), working in cryptographic technology, security and electronic commerce. He has over 20 years of experience in Information Technology (development, research, design and education). He has been serving on the board of directors and on technical advisory boards of a number of technology companies. He is also currently a visiting faculty with Columbia University where he supervises research of Ph.D. students. Dr. Yung was with IBM

Research Division from 1988 till 1996 where he received IBM's outstanding innovation award for his research contributions leading to products. He has published over 200 scientific papers and abstracts, and he is a co-inventor of over 25 patents. Dr. Yung has served on over 45 scientific program committees and steering committees of leading international conferences and has been an invited speaker in over a dozen countries. He is an editor of the International Journal for Information Security and will serve as the program chair for the Crypto 2002 conference.