EUROSMART
The Voice of the Smart Card Industry

Technologies for Identity Applications

Recommendations for European Identity Initiatives, European visa, Passport and eGovernment services

EUROSMART Recommendations for a “smart visa”.

- Annex 1 presents an overview of existing initiatives.
- Annex 2 contains a review as background information on available technologies and criteria for appropriate selection.

Smart cards associated with biometrics is the best technology combination to build cost effective and convenient platforms that meet the requirements of future secure personal ID systems. Smart cards extremely favourably compare with static memory devices, such as 2D bar codes, laser cards or memory cards.

Smart card based identification solutions meet and often exceed the requirements of a wide range of policies and legal mandates.

The smart card is a unique, portable, personal object that easily combines secure identification and authentication functions for both the physical and the digital worlds. Smart cards are well perceived by citizens, offering convenience, security, and crucial personal information privacy management features.

The European smart card technology leads its industry worldwide, and the USA leads the biometrics technology and industry. The European Union recommendations will set a powerful example for the world, including in the USA, and China. Especially if the rationale for the combination of smart cards – that provide security and privacy – and biometrics – that conveniently provide user related data – is strongly affirmed.

Overview

Tragic International events have raised interest in implementing more secure personal identification (ID) systems and border controls.

ICAO as a representative International Organisation has adopted recommendations at the end of May 2003 as guidelines for a Machine Readable Transport Document (a glossary of terms is available at the end of the document) including the use of biometrics technology for faster and more secure control of travellers' identity.

At the same time US Administrations in charge of security, NIST and NSA in particular, also recommended the use of biometrics features for frontier control and the incorporation of several existing information technology standards including Public Key cryptography (PKI) and Digital Signature Standards for any future visa system.

The European Commission is now launching the second generation of Schengen Information System and is recommending the use of biometrics for the overall efficiency of the EU wide visa system. A coherent approach means harmonised solutions not only for documents of non-EU nationals but also for EU citizens passports.

In this context, and in order to assist the European Commission in the preparation of this approach, Eurosmart the largest European Smart Card Industry Association wishes to present its recommendations.

EUROSMART Recommendations

Smart cards associated with biometrics are the best technology combination to build cost effective platforms that meet the requirements of future secure personal ID systems.
It offers in addition, crucial personal information privacy management features.

Coupled with a secure, privacy-sensitive information technology architecture and a strong policy framework, a **smart card based secure personal ID system** :

- **provides accurate personal identification in the physical world**, through classic identity verification by the authorities using a security document. The card body has demonstrated in many countries and applications its capability to embed advanced security features.
- **provides accurate personal identification in the digital world**, using well understood automatic authentication procedures that are commonly used by the banking o the GSM mobile telephony industries for example. The card so enable the authorities to use the very convenient and powerful digital networks to access and verify citizen's related information, and it also enables the citizen to conveniently and securely access e-government on-line services.
- **protects individual's personal information** - that are stored in the card and provided by a voluntary action - and so ensures better acceptance by citizens
- **effectively addresses the policy and legal requirements** that are currently being debated in many countries
- **provides the citizen with a personal device that carries tangible benefits** such as access to convenient on-line governmental services

Recommendations for generic personal ID systems

Many countries have started to study the development and/or implementation of secure personal ID systems (see annex 1) taking into account the following requirements in term of ability to:

- Provide fast and effective verification of an individual's identity
- Guarantee a significant increase of security and trust in respect of the currently existing systems
- Protect the privacy of individual's identity information
- Ensure interoperability between various systems of different countries
- Provide for a given country or a group of countries (like the European Union), access to government services.

Meeting the requirements:

➢ The best suitable **Machine Readable Transport Documents** (MRTD) device is the **smart card** since it offers all naked eyes control capability, while providing additional security features to reduce fraud and provide security and trust for on-line systems. Moreover smart cards better cover the privacy issues that are essential for the European citizens, important in most European countries culture and way of life, and frequently the source of numerous questions from small but very active organizations.

➢ Smart card based personal ID system have to integrate **biometric technology** *(more information about the technology in the technical annex)* to make the citizens experience at heavy traffic identity verification points like airports and borders a more swift and enjoyable one.

Any biometric sample fits and can be handled by the **smart card technology that exists today**. Several such samples related to different biometrics technologies would fit easily within a relatively low-end smart card. As the silicon and security technologies continues to evolve rapidly, it is certain that even the highest performance cards of today will be commonplace and relatively low-end in the next few years. The card memory capacity and the CPU computing power must be selected according to the data storage and processing needs, and optimised to meet the best performance/cost ratio at the time of large scale deployment. The smart cards features can also be used in a contactless/wireless environment; however expert design must be applied in this case since the contactless/wireless features may come – and is strongly perceived by privacy protection activists to come - at the expense of privacy.

➢ As long as acceptance by public and respect of privacy is ensured, **any biometric data can be used** in secure personal ID system (Face recognition and Fingerprint being the most common candidates, but could be complemented by a third or several other techniques if needed)

➢ **Interoperability between countries** needs to be ensured through the use of a standardized Biometric Application Programming Interfaces (API). Eurosmart, the US based "Smart Card Alliance", the JavaCard Forum and several other industry associations have united their efforts towards such standardization. These efforts would be extremely accelerated by the adoption of a smart card combined with biometrics recommendation by the European Community for its visa, passport and e-government initiatives, **leading to an ISO standard**. A Public Key Infrastructure (PKI) needs to be used, properly architected, in order to ensure exchanges between multiple countries while maintaining the security and privacy requirements.

- **Full biometric Match-On-Card** process is recommended for “One to One” verification. This capability ensures that the biometric sample comparison with the reference sample stored in the smart card is made inside the secure smart card without the original sample ever being exposed outside of the smart card. This is especially true if no official agent is present to control the authentication process.

- For “One to Many” identification, matching can be performed on the central secure database. **Associated with a strong PKI architecture, smart card will ensure** an acceptable security and privacy level.

  Refer to the glossary at the end of this document.

Specific Recommendations for European visa & passports

Specific considerations have to be taken into account when a passport or a visa is issued:

- Issuance is performed by different countries/authorities that those countries/authorities doing the control.

- Visas are delivered in any country (through local representation of issuer country, Consulates, Embassy) and sometimes at the disembarking place in a given country to give access to foreign visitors into the given country.

- Interoperability has to be guaranteed, for reading equipment in particular (this has been achieved since many years for smart card readers thanks to the ISO standards related to smart cards that is universally used).

- Paper form (or naked eyes control) must be maintained for countries that will not be equipped for e-passports and e-visas

- Control of personal data by the holder has to be guaranteed

- Visa is delivered for a validity period that is most of the times shorter than the validity period of the Passport, requiring activation, deactivation and expiration capability.

- A given person can carry several visas simultaneously for various countries

- Visa can be attached (Physically or electronically) to the passport or can be in a separate document.

- The visa has to be checked at the same time as the passport, meaning that Border Passport Control organisations and systems have to be able to ensure both.

Taking these requirements into account, Eurosmart would recommend that EU visas could be based on ICAO recommendations on MRTD and Biometrics for MRTD.

However, in an attempt to further reduce risks of identity fraud and to allow EU countries to be able to use the same supports and infrastructures for both ID Travel documents and national ID cards, we strongly suggest the following changes to ICAO recommendations:

Domain/ Topic	**ICAO Recommendation**	**EUROSMART Recommendations**
Form for Passport	Paper Booklet + Embedded electronic label	**Smart card only (Medium - Long term)** **Smart card + paper Passport (Short term) ***
Form for Visa	electronic label sticker (1 per issued valid visa)	**e-visas loaded on Passport smart card**
Electronic technology	Contactless ISO 14443	**Conventional (contact interface) smart card, or dual interface (contact and contactless) smart card *(see previous remarks regarding privacy protection)*, <u>the contact interface being mandatory</u> (in particular to ensure privacy).**
Biometric Templates	‣ High quality picture for face recognition ‣ Fingerprint	‣ High quality picture for face recognition ‣ Fingerprint
Memory size	32 or 64 Kbytes E2Prom	32-64 Kbytes E2Prom (depending on requirements, however by the time of volume deployment 64K will have reached a similar cost point compared with 32K)
O/S type	Dedicated (Multi-applications is optional)	**Multi-application** (depending on requirements) **with Common Criteria EAL4 or EAL5 security certification**
Encryption	PKI	PKI
Manufacturability	<u>Chip</u> : Silicon supplier <u>O/S</u> : O/S supplier <u>Label</u> : e-Label manufacturer (Large chip technology to be developed) <u>Passport</u> : Passport manufacturer with specific embedding process *4 actors involved*	<u>Chip</u> : Silicon supplier <u>O/S</u> : Smart card suppliers. Open (non-proprietary) operating system. OS's implementations can differ from one supplier to another if all are certified . <u>Smart Card</u> : Smart Card supplier (proven volume mature low-cost technology) <u>Passport</u> : Passport manufacturer (regular process) ***2 actors involved for Smart Cards*** ***1 actor for Passport***
Issuance	Contactless mode personalization (to be developed)	**Contact mode personalization** (mature, proven and secure technology)
Control	Visual/ Optical Character Recognition (OCR) /Contactless systems	**Visual / OCR / Contact / Contactless systems**
Lifetime / Reliability	Unknown (large chip labels)	**5-10 years desirable. Can be achieved with high-end card bodies. However 3 years is current state-of-the-art for any given security level certification.**
Additional Use	Optional in contactless mode	**Possible for contact and contactless:**

		- National ID cards - eGovernment services - Airlines loyalty programmes - eTickets - Asylum seekers - International driver license - EU insurance card - Work permit
Security printed Features	Only on paper passport booklet	**Duplicated (Passport and card)**
Security of electronic data	To be proven (contactless)	**Proven (contact mode)** To be proven (contactless mode)
Electronic control at border	Complex (anti-collision for multiple visas labels)	**Easy (single smart card)**
Personal Data Privacy	Control at issuance and checking points using the reading system of the issuance body	**Control possible by personal smart card reader (contact mode) independent of issuance authority**

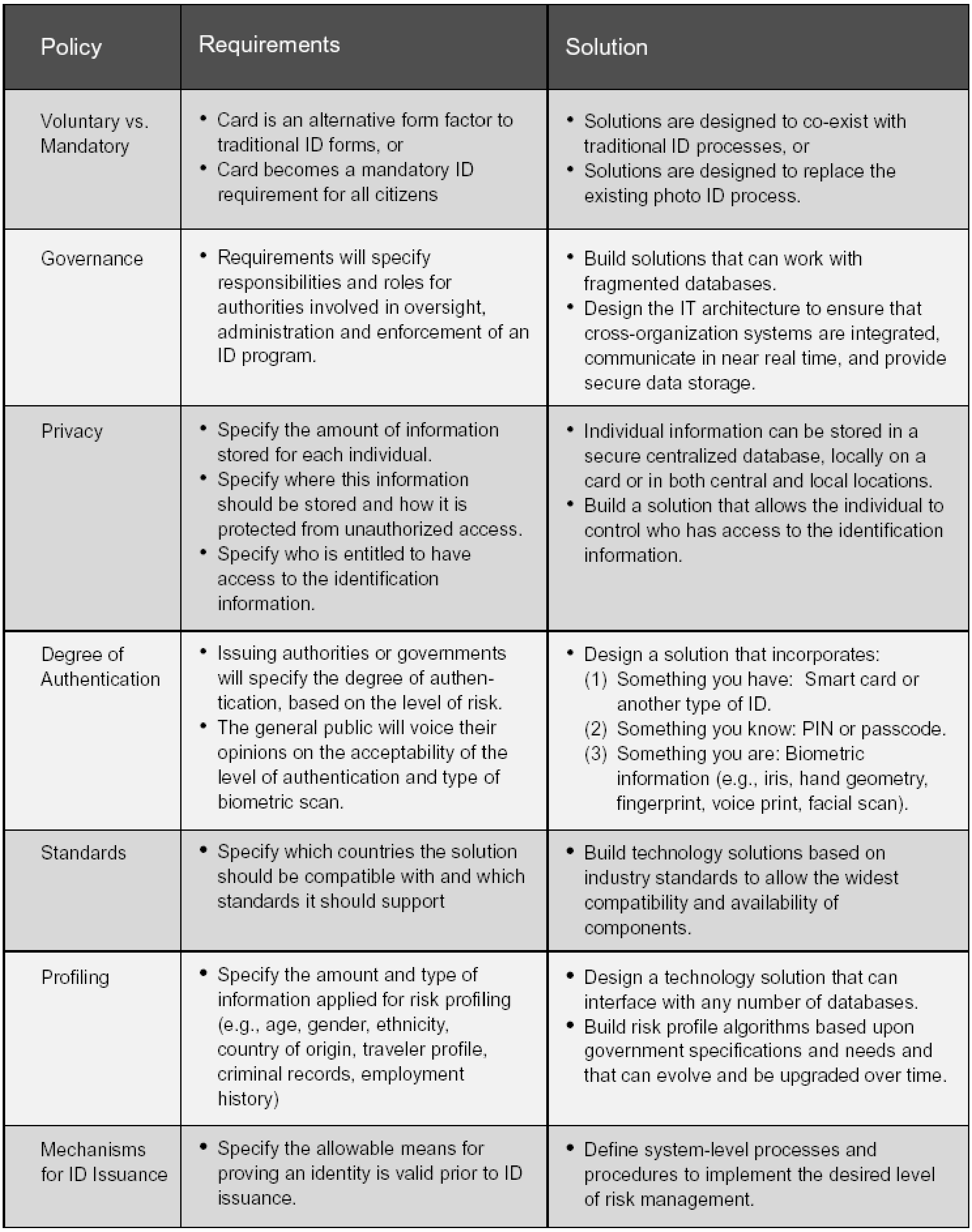
* The proposal is a migration path where the smart card will be first used for eVisas , then additional applications, then epassport

Eurosmart wishes to point out the real advantages and justification for choosing a smart card compared to a electronic label/sticker/lasercard as shown on the table. In fact, some other solutions as the 2D barcode or the Lasercard do not offer the same level of security to protect the privacy: all information are directly readable without any access control. Even if the data is encrypted on this kind of supports, some Hackers are able to crack, modify and reproduce them more easily than a smart card.

Smart Card Technology can implement all requirements of the ICAO recommendations and offers more security, privacy, durability and capability to develop more services (read more about the advantages of the technology in the technical annex).

Smart card is the tool corresponding to the European legislation in force on the protection of personal data and on digital signature. Recommendation for smart cards in the visa and passport applications by the European Community would further support the past and current initiatives aiming at providing security and trust for commercial on-line services, while preserving the citizens privacy, and represents a straightforward progress for future development of e-government services.

Figure 1: Policy Issues Considered in a Secure Personal ID System Implementation



Policy	Requirements	Solution
Voluntary vs. Mandatory	• Card is an alternative form factor to traditional ID forms, or • Card becomes a mandatory ID requirement for all citizens	• Solutions are designed to co-exist with traditional ID processes, or • Solutions are designed to replace the existing photo ID process.
Governance	• Requirements will specify responsibilities and roles for authorities involved in oversight, administration and enforcement of an ID program.	• Build solutions that can work with fragmented databases. • Design the IT architecture to ensure that cross-organization systems are integrated, communicate in near real time, and provide secure data storage.
Privacy	• Specify the amount of information stored for each individual. • Specify where this information should be stored and how it is protected from unauthorized access. • Specify who is entitled to have access to the identification information.	• Individual information can be stored in a secure centralized database, locally on a card or in both central and local locations. • Build a solution that allows the individual to control who has access to the identification information.
Degree of Authentication	• Issuing authorities or governments will specify the degree of authentication, based on the level of risk. • The general public will voice their opinions on the acceptability of the level of authentication and type of biometric scan.	• Design a solution that incorporates: (1) Something you have: Smart card or another type of ID. (2) Something you know: PIN or passcode. (3) Something you are: Biometric information (e.g., iris, hand geometry, fingerprint, voice print, facial scan).
Standards	• Specify which countries the solution should be compatible with and which standards it should support	• Build technology solutions based on industry standards to allow the widest compatibility and availability of components.
Profiling	• Specify the amount and type of information applied for risk profiling (e.g., age, gender, ethnicity, country of origin, traveler profile, criminal records, employment history)	• Design a technology solution that can interface with any number of databases. • Build risk profile algorithms based upon government specifications and needs and that can evolve and be upgraded over time.
Mechanisms for ID Issuance	• Specify the allowable means for proving an identity is valid prior to ID issuance.	• Define system-level processes and procedures to implement the desired level of risk management.

1. Smart Card technologies

As the most secure and reliable form of electronic identification, smart cards act as the cardholder’s access key to information and services in both on and off-line mode. With the ability to store, protect and modify information written to the card’s microchip, smart cards offer unparalleled flexibility and options for information sharing and transfer. The card’s dynamic ability to communicate with information systems expedites traditionally lengthy identification processes, virtually eliminating paperwork and manual data entry, while streamlining operations and reducing costs. Moreover, the smart card’s ability to host multiple applications enables consolidation of multiple services on one card, promoting additional cost savings and efficiency.

Thanks to its multi-application functionality and flexible nature, a smart national ID card plays pivotal role in customizing services to a targeted population. For example, a specific program applying only to an exclusive section of the population, such as a social assistance program, can be loaded to the ID cards for that population alone, rather than loading it onto all cards issued. In addition, the duration of such services can be customized per cardholder, enabling the addition or expiration of services without requiring card re-issuance.

Overall, the use of smart ID cards for the provision of information and services offers significant benefits for both citizens and governments. Citizens using smart ID cards enjoy greater satisfaction through quicker and hassle-free access to information and services. The efficiency, consolidation of programs and the maximum security features provided through the use of smart ID cards, enables governments to achieve their perennial objective: securely improving services to their populations while reducing operating costs.

The smart card is a unique device, easily combining identification with authentication both in the physical and digital world:

Physical identification is provided by visual printed information combined with security printing technologies.

Either using unique PIN card number or storing biometrics information of the cardholder (fingerprint(s)) into the chip, provides physical authentication. Both of them will allow operations that prove the link between the card owner and his/her identity.

Digital identification is provided by demographic data that are stored into the chip (name, age, etc…) and into the digital certificates.

Digital authentication is provided by cryptographic keys and digital certificates stored in the chip, securely linked to demographic data.

And more advantages…

Strong security: Even if certain traditional cards are difficult to forge, they are still subject to unauthorized reproduction and therefore are not secure. Smart cards offer maximum security, through the use of special printing security features (guilloches, OVI, Ultraviolet printing, holograms…) and chip-based security features (cryptography, PKI, biometrics and a unique reference number for each chip). Thus, they are almost impossible to duplicate or counterfeit, and data in the chip cannot be modified without proper authorization and access to keys.

***Off-line verification*:** With a small, portable reader, cards can be checked and are able to provide information from any place, at anytime without further need to access on-line databases. For example, after a vehicle accident, a police officer on site can instantly verify an individual’s identity. Furthermore, pending parking and traffic fines can be read directly from the card, enabling an officer to issue new fines for violations on the spot, simply by updating the infraction directly onto the chip.

Privacy protection: The card’s unique ability to verify the authority of the information requestor allows it to be the perfect guardian of a citizen’s personal information and privacy. Its unique off-line verification capabilities eliminate the need for on-line access to a central database by restricting the data shared to an individual entity, thus controlling citizen privacy.

All of the cardholder's personal information does not need to be revealed every time in order to prove identity. The information required for identification can vary depending on the specific "role" of the individual at a given point in time. I.e. only the data necessary for a defined identification purpose have to be presented to the government authority in question. For example, to the above police officer for a road control (see off-line Verification above), a smart card will present information related to the motor vehicle authority (this information may vary depending on the country or state issuing the license). To a retail shop owner selling alcohol or tobacco, a smart card will only present information related to the age of the ID cardholder, with no reference to the individual's name and address.

Digital signatures: More countries are adopting laws on digital signatures in order to facilitate on-line business and exchanges. Smart cards are considered the best digital signature creation device as it provides maximum security when used within a PKI. Public-key smart cards can securely store private/public owner keys and certificates, and are able to perform digital cryptographic operations such as digital signatures without exposing the private keys outside of the chip.

***Memory capacity*:** While the memory capacity of the traditional magnetic stripe card is very limited, the memory capacity of a smart card is quite significant. For example, today's smart cards offer enough memory to store an identification photo, digital fingerprints and alphanumeric files. Data storage of up to 128 Kbytes is today available for chip cards, but storage capacity could reach 512 or 1024 Kbytes easily if the market requests such products. Costs will vary accordingly. The state of the art silicon technologies offer easily data retention exceeding 10 years.

***Read and write capability*:** The necessity of reading information from, and writing information to a card is obvious in applications such as library services, social assistance services, and parking and traffic violations, to name a few.

A key feature of the smart card is the security level associated with the write and read commands. Indeed only authorized persons can perform these actions, so that the card has to be considered as a vault from privacy point of view .

***Multi-application capability*:** A smart card can host multiple applications for maximum convenience and cost-effectiveness. The same card can be used to access certain protected web sites, to identify oneself to a specific administration, to secure online transactions, and to memorize a personal profile.

In addition to on-line services, that same card can provide city-based services such as social assistance, student and library services, as well as access to city parks, museums and recreational programs.

***Multi-services*:** Different organizations or service providers for the administration of various services can use the same card. For example, the same card can be used by city authorities for secure physical and logical identification, e.g. by the city's Department of Education for student record and campus services, or by the city's social assistance agency for the administration of social assistance services.

***Dynamic card*:** Unlike a traditional ID card, which becomes passive once issued, a smart ID card becomes dynamic. It can guarantee transactions and create connections between unlinked networks, ensuring that card updates can be made on a continuous basis.

***Contactless capability*:** Smart cards also support the use of contactless technology, enabling practise in applications that require rapid and secure identification, such as physical access to buildings and transportation services. The contactless available products today are limited to small memory size because of current market requirements, but data memory size of up to 64 Kbytes is straightforward . 128 Kbytes will appear if required by the market in one year or so .

Card management system : In charge of managing the smart card life cycle , this system can provide a powerful interface between the card itself and the central ID system, as well as manage the applications provisioning, activation and deactivation on the smart card device .

As a conclusion, the smart card industry has developed and deployed products which can easily fulfil the requirements for personal privacy sensitive ID systems. The communications with external networks can be done either through ISO 7816 contact protocol (Enrolment ID control by authority, logical access), or through ISO 14443 contactless whenever it's more convenient (passport, immigration control, airport or other secure areas access control) . Chip and card technology could even combine these two communications approaches, so that the same secure chip with its embedded operating system can be used for various identity applications.

2. ID card technologies alternatives

Various commercially available technologies can be considered as a carrier for personal ID.
We will here review those technologies and identify their respective pros and cons in the deployment of a privacy sensitive personal ID system. Such card provides an easy tool to authenticate the cardholder. However, it can easily be counterfeit.

Plastic cards. Simple plastic cards with printed visual identification information (e.g. individual name, address, photo) are used in numerous applications where information is visually verified when the card is presented for identification.

Bar codes. Bar codes can store personal information and can be printed on plastic cards or paper. Linear bar codes are used to store simple alphanumeric data (e.g. in retail applications). Two-dimensional bar codes can now store significantly more data in a small amount of space. Data is translated into a bar code and embedded on the card during the printing process. The card is then scanned at the point of interaction. Counterfeit of bar code is quite simple to do; anti fraud would require tamper resistance embedding techniques of the bar code on its support and signature or encryption of the data contained inside.

Magnetic stripe cards. Magnetic stripes have been used on cards since the 1970s for a wide range of applications – from financial credit cards to transit cards to driver’s licenses. Identification information is written to the magnetic media during the personalization process and then read by swipe or insertion readers at the point of interaction. A new magnetic stripe standard for cards will provide more memory capacity than available with previous cards. Like bar code printing, serious anti fraud techniques have to be considered to avoid counterfeit.

Optical stripe cards - Optical stripe cards use a technology that is similar to the one used to read and write CDs. Cards with an optical stripe use Write Once Read Many (WORM) recording technology, allowing data to be read and added, but not deleted or erased. Optical stripe cards have an extremely high (multiple megabytes), non-volatile memory capacity and are used in identification, healthcare, logistics management and other applications requiring storage of a large amount of data.

Smart cards - A smart card includes an embedded computer chip that can be either a microprocessor with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microprocessor, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are used worldwide in financial, telecommunications, transit, healthcare, secure identification and other applications.
Such device can combine logical securities (due to the embedded chip) and physical securities (hologram, micro-printing, high durability plastic material …) for visual inspection.

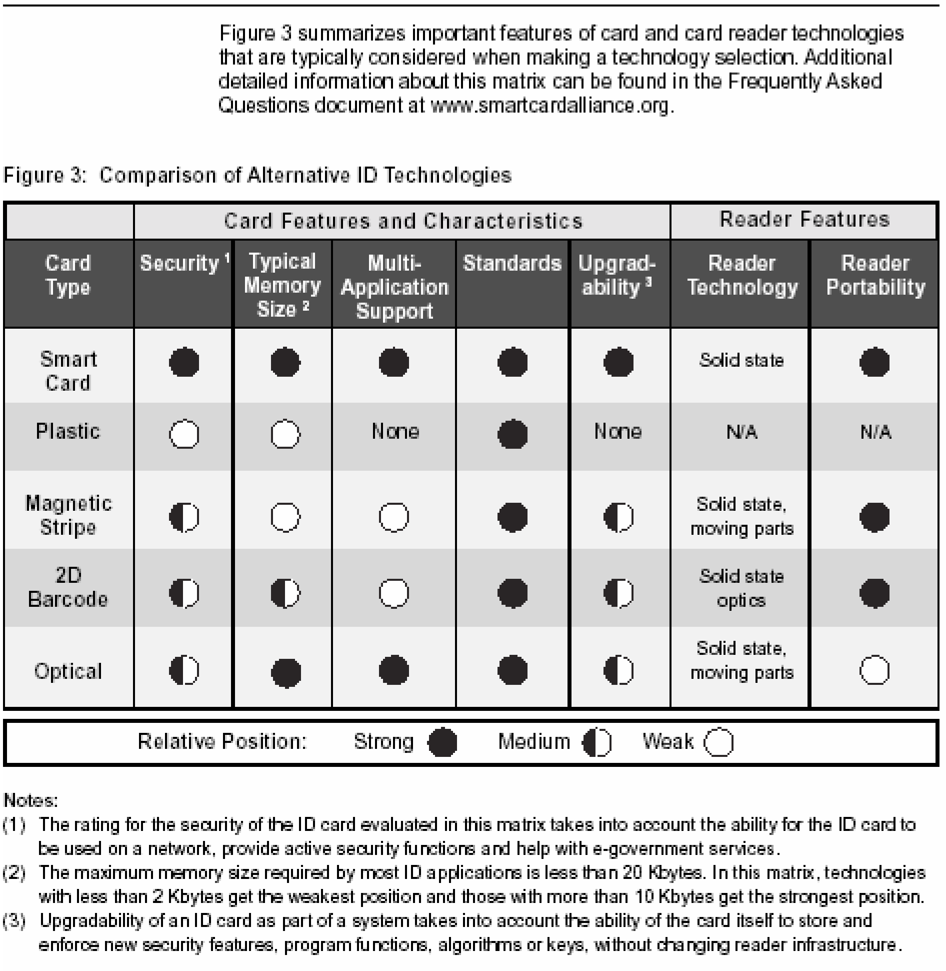


Figure 3 summarizes important features of card and card reader technologies that are typically considered when making a technology selection. Additional detailed information about this matrix can be found in the Frequently Asked Questions document at www.smartcardalliance.org.

Figure 3: Comparison of Alternative ID Technologies

	Card Features and Characteristics					Reader Features	
Card Type	Security[1]	Typical Memory Size[2]	Multi-Application Support	Standards	Upgradability[3]	Reader Technology	Reader Portability
Smart Card	●	●	●	●	●	Solid state	●
Plastic	○	○	None	●	None	N/A	N/A
Magnetic Stripe	◐	○	○	●	◐	Solid state, moving parts	●
2D Barcode	◐	◐	○	●	◐	Solid state optics	●
Optical	◐	●	●	●	◐	Solid state, moving parts	○

Relative Position: Strong ● Medium ◐ Weak ○

Notes:

(1) The rating for the security of the ID card evaluated in this matrix takes into account the ability for the ID card to be used on a network, provide active security functions and help with e-government services.

(2) The maximum memory size required by most ID applications is less than 20 Kbytes. In this matrix, technologies with less than 2 Kbytes get the weakest position and those with more than 10 Kbytes get the strongest position.

(3) Upgradability of an ID card as part of a system takes into account the ability of the card itself to store and enforce new security features, program functions, algorithms or keys, without changing reader infrastructure.

From the above Fig 3 Table (Source: Smart Card Alliance Report), it becomes very clear that Smart Card is the most appropriate technology for ID applications .