SECURE COALITION ID

Protecting Identity with Technology

Testimony of

Neville Pattinson, Vice President Gemalto

On behalf of the Secure ID Coalition

Before the Subcommittee on Government Management,

Organization and Procurement of the

Committee on Oversight and Government Reform

# *Technology for Secure Identity Documents*

**October 18, 2007**

Good afternoon Chairman Towns and Ranking Member Bilbray. Thank you for including me on behalf of the Secure ID Coalition on this panel to discuss the increasingly important issue of identity management and technology for secure identity documents.

For the record I must offer a disclosure. I presently serve as a special government employee to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee (DPIAC). Nothing I say here today represents the views or opinions of the Committee or the Department of Homeland Security. My views expressed today are those of myself, my employer, Gemalto and the Secure ID Coalition.

This important hearing comes at a critical point in the public policy debate as concerns about border crossing, immigration, homeland security and REAL ID have created demand for secure identity credentials. As part of this testimony I will detail and differentiate technologies used in current ID documents and describe what features are needed to create a secure document that can not be tampered with, forged or cloned.

IT IS CRITICAL THAT ANY DOCUMENT USED FOR IDENTIFICATION OF A PERSON MUST INCORPORATE THE HIGHEST LEVEL OF SECURITY AND FEATURES THAT PROTECT PERSONAL PRIVACY.

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents. Our mission is to promote the understanding and appropriate use of identity technology that achieves enhanced security for ID management systems while maintaining user privacy. Member of our coalition manufacturer many different varieties of ID technologies so, we are uniquely positioned to offer expertise in this area.

My company, Gemalto, is a member of the Secure ID Coalition and is a leader in digital security with operations in about 100 countries and over 10,000 employees including 1,500 R&D engineers. Gemalto provides end-to-end digital security solutions, from the development of software applications through design and production of secure personal devices, often termed Smart Cards, which incorporate a small highly secure computer chip. Part of our portfolio includes smart ID cards, SIMs, e-passports, and tokens which all help the administration and deployment of identity management services for our customers. More than a billion people worldwide use the company's products and services for telecommunications, financial services, e-government, identity management, multimedia content, digital rights management, IT security, mass transit and many other applications.

Smart ID cards have been adopted and deployed in many important government programs around the world including: driver's licenses, health benefits, border crossing, defense, voting and in some countries national ID cards. In the U.S. Gemalto continues to supply smart card technology to the Department of Defense's Common Access Card program; to agencies rolling out HSPD-12 compliant PIV cards; to the Department of State's electronic-Passport program; we have provided cards to the Transportation Worker Identification Credential (TWIC) program; State Assistance programs such as WIC and Medicaid in Texas are now also using our Smart Cards to prevent fraud and abuse of those benefit programs.

What is a smart card and what can it do for securing somebody's identity? Put simply smart card technology consists of a sophisticated electronic computer chip embedded in a plastic card body. The chip has an operating system which provides the features and functions for a particular application. The success of smart card technology is in it's ability to provide strong security and privacy protections to each individual, in a convenient form. Consider the computer chip as an electronic security agent, representing the issuer of the ID, in the hands of the user. The chip security and communication protocols ensure information security and privacy. Many variations of smart cards exist that are all based on International Standards (ISO 7816 & 14443) and are designed to meet the challenges of each specific application. Some cards communicate either directly (contact) to a reading device or over short range wireless connections (contactless). Whatever method used in a secure smart ID card the underlying security ensures both electronic document authentication and user authentication before transacting any credential information. No other technology can offer all these features in a cost effective and convenient manner to ensure identity security and authentication.

Over the past six years there has been a proliferation of ID programs within the federal government. In most cases these ID programs are developed and implemented independent of similar work taking place within other agencies; often operating as islands or stove pipes developing and requiring different rules and different technologies for programs that are, for the most part, trying to accomplish the same thing. One of the major failings currently in government ID management and ID programs is that there is no unified policy for identity and credentialing processes or documents. In every case, the decision on how to address security of the system and the document itself and the privacy protections of those to be credentialed in the ID systems, are left up to the agency implementing the program. There is no guidance for an appropriate policy framework and very limited oversight.

Instead of learning from the other agencies or departments' implementation challenges and successes each agency is forced to go it alone and "reinvent the wheel" when they decide or it is mandated that they implement an ID program. In many cases hard working federal employees take the time to research other government uses and understand industry best practices and then use those tools to their advantage to meet their challenge. However, in some instances unrealistic programs proposals are proffered without any sense of understanding about the technologies available or the best practices and standards for security of the program and the privacy of those individuals to be credentialed.

Many ID programs are being implemented because of the need for added security to know who is entering either a government building, military installation, port, computer network or, and I would suggest most important, our country across our borders. In some cases programs are being developed and implemented with security flaws that allow for elementary and easy exploitation. These mistakes are being made because there is limited understanding about the technologies being suggested and no clear guidelines that have been established as a point of reference. Further the vulnerabilities exist in some cases because there is pressure to "just get it done". Efforts to quickly get a program up and running often lead to short cuts the inevitably undermine the programs goals and objectives.

As much as security is the foundation of the all the new identity programs and the guise under which they are being taken up, privacy plays a central and critical role in any ID program. If users, and in many cases, citizens don't have confidence in the technology they are being issued, then programs will immediately become ineffective. Privacy must be accounted for in the design, evaluation and implementation of any identity system. It is for this reason that we are alarmed to understand even though government programs are required to go through a Privacy Impact Assessment (PIA) process in many cases the assessment does not sufficiently address the ID document and those assessments are started many months after the program is well underway. At that point there is almost no ability or willingness to make design or technology changes that will enhance the privacy of those in the system.

Identity documents are a special category of documents which require special consideration. An identity document once issued must attest to the identity of an individual and offer a credential which can be trusted. The presentation of an identity document is usually in connection with the individual having been enrolled in a program and issued an ID. That same individual is now requesting access to a facility or service bound by the presentation of a particular ID. If there is a weak chain of trust in between the ID document, the individual and the ability to authenticate the claimed identity, there opens up a vulnerability which maybe exploited. The consequences of this vulnerability may lead to the impersonation or fraudulent use of the credential which will have significant repercussions to the integrity of the identity system and the assets it is protecting. . Therefore the more effort taken to ensure that a chain of trust can be established between the ID document presented, the user presenting the ID and the validity of the credential, the more confident we are that this person is who they claim to be and the ID does belong to them.

To reinforce the chain of trust in an ID system, a number of technologies exist today that are often aggregated together in different combinations to address specific ID system challenges. Where high levels of identification assurance are required several types of security and authentication technologies are combined together. Government issued ID cards today mostly incorporate physical, forensic and electronic document authentication.

Figure 1: Security Features as applied to existing US Government ID programs

| | | | **Security Features** | | | | |
|---|---|---|---|---|---|---|---|
| **Programs** | **Physical Security Printing** | **Basic Access Control** | **Encryped Comms** | **Mutual Auth.** | **MRZ** | **RF Distance** | **Electronic PII** |
| ***e-Passport*** | Yes | Yes | Yes | Yes | ICAO | 4" | Yes |
| ***TWIC*** | Yes | | Yes | Yes | | 4" | Yes |
| ***DOD - CAC*** | Yes | | Yes | Yes | | 4" | Yes |
| ***HSPD-12*** | Yes | | Yes | Yes | | 4" | Yes |
| ***PASS Card/EDL(RFID)*** | Yes | | No | No | ICAO | 30' | DB Number |
| ***REAL ID (proposed)*** | Expected | | | | Bar Code | | |

Identity Card Technologies and features may be classified into one of four classes. These classes are;

1. Physical Security features which are used for
    a. Visual document authentication, such as:
        i. Rainbow color shading
        ii. Color changing inks
        iii. Printed security patterns
        iv. Holograms
        v. Optical variable devices
        vi. Laser marked overlays
    b. Secondary document authentication, such as:
        i. Microprinting
        ii. Printed fine line patterns
        iii. Hidden or deliberate error features
        iv. UV inks

v. Infrared reactivity

c. Personal Card holder verification

i. Printed Facial photo

ii. Printed Biographical information

2. Forensic security features for detailed document authentication

a. Taggants (Unique chemical markers)

b. Chemical ink composition

c. Plastic body lamination chemistry

3. Machine readable Identifiers;

a. Bar codes

b. Magnetic stripe

c. Laser stripe

d. Electronic RFID numbers

e. Optical Character Recognition

4. Electronic Authentication technology (e.g.Smart Card); used for

a. Electronic Document authentication

b. Terminal (external equipment) authentication

c. Credential authentication.

d. Card holder authentication

i. PIN codes

ii. Biometric matching

e. Secure, confidential encrypted transmission of information

f. Perform non-repudiation of cryptographic based transactions

g. Maintaining privacy and security of credential whilst ensuring vigilant access controls

h. Exponentially increasing the difficulty to counterfeit the document

When considering an identity program the security document technologies and features just mentioned are available to address a wide range of issues. The more features the harder the document will be to counterfeit or misuse. However, the inclusion of smart card technology is essential to any true secure identity document as proven in U.S.

government programs. Any identity program that is established to protect our national security and homeland must incorporate smart card technology. Smart cards are incredibly difficult to tamper with, forge or clone and, provide a deterrent to those attempting to do us harm. Programs that go forward without secure electronic authentication technologies offer an open invitation to be exploited. Smart cards are cost effective, proven technology that is highly adopted in identity programs to protect assets in the U.S. and around the world.

In conclusion we offer three recommendations to the Subcommittee as they begin to address concerns about identity management programs and look at security of identity documents themselves.

1) We ask the Subcommittee to examine programs used to identify citizens on a government wide basis and ensure that they utilizes the highest levels of document security and include citizen privacy protections.

2) Further, we ask the Subcommittee to task the National Institute of Standards and Technologies (NIST) to develop a comprehensive body of work that reviews all standards and technologies associated with identity and evaluate them based on the security needs of our country, and privacy concerns of our citizens. The output of this directive must establish a national standard for identity credentials to which programs must adhere.

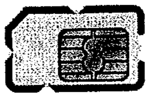
3) On a more immediate note we ask that the Subcommittee review the proposed implementation of two U.S. Government identity programs that have raised concerns of the identity industry and privacy community because they fail to meet minimal security best practices and citizen privacy protections. These programs are the proposed WHTI PASS Card and the recently fashioned Enhanced Driver's License, which are both incorporating technologies that do not provide adequate security and privacy protections for our citizens' identities.

The Secure ID Coalition looks forward to working with the Subcommittee as you begin to address this important and critical issue area of secure identity documents. Please consider our group a resource for expert information and technical assistance. Thank you for your time and I am prepared to answer any questions the Subcommittee might have at this time.

Attachment 1:

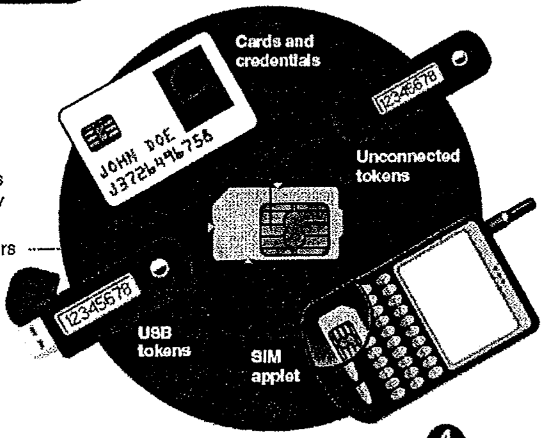
# Gemalto's microprocessor card technology

## WHAT IS A SMART CARD?

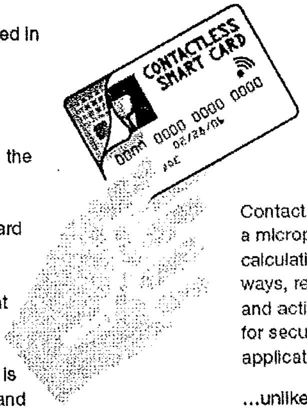


1 A smart card is **a little computer** with 100s of built-in security features.

2 It has many form factors



3 It can be used in contactless situations



At a retailer, the card owner simply holds the card within two inches of the payment reader.

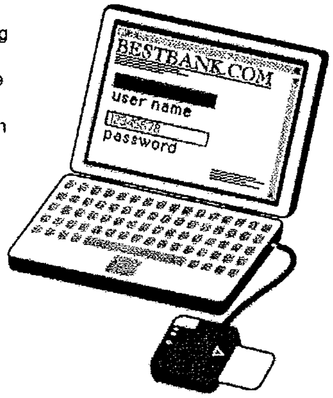
No swiping is necessary and the card never leaves the owner's hand.

Contactless smart cards contain a microprocessor that makes calculations, communicates both ways, remembers new information and actively uses these capabilities for security and many other applications...

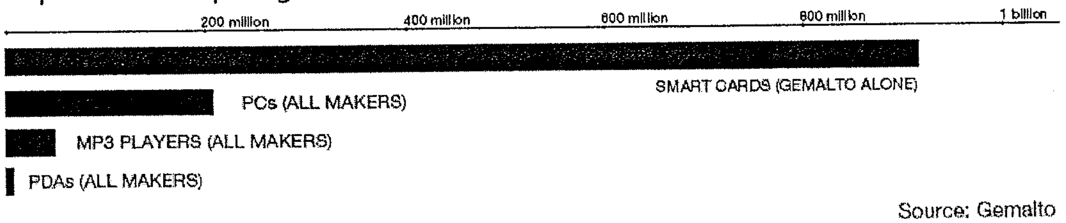
...unlike RFID tags, which are devices that typically have a read-only chip storing a unique number but with no processing capability.

4 It can be used in contact situations

Smart cards make online banking and purchasing more secure, and can create a vault where passwords can be accessed, all via a single card inserted into a reader.



Shipments of computing devices, 2005



Source: Gemalto

Attachment 2:

# The difference between contactless smart cards & RFID tags

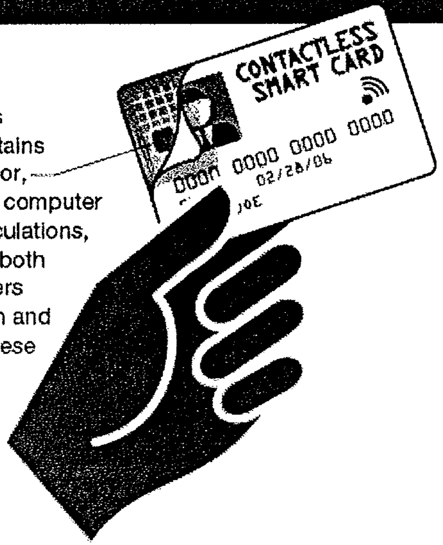
## Overview: what happens in RF (radio frequency) communication

1 When a contactless smart card or an RFID tag passes within range, a reader sends out radio frequency electromagnetic waves.

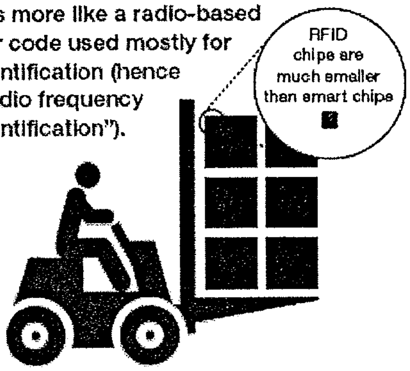
2 The antenna, tuned to receive these waves, wakes up the chip in the smart card or tag.

3 A wireless communications channel is set up between the reader and the smart card or tag.

The contactless smart card contains a microprocessor, a small but real computer that makes calculations, communicates both ways, remembers new information and actively uses these capabilities for security and many other applications.



RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. It is more like a radio-based bar code used mostly for identification (hence "radio frequency identification").



## Characteristics of a contactless card

- Strong security capacities:
  - mutual authentication before providing access to information
  - access can be further protected via PIN or biometric
  - encryption to protect data on card during exchange
  - hardware and software protection to combat attacks or counterfeiting
- Hundreds of security features mean an individual's personal ID, financial details, payment transactions, transit fares or physical access privileges can be safely stored, managed and exchanged
- Read and write memory capacity of 512 bytes and up, with very large memory storage possible
- Short distance data exchange, typically two inches

Source: Gemalto

## Characteristics of an RFID tag

- Minimal
  - one-way authentication; card cannot protect itself
  - insufficient storage for biometrics
  - no on-chip calculations of new information
  - relies on static keys
- Single function; used to help machines identify objects to increase efficiency. Example: inventory control
- Small memory (92 bytes); often read-only
- Larger distance data exchange, typically several yards

Because of their more restricted capabilities, RFID tags are generally cheaper.

Attachment 3:

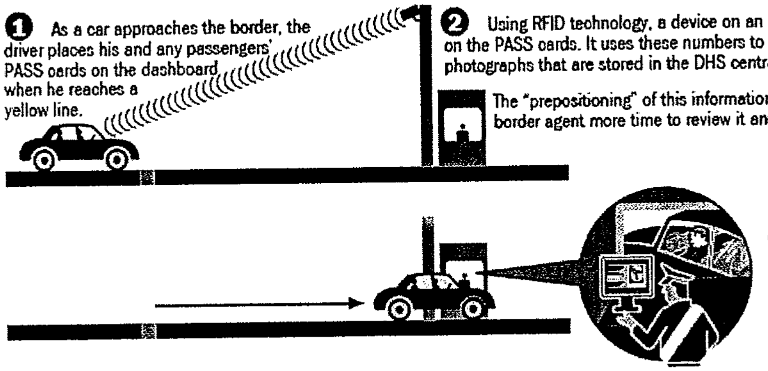
# PASS cards: Smart card technology is better than RFID

## OVERVIEW

The State Department in conjunction with the Department of Homeland Security is developing PASS cards–a nev way for Americans to re-enter the United States from Canada and Mexico.

The purpose is to increase security at the borders, where currently all you need is a driver's license. PASS cards are intended to be a lower cost alternative to passports.

## HERE'S ONE PROPOSAL: USING INSECURE RFID TAGS



1 As a car approaches the border, the driver places his and any passengers' PASS cards on the dashboard when he reaches a yellow line.

2 Using RFID technology, a device on an overhead gantry 30 feet away reads the numbers on the PASS cards. It uses these numbers to look up the card holders' identity information and photographs that are stored in the DHS central database.

The "prepositioning" of this information will give the border agent more time to review it and make decisions.

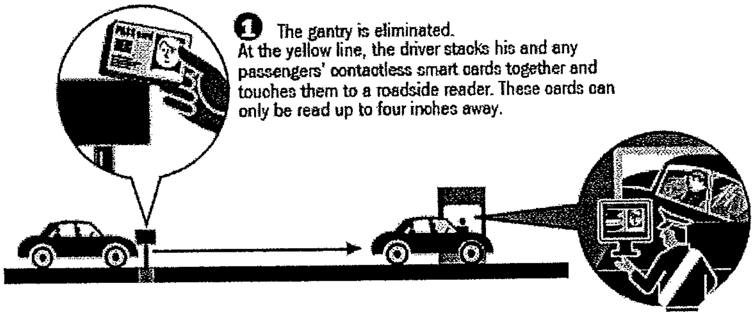
3 The car moves on to the red line where a border official sees that the driver and passengers match the photos received from DHS servers.

## PROBLEMS WITH THE RFID METHOD

Because RFID technology is designed for product tracking, it's not a technology that protects people's identities...

- **...it's not secure**
  Anyone (with an RFID reader) within 30 feet of the traveler can read the card and clone it.
- **...there are privacy issues**
  Anyone with a PASS card can easily be identified as an American.
- **...it won't speed up traffic flow**
  The PASS card is not like a toll collector tag for your car, where you just roll through; here, all drivers must stop for a visual verification.

## A BETTER METHOD: SECURE SMART CARDS



1 The gantry is eliminated.
At the yellow line, the driver stacks his and any passengers' contactless smart cards together and touches them to a roadside reader. These cards can only be read up to four inches away.

2 At the red line, the border official checks the prepositioned data on his computer screen to verify the driver's and passengers' identities.

No one other than the border official can read the cards because the information sent from the smart cards is encrypted.

## ADVANTAGES WITH THE SMART CARD METHOD

Because a contactless smart card is **a small computer** with 100s of built-in security features that protect the information in it...

- **...it's secure**
  The card encrypts all communications, has a short read range of four inches, and only transmits to a validated reader.
- **...it protects privacy**
  No unauthorized person can "read" the information on the card, preserving the citizens' privacy.
- **...it's just as fast**
  Information can be prepositioned in the same way as with insecure RFID tags.

**Source: Gemalto**