WRITTEN TESTIMONY OF KATHRYN K. ALSBROOKS
DIRECTOR, US FEDERAL PROGRAMS
LaserCard CORPORATION

Before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Government Management, Organization and Procurement

Thursday, October, 18, 2007 2:00 p.m.
Rayburn House Office Building Room 2247

Chairman Towns, Ranking Member Bilbray, and other distinguished members of the subcommittee – I thank you for the opportunity to appear before you today to discuss LaserCard's role in secure ID programs currently underway and our experience in addressing the challenge of "how to make a secure, tamper-proof ID card" – one that delivers both automatic biometric ID verification *and* fulfills today's need for reliable visual inspection – that is, use as a "Flash Pass" - when automatic authentication is not available.

LaserCard Corporation:
LaserCard is a publicly held US company headquartered in Mountain View, California. For 20 years we have been an industry leader; conducting research, development and manufacture of highly secure, multi-biometric identity and credentialing technologies.

While LaserCard's optical memory card fully addresses the needs across a spectrum of ID application requirements, today, I will focus my remarks on visual and physical security of ID cards utilizing LaserCard's optical memory technology.

The technology is deployed today in the following national-level secure ID applications:

a) The U.S. Permanent Resident Card "Green Card" issued by U.S. Department of Homeland Security.
b) The "Laser Visa" Border Crossing Card issued by U.S. Department of State to screened Mexican citizens who frequently cross the border into the United States.
c) The Canadian Permanent Resident Card issued by Citizenship and Immigration Canada.
d) The Italian Citizen ID Card and Foreign Resident Card, both issued by the Italian Ministry of Interior.
e) And the Saudi National ID Card issued by the Saudi Ministry of Interior.

More than 30 million of these cards have been issued to date. The pre-eminence of optical memory in North American ID security is reflected in these two facts:

First, according to statistics published by US-VISIT, the roughly 20 million optical cards in circulation in the Western Hemisphere represent almost 80% of all US land border entries by foreign nationals.
Second, in over 15 years of use, the digital data security of the optical memory card has never been compromised.

LaserCard has also supplied the U.S. Department of Homeland Security with more than 1,000 Biometric Verification Systems which are used at Ports of Entry to automatically authenticate these cards and, where appropriate, verify the cardholder's identity with fingerprint biometrics.

Western Hemisphere Travel Initiative
To meet the requirements of the Western Hemisphere Travel Initiative (WHTI) - LaserCard has developed the polycarbonate-based LaserPass, which combines the convenience and facilitation advantages of RFID with the unbeatable visual security of optical memory.

In this world of advanced machine readable technologies – including our own - why do we maintain our constant focus on visual security as a fundamental requirement? The answer is simple: today, visual inspection of ID cards is *the norm*. The implementation of comprehensive infrastructures to machine-read and authenticate ID documents is a huge undertaking – indeed, Customs and Border Protection officials have stated that RFID readers will be installed at only 39 land Ports of Entry. Clearly, visual inspection will remain an essential border entry procedure for the foreseeable future.

Secondary Uses of WHTI cards – Establishing Identity: The more successful the WHTI card deployments (including the PASSport Card, Border Crossing Card, Nexus-Sentri & FAST) the more widely they will be accepted, requested and inspected as the *de facto* means for establishing identity in "flash pass" scenarios, such as airline check-in, airport security, and boarding, employment eligibility, building entry, provision of government services, and banking. And, let's make no mistake here – some of these cards will confirm US Citizenship. An easily copied document will become the counterfeiter's product of choice.
For all these reasons, the highest level of visual security in the WHTI cards is absolutely essential.

Document Security

Document security requirements include:
- Ease of visual authentication,
- Strong resistance to counterfeiting and tampering, and
- Certainty of automatic authentication.

Visual Authentication
Today, visual inspection of identity documents is the norm. The implementation of a government wide infrastructure to authenticate and read an ID card is an enormous undertaking. Given that issuance of new ID cards to millions of cardholders will take years, visual inspection will remain with us at least in the interim. The more successful the program is, the more widely will the card be accepted, requested and inspected as the *de facto* means of ID. In such a situation ease of visual authentication is essential.

Optical memory is unique among all advanced ID card technologies in being able to fully meet the needs of today's reality - visual inspection - and provide a transition to tomorrow's environment of fully automatic authentication and transactions. And optical memory supports this transition while preserving the highest level of security. In addition to storing digital data in a highly secure manner, optical memory incorporates easily verified visual security features that support authentication of the card *and* verification of the card holder's information and identity. These features *cannot* be altered and serve to confirm other information visible on the card.

Additionally, optical memory can include covert features (requiring a simple magnifier) supporting second level verification, and forensic features supporting laboratory inspection and criminal investigation. This layering and blending of overt, covert and forensic features provides progressive, hierarchical steps in the visual authentication process and an unequalled level of counterfeit resistance.

Counterfeit and Tamper Resistance

Typical criminal attacks on ID documents include the production of "look-alikes" or the altering of genuinely issued documents to another identity, e.g., by photo or image substitution.

Forensic experts strongly advise card and document issuers not to rely on one security feature alone for counterfeit and tamper resistance. They generally favor a "layers on the onion" approach where a combination of features collectively raises the hurdle for criminals seeking to compromise the system. As described above, optical memory provides an intrinsic and unique layering of security features - overt, covert and forensic - combined in a physically unalterable medium to provide certain visual authentication.

Added to this, digital data stored on optical memory *cannot* be altered. This is in stark contrast to inherently erasable storage media. The best-case result of a successful attack on erasable memory (i.e., the attack is detected) is likely to be the enormous logistical and cost burden of replacing all issued cards. The worst case - where the attack may not be detected for a period of time - can result in a catastrophic security breach.

It is worth restating at this point: Optical memory is non-erasable; *its stored data cannot be fraudulently altered.*

In many jurisdictions, information stored on such optical storage media is accepted as evidence in criminal proceedings. The optical memory's ability to store a complete audit trail or history of events in the card's life supports the testimony of forensic experts in counterfeiting and forgery prosecutions. No erasable memory form can comply with this requirement.

Automatic Authentication

Inherently erasable card memory generally needs the support of on-line verification as a defense against criminal attacks. This can include the need for Public Key Infrastructure

(PKI), a complex, costly means of authenticating the card and its transactions. In addition, dependence on on-line functionality may represent an unacceptable risk since the network, as the principal target of hackers (whether mischievous, criminal or terrorist in their intent), potentially becomes a single point of failure.

Optical memory has the advantage of not requiring PKI *and* it can be used securely off-line, obviating the need for a high-cost, totally ubiquitous network infrastructure. Additionally, even in a traditional on-line environment when networks slow down due to overload (or go down due to failure or malicious attack), optical memory can still run securely off-line, maintaining the functionality and integrity of the system.

It is also worth considering that the optical memory acts as a robust back-up to erasable memory which may be accidentally or deliberately erased or corrupted by electromagnetic forces.

Identity Verification

Biometrics

The only way to reliably verify an established identity is through the use of biometrics. While debate continues about which is the most effective, reliable and secure biometric method, it is clear that not all inspection authorities and government agencies will use one and the same biometric technology. This introduces the need to accommodate multiple biometrics and to assure transportability of the data used for ID verification. The use of multiple biometrics, e.g., face and fingerprint, can enhance security where they are used in combination or at random.

Thus the ultimate key to efficiently and effectively verifying a person's identity in multiple agency settings is to provide portability of multiple biometrics.

Whatever biometrics are used, it is very important to be sure that this data cannot be altered to coincide with an impostor's identity. Ultimate surety rests in a memory form than cannot be fraudulently altered.

Transportability

Optical memory has a significant advantage here in that it can store effectively any and all biometric data likely to be used while other memory forms are limited in capacity and flexibility. Not only can optical memory store any number of biometric templates, it also easily accommodates the storage of the original images, such as fingerprints and face, as recommended by NIST and other bodies for transportability of biometrics across system boundaries.

The storage of original images requires a significant memory capacity and, today, the only available proven, secure and durable card technology with sufficient capacity is optical memory.

Other Considerations

Future proofing

Without question, any card solution adopted for government-wide and long-term programs must be as "future-proof" as possible. Only optical memory among all card technologies has the capacity and updateable storage to handle any unforeseen eventualities *without the need to re-issue the card*.

Thus program designers are not constrained to foresee every use of the card from Day One and have the comfort of knowing that the optical memory's "scalable" storage can comfortably accommodate any upgrades, updates and additions through time.

Protection of Privacy

Optical memory's capacity to securely store personal information allows the cardholder to volunteer information on the card, under the principle of "informed consent", by deliberately handing the card over or inserting it into a card slot.

Optical memory cannot be remotely interrogated by radio frequency technologies.