



**Smart Card
Alliance**

Secure Personal Identification Systems:

Policy, Process and Technology Choices
for a Privacy-Sensitive Solution

Frequently Asked Questions

February 2002

Smart Card Alliance
191 Clarksville Road
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 212-571-0100

Frequently Asked Questions

1. **Why is a smart card the ideal alternative for a privacy-sensitive secure personal ID system?**

A smart card is the only alternative that can securely combine several applications and technologies onto one card, providing both convenience and security while minimizing the need to present personal, private information. With a smart card-based system, there is no technical requirement to have a central database system that observes all requests for services. Because the smart card is an active device (a small computer), the card is able to give only that information that is required for the specific service at the time the card is presented.

2. **Are privacy rights of individuals at risk as we move closer to a standardized identification system?**

Yes. There are potential impacts on privacy with any new identification system, particularly one that relies on large interconnected databases. It is prudent that privacy concerns be kept in the forefront during the design of identification/security systems. But, as mentioned previously, a smart card-based system does not require a central database of information and can have an active interaction with the information requestor. Services and participant information can be distributed to those points where the service takes place. The unique ability of the smart card to verify the authenticity and authority of the service request allows it to be the best guardian of the card owner's personal information.

3. **Aren't biometric systems alone enough to prove an individual's identity as they pass through critical check points such as airports or border crossings?**

They may be, but having only a face, fingerprint, or other biometric available for identification requires a large, very fast and as yet undefined infrastructure. Having a smart ID device, which supports existing authentication infrastructures and which can compare the biometric at the point of interaction, allows much more flexible identity authentication with less impact on privacy. This is because it is not necessary to record who passed a security point, only to verify that the individual's identity had been previously authenticated.

4. **What prevents a smart card from being counterfeited?**

Smart cards are created with a unique identifier and contain keys that are unique to each card. In order to create a new card, some cryptographic keys are required which are in none of the smart cards in the field, but only available from a secure card initialization center where the cards are issued. Duplication of a smart card requires access to the entire memory of the card, including the private areas, or private objects, which the card never reveals.

5. How is a biometric template created on a smart card, and what stops someone from overwriting the card with his/her own biometric?

A biometric template is an encrypted hash of the actual biometric itself. Once created, the template is digitally signed and locked onto the card by the issuing authority. Any attempt to overwrite would not be authenticated by the issuing authority as the smart card prevents modifications of its memory by anyone who is not correctly authenticated.

6. What protection is there from stealing the biometric template from a stolen card?

Smart cards are tamper resistant and are often the most secure link in the whole security chain of an application. Smart cards contain internal thresholds which allow them to detect if the card environment is being "hacked". Under these circumstances, the card will either shut itself down (stop responding to the reader) or, if the application demands, even destroy its memory to protect its private objects.

7. Optical cards are growing in use as secure identity cards for various applications; do these provide a strong alternative to the smart card?

Optical cards have an advantage in that they can store megabytes of data and have very strong counterfeit resistant features built in the card material during manufacturing, issuance and update of the information on the card. They are passive Write Once Read Many (WORM) memory devices with no ability to actively protect access to secret data (such as private keys or personal information) or to process data (such as digitally signing information). Applications such as immigration control, which can secure and control access to the readers/encoders required by optical cards, can use the optical card security features and rely on its visual security features to detect potential fraud. Developing a similar manufacturing capability and getting access to the optical card readers/encoders is difficult for counterfeiters because they are subject to strictly controlled distribution.

8. Aren't there alternative form factors (other than cards) that could be used for identification?

Yes, there are alternative form factors, such as USB tokens and PCMCIA cards, that could be considered. These form factors, however, are more typically considered when there is no need for a photo on the identification card or when the identification token is being used with a computer for secure network identification. In most applications where an ID token is used for the physical identification of an individual, a visual photo ID is critical to support backup identification processes.

-
9. **Why do optical memory cards, which have been used successfully by the Immigration and Naturalization Service in the US since 1998, get only a medium security grade rating in the technology comparison matrix in your paper?**

Optical memory cards used by US Immigration are very secure documents relying on the highly sophisticated laser printing technology used to manufacture and encode them. This, added to the fact that the readers/encoders are always in a secure environment and reader/encoder distribution is either controlled or regulated, makes the use of such cards a secure solution for this application. However, when ID cards need to be used by their legitimate users over non-secure networks (such as the Internet) to benefit, for example, from e-government services, they need to be intrinsically secure and be able to support active authentication, independent of the card readers/encoders. Both the ID cards and the ID card readers may be used in potentially hostile environments, such as on home and corporate networks.

10. **Why does the technology comparison matrix in your paper show that optical memory cards get the same memory “grade” as smart cards, which have much less memory space available?**

Optical cards have a much larger memory size than existing smart cards (4.1 Mbytes compared to 64 Kbytes for commonly used smart cards). The comparison matrix gives the same rating to both technologies (maximum) since most ID applications do not require more than 20 Kbytes, including a cardholder’s picture, biometric templates and digital certificates.

11. **What is the meaning of “Upgradability” for a card in the technology comparison matrix in your paper?**

Upgradability of a card is not a function of its ability to store a large amount of data. Smart cards get the maximum rating for this feature for their unique ability to be securely directed to change their internal programs, algorithms, application features and even keys without any impact on the infrastructure or the reader programs. For example, when a new application decides to use a new authentication algorithm, or a different key size, only the program which will be downloaded in the cards needs to be changed. Existing readers and cards without the new application do not need to be modified, making the system easier to upgrade.

12. How big is the investment in the infrastructure required for an identification system?

The investment size will depend on the technology chosen and the breadth of deployment. The total system cost includes ID card design, issuance and management costs, card reader cost, biometric reader cost (to read the individual's physical biometric, if required), and other supporting infrastructure costs. Costs also include the redesign of identity verification processes, and personnel retraining and staffing. The design of any secure personal ID system must balance the total cost (initial and on-going) with the desired risk management profile. For systems requiring a high degree of security, smart cards provide a proven, cost-effective solution, balancing initial cost with the highest security architecture and the flexibility to more easily modify and upgrade the system over time.

13. If the identification system is voluntary, why would an individual choose to participate?

An identification system that combines a smart card with other identifying technologies, such as a biometric, greatly boosts security while easing the frustration of individuals waiting to pass through checkpoints. Any voluntary identification system will need to consider incentives to encourage individuals to obtain the personal ID card. For example, a system supporting airport security might offer personal smart cards carrying biometric data to frequent travelers that agree to background checks. Those carrying the ID cards may then be allowed to bypass more lengthy security processes.

14. How do you prevent a “bad guy,” with no previous criminal history or with a stolen identity, from obtaining a valid ID card?

Any security system is only as good as its enrollment process. If someone presents stolen or fraudulent identity information, such as a stolen or counterfeit passport, at the time of enrollment and card issuance, then this imposter could potentially be given a valid ID card. The enrollment process must take the necessary precautions to validate an individual's identity before issuing an ID card.

15. Won't the widespread use of machine-readable ID cards give us all a false sense of security, thus relaxing our human vigilance?

Maintaining a high degree of security requires a process that includes both human and technology elements. A machine-readable secure personal ID card can help to limit the personal bias or judgment errors of humans verifying identity and provide a more robust identification process. They do not, however, remove the need for trained security staffing at security checkpoints.

16. For the highest security, shouldn't there always be an online identity verification process that validates identity using a central database?

This would depend on the desired level of risk management that the system must implement. While online verification would give the most "accurate" information in terms of the "last update," it would require a secure and fast linkage to accomplish, raising the system cost and increasing the time required for the identity validation process. In many situations, it may be risk acceptable to do a local risk evaluation to determine whether or not to go online (as done with EMV card implementations worldwide). For example, using smart card technology, it would be possible for a police officer to record immediately in the card when a ticket is issued. This information could include a note of "judgment or payment pending" until the next time the card connects to the central database and gets an update. It would also be possible to note in the smart card the last time the card was online with its issuer. A smart card based system can improve privacy, help speed identity validation processes, and still be very secure. Smart cards allow each business to adjust to the level of security compatible with its desired risk management profile.

17. What are other implementation issues that need to be considered in addition to the selection of the identity token?

The selection of the identity card technology is one factor that needs to be considered in the design and implementation of a secure personal ID system. As discussed in the paper, there are policy issues to consider, upfront identity validation, card issuance and card management processes to be defined, system infrastructure to be developed and security personnel to be re-trained. The overall process and system design must take these factors into account since they affect the overall cost and complexity of a system implementation. The selection of identity token or card technology is an important factor in the overall system design, cost and risk management capabilities.

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, healthcare, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.

Publication Acknowledgements

This FAQ was developed by the Smart Card Alliance to discuss the implementation and technology issues associated with secure personal identification systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance. The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their comments and contributions.

Task force members include:

Paul Beverly, SchlumbergerSema
Alan Bondzio, ADB
Kirk Brafford, Xansa
Thierry Burgess, Oberthur
John Burke, Foley Hoag
Peter Cerra, Consultant
Chris Corum, AVISIAN Inc.
Mike Dinning,
US Dept of Transportation
Donna Farmer, Smart Card Alliance
Greg Garback, WMATA
Alex Giakoumis, Atmel
Kevin Gillick, Datacard Group
Bill Holcombe, GSA
Karen Jones, IBM
Mansour Karimzadeh, ACI Worldwide
Jeff Katz, Atmel
Diana Knox, Visa
Colleen Kulhanek, Datakey

Gilles Lisimaque, Gemplus
Cathy Medich, Consultant
Bob Merkert, SCM Microsystems
John Moore, GSA
Sandy Morris, MasterCard
Jim O'Connell, Caradas
Tate Preston, Datacard
Bill Randle, Huntington
Keith Saunders, MasterCard
Louis Sciupac, LaserCard Systems
Jennifer Spade,
CrossCom National
Jeff Staples, AVISIAN Inc.
Guy Tallent, Identrus
Charles Walton, Caradas
Mike Weekes, IBM
Bob Wilberger,
Northrop Grumman IT
Jody Zimmerman, Consultant

Copyright Notice

Copyright 2002 Smart Card Alliance, Inc. All rights reserved.