Smart Cards and Biometrics
White Paper

Frequently Asked Questions

May 2002

Smart Card Alliance
191 Clarksville Road
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

Frequently Asked Questions

1. What is a smart card ID?

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. A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, a magnetic stripe, a barcode and/or an optical stripe. Smart cards are used worldwide in financial, telecommunications, transit, healthcare, secure identification and other applications.

2. 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.

3. 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 data bases. 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.

4. How does the white paper define privacy?

Privacy is a broad topic, one that invokes differing definitions often colored by cultural, political, and economic factors. To many people, privacy is that imaginary protective bubble surrounding our personal lives. It is an insulating barrier between ourselves, and those we care about, and the outside world. To others privacy might include a sense of secrecy, an ability to carry out our daily activities without the knowledge of others. And to some privacy can

even mean outright anonymity, where we are able to remain nameless or unrecognizable in our dealings with other individuals or entities. The white paper defines a "privacy-sensitive" secure ID system as one that has technology, policies and processes in place to protect the individual's personal information and that provides the ability for the individual to control who has access to the personal information used by the secure ID system.

5. What are examples of ID system implementations that use smart cards and biometrics today?

There are numerous government ID systems implemented worldwide that are using smart card and biometric technology, including:

- U.S. Department of Defense Common Access Card - with photo, biometrics (fingerprint), and smart card chip.
- Malaysia's national ID (Government Multi-Purpose Card) - with photo, biometrics (fingerprint) and smart card chip.
- Spain's social security card - with biometrics and smart card chip.
- Netherlands' "Privium" automated border crossing system - with photo, biometrics (iris) and smart card chip.
- Brunei's national ID - with photo, biometrics (fingerprint) and smart card chip.
- U.K.'s Asylum Seekers Card - with photo, biometrics (fingerprint) and smart card chip.

6. 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 the identity of whoever it was had been previously authenticated. A combined smart card and biometrics ID system also delivers the highest security, supporting two- or three-factor authentication.

7. 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.

8. What protection is there from stealing the biometric template off of a stolen card?

Smart cards are very tamper resistant, and as such 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 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.

9. How much memory is required to store biometric information?

Biometric systems store either the full biometric image or a biometric template. Biometric template sizes are small, and, according to Frost & Sullivan, range from 9 bytes for hand geometry to 300-1200 bytes for a fingerprint scan to 512 bytes for iris recognition to 1500 bytes for voice verification. Smart cards have sufficient on-card memory to store one or more biometric templates.

10. What standardization efforts are underway for biometric systems?

Several significant international organizations are working on developing biometric standards, including:

- **BioAPI**. The BioAPI Consortium (www.bioapi.com) is concerned with standardizing the way applications communicate with biometrics and how data are manipulated and stored. The BioAPI specification focuses on providing a high-level generic biometric authentication model suited for any form of biometric technology. Many major information technology vendors currently support BioAPI. Both the U.S. Department of Defense and General Services Administration require biometric solutions vendors to provide products compliant to BioAPI. The BioAPI specification was recently approved as an ANSI standard: ANSI/INCITS 358-2002 - "Information Technology - BioAPI Specification," approved February 13, 2002.
- **Common Biometric Exchange File Format** (CBEFF). The Common Biometric Exchange File Format specification focuses on the interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. CBEFF describes a set of data elements necessary to support biometric technologies in a common way. The National Institute of Standards and Technology (NIST) has published: "Common Biometric Exchange File Format (CBEFF)," January 3, 2001, as NISTIR 6529 (http://www.nist.gov/cbeff). CBEFF is being augmented under the NIST/Biometric Consortium Biometric Interoperability, Performance and Assurance Working Group (http://www.nist.gov/bcwg).
- **Biometric Device Protection Profile** (BDPP). The Biometric Device Protection Profile is a specification (draft 0.8 in September 2001) from the U.K. government Biometrics Working Group (http:/www.cesg.gov.uk/technology/biometrics/). The intent of the Biometric Device Protection Profile is to specify functional and assurance requirements applicable to commercially available biometric devices that are used to identify or verify previously enrolled individuals for entry to a portal.

11. Can contactless smart cards be used with biometrics?

Yes. Low cost, contactless smart cards with high communication speeds are now available that have enough memory to store a unique fingerprint template or photographic representation. This means the higher security benefits of a biometrics-based ID system can use contactless smart cards to achieve a range of security and cost goals.

12. Are contactess smart cards as secure as contact smart cards?

Contactless smart card solutions are available today that offer the same cutting edge cryptography and security as contact smart card products. All of the security capabilities available in contact smart cards can now be applied at the full 10cm range attainable by products meeting the ISO14443 standard. Cards that are both contact and contactless (combi cards) can be chosen when certain tasks (for example, loading the biometric template or changing keys) are considered too sensitive to implement with a contactless card.

13. What contactless smart card standards are supported by card and biometrics vendors?

Cards supporting the ISO14443 standard have been successfully applied for several years with over 250 million cards (and thousands of readers) deployed using products from multiple vendors. Multiple biometrics vendors also offer contactless systems based on ISO14443. The major smart card vendors and companies specializing in biometrics can deliver integrated readers and locks combining contactless technology and biometric image processing.

14. What are the advantages of contactless smart cards?

Contactless smart cards bring many benefits to secure ID systems when factors such as high throughput and usage, harsh environments, and reader maintenance and reliability are important. Because the contactless card chip and the reader communicate using radio waves, there is no need to physically make an electrical connection. Maintenance of readers is minimized while reliability is improved since there are no worn contacts to be replaced or openings to be unblocked. Cards also last longer because removing them from their regular carrying place is not necessary for use. Readers or kiosks can also be sealed so there is no limitation to deploying contactless ID systems in almost any environment.

15. 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. An enrollment process that captures biometric information would be able to ensure that only one ID is issued to an individual by determining if the same applicant had previously enrolled with a different name.

16. 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.

17. How does a secure ID system handle lost, stolen or revoked cards?

This will depend on the overall security requirements and processes in specific ID systems. Each ID system will provide cardholders with a process to report lost or stolen cards so that system information can be updated. If the card includes a biometric, it will not be able to be used at biometric stations by anyone but the rightful owner. The system life cycle management processes need to define how a card is revoked (i.e., if the cardholder is no longer granted the privileges that the card provides access to). Systems requiring the highest security and near-zero risk will require real-time verification that the ID is still valid (for example, a notification of a fraudulently obtained airport access card). Systems that can tolerate some degree of acceptable risk (e.g., offline credit card systems) may instead support periodic updates to a list of revoked cards stored in the local readers.

18. 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.

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms 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 combination of smart card and biometric technology in 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 contributions.

Copyright Notice