Smart Card Alliance

# Identity Management Systems, Smart Cards and Privacy: Frequently Asked Questions

### 1) How does information security affect privacy?

The essential debate about fears regarding the loss of privacy revolves around the trust that personal information cannot, and will not, be revealed to anyone but those who need it for official business and for legal purposes. Information security while the information is being stored, transmitted or used is vital to maintaining and protecting privacy. If unauthorized users can access information too easily, the information can hardly be private. The fact that the information is protected and available only to authorized people and for legal purposes is the essence of privacy.

Technologies that ensure information integrity (i.e., information has not been modified or replaced) and confidentiality (i.e., information is not able to be viewed or copied by unauthorized persons) are critical factors for ensuring information security and information assurance. Authentication technologies offer the certainty that the information that we trust can neither be modified nor viewed by unauthorized people, helping to guarantee privacy.

### 2) How do I know that the organization that issues my ID will keep my information private?

Organizations that collect and store data for ID purposes are governed by legislation, rules and policy that prohibit them from making any other use of the data than the use for which it was collected and that requires them to prevent access to the information by entities that are not related to the issuing organization and its purposes. It is in an issuing organization's best interest to keep data inaccessible to other organizations and people. There are also a number of laws in place that require organizations to keep data private. FAQ #7 reviews some of the key U.S. laws that govern individual privacy.

When submitting personal information, individuals should review the organization's privacy policy and understand what personal information is to be collected, how the information will be used, who can access the information, how the information will be protected, and how the individual will control its use and provide updates to the information over time. The privacy policy should be clear and should satisfy concerns about the privacy of personal information being collected.

### 3) What are some examples of the ways an organization issuing and verifying IDs can protect privacy?

Organizations that issue and verify IDs need to establish and implement policies, operational practices and identity management system technologies to protect the privacy of an individual's personal information.

First, the organization must define its privacy and security policies. For example:

- Only the minimum information necessary to validate an individual's identity should be gathered. Individuals should be informed of the reason for the data collection, and should be permitted to choose whether or not to participate.
- Only well-screened, well-trained personnel should be given access to individuals' personal information. All personnel must be accountable for each access to the data.

- Only the minimum data required to perform a given transaction should be accessed.
- Displaying or transmitting unencrypted personal information should be avoided. Truncated fields should be used for displayed or printed content.
- Policies should prevent data generated by the use of an ID card or token (i.e., time and place of the transaction) from being connected to the content of the transaction, so that the movements of the individual user cannot be captured and tracked.

Second, the organization should put in place system technical capabilities and practices that are privacy-protective. For example:

- All personal information should be stored and transmitted only in encrypted form. Original unencrypted information should be destroyed after encryption and storage.
- The identity management system should be fully secured with layered protection that does not rely on any single component to prevent, monitor and remedy attempts to compromise the information.
- Information captured by ID readers should be removed and destroyed immediately upon completion of the transaction.
- Every data field in an ID card or token should have its own checklist of access privileges that specify for which transactions and to which authorized readers or personnel the data may be released.
- Offline identity verification that doesn't require transmission of information is safer and faster than online verification. Specifically, smart ID cards or tokens have the ability to perform on-card checks and verifications of a personal identification number (PIN), password and/or biometric information, without releasing any of the private information from the ID.
- Strong information security should be implemented throughout the identity management system, including protecting any personal information stored in databases and implementing ID card or token features that thwart tampering and attempts to gain access to personal information stored on the card. For example, a smart ID card is extremely difficult to duplicate or forge, has built-in tamper-resistance, can encrypt information stored on the ID, and can also encrypt communication between the smart-card-based device and the reader to prevent eavesdropping. The release of any personal information on the card can also be linked to a technique that seeks the individual's permission before the information is made accessible (e.g., with a PIN, password or biometric factor). Additional security technologies may also be used to ensure information integrity.

By providing an accurate and reliable means of verifying the identity of individuals, a well-designed and properly-implemented identity management system can protect privacy and eliminate the need for more privacy-invasive techniques used with other ad hoc identity verification approaches.[1]

### 4) How do smart cards help to protect privacy?

Smart cards offer a number of features that can be used to provide or enhance privacy protection in systems. The following is a brief description of some of these features and how they can be used to protect privacy.

- *Authentication*. Smart cards provide mechanisms for authenticating others who want to gain access to the card. These mechanisms can be used to authenticate users, devices, or applications wishing to use the data on the card's chip. These features can be utilized by a system to protect privacy by, for example, ensuring that a banking application has

[1] See the article, "It's Not Just a Driver's License Anymore," by Amitai Etzioni at http://www2.gwu.edu/~ccps/etzioni/B456.html for additional discussion of this point.

been authenticated as having the appropriate access rights before accessing financial data or functions on the card.

- *Secure data storage*. Smart cards provide a means of securely storing data on the card. This data can only be accessed through the smart card operating system by those with proper access rights. This feature can be utilized by a system to enhance privacy by, for example, storing personal user data on the card rather than in a central database. In this example, the user has better knowledge and control of when and by whom their personal data is being granted access.
- *Encryption*. Smart cards provide a robust set of encryption capabilities including key generation, secure key storage, hashing, and digital signing. These capabilities can be used by a system to protect privacy in a number of ways. For example, a smart card system can produce a digital signature for the content in an email, providing a means to validate the email authenticity. This protects the email message from subsequently being tampered with and provides the email recipient with an assurance of where it originated. The fact that the signing key originated from a smart card adds credibility to the origin and intent of the signer.
- *Secure communications*. Smart cards provide a means of secure communications between the card and card readers. Similar in concept to security protocols used in many networks, this feature allows smart cards to send and receive data in a secure and private manner. This capability can be used by a system to enhance privacy by ensuring that data sent to and from the card is not intercepted or tapped into.
- *Biometrics*. Smart cards provide mechanisms to securely store biometric templates and perform biometric matching functions. These features can be used to improve privacy in systems that utilize biometrics. For example, storing fingerprint templates on a smart card rather than in a central database can be an effective way of increasing privacy in a single sign-on system that uses fingerprint biometrics as the single sign-on credential.
- *Personal device*. A smart card is, of course, a personal and portable device associated with a particular cardholder. The smart card plastic is often personalized, providing an even stronger binding to the cardholder. These features, while somewhat obvious, can be leveraged by systems to improve privacy. For example, a healthcare application might elect to store drug prescription information on the card instead of in paper form to improve the accuracy and privacy of a patient's prescriptions.
- *Certifications*. Many of today's smart cards have been certified that they comply with industry and government security standards. They obtain these certifications only after completing rigorous testing and evaluation criteria by independent certification facilities. These certifications help systems protect privacy by ensuring that the security and privacy features and functions of the smart card hardware and software operate as specified and intended.

### 5) Is there any difference between contact smart cards and contactless smart cards in their ability to protect personal information?

Both contact and ISO/IEC 14443-compliant contactless smart cards are **equally able** to protect personal information.

While contact smart cards must be physically inserted into a card reader for communications, ISO/IEC 14443-compliant contactless smart cards use electromagnetic fields to communicate with the reading device, when placed within a range of up to 10 centimeters (4 inches). Contactless technology is an excellent technology for access control applications, as it supports short transaction times while preserving system security.

Because contactless cards can be operated without being physically inserted into a card reader, a number of precautions can be taken to ensure that user privacy is protected during a transaction.

- User data can be digitally signed by the issuing authority to guarantee that it has not been tampered with.
- Communication between the card and the reader can be encrypted so that eavesdroppers cannot obtain access to cardholder information.
- Authentication mechanisms can ensure that cards only present information to authorized reading devices.

### 6) Why are smart cards better than other ID token technologies?

Smart cards are widely acknowledged as one of the most secure and reliable forms of an electronic identification (ID) token. A smart card includes an embedded integrated circuit chip that can be either a microcontroller chip with internal memory or a secured memory chip alone. The card communicates with a reader either through direct physical contact or with a remote contactless electromagnetic field that energizes the chip and transfers data between the card and the reader. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., data storage and management, encryption, decryption, and digital signature calculations) and interact intelligently with a smart card reader.

A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, magnetic stripe, barcode and/or an optical stripe. By combining these various technologies into a smart card ID token, the resulting ID can support both future and legacy physical and logical access applications. They can also support other applications that have traditionally required separate ID processes and tokens.

### 7) What regulations or laws are in place that help to protect an individual's privacy?

There is no single U.S. law that deals with protecting an individual's private information, but there are numerous laws for protecting privacy in specific industries or applications. It is important to note that, regardless of whether or not technology is implemented to support compliance with legislation, agencies or organizations must first establish policies and procedures that ensure information privacy. Then any technology implemented is only meant to streamline and enhance an organization's ability to follow and enforce those policies and procedures.

Some examples of privacy legislation include the following:

- The Privacy Act was passed by Congress in 1974 to provide safeguards against the misuse of records by Federal agencies. It establishes a set of policies and procedures Federal agencies must follow as a means of protecting an individual's privacy.
- The Health Insurance Portability and Accountability Act (HIPAA) provides standards for security and privacy of individually identifiable health information.
- The Gramm-Leach-Bliley Act includes provisions to protect consumers' personal financial information held by financial institutions.
- California's SB 1386 identity theft law went into effect July 1, 2003, and requires companies that do business with California residents to inform customers when their private information has been accessed by an unauthorized person.

### 8) Where do organizations find best practices for implementing privacy-protective ID systems?

It is recommended that organizations first establish an overall privacy policy for the identity management system and then conduct a privacy impact assessment. A privacy impact assessment can ensure that the privacy policy is considered and adhered to throughout the design, deployment and on-going operation of the identity management system. Several resources are available to assist with developing a privacy impact assessment:

- Canadian Government Privacy Impact Assessment Policy, available at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp.
- "How to Do a Privacy Assessment: Smart, Optical and Other Advance Cards," published by ACT Canada and available at http://www.actcda.com/resource/articles.htm.
- "Multi-Application Smart Cards: How to Do a Privacy Assessment," published by ACT Canada and available at http://www.actcda.com/resource/articles.htm.

Other resources include the following:

- The Fair Information Practices defined by the Organization for Economic Development (OECD, see http://www1.oecd.org/publications/e-book/9302011E.PDF) are being used internationally to form the operational basis for privacy safeguards and data protection. The commonly-accepted fair information practice principles are: notice and awareness; choice and consent; individual access; information quality and integrity; update and correction; enforcement and recourse. Other guidelines and principles can be found in the European Union (EU) Data Protection Directive (1995), available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html, and the U.S. Department of Health, Education and Welfare (HEW) Fair Information Practices: "Records, Computers and the Rights of Citizens" (1973), available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.
- "Guide to Biometrics," by Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha and Andrew Senior. This book describes biometric technology, explains the definition and measurement of performance, and examines the factors involved in choosing between different biometrics.
- "Automatic Fingerprint Recognition Systems," by Nalini Ratha, Ruud Bolle and Nalini K. Ratha. This book covers the history of fingerprint recognition and discusses fingerprint identification system design, standards and technologies.

### 9) Almost every identity management system needs to assign a unique identifier to the individual holding the identity credential and this can create privacy concerns. How can smart cards help with this?

One of the reasons for privacy concerns around identity management systems is that, yes, a unique identifier must be assigned to each individual holding an identity credential, and the identity management system can tie that identifier to the individual's personal information that it is meant to protect. The concern is how easily an identity management system can track ID credential holder activity. Regardless of the ID management system or the type of credential used (smart card or other), the system's ability to track usage and collect ID holder information depends on the purpose and design of the system.

Using smart cards as credentials offers several advantages in that they provide an identity management system with more flexibility in offering ID holders more anonymity if required or desired. The verification credentials can be stored on the smart card, and if the smart ID card is proved to be authentic, then future validation need only be done against the smart ID card without referring back to credentials stored on a central database. In addition, the validation may only need to prove that the credential is good or bad, and not reveal or record the actual identity of the credential holder, thereby reducing the amount of tracking or logging of the individual's activity.

It is the system design itself that needs to explicitly define what the ID will be used for and what the policy for tracking is.

### 10) Biometrics are used in many new identity management systems to improve the accuracy of identifying individuals. How can smart cards be used to help assure privacy in a biometrics-based system?

Smart cards provide a highly effective mechanism to protect the privacy of an individual that has a requirement to use a biometric identity system.

1. The biometric information can be stored on the smart card rather than in an online database, allowing the biometric owner the opportunity to manage the physical possession of the card holding the individual's biometric information.
2. The biometric data can be secured with state-of-the-art encryption techniques while providing full three-factor authentication capability at the card/reader level.
    - Something you have - the card with all of its security capabilities
    - Something you know - a passkey
    - Something you are - the biometric

   In a non-smart-card-based application, the passkey and biometric would be stored in an online database outside the control of the individual and the biometric information would be captured and passed to an application for matching.
3. The individual's biometric can be captured by a reader and passed to the smart card for matching, rather than passing the stored biometric information to the reader for matching. The individual's biometric information would never leave the card, preventing virtually any possibility of compromise.

**11) Smart cards cost more than other ID tokens. How much does it cost to implement a smart-card-based identity management system?**

While a smart-card-based ID may cost more per card than other ID technology, the cost of the ID is a small fraction of the total cost of an organization's identity management system, with smart cards providing significant security, privacy and functionality benefits that may result in other system or cost improvements. The actual cost of the smart card will depend on many factors, including the memory size, microcontroller features and speed, operating system and volume of cards deployed.

Deploying a new identity management system is typically a large-scale IT project. Investment is required for business process reengineering, project management, system design and deployment, technology acquisition, user training, and on-going management and support. The justification for implementing a new identity management system may be based on requirements to comply with new legislation or regulations, a strategic or tactical decision to improve security for the organization, or cost savings from improved user convenience and productivity or other changes to the organization identity verification infrastructure.

**12) What are the privacy implications of using a biometric image vs. a biometric template for authentication?**

From the early 1890s, fingerprint images have been used to match individuals to samples left on an object. These images were kept on cards with various methodologies used to file them based on certain image characteristics. This process created a need for officials to physically protect the images from compromise due to the possibility of the images be stolen and used in an illegal manner. The demand for automated systems stems from the success experienced by the early, mostly law enforcement, efforts to use biometrics to identify criminals. Biometrics can be used to protect us and verify our identities at our discretion.

Today's physical and logical access systems typically use biometric templates rather than the actual image to perform matching operations. A template is a mathematical representation of the biometric information rather than the biometric image itself. As the biometric is scanned at enrollment, it is converted to a template. Therefore, the biometric image is never actually stored in any data storage system. In the event an unsecured template is compromised, the hacker would be unable to recreate the original image from the template. This results in identity management systems using biometric templates being considered more privacy-protective than those that use biometric images.

**Other Smart Card Alliance Resources**

“Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” Smart Card Alliance report, February 2003

“Secure Identification Systems: Building a Chain of Trust,” Smart Card Alliance report, March 2004

### About this Document

The Smart Card Alliance wishes to thank the Alliance members who participated in the project to develop a briefing on identity management systems, smart cards and privacy. Contributors included individuals from the following organizations: AMAG Technology, Atmel Corporation, CardLogix, Fargo Electronics, Gemplus, EDS, Hitachi America, IBM, Lockheed Martin, MartSoft Corporation, Northrop Grumman Corporation, Philips Semiconductors, SafeNet, Inc., Smart Commerce, Inc., SuperCom, Inc., VeriFone.

### 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. 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. and Latin America. For more information, visit www.smartcardalliance.org.