

Identity Management Systems, Smart Cards and Privacy

No matter where you go today, it is likely that at some point someone will ask to see your ID. Today identity verification is routinely requested in a variety of familiar situations—when someone wants to obtain health care, enter a public building or corporate office, or get on an airplane.

Organizations that need to verify identities find that concerns about privacy and the protection of personal information quickly emerge as key issues when they consider new identity management systems. An organization's specific requirements for safety and security must be balanced against the genuine desire to protect the privacy of the individuals whose identities need to be verified. This requirement—how to identify people unequivocally while also protecting their privacy—shapes every discussion of how to design, build, or implement a new, secure, identity management system.

Designing a new identity management system is complex, and the requirement to balance security and privacy affects everything about a system design, from the policies and processes formulated to support and maintain the system to the system's architecture and the particular technology chosen to authenticate individuals. For example:

- The organization must have a privacy and security policy that clearly defines 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 enrollment and identity proofing process must verify that the information presented is accurate and protect the confidentiality and integrity of that information.
- The system must protect each individual's information at all times, including while the information is being stored and while it is being used.
- The ID an individual carries must protect its contents from being copied, altered, or hacked, to prevent unauthorized use, misuse, or disclosure of the personal information it carries.
- The exchange of data between the ID and whatever device reads the ID must be protected to prevent unauthorized capture and use of data to impersonate an individual.
- Access to the personal information should be granted only after an issuer-defined authentication process. Only necessary information should be released and only to authorized systems or individuals.
- All personnel involved in using the system must be carefully trained and monitored to ensure strict conformance to the system's policies and practices. Compromising these policies and practices means compromising the identity management system itself.

Designing an identity management system to guard individual privacy therefore involves more than simply selecting a particular type of ID technology. The organization issuing the ID must design information privacy and security into the overall system, have the appropriate policies and

processes in place to support the privacy and security requirements, and implement the technologies that deliver these features. Issuing organizations must also have the operational practices in place to monitor and ensure that privacy and security policies are implemented and strictly followed.

ID Technology Selection

The selection of an ID technology is also critical. The ID technology must be one that can both facilitate and reinforce the system's privacy and security design and goals. Many ID or badging systems currently rely on technologies such as magnetic stripes or bar codes. Such technologies are no longer appropriate, since they cannot meet the requirement to provide strong security while guarding privacy. IDs based on these technologies are tamper-prone, can easily be counterfeited, and provide little or no protection for the information they carry.

Only IDs that use smart card technology have the strong security features that can enhance privacy protection in a well-designed and properly-implemented system. IDs using smart card technology include a secure microcontroller, or equivalent intelligence, and internal memory and are available in a variety of form factors (for example, plastic cards, documents or other handheld devices). Relying on smart card technology provides an identity management system with the following advantages:

- **Strong information protection.** Smart card technology protects identity data stored on the ID completely and constantly. Smart-card-based IDs can encrypt the identity information stored on them and encrypt communications between the ID and the device that reads the ID, preventing eavesdropping. Smart card technology can also lock the personal information on the ID and release it only after the owner authorizes the release by providing unique information such as a personal identification number (PIN), a password, or a biometric factor, such as a fingerprint.
- **Strong ID security.** IDs incorporating smart card technology are extremely difficult to duplicate or forge. In addition to the obvious visual anti-counterfeiting and tamper-resistance features such as holograms, micro-printing and optical variable devices, smart card chips have built-in tamper-resistance. The chip in a smart-card-based ID includes a variety of hardware and software capabilities that immediately detect and react to tampering attempts, countering possible attacks.
- **Sophisticated "on-card" processing.** Smart cards accomplish many identity management functions within the secure processing environment on the card itself. Smart cards store data, which they can then manage securely, protecting the information both while it is stored and while it is being accessed. On-card processing enables smart-card-based IDs to perform on-card functions (for example, encryption, decryption and other data processing) and to interact securely and intelligently with a card reader. These capabilities have particular importance when an identity management system relies on biometric information to verify the identity of an individual. Smart ID cards can securely store the biometric information and perform the comparison of the biometric inside the smart card chip to verify the individual's identity. This offers increased privacy since the individual's stored biometric information never leaves the ID (which remains in the

individual's possession) and the match of the stored to captured biometric is done within the smart card chip's secure processing environment.

- **Authenticated and authorized information access.** The smart card's ability to process information and react to its environment is unique. When secure card access is a requirement, only a smart-card-based ID can verify the authenticity of the ID reader and prove its own authenticity to the reader. Smart cards can also verify the authority of the information requestor and then restrict access to only the information required by that particular request. Stored personal information can be further protected by a unique PIN or biometric that the cardholder provides before any access to the information is granted.

Implemented properly, smart card technology strengthens the ability of any organization to protect the privacy of individuals whose identity the organization needs to verify. Unlike other IDs, smart-card-based IDs can implement a personal "firewall," releasing only required information and only when it is genuinely required. Smart cards are excellent guardians for personal information and individual privacy.

Conclusion

The Smart Card Alliance believes that protection of individual privacy is a critical goal for any identity management system. The Smart Card Alliance recommends that organizations considering new identity management systems follow several guidelines:

- Develop and communicate a strong, clear privacy and security policy to govern the identity management system.
- Follow system design guidelines and operating practices that support these policies.
- Implement the identity management system using technologies that enforce these policies.
- Use smart-card-based identity credentials as a component of the system.

The use of smart card technology in the design of an identity management system represents a smart first step to preserving and protecting individual privacy while achieving secure, strong identity verification.

For more information about smart cards and the role that they play in secure identification and other applications, please visit the Smart Card Alliance web site at <http://www.smartcardalliance.org> or contact the Smart Card Alliance directly at 1-800-556-6828.

- [Click here read frequently asked questions about identity management systems, smart cards and privacy.](#)

Other Smart Card Alliance Resources

- ["Identity Management Systems, Smart Cards and Privacy: Frequently Asked Questions,"](#) March 2005

- [“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 <http://www.smartcardalliance.org>.

From: <http://www.smartcardalliance.org/pages/publications-identity>

Accessed on-line October 10, 2007