Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology

A Smart Card Alliance White Paper

Publication Date: February 2003

Publication Number: ID-03001

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

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, health care, 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**.

Table of Contents

Executive Summary

What is Meant by Privacy?

Individuals today are required to confirm their identity with increasing frequency and for more diverse reasons. Increasing requirements for identity confirmation and for transactions of almost any kind to require personal identification have caused the definition of privacy to change. Modern privacy requires constraints on the collection, use and release of personal information, as well as the imposition of measures to protect such information.

Protecting privacy means protecting individuals' rights to control how personal information is collected and promulgated. Protecting privacy also includes protecting against identity theft, or the use of an individual's personal information for fraudulent purposes. A critical component of protecting privacy is information security — protecting the confidentiality, integrity, and availability of information that identifies or otherwise describes an individual. To be considered privacy-enabled, an identification system must be designed to satisfy these parameters.

Smart Cards Help to Protect Privacy in Identification Systems

Both privacy and security must be considered fundamental design goals for any personal ID system and must be factored into the specification of the ID system's policies, processes, architectures, and technologies. The use of smart cards strengthens the ability of the system to protect individual privacy and secure personal information.

Unlike other identification technologies, smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes;
- Segregate multiple applications on the card;
- Support multiple single-purpose IDs;
- Provide authentication of other system components;
- Provide on-card matching of cardholder verification information; and
- Implement strong security for both the ID card and personal data.

Smart cards provide solutions that can enhance privacy protection and guard against identity theft in different ID system architectures.

ID System Designers Should Follow Privacy Protection Guidelines

A number of government organizations and industry groups have developed recommendations for fair information practices and guidelines to protect individual privacy. System designers need to consider business practices, security policies, and system architectures, as well as technologies. A privacy-enabled system must consider how information is protected and used throughout its entire life cycle. While smart cards, by themselves, are privacy-neutral, their on-card intelligence uniquely enables systems that use them to comply with many of the recommended privacy guidelines.

About This White Paper

This white paper was developed by the Smart Card Alliance to describe how smart card technology can help to protect privacy and ensure security in an ID system. This paper provides answers to commonly asked questions such as:

- What privacy and data security issues must be considered when developing an ID system?
- How can smart cards protect privacy during identity verification?
- What advantages can smart cards offer over other forms of personal identification technology?
- What guidelines can be used to assist in designing processes and selecting technologies to be used by ID systems?
- How can smart cards help to prevent identity theft?

Introduction

Individuals are currently required to confirm their identity for many diverse purposes, such as verifying eligibility within a health care system, accessing a secure network or facility, or validating their authority to travel. In almost every discussion about implementing personal identification (ID) systems to improve identity verification processes, concerns about privacy and the protection of personal information quickly emerge as key issues. Government agencies and private businesses that are implementing ID systems to improve the security of physical or logical access must factor these issues into their system designs. While technologies are available that can provide a higher level of security and privacy than ever before, ID system complexity coupled with increasing public awareness of the risks of privacy intrusion require that organizations focus on privacy and personal information protection throughout the entire ID system design and implementation.

A secure personal ID system must address policy and technical requirements as well as individual privacy concerns. The system must be secure, provide fast and effective verification of an individual's identity, and protect the individual's privacy. To implement a privacy-sensitive ID system, policies, processes, system architecture and technology choices must be carefully considered and designed to enhance individual privacy. Smart card technology can provide a privacy-enabling platform for implementing identification systems that meet both governmental and business needs for secure and accurate identification.

This white paper defines privacy as the concept applies to an identification system and discusses how privacy considerations affect system design and implementation. It reviews how smart cards can provide a privacy-enabling technology for different ID systems, how they interact with other system components (e.g., smart card readers and host systems), and how smart cards can address the growing problem of identity theft. The paper recommends key guidelines for business practices and system designs that can help protect privacy. Finally, the paper describes two smart card-based identity applications that address individual privacy.

Defining Privacy in an Information Context

The definition of privacy dates at least as far back as 1890, when a United States Supreme Court justice defined privacy as "*The right to be left alone.*"[1] This extremely broad definition is open to wide interpretation and has evolved as our lives and interactions with other components of society have become more complex.

In 1967, Alan Westin defined privacy as "*the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.*"[2] This definition focuses on the protection of personal information and reflects both the modern necessity to interact with others and the modern requirement that information in one form or another flow between the different components of society.

There have been many further attempts to define privacy, based both on the concept of leaving the individual alone and on the more modern concept of protecting the collection, storage, and transmission of information.[3] These definitions tend to range from generic definitions (like the two examples above) to very specific and detailed definitions that attempt to identify every component involved in a privacy-aware process or system.[4] One author even argues that the privacy principles are more important than agreeing on a concrete definition of privacy.[5]

For the purposes of this paper, Alan Westin's definition offers a context within which to make technology and process choices in an information system. It enshrines the right of the owner of information to decide how, where, and by whom that information is used. Usage of information in this context encompasses initial collection, when the owner of information presents it to a collecting body and consents to its use, and all subsequent use, either by the collecting body or by others to whom the information has been transmitted.

Another important component of privacy in an information system is the protection of personal information during its lifecycle, from collection through usage and storage to eventual destruction. What personal information is considered private also varies, depending on the situation. Such information may include an individual's Social Security number, biometric information, financial transaction histories, and other information such as medical, employment, academic, driving, and income tax records.

Privacy Parameters

The protection of privacy in a modern information system is concerned with the following broad areas:

- When, how, and why information is collected from an individual.

[1] Samuel Warren and Louis Brandies, "The Right to Privacy," *Harvard Law Review* 193 [1890].
[2] Alan F. Westin, *Privacy and Freedom*, New York, NY: Atheneum, 1967.
[3] A search on "definition of privacy" on http://www.google.com returned 1,740 entries.
[4] One example is the "Privacy Framework" from the International Security, Trust and Privacy Alliance (http://www.istpa.org). The ISTPA definition of privacy is: "The proper handling and use of personal information throughout its life cycle, consistent with the preferences of the subject."
[5] Robert Gellman, "Privacy, Consumers and Costs," March 2002. Available at: http://www.epic.org/reports/dmfprivacy.html.

- When, how, and why collected information is accessed by authorized entities.
- When, how, and why collected information is destroyed.
- How information is protected from accidental or deliberate disclosure to, or modification by, unauthorized parties, from collection to destruction.
- How an individual can control whether information will be collected and, if so, subsequently used and retransmitted.
- How an individual's usage preferences are enforced if information is retransmitted to additional information systems.

The Fair Information Practices defined by the Organization for Economic Development (OECD)[6] 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)[7] and the U.S. Department of Health, Education and Welfare (HEW) Fair Information Practices: "Records, Computers and the Rights of Citizens" (1973).[8]

Security Parameters

Information security is a vital element in the design and implementation of a privacy-sensitive system. If unauthorized users can access information too easily, the information can hardly be private.

The broad definition of security has been standardized for a number of years to mean maintaining the confidentiality, integrity, and availability of information (with various subdivisions). When the main concern is protecting privacy, maintaining confidentiality receives the most focus. However, all aspects of security are critical to protecting the privacy of information.

In the context of information security, confidentiality pertains to the secrecy of information. Once an individual's information has been passed to a collector, how that information is entered, transmitted and stored so that an unauthorized entity cannot access or alter the information, is critical. Is it encrypted, or stored in a "locked" container? What is the strength of the "key" and encryption algorithm used to protect the information? Is the information protected while it is being collected (e.g., during Internet collection)? What are the processes and procedures that govern how an authorized entity uses the information? If the confidentiality of information is compromised, the information can easily and quickly be copied and disseminated.

Integrity in this context pertains to the accuracy of information held about an individual. Integrity considers not only whether the information has been protected from tampering, but also whether the information is accurate when it is used. In a privacy-enabled system, the integrity of information is crucial. If the integrity of information is lost (for example, if the information is incorrect or outdated), then the owner's privacy may be violated when incorrect decisions are made based on unreliable information.

[6] See http://www1.oecd.org/publications/e-book/9302011E.PDF
[7] See http://www.cdt.org/privacy/eudirective/EU_Directive_.html
[8] See http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm

Availability in this context pertains to access control (i.e., who can access the information). The processes, procedures, and technology used to control access are crucial to preventing information leakage, either to external third parties or unauthorized insiders. In many cases poor access controls are the means by which private information is leaked from an organization to the outside world. Poor access controls can negate the best secrecy technology.

Design and Implementation Goals

Both privacy and security must be considered fundamental design goals for any personal ID system and factored into the specification of the ID system's policies, processes, architectures, and technologies.

When implementing an ID system (especially in non-corporate situations) there are three main choices:

1) Use an existing ID as the de facto choice. For example, in the United States, the Social Security number is used as a general identifier for numerous systems.
2) Deliberately use another ID that is not associated with the specific application. For example, in the United States, the driver's license is used for boarding aircraft.
3) Design an ID system for the specific application. Select a solution that is appropriate for the task to be performed with appropriate controls, technology choices, and processes. This is the most effective mechanism for protecting privacy.

Privacy considerations map to the various aspects of an ID system as follows:

- The enrollment system must ensure the accuracy and integrity of the information presented to validate an individual's identity and also protect the confidentiality and integrity of this information.
- The ID token must protect the credential against copying or intrusion to prevent unauthorized use or disclosure of the ID information.
- The ID token and ID validation entity must protect any exchange of validation information to prevent spoofing of an ID (e.g., unauthorized capture and use of data to impersonate an individual).
- When a valid ID is presented, the ID system must ensure that only the information necessary to the task being performed is released.

The design of a privacy-sensitive ID system therefore covers much more than the choice of the token used to carry the identity information. The entire system design, from the enrollment process through the use and final destruction of the ID, including policies and procedures as well as technology, needs to be privacy-aware. A well-defined security policy can specify how personal information is protected and managed; however, the policy alone cannot ensure that the system meets the policy requirements. One common approach taken to address this issue is to design tests that validate that the system is operating as intended, with different security methodologies, processes and technologies used to ensure the strength of the identification mechanism in the implementation. Common Criteria[9] is an extensive security standard that can be applied to the problem of system validation.

[9] See http://www.commoncriteria.org

Most of the tokens that could be chosen for an ID system are privacy-neutral. It is how the system overall is designed that determines whether the system is a privacy risk or benefit. Smart cards are one of the few ID technology choices that have the strong security mechanisms required to enhance the privacy aspects of a well-designed ID system.

Personal Identification vs. Personal Information – Privacy and the Role of Smart ID Cards

Establishing a person's identity is often necessary to ensure that the person is entitled to perform a transaction or access a location, system, or service. Establishing a person's identity (personal identification) typically requires access to that individual's personal information.

While personal identification is not necessarily a violation of the individual's privacy, access to an individual's personal information without the individual's consent is. Systems that use personal information must therefore be designed to ensure that the information is protected securely.

This section discusses the privacy issues with personal identification processes and personal information protection and presents the role of and benefits delivered by smart cards for protecting privacy.

Personal Identification

Identification processes include two primary uses for an ID:

- Initial identification. Initial identification means establishing who the individual is at the time the individual is enrolled into an ID system and issued an ID card.
- Subsequent identity verification. Subsequent identity verification means validating that the person using the ID card is the person who initially enrolled in the system and was issued the ID card.

Initial Identification

An individual's identity must be established when the individual is initially enrolled in an ID system and issued an ID card. Enrollment of a person into an identity system is a crucial event, and the credentials presented for enrollment (e.g., birth certificate, passport, driver's license) must be thoroughly authenticated. The enrolled identity will persist for the lifetime of the ID card or token.

Whatever the credentials being presented by an individual, an ID system can be designed to search existing databases of identities to validate that individual's identity. This approach requires that the individual be known to the database (i.e., already "enrolled" in that database). Types of databases that may be used include:

- **Enrolled Community Databases:** The driver's license records maintained by each state or resident alien and permanent resident databases are examples of enrolled community databases.

- **Criminal Record Database**: A criminal records database represents a different form of an enrolled identity database. Individuals are enrolled at the time of conviction and the information is maintained by the authorities.

Information obtained directly or indirectly from an individual can be used to search one or more databases for a match. If no match is made, the individual is either not known to the database or the search has returned a false negative.

Establishing a person's identity so that the person can be enrolled in an ID system or proceed to the next stage of accessing a facility or service that they are requesting is not a violation of their privacy. After all, the person can choose not to request a privilege that requires the individual's identity to be established in the first place. However, in some situations identity establishment is not optional. Currently individuals are often required to show an ID (such as a driver's license or passport) to access or obtain certain services (e.g., to enter and progress through the air transportation system or to cross an international border). The options available to an individual should be clearly stated.

Identity Verification

Verification of identity validates that the individual presenting an ID card is the person who owns the credentials on the card. Verification of identity ensures that an imposter has not come into possession of the card. The use of secondary or tertiary authentication factors, such as personal identification numbers (PINs), passwords, or biometrics, can verify that the cardholder is indeed the person who was initially enrolled.

Matching a card with a cardholder does not necessarily require access to an identity database. A smart ID card can perform the match by itself (on-card) and use a secure communication channel to indicate to external equipment, such as a door lock, terminal, or computer, that the correct holder of the card is present along with the smart ID card. In this case, information accessed by the door lock, terminal, or computer must be updated periodically to ensure that expired or revoked ID cards and credentials are not validated.

Anonymous Go/No Go. When on-card matching is used, smart ID cards offer an important privacy benefit. If the smart ID card is determined to be authentic (enrolled and not revoked, expired or counterfeit) and the cardholder's identity is verified, the person's identity does not have to be divulged externally. The identity of the cardholder can be verified by means of a single secure message, sent externally by the smart ID card indicating a correct or incorrect match. The door, terminal equipment, or computer should not be able to record the actual identity of the person being verified. The equipment records only that what was presented was an authenticated smart ID card and that a good or bad credential match resulted.

Some systems do store the verification credentials in central ID system databases. When the ID cardholder's identity needs to be verified online, verification is performed by accessing one or more of these system databases. In this case, a smart ID card can perform some functions offline (e.g., PIN verification) and can provide the appropriate information about the credential contained within it to be checked against the database.

Tracking. One key privacy concern is whether an ID system tracks ID holder activity. A device that captures a biometric authentication factor and communicates it to a smart ID card can clearly also record the ID card's activity and usage (to check for suspicious activities, such as multiple sequential invalid presentations, for example).

In this context, a smart ID card is no different than any other device or form of identification. Logging usage and collecting information within an ID system is determined by the design, implementation, and configuration of the

overall system. To what extent this information can be used to track an individual depends on several factors, including whether someone's personal identity can be established directly in conjunction with usage of an ID card. Direct correlation between use and identity may or may not be desirable depending on the system design. Unless there are system requirements to identify usage or access (e.g., for employees accessing a secure facility or restricted information), it may be acceptable to allow the individual to be anonymous at the time of usage.

When defining a secure ID system involving smart ID cards, it is recommended that:

- Policies are established that address tracking smart ID card usage;
- Policies are established about correlating cards to individuals; and
- The system is designed to enforce the policies that have been set.

Cost-Effective Offline Verification. Verification of cardholder identity is often required at multiple locations. For example, there are multiple locations in an airport that may require security measures for physical access. When multiple checkpoints are necessary, the costs of equipping every check-in desk, security checkpoint, and boarding gate with ID verification technology are a consideration. A smart card-based ID system can be deployed cost-effectively at multiple locations by using small, secure, and low-cost portable readers that take advantage of a smart card's ability to provide offline verification.

Convenient Identity Verification. Smart cards can provide convenient identity verification. A smart ID card can contain information such as biometric characteristics (one or more as necessary) or other data to assist with the confirmation of the cardholder's identity. In certain situations (such as at unstaffed locations), a smart ID card and suitably equipped reader can verify an individual's identity quickly and efficiently, offering a good balance between security and cardholder convenience.

Personal Information

When an ID card is issued to an individual, it may be the policy of the issuer to include information in the card that is not required to either establish or verify the cardholder's identity. This additional information may include information such as the person's age, nationality, ethnic background, religion, address, or telephone number. In addition, an ID card may also contain service-related information, such as account numbers, medical insurance information, training achievements, employee information, or level of security clearance.

When this type of personal information is loaded onto an ID card, the individual must be given the opportunity to consent to the collection, storage, and dissemination of the information. In addition, the system must ensure that external parties who wish to access the information can do so only after demonstrating appropriate access rights. Smart card technology provides system implementers with unique capabilities that help to protect the privacy of personal information.

Personal Firewall: To protect personal information, each smart ID card can contain a personal firewall. The firewall is implemented to ensure that data objects are served from the card only when an external system is

authenticated as having predetermined access rights to the data. The provision of any personal information on the card can be linked to a technique that seeks the permission of the cardholder before the information is released. The permission can be a cardholder's PIN, password or a biometric factor. If the smart ID card is able to verify the PIN, password, or biometric, it can then release the appropriate information.

Authenticated and Authorized Information Access: The information required to identify an individual typically depends on the individual's role in the situation. For example, when cigarettes are being purchased, the only identification information required may be the individual's age. Whether the individual can drive and where the individual lives may be irrelevant.

The smart card's ability to process information and react to its environment gives it a unique advantage in providing authenticated information access. Unlike other forms of identification (such as a passive printed driver's license), a smart card does not expose all of an individual's personal information (including potentially irrelevant information) when it is presented.

A smart card is able to release only the information required and only when it is required. The card's unique ability to verify the authority of the information requestor makes it an excellent guardian of the cardholder's personal information. For example, to a police officer, a driver's license that is also a smart ID card can present only information that is related to the motor vehicle authority. By allowing authorized, authenticated access only to the information required by a transaction, a smart card-based personal ID system can protect an individual's privacy while ensuring that the individual is properly identified.

Strong ID Card Security. When compared with other tamper-resistant tokens, smart cards currently represent the best tradeoff between security and cost. Smart cards also allow compatibility with other installed card systems, since hybrid cards can include a magnetic stripe, bar codes, embossing, or visual printing. When used in combination with other technologies such as public key cryptography and biometrics and when properly implemented, smart cards are almost impossible to duplicate or forge, and data in the chip cannot be modified without proper authorization (e.g., with passwords, biometric authentication, or cryptographic access keys). As long as system implementations have an effective security policy and incorporate the necessary security services provided by smart cards, users can have a high degree of confidence in the integrity of their information and its secure, authorized use.

Data Security. Privacy, authenticity, and integrity of data encoded on ID credentials are primary requirements for a secure ID system. Sensitive data is typically encrypted, both on the smart ID card and during communications with the external reader and system. Digital signatures can be used to ensure data integrity, with multiple signatures required if different authorities created the data. To ensure privacy, applications and data on the ID credential must be designed to prevent information sharing.

System Challenges and Privacy. For the most robust security and privacy, the secure ID system may require that system components authenticate the legitimacy of other components during the identity verification process. This can include the smart ID card verifying that the automated reader is authentic and the reader in turn authenticating the validity of the smart ID card. The

smart ID card can also ensure that the requesting system has established the right to access the information being requested.

Smart Cards and Privacy Protection

Because smart cards are programmable, ID systems that incorporate them are flexible. They can be privacy-invasive, privacy-protective, or privacy-neutral, depending on the motivations driving the overall system design. This section examines the potential of smart cards for use as a privacy-enhancing technology.

Roger Clarke lists ways in which smart cards can be used as a privacy-protective measure:[10]

- Implementing **anonymous** but secure schemes.
- Developing **pseudonymous** schemes; in particular, designs using protected indexes and eligibility authentication.
- Using **multiple, secure zones** in smart cards to segregate **applications**; supporting multiple **single-purpose IDs** that relate to a person's role rather than to a person, enabling an individual to use different identifiers and segregate **data trails**, such that the transaction trails generated in the context of one relationship are not available to other organizations.
- Designing in **two-way device authentication** such that chips verify the authenticity of devices that seek to transact with them rather than merely responding to challenges by devices.

The design of privacy-protective smart cards must revolve around providing the individual with control. This can be accomplished through such measures as placing the ownership of cards in the hands of the individual and ensuring design transparency of smart card-based ID systems.

On-card identity verification schemes can be more conducive to privacy protection because they do not rely on a centralized database. Such systems store private information (e.g., private keys and biometric information) on the card itself. As a result, the data is under the control of the individual and is also less accessible to hackers.

Another smart card privacy protection measure is the use of software tokens. Software tokens are unique identification strings that can be stored on smart cards. Software tokens can be used in combination with passwords or PINs, card readers, and at times, encryption.[11] Using software tokens restricts the information accessed to only the information that is required for the purpose at hand. For example, security staff at a workplace would access only information describing the areas of the facility to which a worker has access, not the worker's pay and benefits information.

Smart cards can also help to deter counterfeiting and thwart tampering with an ID card. Smart cards include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks, including: voltage, frequency, light and temperature sensors; clock filters; scrambled memory; constant power sources; and chip designs to resist analysis by visual inspection, micro probing or chip

[10] Roger Clarke, "Chip-Based ID: Promise or Peril," Proc. Int'l Conf. on Privacy, Montreal, September 1997.

[11] Ann Cavoukian, Ph.D., "Identity Theft: Who's Using Your Name?" Information and Privacy Commissioner/Ontario, June 1997.

manipulation. Where smart ID cards will also be used for manual identity verification, security features can also be added to a smart card body, such as unique fonts, ink color and multicolor arrangements, micro printing, high quality ultraviolet ink on the front and rear, ghost imaging (secondary photograph of the holder in an alternative location on the card), and multiple-layered holograms, including three-dimensional images.[12]

While privacy breaches can still occur with the use of smart cards, the measures discussed here can significantly prevent fraud or identity theft, deter counterfeiting and protect private information.

[12] State-wide Grand Jury Report: Identity Theft in Florida.

Smart Cards and Identity Theft

The growing problem of identity theft represents a significant privacy concern. According to the Federal Trade Commission, identity theft accounted for 43% of the 380,000 fraud complaints lodged in FTC's Consumer Sentinel database in 2002.[13] Consumer credit reporting agencies have estimated that their 7-year fraud alerts involving identity theft increased 36 to 53 percent in recent years.[14]

What is Identity Theft?

Identity theft is the unauthorized use of someone else's personal information for fraudulent purposes. Information is typically obtained through mail theft, interception of change of address forms, and telephone and Internet "spoofing."[15] Spoofing occurs when false messages are sent over the Internet in an effort to collect private information. For example, identity thieves posing as travel agents or other service providers can obtain a credit card number given to purchase a nonexistent ticket or service.[16]

In many cases, identity theft is "low-tech." Perpetrators seize information by stealing wallets, dumpster diving, accessing credit reporting data bases, accessing human resource files in the workplace, and spying on other people's unprotected use of passwords and PINs.

Using Biometrics to Counter Identity Theft

One potential tool for curbing identity theft is the use of biometric technologies as part of an ID system that verifies identity. Biometric technologies offer automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.[17] Biometric technologies include: fingerprint, hand geometry, iris, retina, face, signature, and voice recognition. Biometric characteristics can be used to identify an individual by digital comparison using an automated process.

Biometric characteristics cannot be stolen or mimicked as easily as can passwords or PINs. Thus, using smart cards in conjunction with techniques such as biometric on-card matching can provide a more secure means to verify transactions, authorize release of personal information or validate identity.

Additional information on how smart cards and biometrics can be combined in an ID system can be found in the Smart Card Alliance white paper, "Smart Cards and Biometrics in Privacy-Sensitive Secure ID Systems."

[13] "FTC Releases Top 10 Consumer Complaint Categories in 2002," Federal Trade Commission press release, January 23, 2003.
[14] Ibid.
[15] Beth Givens, Privacy Rights Clearinghouse.
[16] Cavoukian, op. cit.
[17] "Smart Cards and Biometrics in Privacy-Sensitive Secure ID Systems," Smart Card Alliance white paper, May 2002.

Using Multi-Factor Authentication to Counter Identify Theft

Identification systems can best enhance privacy protection and be more effective at combating identity theft when they incorporate multi-factor authentication. In order to authorize or authenticate a person, a system can depend on three main categories of authentication factors:[18]

1) Something the user knows (e.g., password, PIN)
2) Something the user has (e.g., token, smart card)
3) Something the user is (e.g., fingerprint, iris scan)

Multi-factor authentication systems can use more than one of these three factors to authenticate users.

Identity theft is taking place on an increasingly large-scale basis. Smart card-based systems have a role to play in deterring such abuses by securely protecting and authorizing access to personal data. For example, the identity fraud recently perpetrated against Experian and other credit bureaus highlights the risk associated with relying on password protection for securing information systems and databases.[19] Any system to which access is protected only by passwords is vulnerable to fraud.

Building smart cards into a system for privacy protection enhances the security of the system. Because smart cards can incorporate such security measures as digital signatures, encrypted data storage and biometrics, they can provide a higher security level than simple passwords. In systems using multi-factor authentication, presentation of both a secure smart card (something one has) *and* either something one is (a biometric) or knows (a PIN or password) would be required before access to personal information is granted.

[18] See http://packetstormsecurity.nl/crypt/srp/others.html

[19] "Smart Cards Can Prevent Experian Type Password Fraud," Smart Card Alliance press release, November 25, 2002.

Practical Guidelines for Privacy Protection in Smart Card Identification Systems

To be successful, a privacy-enabled smart card-based identification system must satisfy two critical objectives:

- Maximize protection of individuals' private information.
- Instill confidence among users that private information is being protected.

This section recommends key non-technical and non-legal considerations and practices for achieving these two objectives within two broad areas: business practices and ID system design considerations. The section does not attempt to offer comprehensive guidelines on all aspects of privacy protection. Two concepts, privacy protection and data security, overlap considerably in this context. Achieving the former depends greatly on achieving the latter. If data are insecure or too easily inappropriately accessed, they can hardly be private. Thus, some of these guidelines necessarily allude to security and data handling practices.

The guidelines below focus on how to design a system that has strong privacy protection. It is important to remember that some ID systems will have other requirements that are a higher priority than privacy protection (e.g., auditing who has accessed a bank vault). The design of any ID system, however, should include consideration of all of the potential privacy issues and select the appropriate policies and implementation approaches.

Business Practice Guidelines[20] [21]

The following business practices can help enterprises protect the privacy of individuals enrolled in an ID system:

- Develop and adhere to a comprehensive privacy policy that includes information handling practices.
- Conduct regular staff training and spot checks on proper practices.
- Conduct employee background checks, and screen temporary service providers.
- Collect only the minimum data required to perform transactions.
- Avoid displaying personal data on cards or in printouts (for example, Social Security numbers, biometric images). Truncate displayed or printed account numbers.
- Restrict access to individuals' personal information to only those who need the information to perform transactions. Enforce this restriction by requiring rigorous staff identity verification at the time of each transaction.
- Before collecting personal information from individuals, tell them why it is being collected, what it will be used for, who will be able to see it, how it will be protected, the consequences of not providing the information, and the rights of redress if the policy is violated. The individual can then decide whether to provide the information.

[20] Privacy Rights Clearing House, 2000 (http://www.privacyrights.org/).
[21] Electronic Privacy Information Center, 1994 (http://www.epic.org).

System Design Considerations and Guidelines[22] [23]

The following system design guidelines are recommended to protect privacy.

- Consider all media on which information is stored and transmitted, not only the information stored on the ID card. Store all personal information in encrypted form in the ID card and in any database. Destroy original unencrypted personal information after encryption.
- Transmit only encrypted information.
- Remove any information captured by an ID card reader or at any intermediate system transmission point from the reader or transmission point as soon as the transaction is complete.
- Use checklists for individual data fields to determine what rights each authorized group has to view, add, change, or delete data in the field.
- Enable cardholders to authorize card content extraction with a password, PIN, and/or biometric verification for all transactions.
- Maximize the offline portion of transactions (involving the card and reader only) and minimize online access, transmission of data, and recording of transaction activity in remote databases. Perform on-card verification of identity where possible. This practice provides an additional benefit: it speeds up transaction processing and reduces telecommunications expenses.
- Construct identification verification applications that extract from the card only the information required to execute a transaction. For example, authorization for the purchase of alcohol or tobacco requires only two pieces of data: data verifying the cardholder's identity and data verifying that the cardholder meets the age requirement. This transaction does not require and should not be permitted to include personal information such as the cardholder's age, address, or requirement to wear corrective lenses while operating a motor vehicle.
- Construct applications so that transaction records cannot be used as surveillance tools. The Information and Privacy Commissioner/Ontario states, "Data generated from the use of the card, such as where and when it was used, can never be matched to the transaction information and its content. The systems design ultimately used should be incapable of permitting such matching to take place."[24]

While privacy must be designed into the entire system, smart cards, with on-card intelligence and processing capabilities, are uniquely capable of enabling compliance with the above guidelines.

[22] Privacy Rights Clearing House, 2000 (http://www.privacyrights.org/).
[23] Information and Privacy Commission of Ontario, 2001 (http://www.ipc.on.ca).
[24] Ibid.

How Smart Cards Protect Privacy and Ensure Security with Different ID System Architectures

This section discusses how smart card-based ID systems address the requirement for protecting the privacy of user information when using different system architectures. The section also addresses how smart cards protect privacy when used with multiple applications.

Privacy of the individual is concerned with protecting individual information by controlling both access to that individual's personal information and use of the information, consistent with the preferences of the individual. Smart cards allow personal information to be kept private by allowing only the cardholder and any authorized and authenticated requestors to have access to the data.

Alternative Smart Card-Based ID System Architectures

Smart card based ID systems typically use two main architectures: software token-based and on-card information-based.

Software token-based smart card ID systems are implemented by including one or more secure software tokens or credentials on the smart card. Each software token relates to an application and identifies the card to a host system. All user-related data is held on the host system. When the card is prompted by a host system, the software tokens indicate the presence of valid credentials. These credentials, together with a secondary authentication factor, such as PIN entry, allow the host system to recognize the card as a valid card.

This authentication method does not divulge the identity of the cardholder. Only the digital credentials are sent to the host, protecting the privacy of the cardholder. In addition, authenticating the cardholder allows the system to secure the transaction channel between the card and the host. The presence of a secure channel further enhances the security and privacy of all transmitted data.

The use of on-card processing is another important benefit of implementing a smart card-based ID system. In an on-card information-based architecture, the smart card itself contains personal information about the cardholder. When the smart card is presented to the requesting device, all processing is done on the card and only the results are sent to external devices. Information on the card is not revealed to any external parties. To ensure privacy, the cardholder data is only visible to the cardholder or other users with the appropriate level of authorization.

The use of biometric technologies represents one example of this type of smart card usage. The biometric template (for example, of a fingerprint) can be stored securely on the card when the card is issued to the cardholder. When the card is requested for authentication, the fingerprint of the cardholder is scanned. The scanned data is then presented to the smart card as a template. The smart card compares the new template with the biometric information stored on the card. The on-card chip generates a positive or negative message indicating whether the templates match (at a pre-determined threshold) and sends the result to the requesting device.

At no time is the cardholder's registered fingerprint template exposed to an outside system. There is no need for any other private information to be exposed by the smart card. Once the data on the card is initialized (when the card is issued), all personal information is secure and inaccessible to external systems without proper authentication and authorization. The only information exposed is the result of the matching done on the card itself.

Smart Card Readers

Any ID system that uses smart cards, regardless of architecture, requires a smart card reader. The reader is the interface between the smart card and other external systems. The amount of intelligence included in a smart card reader is determined by the design of the overall system (that is, the intelligence is located where system designers decide it is needed).

In systems that involve offline usage, the reader must have a higher level of intelligence to be able to authenticate the card or perform other offline functions. In cases where processing is done online at a host system, workstation or controller, the reader needs to have enough intelligence to support messaging between the smart card and the host. In some cases, smart card readers need to be used within a trusted secure environment.

In any secure ID system, neither the reader nor any other intermediate transmission point in the ID system should retain data related to messages passing through the reader.

Multiple Applications on Smart Cards

The trend in smart card usage has been to allow multiple applications to reside on a single smart card. The presence of multiple applications on a single card has numerous advantages, including cost benefits (the cost of the card is shared between all applications on the card).

Smart card operating systems in use today separate the areas on the chip used by each application, with each area secure from access by other applications. When the smart card is presented to a requestor, only the appropriate application is accessed. Because of the partitioning between applications on the card, personal information required by one application is kept secure and private from other applications.

The host systems for a multi-application smart card may also be separate. For example, if the smart card is being used with both a transit application and a credit application, only the authority that runs the transit application handles the transit transactions. The credit application messages are acquired and sent to the issuing bank. The host systems are completely independent.

As discussed throughout the paper, smart cards have unique card security features that help to thwart identity theft, deter counterfeiting, resist tampering and protect on-card information. As a system component, smart card technology enables privacy-sensitive ID system architectures and provides a privacy-enhancing solution for any ID system.

Smart Card Application Examples

Simultaneous requirements for information accuracy, convenience, controlled access, privacy, and security confront society every day. Efforts must be taken to create easy-to-use, non-intrusive systems that do not inconvenience users in any part of the information chain.

The following two examples describe successful implementations of smart card-based, privacy-sensitive, secure identification systems. Each example illustrates how smart cards are used to improve security and enhance the privacy of an ID system. The examples illustrate implementations that are functional and secure and protect the privacy of the individual's personal information.

GSM[25] Privacy Case

According to the GSM Association, over 750 million smart cards have been deployed around the world for use in GSM mobile phone handsets. These smart cards, called Subscriber Identity Modules (SIMs), are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network. Without a SIM card, a GSM mobile phone cannot function effectively (typically reduced to emergency service only).

The GSM SIM cards do not contain the mobile phone user's credentials or even their actual phone number. Anybody can use any phone, providing that they have possession of it and are in a coverage area and that the phone is able to authenticate to a network. In most instances, however, it can be assumed that the phone is being used by the authorized (and paying) subscriber. The GSM system implementation is based on device authentication rather than subscriber or individual identity authentication or verification.

Connecting to a GSM network: The device authentication incorporated into the GSM implementation is well documented in various papers, books, and specifications. In brief, the issuer of the SIM card (the primary service provider for the subscriber) assigns a unique secret code and SIM identity number for each SIM. The number is maintained within the provider's network authentication equipment. The same data is securely loaded into the corresponding SIM card at manufacture. For the network to be assured of the validity of the phone requesting service, the network equipment issues a challenge to the SIM in the phone. If the cryptographic result presented by the SIM is computed using the correct authentication algorithm, secret key, and challenge, the network equipment can verify the SIM's authenticity.

Making calls: When a GSM mobile makes calls, it uses signaling mechanisms to present the number being dialed to the network. The network then translates the signals into information relating to the International Mobile Subscriber Identity (IMSI), which is also loaded into the SIM. The IMSI is a unique representation of the SIM for any GSM network. The network equipment translates the dialed number into a corresponding IMSI when a call is being placed. This allows the network to locate the subscriber equipment (mobile or SIM) by virtue of a fixed device number,

[25] Global System for Mobile Communication.

rather then a potentially complex, country-specific, and variable-length phone number.

Billing: Once a GSM call is completed, the GSM network equipment generates a call duration record (CDR). The CDR, which includes the IMSI, is then transmitted to the provider's billing system and routed to the subscriber's account. Only the provider's billing system can post the IMSI-based CDRs to actual subscriber accounts, thus matching a call to an individual who pays for it.

Prepaid GSM: A different implementation of GSM creates total anonymity for the user. In this implementation, the user buys a phone and SIM card that is loaded with a monetary value for making calls. The user is not required to reveal any personal information to activate the service; all the user is required to provide is cash. As the user makes each call, charges are deducted directly from the available balance until all funds are consumed. Depending on the issuer, the implementation may also include the ability to reload monetary value to maintain or re-enable the service.

Summary: The role of SIM cards in the GSM implementation is a good example of how the privacy of an individual is maintained while using mobile telephone service worldwide. Very restricted network equipment translates a phone number to an IMSI. The equipment cannot identify the subscriber. Only the billing system maintained by the issuer of the SIM can close the loop between a completed call and the entity that pays for the call. In the prepaid implementation, the individual is not required to provide any personal information whatsoever and no cross-reference to the user is possible.

Western Governors' Association Health Passport

The Health Passport Project (HPP) is an initiative sponsored by the Western Governors' Association (WGA), with pilot implementation conducted in Bismarck, North Dakota, Cheyenne, Wyoming, and Reno, Nevada. The project was originally designed to provide a secure, versatile, multi-purpose electronic card to streamline access to and delivery of a variety of public and private services and benefits. The current phase is bringing the infrastructure into compliance with HIPAA (Health Insurance Portability and Accountability Act).

HPP allows people to use smart cards to receive benefits and give up-to-date information to their health care providers, including physicians, nurses, nutritionists, and early childhood educators. The Health Passport has been issued to an estimated 25,000 pregnant women, mothers, and children eligible for a variety of health care programs.

HPP facilitates information-sharing and improves administrative efficiency among public and private health care providers, nutrition programs, and Head Start educators while placing individuals firmly in control of the information on the card. The program has the following key goals:

- Reduce health care costs — in terms of time and money — for patients and health care providers by making accurate information available where and when it is needed.
- Improve the quality of care by giving patients better access to the care for which they are eligible.
- Reduce gaps and duplication in patient records.

- Give individuals more control over their information so they can take more responsibility for their health and the health of their family.
- Improve customer satisfaction with public health services.

Overview of the Health Passport System[26]

The Health Passport system is a health information management and benefits delivery system that enables health care providers to share client information and allows retailers to provide food benefits to clients electronically. The Health Passport system consists of a Health Passport card, special card readers attached to a health provider's personal computer (PC) or retailer's in-lane checkout system, servers to maintain backup databases, kiosks, and a network for sharing Web-based data.

The Health Passport card contains demographic and medical information for participants in the project. It also contains benefit information for the pilot sites with Special Supplemental Nutrition Program for Women, Infants and Children (WIC) electronic benefits transfer (EBT). HPP is composed of the following four applications.

HPP Application. The HPP application provides users with functions for reading and writing data to a smart card. Both standalone and integrated HPP applications are available. The standalone application runs on a computer in a provider's office and is not integrated with any existing applications. The integrated application allows the user to read data from or write data to the Health Passport card through an existing (legacy) information system (thus avoiding double data-entry for staff). Data from the legacy system and the card are compared to identify the most accurate and up-to-date information.

WIC EBT Application. The WIC EBT application allows WIC food prescriptions to be written to and read from the HPP card. At the WIC clinic, benefits are authorized and sent to the WIC EBT server. From the WIC EBT server, the benefits are downloaded to three cardholder-selected retail stores to be used to purchase WIC foods. Once benefits are downloaded, the client can shop at any participating store.

Kiosk Application. The kiosk application operates on freestanding kiosks placed in the community. This application reads the card and allows the cardholder to view benefits, appointments, health information, and other program information through a touch screen. It also allows documents such as an immunization certificate to be printed.

HPP Application Programming Interface (API). The HPP API is software that allows data to be read from or written to the card through a legacy system. The HPP API also performs other card- and user-management functions, incorporating commands that can be used to interact with the smart card.

[26] Used by permission The Urban Institute: The Health Passport Project: Assessment and Recommendations, Executive Summary, December 2001. (www.urban.org)

Privacy and Security

Client demographic and health status information is recorded on the HPP smart card by participating health care providers to bring the card up-to-date after each appointment. Health Passport does not change the type of information that is currently collected by health care providers; it simply makes this information more easily available while ensuring security and complete privacy.

The Health Passport card is carried by the client. The cardholder controls access to the information on the card with a PIN. Without the correct PIN, nothing on the card can be read.

The cardholder and the participating health care providers — with the cardholder's consent — are the only people with access to information on the card. By entering a PIN into a card reader, the client gives a health care provider the ability to view information appropriate to that provider. This information is unlocked by the combination of the client's PIN and the provider's PIN. The unique combination of these two PINs gives the provider access to only the information authorized for that person. For example, an administrative person has access only to an address and phone number; a nurse may be able to see selected test results; a doctor may be able to see more complete medical information. A food retailer sees no information and is only allowed to download authorized WIC food benefits. This system prevents unauthorized individuals from looking at confidential personal information.

Current Status

Chris McKinnon, Project Director, WGA,[27] wrote: “After a successful two-year demonstration pilot period in three cities ending in December 2001, the host states spent 2002 continuing the pilots while simultaneously examining options for long term continuation and or expansion of the pilots. Decisions will be made on the future of Health Passport by each host state independently by the middle of 2003.”

WGA and interested parties in San Diego are currently designing a new pilot to build on the offline smart card-based health data-sharing pilot. The new pilot will test online health data-sharing among providers. Like the first pilot, the second pilot will be optional for clients or patients. Unlike the first pilot, the new pilot will use card-based public key functionality, instead of or in addition to PINs, to authorize access to health data.

[27] Christopher McKinnon, Project Director, Western Governors’ Association, Denver CO.

Conclusion

Both public and private organizations are implementing new or upgraded ID systems to improve the accuracy of individual identity verification and to add new capabilities that will improve the current system's security, functionality, or convenience. Privacy and security must be designed into the ID system. Requirements must be considered both during the definition of the ID system's policies, processes, and architecture and when selecting technologies for implementation. Privacy issues or concerns within an ID system are independent of any technology. A privacy-sensitive system will base its design and privacy architecture on practices and guidelines that follow internationally accepted fair information practices.

The Smart Card Alliance recommends that organizations follow design guidelines and practices that promote a privacy-sensitive ID system. Smart cards help to protect privacy. When used appropriately and correctly, smart cards can provide a privacy-enhancing platform for ID systems and provide unique features that both improve the system's security and protect the individual ID cardholder's privacy. Through the appropriate use of smart card technology in the overall ID system design, organizations can meet their requirements for secure and accurate identification while still protecting the individual's privacy.

The Smart Card Alliance urges businesses and government officials to familiarize themselves with the enhanced functionality, operational, and security advantages that smart card-based IDs can provide to improve identification processes and reduce identity fraud.

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 www.smartcardalliance.org or contact the Smart Card Alliance directly at 1-800-556-6828.

References and Resources

Ross Anderson, *Security Engineering - a Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001.

Ann Cavoukian, Ph.D., Commissioner, "Identity Theft: Who's Using Your Name?" Information and Privacy Commissioner/Ontario, June 1997.

Center for Democracy and Technology, http://www.cdt.org

Roger Clarke, "Chip-Based ID: Promise or Peril," Proc. Int'l Conf. on Privacy, Montreal, September 1997.

Common Criteria, http://www.commoncriteria.org

Department of Justice: *Overview of the Privacy Act of 1974*, May 2002. (http://www.usdoj.gov/foia/04_7_1.html)

Electronic Privacy Information Center, http://www.epic.org

EU Data Protection Directive (1995). http://www.cdt.org/privacy/eudirective/EU_Directive_.html

"FTC Releases Top 10 Consumer Complaint Categories in 2002," Federal Trade Commission press release, January 23, 2003.

Robert Gellman, "Privacy, Consumers and Costs," March 2002. Available at: http://www.epic.org/reports/dmfprivacy.html.

HEW Fair Information Practices: "Records, Computers and the Rights of Citizens" (1973). (http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm)

Information and Privacy Commission of Ontario, http://www.ipc.on.ca/

International Security, Trust and Privacy Alliance, http://www.istpa.org

Office of Management and Budget: Information Policy, IT & E-Gov. (http://www.whitehouse.gov/omb/inforeg/infopoltech.html#prm)

OECD Guidelines: "Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980). (http://www1.oecd.org/publications/e-book/9302011E.PDF)

Privacy and Human Rights: An International Survey of Privacy Laws and Developments, Electronic Privacy Information Center and Privacy International, 2002.

Privacy Impact Assessments for Information Technology, February 25, 2000. (http://www.cio.gov/documents/pia_for_it_irs_model.pdf)

Privacy International, http://www.privacyinternational.org

Privacy Rights Clearinghouse, http://www.privacyrights.org/

Safe Harbor, http://www.export.gov/safeharbor/

“Secure Personal Identification Systems: Policy, Process and Technology Choices for a Privacy-Sensitive Solution,” Smart Card Alliance white paper, February, 2002. Available at http://www.smartcardalliance.org.

Selected Recent Privacy Initiatives by the U.S. Federal Government, September 25, 2000. (http://www.cio.gov/documents/09_25_00privacylist.html)

“Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems,” Smart Card Alliance white paper, May, 2002. Available at http://www.smartcardalliance.org.

“Smart Cards Can Prevent Experian Type Password Fraud,” Smart Card Alliance press release, November 25, 2002. Available at http://www.smartcardalliance.org.

The Urban Institute: The Health Passport Project: Assessment and Recommendations, Executive Summary, December 2001 (www.urban.org).

Samuel Warren and Louis Brandies, "The Right to Privacy," *Harvard Law Review* 193 [1890].

Alan F. Westin, *Privacy and Freedom*, New York, NY: Atheneum, 1967.

Publication Acknowledgements

This position paper was developed by the Smart Card Alliance to discuss how smart card technology can help to protect privacy and ensure security in a secure ID system. 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. Members from 19 organizations, both public and private, were involved in the development of this white paper including: ASSA ABLOY ITG, Atmel, Datakey, EDS, GSA, IBM, LaserCard Systems, MasterCard International, MGM Security Consulting, Northrop Grumman IT, Office of the Information and Privacy Commissioner (IPC)/Ontario, Omnitek, Philips Semiconductors, SC Solutions, SchlumbergerSema, Smart Commerce Inc., U.S. Department of Defense, U.S. Department of the Treasury, Wave Systems.

Special thanks go to the Task Force members who wrote, reviewed and edited this white paper.

Laura Boyd, IPC/Ontario
Patricia D'Costa, IPC/Ontario
Mansour Karimzadeh, Smart Commerce Inc.
Jeff Katz, Atmel
Colleen Kulhanek, Datakey
Mark McGovern, MGM Security Consulting
Cathy Medich, Consultant and Task Force Co-Chair
Neville Pattinson, SchlumbergerSema
James Russell, MasterCard International
Keith Saunders, MasterCard International
Dale Underwood, U.S. Dept. of the Treasury
Randy Vanderhoof, Smart Card Alliance
Michael Vermillion, EDS
Michael Willett, Wave Systems
Craig Wilson, U.S. Dept. of Defense Access Card Office

Copyright Notice

Appendix A: The Privacy Act of 1974

Smart card-based systems are privacy-neutral, yet business policies and processes need to be in place when smart cards or other technologies are used for the collection, maintenance and dissemination of personal information. In the Federal government, agencies that are planning to use smart card technology to improve physical and logical access or for other purposes need to know how The Privacy Act of 1974 affects the agency's use of the records that are needed to issue, maintain and revoke smart cards.

Congress passed The Privacy Act of 1974, 5 U.S.C. 552a[28], to provide safeguards against an invasion of privacy through the misuse of records by Federal agencies. It establishes a set of policies and procedures for Federal agencies as a means of protecting an individual's privacy. The Act also requires an agency to publish in the *Federal Register* a notice of the existence and character of all systems of records maintained by the agency. The Act focuses on the characteristics of the records and the means of retrieving them rather than the technology employed to collect, maintain, or disseminate the records.

Some of the procedural requirements of the Privacy Act include the following: not collecting any information until the Privacy Act notice has been published in the *Federal Register*; maintaining the accounting of disclosures; collecting information directly from the individual; placing the Privacy Act statement on the form or at the point at which the information is collected from the individual; determining whether a disclosure is compatible with the purposes for which the information was originally collected; providing access to and amendment of records; and preparing a report to the Office of Management and Budget and Congress.

Contractors and vendors need to be aware that subsection (m) of the Privacy Act extends provisions of the Act outside the Federal government when the design, development, or operation of a system of records on individuals requires a contractor to accomplish an agency function. The Federal Acquisition Regulations System requires the following clause to be inserted in solicitations and contracts that affect records subject to the Privacy Act:

> "The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties." (48 CFR 52.224-1)

Unlike the Freedom of Information Act, the Privacy Act provides for civil remedies that apply when an agency decides not to amend an individual's record, refuses to provide access to a record, fails to maintain a record for an individual that is accurate, relevant, timely, or complete and the record is used in making a determination concerning a right or benefit the person is entitled to, and fails to comply with any other provision in such a way as to have an adverse effect on an individual.

[28] See http://www.usdoj.gov/foia/privstat.htm

Criminal penalties also apply to any employee of an agency who discloses a record to any person not entitled to receive it or who maintains a system of records without publishing a notice in the *Federal Register.* An individual who requests a record from an agency under false pretenses shall be guilty of a misdemeanor and can be fined not more than $5,000.

Federal agencies developing a smart card-based system for physical or logical access or for other functions should contact the agency's Privacy Act officer during the initial stages of development to obtain guidance in meeting the procedural requirements of the Act and Appendix I to OMB Circular A-130, "Federal Agency Responsibilities for Maintaining Records about Individuals," dated November 30, 2000.

Other Resources

Department of Justice: *Overview of the Privacy Act of 1974*, May 2002. (http://www.usdoj.gov/foia/04_7_1.html)

Selected Recent Privacy Initiatives by the U.S. Federal Government, September 25, 2000. (http://www.cio.gov/documents/09_25_00privacylist.html)

Privacy Impact Assessments for Information Technology, February 25, 2000. (http://www.cio.gov/documents/pia_for_it_irs_model.pdf)

Office of Management and Budget: Information Policy, IT & E-Gov. (http://www.whitehouse.gov/omb/inforeg/infopoltech.html#prm)

Appendix B: Statutes Providing Protection for Information Privacy In Addition to the Privacy Act of 1974

The Privacy Act of 1974, described in Appendix A, applies to Federal agencies. The following statutes embody the same types of individual privacy rights and fair information practices as the Privacy Act. This list is not exhaustive. Other confidentiality provisions are found in additional statutes, including the Census Act (13 U.S.C. 9214), the Social Security Act (42 U.S.C. 408(h)), the Child Abuse Information Act (42 U.S.C. 5103(b(2)(e))).

Fair Credit Reporting Act of 1970 (Public Law 91-508, 15 U.S.C. 1681). Requires that credit investigation and reporting agencies make their records available to the subject, provides procedures for correcting information, and permits disclosure only to authorized customers.

Crime Control Act of 1973 (Public Law 93-83). Requires that State criminal justice information systems developed with Federal funds be protected with measures to ensure the privacy and security of information.

Family Educational Rights and Privacy Act of 1974 (Public Law 93-380, 20 U.S.C. 1232(g)). Requires schools and colleges to grant students or their parents access to student records and procedures to challenge and correct information, and limits disclosure to third parties.

Tax Reform Act of 1976 (26 U.S.C. 6103). Protects confidentiality of tax information by restricting disclosure of such information for nontax purposes. The list of the exceptions has grown since 1976.

Right to Financial Privacy Act of 1978 (Public Law 95-630, 12 U.S.C. 3401). Provides bank customers with some privacy regarding records held by banks and other financial institutions, and provides procedures whereby Federal agencies can gain access to such records.

Privacy Protection for Rape Victims Act of 1978 (Public Law 95-540). Amends the Federal Rules of Evidence to protect the privacy of rape victims.

Protection of Pupil Rights of 1978 (20 U.S.C. 1232(h)). Gives parents the right to inspect educational materials used in research or experimentation projects, and restricts educators from requiring intrusive psychiatric or psychological testing.

Privacy Protection Act of 1980 (Public Law 96-440, 42 U.S.C. 2000(a)(a)). Prohibits government agencies from conducting unannounced searches of press offices and files if no one in the office is suspected of committing a crime.

Electronic Funds Transfer Act of 1978 (Public Law 95-630). Provides that any institution providing EFT or other bank services must notify its customers about third-party access to customer accounts.

Intelligence Identities Protection Act of 1982 (Public Law 97-200). Prohibits the unauthorized disclosure of information identifying certain U.S. intelligence officers, agents, informants, and sources.

Debt Collection Act of 1982 (Public Law 97-365). Establishes due process steps (e.g., notice, reply) that Federal agencies must follow before they can release bad debt information to credit bureaus.

Cable Communications Policy Act of 1984 (Public Law 98-549). Requires the cable service to inform the subscriber of the nature of personally identifiable information collected and of any use of such information, the disclosure that may be made of such information, the period during which such information will be maintained, and the times during which an individual may access such information. It also places restrictions on cable service collection and disclosure of such information.

Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. 6501-6505). Requires that operators of commercial Web sites and online services directed to children under 13 and other sites that know they are collecting personal information from a child provide parents with a notice of their information practices (among other things); obtain verifiable parental consent before collecting a child's personal information, with certain limited exceptions; not require a child to provide more information than is reasonably necessary to participate in an activity; and maintain the confidentiality, security, and integrity of information collected from children.

Gramm-Leach-Bliley Act (15 USC, Subchapter I, Sec. 6801-6810). Provides a standard for the disclosure of nonpublic personal information by financial institutions

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191). Provides standards for security, electronic signatures, and privacy of individually identifiable health information.

Electronic Communications Privacy Act (18 USC 2510).