Best Practices for the Use of RF-Enabled Technology in Identity Management

January 2007

Developed by:
Smart Card Alliance Identity Council

Best Practices for the Use of RF-Enabled Technology in Identity Management

With the current debate and concern about technology implementation for identity management, the Smart Card Alliance advocates these best practice guidelines for use of radio frequency (RF)-enabled technology for identity management. Smart card-enabled RF technologies supported by the Smart Card Alliance are able to provide these security and privacy protections.

Implementation Principle

Any application involving the verification of an individual's identity and the use of RF technology must include appropriate security techniques throughout the identity verification system to ensure the confidentiality, integrity and validity of identity information when data is being stored, transported, or accessed. This protects the individual by ensuring that all information remains secure and confidential.

The following best practices are strongly recommended:

Security: Ensure use of appropriate security

1. Implement security techniques, such as mutual authentication, cryptography and verification of message integrity, to protect identity information throughout the application.
2. Ensure protection of all user and credential information stored in central identity system databases, allowing access to specific information only according to designated access rights.
3. Verify identification credentials for both integrity and validity.

Personal Privacy Protection: Provide notice, disclosure and ability for redress

1. Notify the user as to the nature and purpose of the personally identifiable information (PII) collected – its usage and length of retention.
2. Inform the user about what information is used, how and when it is accessed, and who has access to it.
3. Provide the user with a redress mechanism to correct information and to resolve disputes.
4. Utilize the minimum PII needed to satisfy the application and no more.
5. Ensure use of the PII only for the purpose originally disclosed.
6. Ensure that the user has provided explicit consent for the operational use of the credential in all application scenarios.
7. Educate the user on their responsibilities for using and safeguarding the credential and for reporting a lost or stolen credential.

In addition to the recommendations above, organizations issuing government identity credentials also need to consider Federal and state regulations for information privacy when implementing an identity verification system.

The Smart Card Alliance recommends that all applications of RF technology for identity management consider the needs of the credential holder as well as the issuer when implementing an RF-enabled identity management system and embrace these security and privacy guidelines.

Frequently-Asked Questions: Best Practices for the Use of RF-Enabled Technology in Identity Management

The Smart Card Alliance Identity Council developed this FAQ to provide additional detail on the best practices that are advocated by the Smart Card Alliance when using RF-enabled technology in identity management systems.

1) What are different forms of radio frequency-enabled technology?

There is a wide range of technologies available that incorporate radio frequency (RF) communications to enable a variety of applications – from product and animal tagging to secure payment and identification. Each RF technology has different operational parameters, frequencies, read ranges and capabilities to support security and privacy features. For example:

- **RFID tags** that are used to add value in manufacturing, shipping and object-related tracking operate over long ranges (e.g., 25 feet), were designed for that purpose alone, and have minimal built-in support for security and privacy.
- **RF-enabled smart cards**, on the other hand, use RF technology, but, by design, operate at a short range (less than 4 inches) and support a wide variety of security features enabling identification and payment applications. This technology is also referred to as “contactless smart card technology.”

RF-enabled smart cards comply with international standards for contact and contactless smart cards (ISO/IEC 7816 and ISO/IEC 14443) and implement security features to protect payment, access and identity applications.

2) Is RF-enabled smart card technology the same as RFID?

No. There is significant confusion in discussions of RF-enabled technologies, with RF-enabled smart card technology often incorrectly categorized as "RFID." There is a wide range of RF technologies used for a variety of applications – each with different operational parameters, frequencies, read ranges and capabilities to support security and privacy features. For example, the RFID technologies that are used to add value in manufacturing, shipping and object-related tracking operate over long ranges (e.g., 25 feet), were designed for that purpose alone, and have minimal built-in support for security and privacy. RF-enabled smart cards, on the other hand, use RF technology, but, by design, operate at a short range (less than 4 inches) and can support the equivalent security capabilities of a contact smart card chip.

3) Should RFID tag technology be used for identifying people?

No. RFID tag technology was designed to automate the tracking of products and pallets through a supply chain, not to identify people. It is not the appropriate technology for securing human identification systems. The technology does not support the security features necessary to ensure the confidentiality, integrity and validity of identity information or the necessary security safeguards to protect against cloning or counterfeiting the identity credential.

RF-enabled smart card technology, on the other hand, **is** the correct technology for identity verification systems. RF-enabled smart card technology supports security features that ensure the integrity, confidentiality, and privacy of information stored on or transmitted by the card and that can be used to verify the authenticity of the identity document and its contents.

4) How does an identity application use RF-enabled technology?

An identity application would incorporate RF-enabled technology by building an integrated circuit chip and an antenna into the identity credential, allowing the credential to communicate with readers wirelessly using radio frequencies.

5) Why are identity applications now using or considering the use of RF-enabled technology?

RF-enabled technology can deliver a number of benefits to an identity verification application. For example:

- Speed and convenience. RF-enabled technology can improve the speed and convenience of the identity verification process. A user can simply hold an RF-enabled identity credential in close proximity to a reader and have the required identity information quickly communicated to the identity verification system. This can improve throughput vs. processes that require the user to insert or swipe an identity credential.
- Durability and reliability. RF-enabled technology is well-suited to identity verification systems that are exposed to the elements and have high usage. RF-enabled smart cards are durable and reliable. RF-enabled smart cards and sealed RF readers prevent damage when identity credentials and readers are exposed to dirt, water, cold, and other harsh environmental conditions.
- Security. RF-enabled smart card technology can improve the security of the identity verification process and credential – providing secure storage and communication of identity information and making it much more difficult for identity credentials to be forged or modified.
- Privacy. RF-enabled smart card technology implements and enforces the issuer's privacy policies to protect an individual's privacy.

6) What procedures should be followed if personal information is unduly disclosed and compromised?

A redress procedure should always be part of any system dealing with private information; this applies to RF-enabled identity verification systems as well. Redress procedures must define how to modify incorrect data, as well as how to assign new identification numbers when they have been compromised. It is important to design the identification system to allow redress for compromised personal information and not rely exclusively on the security measures that were put in place to protect private information in the first place. For example, if a number attached to an individual is made "permanent" by the identification system, it is very hard to change the number if it has been disclosed to unauthorized parties.

Using a credential number (such as with credit cards) allows the identification number to be changed when something bad happens. In RF-enabled identification systems, it is highly recommended that the identity credential number (personal information called an attribute) be linked to a person's record but not to use that number as a person's unique identification number in the architecture of the system.

7) What security techniques can be implemented with RF-enabled smart card technology to improve the privacy and security of an identity verification system?

The following are examples of security techniques that can be implemented with RF-enabled smart card technology.

- Mutually authenticating the identity credential and authorized interface devices or systems to ensure that only authorized valid credentials are accepted and only authorized systems can access information on the identity credential.
- Encrypting the information communicated over the air interface to prevent skimming and eavesdropping.
- Verifying the integrity of information communicated, to prevent modification or substitution of the information.

- Ensuring that the user performs a conscious action to authorize the use of the credential (such as registering the credential with a system or entering a personal identification number or biometric).
- Transmitting only the minimum information needed by the application to complete the transaction.
- Randomizing any identification number communicated over the air interface to prevent the association of a specific RF-enabled credential with any particular individual or system.
- Employing protections at the chip level to prevent tampering, probing, and attacks using differential power analysis to gain access to information contained on the chip.

8) How can identification credentials be verified for integrity and validity?

Verifying the integrity and validity of a credential is essential to ensure that the credential is authentic, has not been tampered with, and is still authorized to be used for identification. Techniques that may be used include:

- Using symmetric shared secret keys or asymmetric public/private keys with a challenge/response communication with the reader to authenticate the validity of the credential.
- Employing cryptographic techniques such as digital signatures to verify that the information stored on the credential is from a valid issuer.
- Checking the credential status in real-time (e.g., a credential's public key certificate) to verify that the credential has not been revoked.
- Verifying that the credential's physical security features (e.g., micro printing, rainbow printing, optically variable device, specialty inks) are valid.
- Verifying that the data stored on the identity credential is the same as the information printed on the credential.

9) What applications are currently using RF-enabled smart card technology?

RF-enabled smart cards are currently used worldwide for many applications, including financial, transit, access and secure identification. Examples of implementations in the United States include:

- The new ePassport being issued by the Department of State, incorporating technologies certified by the International Civil Aviation Organization (ICAO) and used by over 50 countries worldwide.
- The U.S. Federal Government Personal Identity Verification (PIV) card being issued by all Federal agencies for employees and contractors.
- Payment cards and devices being issued by American Express, Discover Network, MasterCard and Visa.
- Transit fare payment systems currently operating or being installed in such cities as Washington, DC, Chicago, Boston, Atlanta, San Francisco and Los Angeles.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use, and widespread application of 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 United States and Latin America.

The Smart Card Alliance Identity Council is focused on promoting the need for technologies, legislation, and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud, and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Additional information about the Identity Council and about the use of smart cards for secure identity applications can be found at http://www.smartcardalliance.org.