Contactless Smart Cards vs. EPC Gen 2 RFID Tags: Frequently Asked Questions

July, 2006

Developed by:
Smart Card Alliance Identity Council

Contactless Smart Cards vs. EPC Gen 2 RFID Tags: Frequently Asked Questions

Different global technology standards have been developed for different types of radio frequency (RF) applications. This frequently asked questions document has been written to help provide a better understanding of the different standards and to remove confusion between different RF technologies used on a global scale, specifically contactless smart cards that are produced under ISO/IEC 14443 and ISO/IEC 7816 international standards and EPC Gen 2 Class 1 RFID tags.

1) What are the ISO/IEC 14443 and ISO/IEC 7816 standards?

ISO/IEC 14443 is the international standard for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz and includes specifications for the physical characteristics, radio frequency power and signal interface, initialization and anticollision protocols and transmission protocol.

ISO/IEC 7816 is the international standard for contact smart cards. ISO/IEC 7816 Parts 4 and above are used by both contact and contactless smart card applications for security operations and commands for interchange.

2) What is the EPC Gen 2 standard?

EPC Gen 2 is short-hand for the Electronic Product Code Class-1 Generation-2 UHF RFID Protocol, the specification developed by EPCglobal for the second generation RFID air interface protocol and one example of a passive RFID tag protocol. EPC Gen 2 was developed to establish a standard for RFID tags used in supply chain applications (e.g., tracking inventory). The current ratified standard for Class 1 devices operates in the ultra-high frequency (UHF) range (860 – 960 MHz), supports operation at long distances (e.g., 25-30 feet), and has minimal support for security (e.g., static passwords to access or kill information on the RFID device). The specification can be found at http://www.epcglobalinc.com/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf

It is important to note that EPCglobal is expected to develop specifications for higher class devices that could incorporate more security. These specifications have not been published at this time. While a number of proposals have been made for security in higher class devices, the proposals are still being discussed in academic papers and have not been incorporated into a ratified specification.

3) What is a contactless smart card?

Contactless smart card technology and applications conform to the ISO/IEC 14443 and ISO/IEC 7816 international standards. A contactless smart card includes an embedded smart card secure microcontroller or equivalent intelligence, internal memory and a small antenna and communicates with a reader through a contactless radio frequency (RF) interface. Contactless smart card technology is used in applications that need to protect personal information and/or deliver fast, secure transactions, such as transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and financial payment cards. Example applications using contactless smart card technology include:

- The U.S. FIPS 201 Personal Identity Verification (PIV) card being issued by all Federal agencies for employees and contractors;
- The Transportation Worker Identification Credential (TWIC) being issued by the Transportation Security Administration;

- The First Responder Authentication Card (FRAC) being issued in Department of Homeland Security pilots;
- The new U.S. ePassport being issued by the Department of State;
- Contactless payment cards and devices being issued by American Express, MasterCard and Visa.
- Contactless transit fare payment systems currently operating or being installed in such cities as Washington, DC, Chicago, Boston, Atlanta, San Francisco and Los Angeles.

Contactless smart cards have the ability to securely manage, store and provide access to data on the card, perform on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a contactless smart card reader. Contactless smart card technology is available in a variety of forms – in plastic cards, watches, key fobs, documents and other handheld devices (e.g., built into mobile phones).

For the purposes of this document, "card" is used as the generic term to describe any device in which contactless smart card technology is used.

4) What is an RFID tag?

Radio frequency identification (RFID) tags are used in a wide range of applications such as: identifying animals, tracking goods through the supply chain, tracking assets such as gas bottles and beer kegs, and controlling access into buildings. RFID tags include a chip that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. Some RFID tags contain read/write memory to store dynamic data. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader.

RFID tags are simple, low-cost and commonly disposable, although this is not always the case such as reusable laundry tags. There is little to no security on the RFID tag or during communication with the reader. Any reader using the appropriate RF frequency (low frequency: 125/134 KHz; high frequency: 13.56 MHz; and ultra-high frequency: 900MHz) and protocol can get the RFID tag to communicate its contents. (Note that this is not true of car keys which contain a secure RFID tag.) Passive RFID tags (i.e., those not containing a battery) can be read from distances of several inches (centimeters) to many yards (meters), depending on the frequency and strength of the RF field used with the particular tag. RFID tags have common characteristics, including:

- Low cost designs and high volume manufacturing to minimize investment required in implementation.
- Minimal security in many applications, with tags able to be read by any compatible reader. Some applications like car keys do have security features, most notably provisions to authenticate the RFID tag before enabling the ignition to start the car.
- Minimal data storage comparable to bar code, usually a fixed format written once when the tag is manufactured, although read/write tags do exist.
- Read range optimized to increase speed and utility.

5) What security capabilities do contactless smart cards support?

Contactless smart cards 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 (see below). Contactless smart cards and readers conform to international standards, ISO/IEC 14443 and ISO/IEC 7816, and can implement a variety of industry-standard cryptographic protocols (e.g., AES, 3DES, RSA, ECC).

The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes EPC Gen 2 tags lack – i.e., the ability to securely manage, store

and provide access to data on the card, perform complex functions (for example, encryption and mutual authentication) and interact intelligently via RF with a contactless reader. Applications using contactless smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following:

- *Mutual authentication*. For applications requiring secure card access, the contactless smart card-based device can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.
- *Strong information security.* For applications requiring complete data protection, information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card-based device and the reader can be encrypted to prevent eavesdropping. Hashes and/or digital signatures can be used to ensure data integrity and to authenticate the card and the credentials it contains. Cryptographically strong random number generators can be used to enable dynamic cryptographic keys, preventing replay attacks.
- *Strong contactless device security.* Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.
- *Authenticated and authorized information access*. The contactless smart card's ability to process information and react to its environment allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.
- *Support for biometric authentication*. For human identification systems that require the highest degree of security and privacy, smart cards can be implemented in combination with biometric technology. Biometrics are measurable physical characteristics or personal behavioral traits that can be used to recognize the identity or verify the claimed identity of an individual. Smart cards and biometrics are a natural fit to provide two- or multi-factor authentication. A smart card is the logical secure storage medium for biometric information. During the enrollment process, the biometric template can be stored on the smart card chip for later verification. Only the authorized user with a biometric matching the stored enrollment template receives access and privileges.
- *Strong support for information privacy***.** The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required. The ability to support authenticated and authorized information access and the strong contactless device and data security make contactless smart cards excellent guardians of personal information and individual privacy.

It is important to note that information privacy and security must be designed into an application at the system level by the organization issuing the contactless device, card or document. It is critical that issuing organizations have the appropriate policies in place to support the security and privacy requirements of the application being deployed and then implement the appropriate technology that delivers those features. The ability of contactless smart card technology to support a wide array of security features provides organizations with the flexibility to implement the level of security that is commensurate with the risk expected in the application.

6) What security capabilities can be implemented with EPC Gen 2 Class 1 RFID tags?[1]

EPC Gen 2 RFID tags were designed for supply chain applications (tagging cases and pallets of consumer goods) and had the primary goals to be low cost, to be able to be read from a long distance, and to be able to support dense tag environments (where there are many tags within range of several readers). The EPC Gen 2 Class 1 specification has only minimal security, including only 2 basic security features:

- A static 32-bit "password" that would accompany the "kill" command. With the "kill" command, the tag would self-destruct.
- An optional static 32-bit "password" for access-controlled memory in EPC tags. An EPC reader would need to furnish this "password" to read and write to certain memory locations.

This leaves EPC Gen 2 Class 1 tags open to a number of security vulnerabilities if used in an application with sensitive information.

- EPC tags release their identifiers and product information to any compatible reader, with no ability to authorize that the reader is allowed to access the information prior to releasing the data.
- The kill and access control passwords are static, using no strong cryptographic mechanisms. Guessing or cracking the 32-bit passwords would not be difficult for a determined attacker.
- EPC tags are subject to cloning. They typically include no security features built into the integrated circuit (such as extra metal layers or sensors) to prevent physical probing and tampering. Since EPC tags release their identifiers and product information to any compatible reader, the data that is read could be easily written to a blank EPC tag, creating a duplicate tag.
- EPC tags offer only minimal resistance to eavesdropping and hotlisting. To mask data transmissions, a tag can send a random, temporary 16-bit number to the reader. The reader combines (using an exclusive-or function) this number with sensitive data like passwords to deter casual eavesdroppers. However, this random number generator does not offer cryptographic strength. An eavesdropper merely has to overhear the tag's transmission to intercept data or passwords.

While these vulnerabilities may not be critical in a supply chain application because the information contained on the tags is not sensitive, they are serious issues for any human identification application.

[1] For further information, see the EPC Gen 2 specification at http://www.epcglobalinc.com/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf and "Shoehorning Security into the EPC Standard," Daniel V. Bailey and Ari Juels (RSA Laboratories), 1/23/06, available at http://www.rsasecurity.com/rsalabs/node.asp?id=3048.

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.