Smart Card Alliance

RFID Tags, Contactless Smart Card Technology and Electronic Passports: Frequently Asked Questions

General Questions

1) What is a contactless smart card?

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. 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 interact intelligently with a contactless smart card reader. While offering similar capabilities to contactless smart cards, contact smart cards require physical contact with the reading mechanism rather than using a contactless interface. The contactless interface provides users with the convenience of allowing the contactless card to be read at short distances with fast transfer of data. 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.

2) How do contactless smart cards work?

Contactless smart card systems are closely related to contact smart card systems. Like contact smart card systems, information is stored on a chip embedded within the contactless smart card. However, unlike the contact smart card, the power supplied to the card as well as the data exchanged between the card and the reader are achieved without the use of contacts, using magnetic or electromagnetic fields to both power the card as well as to exchange data with the reader.

The contactless smart card contains an antenna embedded within the plastic body of the card (or within a key fob, watch or other document). When the card is brought into the electromagnetic field of the reader, the chip in the card is powered on. Once the chip is powered on, a wireless communication protocol is initiated and established between the card and the reader for data transfer.

The following four functions describe at a high level the sequence of events that happen when a contactless smart card is brought near a card reader:

- Energy transfer to the card for powering the integrated circuit (chip)
- Clock signal transfer
- Data transfer to the contactless smart card
- Data transfer from the contactless smart card

Hence, once the card is brought within range of an electromagnetic field of the required frequency, the card will be powered up, ready to communicate with the reader. Since the contactless smart cards described in this FAQ are based on the ISO/IEC 14443 standard, this frequency is 13.56 MHz and a reader that complies with the standard would have an activation field (range) of about 4 inches (approximately 10 centimeters). In other words, the card needs to be within 10 centimeters of a reader for it to be effectively powered; however, the effective range for communications for the card to be read will depend on a number of factors like the power of the reader, the antenna of the reader and the antenna of the card.

3) Is it true that it's been proven that contactless smart cards can be read from distances of more than 30 feet or 10 meters?

Applications that need strong information and communications security use contactless smart card technology based on an international standard (ISO/IEC 14443) that limits the ability to read the contactless device to approximately 4 inches (10 centimeters). The contactless smart card must be positioned in a target area extremely close to the reader to function, thus reducing any chance for it to be "read" without the user's knowledge. Additionally, the information stored on the card is typically protected against theft with secure encryption and communication between the card and the reader is secure and authenticated.

4) Can anyone with an RF reader read data from contactless smart card chips?

No. Applications using contactless smart cards can protect stored data in a number of ways. First, in order to access the data from a contactless smart card, the application may require knowledge of specific secret keys. In general, without knowledge of these secret keys, the card's microcontroller and circuitry will block any attempts to access the data on the chip. Second, information stored on cards or documents using contactless smart card technology can be encrypted. In addition, communications between the contactless smart card and the reader can be encrypted to prevent eavesdropping. Secure applications also typically require "mutual authentication," where the contactless smart card first verifies that the reader is authentic and then proves its own authenticity to the reader before starting any further communications. The ability of a contactless smart card application to verify the authority of the information requestor and provide strong chip and data security make it an excellent guardian of personal information and individual privacy.

5) Do the RFID tags used for inventory control have the same capabilities as contactless smart cards?

While both contactless smart cards and RFID tags use RF technology to communicate information, contactless smart cards have fundamentally different capabilities than RFID tags and are used in different applications.

Today's contactless smart cards use advanced chips that incorporate a microcontroller or equivalent intelligence, as well as internal memory, and have the primary goal of securing data on the chip. By contrast, the RFID tags being used for inventory control are becoming simpler and smaller to lower their cost. Achieving the cost levels needed by inventory control applications requires that the RFID tag be stripped down to: single function, single application, read-only capability, minimal security and a usable memory of only 96 bits or less. One can say that contactless smart cards are getting smarter while RFID tags are getting dumber.

Typically, a contactless smart card that targets banking, transport, and ID applications will operate at short range (less than 4 inches or 10 centimeters). This short distance ensures that the user performs a conscious action to transact, avoiding accidental or fraudulent transactions. For inventory management RFID tag applications involved in supply-chain management, it is necessary to be able to read tags over a longer distance of a few yards or meters.

Contactless smart cards typically incorporate processors and memory and are used for multi-function capability. For example, the same contactless smart card may support identity, loyalty and transit applications together and each application uses its own memory area and set of security keys. RFID tags are used for inventory control or for electronic article surveillance (EAS). Typically the RFID inventory control tag has 96 bits or less while contactless smart cards have memory from 512 bits up to 72 Kbytes (and more). Contactless smart cards also have memory that can both be read from and written to. RFID tags on the other hand are generally read-only.

Contactless smart cards may also support **separate** keys for reading and for writing. Thus, being able to read data from a smart card does not enable you to write or update the data, unless the application provider planned it to be so.

Contactless smart cards can also support a variety of encryption algorithms for increased security. This is essential for highly demanding applications such as banking, transport, and secure ID because it provides the highest security level possible. RFID tags do not support encryption.

6) How do I know that my personal information is protected if I have a contactless smart card?

Contactless smart cards by their nature protect the information that resides in their memory. Contactless smart card chips have built-in tamper-resistance, with both hardware and software capabilities that detect and react to tampering attempts. Information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card and the reader can also be encrypted to prevent eavesdropping. Plus, a contactless smart card application can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.

It is important to note, however, 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. Card issuers will usually have a stated privacy policy that describes to cardholders how personal information is used and protected. Card issuers will also typically implement information security requirements throughout a system that will disallow the use of data fraudulently obtained. Given sufficient technology, time, resources and expertise any technology may be compromised. However contactless smart cards are significantly more costly and complex to compromise than other solutions. Furthermore, in general, the security inherent to contactless smart card-enabled applications and systems is such that system-level application countermeasures may be deployed faster than attackers can use the vulnerability created on any individual card.

7) Is it possible for someone to write data to a contactless smart card in my pocket or purse without my knowing it?

Information (data) can only be written into the contactless smart card memory if authority to do so is provided. Authority is given by the card issuer or application provider who is the only entity that knows the secret keys and that knows how to write data to the card. Plus, the card would need to be within close proximity (4 inches or 10 centimeters for ISO/IEC 14443-compliant cards) of a specific contactless reader.

It is important to note that the write protection of the data on the new U.S. electronic passport is very strong and no data can be added, deleted or modified in the passport’s contactless smart card chip once it has been issued to the citizen.

8) If I carry a contactless smart card, can the RF fields cause health issues?

No. Contactless smart cards are passive cards (they do not carry any source of energy) and they do not have any radiation of any kind. Only the RF reader emits energy in the reading process, but it is a tiny fraction of what a cellular phone emits and poses no health risk.

9) Could someone determine my physical location through a contactless smart card that I carry?

No. Contactless smart cards have no capabilities to provide physical location information. They have an extremely limited range of response and do not support any capabilities to identify physical location (unlike the cellular phone system and global positioning system (GPS) technology).

10) Why are organizations implementing contactless smart cards? What's wrong with existing technology?

Contactless smart cards are a secure means of storing and carrying information. In general, contactless smart cards are more secure and more reliable, have higher data storage capacity, and have a longer expected life than most of the other available options (e.g., magnetic stripe cards or tickets, paper documents). For example, because of the high security, reliability and convenience of fast transactions, all smart card applications in mass transportation are implemented using contactless smart card technology.

11) Are "smart RFID tags" the same as contactless smart cards?

Smart RFID tags refer usually to a very basic memory device, which is typically a read-only memory. These components are usually capable of storing an extremely limited amount of information (less the 256 bits (or 32 characters) in the best cases). Smart RFID tags are typically used to uniquely identify goods in a supply chain. The most important capability missing from RFID tags is a **security system**. Passive RFID tags used in inventory control contain only an identification number. Their main goal is to allow their information to be picked up by authorized readers up to distances of approximately 10 feet (3.5 meters).

Contactless smart cards are capable of securely storing up to 72,000 bytes or characters and providing both secure read and write capability. These two main elements place contactless smart cards on the top of the options list when implementing projects that require secure management of a large amount of data – far ahead of the other alternatives.

(See also question 5 which has additional information on the differences between RFID tags and contactless smart cards.)

12) Are "smart labels" smart cards?

No. Smart labels are usually limited read-only memory devices that enable users to mark (tag) objects such as cases and pallets of goods in warehouses or distribution centers. The main idea behind the labels is simply to be able to electronically identify the goods when needed and/or verify their presence. Contactless smart cards, on the other hand, are used to securely manage large amounts of **variable** information, which is typically a great concern to the card issuing authority.

Electronic Passport Questions

13) Who decided that passports should have contactless smart card chips and why?

The International Civil Aviation Organization (ICAO) was established in 1947 to manage international standards for customs, immigration, and documents related to air transport. ICAO decided that contactless smart card chips provided the best means to meet the requirement of biometrically secured border control. A few other options were considered and abandoned. For a full review on the work leading to this decision, see www.icao.int/mrtd.

14) What RF chip technology is being built into the new passport?

The new passports embed a type of contactless smart card technology, which should not be confused with the very simple RFID tags being used to track products. Contactless smart card technology only works when a low power radio frequency signal of 13.56 MHz is applied within a few inches (centimeters) of the passport. The passport chip, having no batteries or power source of its own, relies on getting its power from the reader's RF signal to operate. Contactless smart card technology uses very complex microcontroller-based technology that has a sophisticated operating system and many security techniques at its disposal for ensuring the integrity, confidentiality and privacy of information stored and transmitted. The contactless smart card technology in the new passport uses ISO/IEC standards (ISO/IEC 7816-1,-2,-3,-4 and ISO/IEC 14443) to securely communicate information in a random access manner, using defined protocols, to external authenticated reading equipment. Contactless smart card technology is capable of ensuring reading equipment is authenticated as well as proving its own authenticity to the readers. Communication between the contactless smart card chip and the external reading equipment can be encrypted to counter eavesdropping. Access to any information can also be protected by personal identification number (PIN), password or biometric authentication to counter skimming attacks.

15) Is the technology in the new passport the same as the technology being used by Wal-Mart for inventory tracking?

No. The technology chosen for electronic passports is very different than the RFID technology used by Wal-Mart for inventory tracking. The technology used for electronic passports was intentionally selected because it can only be read from distances less than about 4 inches (10 centimeters), but can quickly transfer up to 64 Kbytes of photo or other biometric information back to the reader. RFID products, like the so called "smart tags" applied to inventory tracking, use very slow communication methods designed to transmit just a few bytes of information from a distance as far as several yards or meters. In addition to the fundamental differences that severely limit the read range of an electronic passport, the secure contactless smart card chips have the ability to use validated security and encryption technology to protect the information stored in them and their RF communications. (See also questions 5 and 11.)

For additional information on how RFID and contactless smart card technologies are used, see the Smart Card Alliance web site at www.smartcardalliance.org.

About this FAQ

With the growing use of both RFID and contactless smart card technologies, Smart Card Alliance members developed this FAQ to compare and contrast the applications and capabilities of the two technologies. The differences are important to keep in mind as the various forms of RF chip technology become pervasive in the market.

The Smart Card Alliance wishes to thank the Alliance members who participated in this project. Contributors included individuals from the following organizations: ASSA ABLOY ITG, Atmel Corporation, Axalto, Honeywell Access Systems (OmniTek), Hypercom, IBM, Infineon Technologies, LEGIC Identsystems, MartSoft Corporation, OTI America, Philips Semiconductors, Smart Commerce, Inc., Sony, SuperCom, Inc., U.S. Department of Transportation/Volpe Center, Visa USA, ViVOtech, XTec Incorporated.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.