# RF-Enabled Applications and Technology: Comparing and Contrasting RFID and RF-Enabled Smart Cards

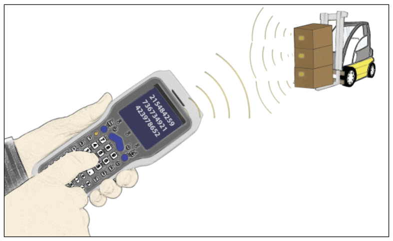
January 2007

Developed by:
**Smart Card Alliance Identity Council**

# RF-Enabled Applications and Technology: Comparing and Contrasting RFID and RF-Enabled Smart Cards

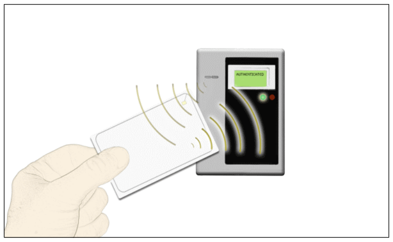
Many applications are now using radio frequency (RF) technology to automatically identify objects or verify the identity of people. These RF-enabled applications range from tracking animals and tagging goods for inventory control to enabling secure payment and identification. While these applications all use radio waves to communicate information, the RF technology used for each has different operational parameters, frequencies, read ranges and capabilities to support security and privacy features.  For example:

- **RFID tags and labels** are used to add value in manufacturing, shipping and object-related tracking. They operate over short to long ranges (e.g., from inches to 25 feet), were designed for that purpose alone and have minimal built-in support for security and privacy.

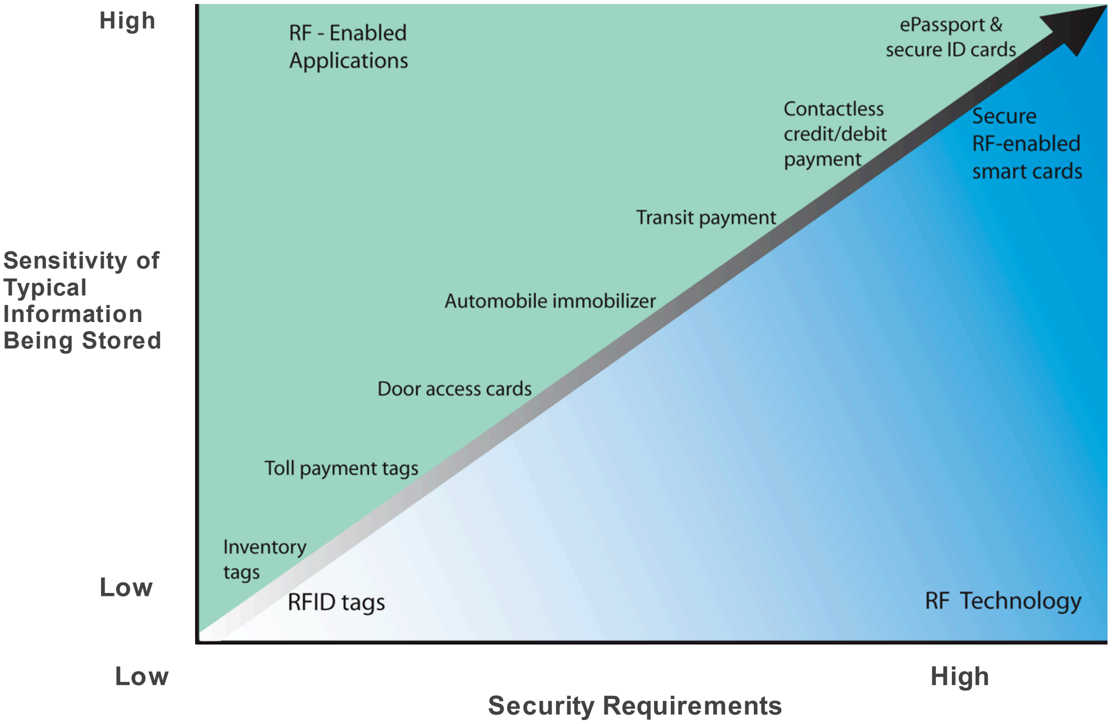


- **RF-enabled smart cards**, on the other hand, use RF technology, but, by design, operate at a short range (less than 4 inches) and support a wide variety of security features for critical applications.  This technology is also referred to as "contactless smart card technology."

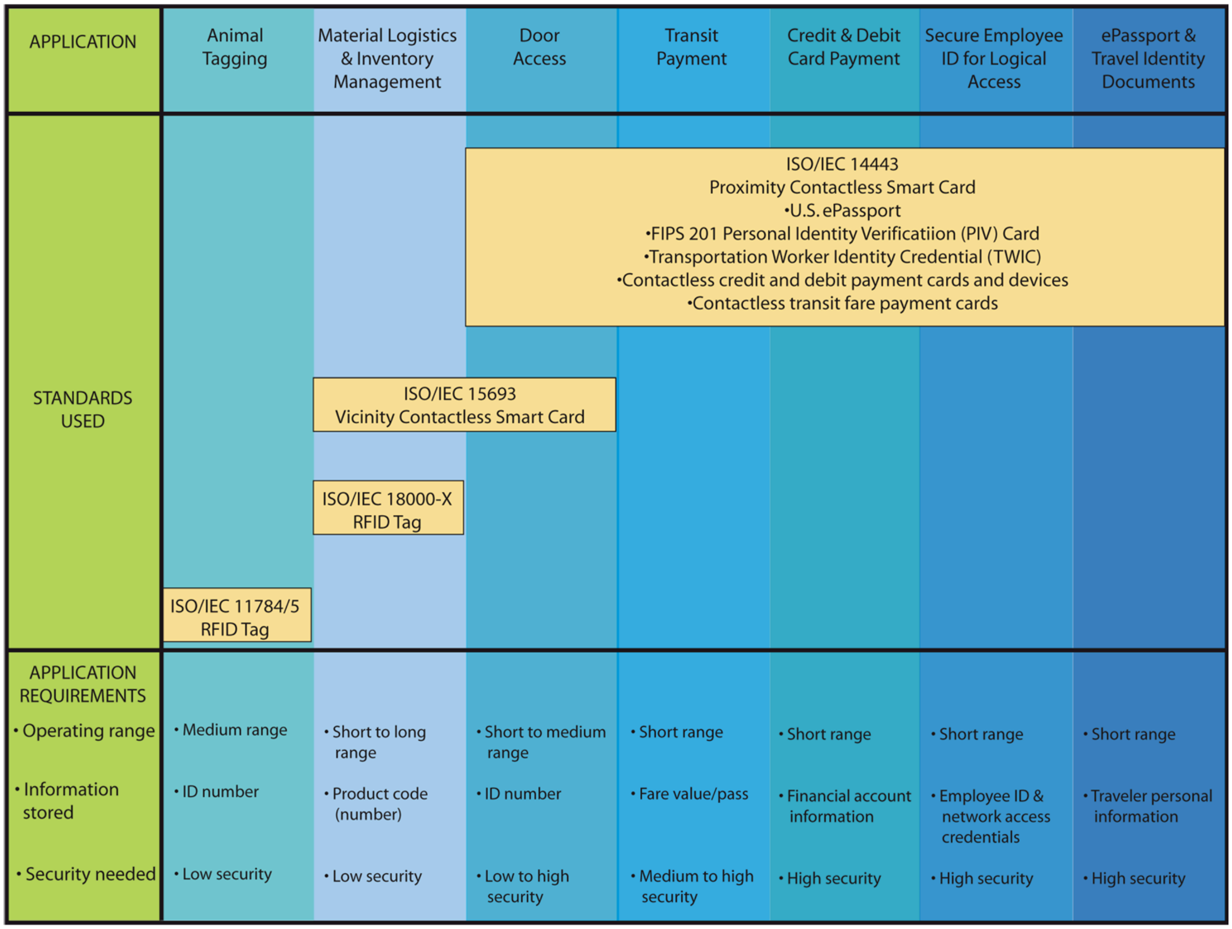
  RF-enabled contactless smart cards comply with international standards for contact and contactless smart card technology (ISO/IEC 7816 and ISO/IEC 14443) and implement security features to protect payment, access and identity applications.



RF-enabled applications have differing requirements in their use of RF technology, with RFID tag and RF-enabled smart card technologies providing very different capabilities. The figure below illustrates the range of security requirements of different RF-enabled applications and technologies.


High
Sensitivity of Typical Information Being Stored
Low
RF - Enabled Applications
ePassport & secure ID cards
Contactless credit/debit payment
Secure RF-enabled smart cards
Transit payment
Automobile immobilizer
Door access cards
Toll payment tags
Inventory tags
RFID tags
RF Technology
Low
High
Security Requirements

Understanding the differences between RFID and RF-enabled smart card technologies is critical in order to correctly assess each technology's fit with a specific application's security and privacy requirements. RFID and RF-enabled smart card technologies comply with different standards, have different operating ranges and widely varying ability to support security features needed by RF-enabled applications. The figure below shows key requirements for common RF-enabled applications and the typical RF technology used for the application.



<table>
<tr><th>APPLICATION</th><th>Animal Tagging</th><th>Material Logistics &amp; Inventory Management</th><th>Door Access</th><th>Transit Payment</th><th>Credit &amp; Debit Card Payment</th><th>Secure Employee ID for Logical Access</th><th>ePassport &amp; Travel Identity Documents</th></tr>
<tr><td rowspan="4">STANDARDS USED</td><td></td><td></td><td colspan="5">ISO/IEC 14443<br>Proximity Contactless Smart Card<br>•U.S. ePassport<br>•FIPS 201 Personal Identity Verificatiion (PIV) Card<br>•Transportation Worker Identity Credential (TWIC)<br>•Contactless credit and debit payment cards and devices<br>•Contactless transit fare payment cards</td></tr>
<tr><td></td><td colspan="2">ISO/IEC 15693<br>Vicinity Contactless Smart Card</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>ISO/IEC 18000-X<br>RFID Tag</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ISO/IEC 11784/5<br>RFID Tag</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>APPLICATION REQUIREMENTS<br>• Operating range</td><td>• Medium range</td><td>• Short to long range</td><td>• Short to medium range</td><td>• Short range</td><td>• Short range</td><td>• Short range</td><td>• Short range</td></tr>
<tr><td>• Information stored</td><td>• ID number</td><td>• Product code (number)</td><td>• ID number</td><td>• Fare value/pass</td><td>• Financial account information</td><td>• Employee ID &amp; network access credentials</td><td>• Traveler personal information</td></tr>
<tr><td>• Security needed</td><td>• Low security</td><td>• Low security</td><td>• Low to high security</td><td>• Medium to high security</td><td>• High security</td><td>• High security</td><td>• High security</td></tr>
</table>

Example applications using RF-enabled 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 new U.S. ePassport being issued by the Department of State;
- 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;
- Contactless payment cards and devices being issued by American Express, Discover, 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.

The Smart Card Alliance provides a variety of resources to assist organizations in evaluating RF technologies and implementing RF-enabled applications. Additional information about the use of and best practices for RF technologies used in identity applications can be found at http://www.smartcardalliance.org.

## 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.

# Appendix: RF-Enabled Applications and Technology: Frequently Asked Questions

## 1) What is a smart card?

A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in GSM mobile phones, and USB-based tokens.

For the purposes of this FAQ, “card” is used as the generic term to describe any device in which smart card technology is used.

## 2) 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. Another name for contactless smart card is "RF-enabled smart card."

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 new U.S. ePassport being issued by the Department of State;
- 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;
- 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 and applications conform to international standards (ISO/IEC 14443 and ISO/IEC 7816). 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).

## 3) What is an RF-enabled contactless smart card?

An RF-enabled smart card conforms to contact and contactless smart card standards (ISO/IEC 7816 and ISO/IEC 14443) and implements security features not achievable with RFID to protect payment, access and identity applications. Security features may include: encryption, hashes and/or digital signature support, dynamic data generation, mutual authentication (with the reader), built-in hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks, PIN and biometric support. Examples include ePassports, contactless and EMV credit cards and debit cards, high security ID cards, some transit payment cards and more.

## 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 data that can be written to the tag. 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.

Examples include RFID package tracking, pharmaceuticals labeling, inventory management, automatic door locks and more.

RFID tags are simple, low-cost and commonly disposable, although this is not always the case such as reusable laundry tags. Generally speaking, 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) Why is it important to distinguish between RFID tags and RF-enabled smart cards?

Understanding the differences is critical in order to correctly assess each technology's fit with a specific application's security and privacy requirements. The term RFID is familiar to most people and is often confused with RF-enabled (or contactless) smart cards. RFID tags were designed primarily to track objects at a distance with little or no concern for security. RFID should not be confused with the RF-enabled smart card technology that is used at very short distances to verify an individual's identity or execute payments and to implement secure applications where speed, security, privacy, and data integrity are considered essential.

### 6) Is RF-enabled and contactless smart card technology the same as RFID technology?

No. There is significant confusion in discussions of RF-enabled applications, with contactless 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. Contactless 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.

### 7) What security capabilities can 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). Contactless smart cards that implement security features are referred to as RF-enabled smart cards.

The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes RFID 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.
- *Protection against transaction replay.* For applications where it is critical that contactless transaction data not be able to be replayed in a fraudulent transaction, contactless smart cards can generate dynamic data every time they are read. Dynamic data generation per read provides logical security and inhibits fraudulent replay of contactless card data that may have been previously read (if the transaction was not protected using one of the techniques described in this question). For example, contactless credit, debit and prepaid payment card data includes a dynamic card verification number (CVC or CVV) or transaction certificate (for an EMV card) that is unique for every transaction. This dynamic data is generated by the contactless card based on a secret key that was stored in its secured memory by the card issuer. This key, along with a random number, transaction counter and a specific algorithm, is used to generate dynamic data every time a contactless payment card is read for a transaction. The same capability exists regardless of the form factor for the contactless smart chip (e.g., card, fob, mobile phone).
- *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.