Portions of this information courtesy of Smart Card Alliance

Q: What is a contactless smart card?
A: 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 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). A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, a magnetic stripe, a barcode, and a 2D barcode. Smart cards are used worldwide in financial, telecommunications, transit, healthcare, secure identification and other applications.

Q: Tell me a little bit about your contactless smart card offering.
A: Identiphoto has the ability to provide you with a contactless smart chip. We work with a number of chip manufacturers including, iClass, Infineon, Atmel, ST, and Phillips. We also have relationships with a number of application software providers that can assist you in meeting your needs.

Q: Do you sell smart card readers and application software?
A: Identiphoto offers a 13.56 MHz contactless iClass, Mifare & Infineon Readers. Depending upon your needs, Identiphoto provides you with application software and a variety of contactless smart cards & readers. By understanding your smart card application, we can assist you in identifying a possible software provider. Identiphoto's expertise is in providing you with the single card; we assist you in finding experts in other required areas.

Q: Why are smart cards better than other ID token technologies?
A: Smart cards are widely acknowledged as one of the most secure and reliable forms of an electronic identification (ID) token. A smart card includes an embedded integrated circuit chip that can be either a microcontroller chip with internal memory or a secured memory chip alone. The card communicates with a reader either through direct physical contact or with a remote contactless electromagnetic field that energizes the chip and transfers data between the card and the reader. 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., data storage and management, encryption, decryption, and digital signature calculations) and interact intelligently with a smart card reader.

A smart card ID can combine several ID technologies, including the embedded chip, visual security markings, magnetic stripe, barcode and/or an optical stripe. By combining these various technologies into a smart card ID token, the resulting ID can support both future and legacy physical and logical access applications. They can also support other applications that have traditionally required separate ID processes and tokens.

Biometrics are used in many new identity management systems to improve the accuracy of identifying individuals. How can smart cards be used to help assure privacy in a biometrics-based system?

Smart cards provide a highly effective mechanism to protect the privacy of an individual that has a requirement to use a biometric identity system.

- The biometric information can be stored on the smart card rather than in an online database, allowing the biometric owner the opportunity to manage the physical possession of the card holding the individual's biometric information.
- The biometric data can be secured with state-of-the-art encryption techniques while providing full three-factor authentication capability at the card/reader level.
    - Something you have – the card with all of its security capabilities
    - Something you know – a password or personal identification number (PIN)
    - Something you are – the biometric

In a non-smart-card-based application, the password or PIN and biometric would be stored in an online database outside the control of the individual and the biometric information would be captured and passed to an application for matching.

The individual's biometric can be captured by a reader and passed to the smart card for matching, rather than passing the stored biometric information to the reader for matching. The individual's biometric information would never leave the card, preventing virtually any possibility of compromise.

Q: What are the main features of a smart card?
A: Smart cards are unique in these primary ways:

- They are highly tamper-resistant. It is nearly impossible to get at stored data without first destroying the chip's functionality
- Information can be both password- and read/write-protected
- Smart cards can both store and process information
- Stored information can be encrypted
- Smart cards can be used for multiple applications
- Smart cards can be updated with new information and capabilities after issuance

Q: Are contactless smart cards as secure as contact smart cards?
A: Contactless smart cards solutions are available today that offer the same cutting edge cryptography as contact smart card products. All of the security capabilities in the contact smart cards can now be applied at the full 10cm range attainable by products meeting the ISO 14443 standard. Unlike other authentication technologies, smart cards can confirm identities in three ways:

Something you have (a secure ID card)
Something you know (a password)
Something you are (a fingerprint or eye characteristic)

Combined, these security layers create the most advanced card security in the marketplace.

Q: What are the advantages of contactless smart cards?
A: Contactless smart cards bring many benefits to secure ID systems when factors such as high throughput and usage, harsh environments, and reader maintenance and reliability are important. Because the contactless card chip and the reader communicate using radio waves, there is no need to physically make an electric connection. Maintenance of readers is minimized while reliability is important since there are no worn contacts to be replaced or openings to be unblocked. Cards also last longer because removing them from their regular carrying place is not necessary for use. Readers or kiosks can also be sealed so there is no limitation to deploying contactless ID systems in almost any environment.

Q: I would like to know what I can use that smart chip for.
A: There are many applications for a smart chip. Most common uses are:

PC Secure Log-On / Network Access
E-purse (vending, transit, cafeteria, bookstore, etc.)
Personal Information (name, address, health records, social security number, etc.)
Physical access control to highly restricted areas such as medical research departments

Based on the applications that are of interest to you, consider investing in a flexible chip and operating system that would allow you to use these applications at some future time.
The Contactless Smart Card can be used for diverse applications such as public transportation, access control, road toll, park & ride, airline ticketing, customer loyalty and ID cards. This card can also be embedded with a contact smart chip module, and further enhanced with a magnetic stripe. We can help with a recommendation.

Q: I am interested in getting a contactless smart card. How much will it cost?
A: There are a number of factors that will affect the investment you make in a smart card.

- The type of chip required (the larger the chip size and the more complex the chip, the higher the cost)
- Requirements for custom artwork on the card (the more artwork, the higher the cost)
- Requirements for magnetic stripes, Debitek stripes, signature panels, etc.

Most common would be a card in the $3.50 to $6.00 range which is comparable to proximity card prices.

Q: I have been working with a smart card provider. However, I want to put the chip on my building access card. Can you help me?
A: Yes. No matter at what stage in the card design process you are, Identiphoto can work with you to provide the best one-card technology solution.

Q: Can you print a photo id on the front of a card with a contactless smart chip?
A: Yes. We would suggest that you consider using a dye sublimation printer that is specifically designed for this purpose. Such printers are available from major manufacturers such as Fargo, DataCard, Zebra/Eltron, etc. You can have the cards printed with the company's logo, employee's name, title or other information, and photo

Q: What is an RFID tag?
A: 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.

Q: Is contactless smart card technology the same as RFID technology?
A: No. There is significant confusion in discussions of RF-enabled applications, with contactless smart card technology often incorrectly categorized as 'RFID.' There are 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.

Q: What are different forms of radio frequency-enabled technology?
A: 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.

Q: Is RF-enabled smart card technology the same as RFID?
A: 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.

Q: Should RFID tag technology be used for identifying people?
A: 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.

Q: How does an identity application use RF-enabled technology?
A: 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.

Q: Why are identity applications now using or considering the use of RF-enabled technology?
A: 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.

Q: What procedures should be followed if personal information is unduly disclosed and compromised?
A: 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.