Contactless Technology for Secure Physical Access: Technology and Standards Choices

Frequently Asked Questions

October 2002

Smart Card Alliance
191 Clarksville Road
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

Frequently Asked Questions

1. What is a smart card?

A smart card includes an embedded integrated circuit chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader through direct physical contact or a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, perform on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

2. What are combination and "combi" cards?

There is confusing terminology used in the market to refer to cards that can support a combination of technologies (for example, contactless, contact, magnetic stripe, bar code). For the purpose of the Smart Card Alliance white paper, we define specific terms for two types of ID cards that contain combinations of technology. Cards are described as "hybrid" when multiple, independent technologies share a common plastic card and do not communicate or interact with each other (e.g., magnetic stripe and contactless, or proximity/125 kHz and ISO/IEC 14443/ISO/IEC 15693). Cards are described as having a "dual-interface" when the card has a single integrated circuit (IC) that can communicate with a smart card reader/terminal via either a contact port (I/O line) or a contactless port (I/O line). '"CombiCard" and "CombiChip" are trademarks of a joint patent held by ADE and Gemplus.

3. What are the advantages of contactless technology and contactless smart cards?

Contactless technology brings 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 electrical connection. Maintenance of readers is minimized while reliability is improved 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.

Contactless smart cards bring the added benefit of larger memory storage that is not available with125 kHz technology cards. Real-time time and attendance records, electronic cash, health information, access privileges and rights, and a host of other data can be stored on the card based on the specific business and application requirements. Contactless smart card technologies also satisfy application requirements for higher security (e.g., with biometric or other advanced authentication techniques), to accommodate multiple applications on a single card (e.g., physical access, network access, payment transactions), and to protect the privacy of cardholder information.

4. Are the different contactless technologies interoperable?

Interoperability means different things to different people. From a pure technology perspective, none of the contactless technologies are 100% interoperable with each other since they are designed around different standards and specifications.

While technology companies could develop a single chip that communicates with 125 kHz, ISO/IEC 14443, and ISO/IEC 15693 technologies, the size, cost and complexity of the chip would likely prevent marketplace acceptance. Instead, companies are developing:

- Hybrid cards, with the different technologies embedded into a single credential.
- Hybrid readers, that can accept different, single technology or hybrid technology cards using advanced reader firmware that can differentiate one technology from another.

All of these solutions have different costs and advantages/disadvantages associated with them.

5. What contactless technologies can be combined on a single card?

In theory, companies could design cards that support all/any combinations of contactless technology. In practice, this is not done since the cost and complexity would limit marketplace acceptance. Because the number of readers for a card application is small relative to the number of cards, many applications require that the reader, rather than the cards, support multiple contactless protocols. As of the date that this white paper was written, hybrid cards supporting both 125 kHz technology and a 13.56 MHz technology (ISO/IEC 14443 or ISO/IEC 15693) are commercially available.

6. What are the differences between the capabilities of wired logic and microcontroller contactless cards?

A microcontroller is analogous to a complete PC in a single chip/card. It has a microprocessor (core), input/output, volatile memory and nonvolatile memory (like a PC's hard disk). Like a PC, it includes a basic operating system that makes use of the resources of the chip to execute applications and to load/run new applications into/from the chip's memory. Other features of the microcontroller (e.g., cryptographic co-processors to implement 3DES or RSA encryption and authentication) can be used flexibly through execution of code to implement conditional access functions, create a secure file system, and securely enable the loading and execution of new applications into card memory. The JavaCard operating system enables application developers to create card programs that will correctly function on different card ICs. The operating system takes care of managing the many security features of a microcontroller that are used to safeguard card contents and prevent unauthorized access (see FAQ #8 explaining the differences in security between microcontroller and wired logic contactless cards). As explained in more depth in the white paper, it is also possible to include the base level communication protocols (drivers) in the operating system of the card making it possible to use different card/IC vendors who supply cards that are interoperable.

A wired logic contactless card, as its name implies, is permanently wired to perform a predefined sequence of functions. To date, these functions include a single method of authentication/cryptography used to interface to a file system for storing an application's information. Basic means of adding or subtracting stored value may also be provided depending upon the IC. A wired logic card file system can support different applications but each of them must operate using the same small set of functions. Because each wired logic IC has a proprietary design, it may be important to choose a solution that is compliant with an ISO standard or industry specification (licensed to multiple suppliers) with a fully defined communications protocol to avoid single supplier availability.

Thus the capability of any given wired logic card is analogous to a single program/application (or set of small applications) that might run with a microcontroller based card's operating system. In fact, using a microcontroller card running a single application instead of a wired logic card may also be appropriate when an application has a high-level security target (see FAQ#8). When low cost and a lower level of security are appropriate, wired logic solutions have been successfully deployed in many applications.

7. Are contactless smart cards as secure as contact smart cards?

Contactless smart card solutions are available today that offer the same cutting edge cryptography and security as contact smart card products. Security capabilities available in contact smart cards can now be applied at the full 10 cm range attainable by products meeting the ISO/IEC 14443 standard. Cards that are both contact and contactless (dual-interface cards) can be chosen when certain tasks (for example, loading a biometric template or changing keys) are considered too sensitive to implement with a contactless card. See FAQ #9 for a discussion of U.S. policy and FIPS.

8. What is meant by the statement: "dual-interface microcontroller smart cards provide contact smart card levels of security." How does this improve upon what is available from wired logic cards?

Contact smart cards, like the Department of Defense Common Access Card (CAC) and now some contactless smart cards, are made using secure microcontroller ICs that include advanced countermeasures against attacks. Independent third parties/laboratories are required to evaluate countermeasures against a target or list of capabilities to ensure a card can counter specific threats anticipated for a given application. Today, the commercial smart card industry uses Protection Profiles as outlined in the Common Criteria standard (ISO/IEC 15408) to specify the security requirement framework that is required for a specific application and that is verified by these labs. FIPS140-2 defines specific levels of cryptographic security requirements for products/applications, like the CAC, used by the U.S. government and affiliated agencies. These countermeasures evolve with the technology that becomes available and with the capability of attackers to ensure that new threats are rendered ineffective as they become known to the industry. Because many of these countermeasures are necessarily not publicly disclosed, it is inappropriate to provide a complete list. The publicly known counter-

measures include voltage sensors, frequency sensors, light sensors, temperature sensors and clock filters. These countermeasures are designed to make observing and/or tampering with an IC to obtain the contents of the memory and cryptographic keys as difficult as possible. A smart card that meets a higher security level/target must be proven capable of defending against such attacks. Unlike microcontroller-based cards, wired logic cards have not been required to meet high-level security targets and do not include the advanced countermeasures necessary to meet higher level (Common Criteria or FIPS140-2) requirements.

9. Can contactless or dual interface cards using a single microcontroller IC meet FIPS140-2 security requirements for a cryptographic module?

There are no technical reasons foreseen that would prevent contactless/dual-interface smart cards using only a single secure, microcontroller IC with appropriate cryptographic capabilities and implementation from meeting the requirements of this security specification. To date, no such certification has been issued for any contactless technology or its implementation.

10. Is there a risk of someone "listening" or "stealing" the information from a contactless card?

In both contactless and contact technologies it is technically possible for an attacker to intercept the communications between the card and the reader. In both technologies, the card and the reader use secure cryptographic channels (as a PC does for a secure session with a web site) to prevent any un-invited listener during critical exchanges. One difference with contactless cards is the ability for the card to be activated when it enters a reader's RF range without the owner being aware of it. A contact card must be inserted by the owner in the smart card reader to be used. To prevent a contactless card activation without the card owner being aware of it, the application can be configured to always ask for the owner's authorization (password, PIN or biometric) before providing any user information or processing on the user's behalf.

The level of security of communication required between the contactless card and the reader must be defined as part of the system design and security controls must put in place so that un-invited listeners cannot intercept the data in any meaningful way. For example, all of the contactless technologies can use data encryption to protect data on the card and during transmission; this helps to ensure that, if information is intercepted, the information cannot be used by the recipient. It is important that all of the application's requirements be understood and defined prior to any technology selection and implementation so that the appropriate security features are designed into the system.

11. What government activities are underway supporting contactless standards?

The U.S. government is working with the international standards community on the interoperability of contactless cards. While FIPS certification

implications are unknown at this time, there is the possibility that FIPS will address contactless technologies in the future.

It is also expected that future enhancements of the Government Smart Card Interoperability Specification (GSC-IS) will include interoperability definitions for contactless smart card technologies, providing an industry resource that can be used for contactless smart card implementations. NIST will be continuing its efforts to integrate contactless smart card interoperability with the current contact smart card interoperability framework defined by GSC-IS version 2.0.

12. What is the difference between ISO/IEC 14443 Type A and ISO/IEC 14443 Type B?

The ISO/IEC 14443 standard defines a way to provide power and communicate between a reader and a contactless smart card. The standard specifies 13.56 MHz as the frequency and also defines a communication protocol between the card and the reader. Type A and Type B are the two communication methods defined by the standard. Differences include the modulation of the magnetic field used for coupling, the coding format and the anticollision method (i.e., how the cards and readers respond when more than one card responds at the same time to a reader's request for data). In 1994, when standardization began, Type A and Type B had slightly different application focus. Today's technological advances have removed this application differentiation. By including both in the final version of the ISO/IEC 14443 standard, the widest base of vendors are able to offer standardized contactless technology.

13. Are MIFARE and ISO/IEC 14443 Type A the same?

MIFARE and ISO/IEC 14443 Type A are not the same. While MIFARE is often viewed as an extension to or subset of ISO/IEC 14443 Type A, it is a proprietary encryption/conditional access protocol owned and licensed by Philips Semiconductors to multiple vendors of card ICs and reader ICs. Because MIFARE has been so predominantly used with products employing ISO/IEC 14443 Type A technology, it has mistakenly become synonymous with the standard. However, ISO/IEC 14443 Type A is a completely open standard when used independently of the MIFARE encryption/conditional access scheme. Please refer to the white paper reference documents for additional information.

14. What changes to contactless standards and technology are expected in the future?

Many vendors are actively developing new technologies to address the increasing market need for secure contactless technologies for a wide variety of applications. Changes in government regulations will also provide opportunities for enhancing contactless technology performance. It is important to note, however, that standards development is a lengthy process so it takes time for new technology developments to be reflected in standards that help to drive the availability of interoperable solutions.

A few examples of new technologies that are expected include:

- Changes to technology based on the ISO/IEC 15693 standard. Contactless cards supporting the ISO/IEC 15693 standard currently operate at 1.65 Kb/sec to meet FCC limits on sideband power in this frequency range. The FCC is expected to lift its restriction in late 2002, which would allow cards based on the ISO/IEC 15693 standard to improve their data rates.
- Changes for higher speed operation. ISO working groups plan to add higher speed modes of operation to ISO/IEC 14443. This will increase the speed supported by this standard from 106 Kb/sec to the 848 Kb/sec that has already been demonstrated by IC manufacturers.
- Alternative access control reader networking solutions. Wireless readers offer a significant advantage in lower costs of installation, particularly in older facilities. New security approaches can ensure strong authenticated channels between hosts or panels and new wireless readers. IP readers also permit direct connectivity to LAN-based management and control applications.
- The ability for a single contactless chip in a card to operate in full ISO/IEC 14443 and ISO/IEC 15693 modes.

15. Can contactless smart cards be used with biometrics?

Yes. Low cost, contactless smart cards with high communication speeds are now available that have enough memory to store a unique fingerprint template or single photographic representation. This means the higher security benefits of a biometrics-based ID system can use contactless smart cards to achieve a range of security and cost goals. It is important to remember, however, that the time required to capture and match a fingerprint decreases the throughput advantage of a contactless system.

16. What contactless smart card standards are supported by card and biometrics vendors?

Cards supporting the ISO/IEC 14443 standard have been successfully applied for several years with over 250 million cards (and thousands of readers) deployed using products from multiple vendors. Multiple biometrics vendors also offer contactless systems based on ISO/IEC 14443. The major smart card vendors and companies specializing in biometrics can deliver integrated readers and locks combining contactless technology and biometric image processing.

Cards supporting both ISO/IEC 14443 and ISO/IEC 15693 standards also support storing biometric templates on the contactless smart card. Multiple biometrics vendors have deployed or are expected to deploy systems supporting ISO/IEC 15693 cards and biometrics, with technologies integrated into access control systems to allow for user authentication prior to unlocking a door.

17. Will contactless card technology replace contact cards?

Contact and contactless cards are getting increasingly close in processing power and costs. Due to the convenience and high throughput that contactless technology provides for many applications, it is foreseeable that contactless technology will proliferate. There is still an important

cost factor to keep in mind about the cost of the card reader. In applications where many cards are used with the same reader, contactless technology will increase in use because of the very low cost of maintenance. On the other hand, in applications where only one card is used with one reader (e.g., access to networks and PCs), the cost of using a contactless reader might be too high for an application. The application will then use a contact or hybrid or dual-interface (contact and contactless) card to get the best cost ratio for the reader/card pair.

18. Are there other form factors than smart cards used for contactless applications?

A wide variety of form factors can be used for contactless devices, including cards, key fobs, tags, watches and wristbands. Form factor is independent of the ISO standards for contactless communications. Only the card form factor is standardized today (with ISO/IEC 7810); as long as it is possible to have an electronic component and an antenna, it is possible to use the same contactless communications standards. It is nevertheless important to remember that not all contactless devices are compliant with the international standards for communication and protocols.

19. Are electronic tags used in stores also contactless technology?

To some extent, yes, retail electronic tags are also using contactless technology; however, these technologies and products are not explicitly covered in this white paper. Tags are typically used for simple identification (read-only numbers) of objects (products or animals) and their cost must be extremely low. They are most often using different frequencies and form factors and are used in different applications from the contactless technology used for physical and logical access applications. Retail electronic tags are sometimes called “electronic bar codes” because of the similarity of use between tags and bar codes in many applications. It is important to note that ISO/IEC 15693 allows for RFID tags to use the Electronic Article Surveillance (EAS) mode of the low cost tags, therefore allowing ISO/IEC 15693-based products to replace them.

20. Are there any problems associated with post-printing on the surfaces of a contactless smart card?

Post-printing any smart card involves the application of print to one or both surfaces of the card in the form of single and/or full color graphics (e.g. photo of card holder, logo of issuer) by specialized card printers. Other printed items such as bar codes and text information are also commonplace. Direct printing technology needs a flat surface to assure a good ink deposition process, with slight surface variations still compatible with the process.

Due to the laminate composition of a contactless card body, it is possible that some areas, or points, on the card surface may present problems for some post-printing techniques. Specifically where sub-surface components are located, such as a contactless chip, it is possible that one or both card surfaces immediately above and below the chip may exhibit post-printing defects, meaning that the ink from a post-printer may not be

deposited evenly or at all. For contactless cards, the thickness variation (typically a few tens of microns) at the chip module location can decrease the printing quality, depending primarily on the design and manufacturing of the layer that incorporates the antenna and the chip (the 'inlet') and the printing equipment.

Personalization printing is generally not recommended in a square 30 mm x 30 mm (sometimes 20 mm x 20 mm) surrounding the chip module location. Clearly these areas can be intentionally avoided when designing the layout of the post-printed items with prior knowledge of the no-go post-print areas.

The re-transfer printing process is more efficient in dealing with surface variations, with the ink printed on a very thin film which is laminated on the card surface. With the re-transfer process, personalization printing can be done on the full contact or contactless card surface.

When specifying any smart card, contactless or otherwise, a full understanding of what the card is going to contain and how the card is going to be issued needs to be understood and the implications of such considered with respect to post-printing. Card body technology can help to minimize the effects that sub-surface components have on post-printing operations. If appropriate, the no-go post-printing area(s) of a contactless card body can be incorporated into common pre-printed areas of the card, allowing the common card printing to be performed prior to card assembly and post-printing operation when the card is issued.

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. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, healthcare, retail and entertainment industries, as well as a number of government agencies. 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.

Publication Acknowledgements

This FAQ was developed by the Smart Card Alliance to discuss the implementation and technology issues associated with contactless technology used for secure physical access systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their comments and contributions. Special thanks go to the contactless working group member team who contributed to this FAQ.

Copyright Notice

Trademark Notices