Contactless Smart Chip Technology: The Business Benefits

Synopsis: This briefing provides an overview of why businesses are implementing contactless smart chip technology in broadly different environments and applications both within the United States and around the world.

Introduction

Contactless smart chip technology, a form of proven smart card technology, is used increasingly in applications that must protect personal information or deliver fast, secure transactions. Leveraging many years of smart card security developments, contactless smart chips have the ability to store, protect, manage, and provide access to secure data and to support the security protocols and algorithms required by an application. In addition, contactless smart chip technology delivers the convenience, durability, and reliability required by applications that must support fast transaction throughput in demanding environments.

A contactless smart chip-based device includes an embedded secure microcontroller or equivalent intelligence, internal memory, and a small antenna, and communicates with a reader through a contactless radio frequency (RF) interface. The contactless interface provides users with the convenience of allowing the contactless device to be read at short distances with fast transfer of data. Contactless smart chip technology is available in a variety of forms – plastic cards, watches, key fobs, documents, and other handheld devices such as mobile phones.

The Business Benefits of Contactless Smart Chip Technology

Governments, corporations, financial service providers, and transit agencies are selecting contactless smart chip technology to implement new, secure identification and payment applications. Various business requirements influence this selection:

- **High throughput and fast transaction times.** Contactless smart chips can enable fast identity or payment transactions, allowing high throughput at border crossings, building entry points, or merchant checkout lines.

- **High security**. Smart card technology has been widely recognized as providing the strongest security features of any identity token or payment card technology, benefiting from over 20 years of service in demanding financial, transit, telecommunications, and identity applications. Applications can leverage the many security features supported by contactless smart chips to ensure the integrity, confidentiality, and privacy of stored or transmitted information and to counter potential security threats. Security features supported by contactless smart chips include the following:

  - *Strong information protection.* Contactless smart chip technology protects data stored on the contactless device. Contactless smart chip-based devices can encrypt the information stored on them and encrypt communications between the contactless device and the reader. Smart chip technology can also "lock" the personal information stored on the contactless device, releasing it only after the owner provides unique information such

as a personal identification number (PIN), a password, or a biometric factor (such as a fingerprint).

- *Strong contactless device security.* Like contact smart cards, contactless smart chip technology is extremely difficult to duplicate or forge and has extensive built-in tamper-resistance countermeasures. Smart chips include a variety of hardware and software capabilities that immediately detect and react to tampering attempts.

- *Sophisticated "on-chip" processing.* Smart chips accomplish many functions within the secure processing environment of the chip itself. Contactless smart chips store data, which they can then manage securely, protecting the information both while it is stored and while it is being accessed. On-chip processing enables contactless smart-chip-based devices to perform functions such as encryption, decryption, and other data processing, increasing security levels and application flexibility.

- *Authenticated and authorized information access.* The contactless smart chip's ability to both react to its environment and process information allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart chip can verify the authority of an information requestor and then allow access only to the particular information required.

- *Sophisticated, secure processing for biometrics.* Identity applications are increasingly requiring one or more biometrics to prove that an individual presenting an identity credential has the right to use that credential. Biometric data must be protected from unauthorized access or use. Contactless smart chip-based devices can store an individual's biometric data securely and prevent unauthorized access to it. In addition, identity applications can use the contactless chip to compare the individual's stored biometric with the live biometric captured by the device reader. On-chip processing protects privacy: the individual's stored biometric remains on the contactless device (which remains in the individual's possession) and the comparison and match of the stored biometric to the live biometric can be done within the smart chip's secure processing environment.

- *Strong support for information privacy.* Unlike other technologies, smart chip-based devices can implement a personal firewall for an individual, releasing only the particular information required at the time it is required. This ability to support authenticated and authorized information access combined with strong contactless device and data security make contactless smart chip-based devices excellent guardians of personal information and individual privacy.

It is critical that information privacy and security be designed into an application at the system level by the organization issuing the contactless device. This includes having the appropriate policies in place to support the security and privacy requirements of the application being deployed, designing the appropriate security and privacy measures throughout the overall system, and implementing the appropriate technologies that deliver the capabilities to meet the application's security and privacy requirements and address potential threats. Features such as encrypting personal data, locking access to data until the individual authorizes access or the device reader authenticates itself to the chip, and encrypting communication between the reader and the contactless smart chip-based device provide immunity to threats from skimming and eavesdropping and prevent unauthorized access to personal information.

- **Convenience for users of contactless devices**. A contactless smart chip-based device is convenient and easy to use. The user simply presents the device to the reader. There is no need to insert, swipe, or scan the device, and no specific device orientation is required.

- **High durability and reliability**. Contactless smart chip-based devices are durable and reliable in high use environments with mass deployments worldwide.

- **Usability in harsh or dirty environments**. Contactless smart chip-based devices are typically sealed, preventing damage when devices and readers are exposed to dirt, water,

cold, and other harsh environmental conditions. Readers do not have mechanical reader heads or moving parts, minimizing maintenance costs.

- **Form factor flexibility**. Contactless smart chip technology can be built into many different form factors, including plastic cards, fobs, watches, and travel documents (such as passports and visas). Issuers can therefore incorporate contactless smart chips into whatever form is most appropriate for an application and most accepted by the application's end user. For example, the use of a contactless smart chip in electronic passports allows the technology to be incorporated into any country's passport, regardless of the design or form of the travel document, and to be read by standards-based readers. This flexibility decreases the expense of moving to more secure machine-readable travel documents for countries throughout the world.

- **Application flexibility**. Standards-based contactless smart chips allow organizations to select technologies based on business requirements rather than implementation constraints. Organizations can implement and enforce a wide range of security policies by deploying a system that is best suited to a particular application. Smart chip technology, in either contact or contactless form factor, provides a flexible platform that can address both current and future needs (for example, physical access, cashless payment, and computer or network logical access). Multi-technology, hybrid, and dual-interface smart cards can also ease the process of migrating from existing systems and incorporate the technologies appropriate for different applications.
- **International standards-based technology**. Contactless smart chip technologies are standards-based, providing interoperable solutions for applications and complying with standards set by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). Global interoperability is achieved by using an RF band (13.56 MHz) that is available worldwide. Products complying with these international standards are commercially developed and have an established market presence. Multiple vendors can supply the standards-based components necessary to implement contactless smart chip-based applications, providing buyers with interoperable equipment and technology at a competitive cost.

Application Benefits

Each business application that uses contactless smart chip technology has its own unique requirements. The following examples illustrate some of the business factors that can contribute to the selection of contactless smart chip technology.

Electronic passports. The International Civil Aviation Organization (ICAO) selected contactless smart chip technology conforming to ISO/IEC 14443 as the international standard for machine-readable travel documents to improve the security of travel documents against increasingly sophisticated document fraud, while also improving border crossing efficiency. The incorporation of a contactless smart chip in the passport allows immigration officers to extract credential information from the document using a convenient, automated mechanism. The extracted data can then be compared manually or automatically to the passport's printed information and to the person presenting the document. Contactless smart chip technology was determined to be the best fit for electronic passports for these reasons:

- Contactless smart chip technology provides a high level of security and can support differing levels of security, depending on a particular country's requirements. The technology also supports security measures that protect the contactless RF communication between the electronic passport and the reader. For example, using features supported by the contactless smart chip, ICAO defined Basic Access Control and Secure Messaging as added security measures to safeguard the passport holder's personal information and protect the electronic passport against the potential threats of skimming and eavesdropping.

- The contactless smart chip and antenna work within the current operational constraints of passports and can be incorporated into travel documents of different shapes and sizes. This

allows countries to leverage their current investment in passport production and personalization and implement electronic passports more quickly and at lower cost.

- Contactless smart chip technology provides a reliable, durable solution, with the performance needed for travel documents that are subject to bending, stamping, and folding.

- Contactless smart chip technology allows electronic passports to be used with commercially available, standards-based readers that can accommodate any passport design.

- Contactless smart chip technology provides a solution that is easy for both the passport holder and the immigration officer to use.

Contactless financial payment devices. American Express, Mastercard, and Visa are in the process of launching contactless smart chip-based payment devices complying with international standard ISO/IEC 14443, with tens of millions of devices expected to be in use within the next 2 to 3 years. Consumers tap their contactless payment devices on (or wave them at) specially equipped merchant terminals, transmitting payment information wirelessly from the consumer to the merchant.

The benefits of contactless payment for the consumer and the merchant have been proven in numerous implementations. Increased convenience for the consumer results in increased sales and faster transaction times for the merchant. Merchants also enjoy lower costs, due to fewer requirements to handle cash, improved operational efficiencies, and lower maintenance costs, resulting from improved reliability of contactless readers. By issuing secure, contactless smart chip-based payment devices, financial service providers are providing consumers with a more convenient payment mechanism and increasing transaction volumes by replacing cash.

Corporate and government employee identification. Both government agencies and corporate enterprises are increasingly implementing smart card-based employee identification badges. These ID badges typically include both a contactless smart chip for secure physical access to buildings and facilities and a contact smart chip for secure logical access to networks and computers.

For example, in February 2005, as a result of Homeland Security Presidential Directive 12 (HSPD 12), the National Institute of Standards and Technology (NIST) published Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors. This standard mandates that all federal employees and contractors have smart card-based ID badges by October 2006. The standard specifies the use of both contact and contactless smart chips, with various levels of security implemented depending on the assurance profile desired, and requires compliance with international standards ISO/IEC 7810, ISO/IEC 10373, ISO/IEC 7816 for contact smart cards, and ISO/IEC 14443 for contactless cards.

A smart card-based employee ID system provides benefits throughout an organization, improving security and user convenience while lowering overall management and administration costs. Smart card technology provides a secure, flexible, cost-effective platform for physical and logical access control and for new applications and processes that can benefit the entire organization.

Transit payment. Today, virtually all new transit fare payment systems either in delivery or procurement use contactless smart chip-based cards as the primary ticket medium. Contactless fare payment cards offer increased customer convenience, which helps to generate ridership growth and improve the transit operator's bottom line. Such cards provide an efficient and convenient substitute for cash, increasing security, reducing fraud, and reducing handling costs for transit operators. Contactless fare payment implementations also lower operating costs, due to increased reader reliability and longer card lives.

Conclusion

Organizations worldwide are placing a high priority on implementing new technologies that improve the security and convenience of identity verification and payment transactions. Contactless smart chip technology is emerging as the smart choice, delivering strong security features along with convenience, durability, flexibility, and reliability. Contactless smart chip

technology provides the features and performance needed to meet the different business requirements that drive a diverse set of applications.

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association working to accelerate the acceptance 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 U.S. and Latin America. For more information, visit www.smartcardalliance.org.