What Makes a Smart Card Secure?

A Smart Card Alliance Contactless and Mobile Payments Council White Paper

Publication Date: October 2008

Publication Number: CPMC-08002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

TABLE OF CONTENTS

1. Executive Summary

Smart card-enabled applications are becoming more prevalent in many of today's businesses. The financial payments industry has moved to smart cards. The majority of the regional financial organizations worldwide have mandated that financial credit and debit cards must be smart card-enabled by a specified date. Plus, there has been rapid acceptance of contactless smart card technology for fast, convenient and secure credit and debit payment. The United States Federal government has adopted smart card technology for its major credentialing initiatives. The Department of Defense Common Access Card uses smart card technology for the credentialing of all military and civilian personnel. The Department of State uses contactless smart card technology for the electronic passport. Smart card-based identity credentials are now being issued to all Federal government employees to meet Homeland Security Presidential Directive 12. Enterprises are issuing smart ID badges to employees to secure physical and logical access. Plus, many government identity programs around the world are issuing smart card-based identity credentials to citizens.

All of these deployments see the use of smart card technology as an essential element for the integrity of their credentialing schemes. Smart cards are portable, personal security devices that can securely carry sensitive information, enable secure transactions, validate an individual's identity within a secure system, and verify that an information requestor is authorized to access the information carried on the card. Smart cards not only maintain the integrity of the information stored on the card, but also make it available for secure interactions with the overall system.

A smart card includes an embedded secure integrated circuit (IC) that can be either a secure microcontroller with internal memory or a secure memory IC alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency (RF) interface. With an embedded microcontroller, smart cards have built-in tamper resistance and have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

The smart card itself is only one component in a smart card-based system implementation. Security mechanisms are typically implemented in the card and at the operating system (OS), software, and system levels, providing layers of security to protect the system and information within the system from unauthorized access. In any smart card system implementation, the issuer needs to determine the risks that the system will be exposed to and implement the security measures necessary throughout the system to address those risks.

The government and financial payments industries have also led the way in establishing security evaluation and certification programs for the various layers of smart card security. Standardized evaluations and certifications use trusted third party labs to empirically verify that specific threats are prevented to a defined level of effectiveness, providing issuers with the confidence that certified products meet specified security requirements.

By placing a secure smart card in the hands of the user, organizations can implement a layered security architecture that addresses the expected risk of security breaches and implements an end-to-end chain of trust.

This white paper was developed by the Smart Card Alliance Contactless and Mobile Payment Council's Security Work Group to provide an educational overview of the security measures designed into the smart card secure IC and of the use of these features and other system-level security measures to enhance the integrity of the overall system that is being deployed. It is intended to provide a basis of information on security considerations in smart card-based systems for those organizations that are intending to deploy smart card technology for payment, security or identity applications. The white paper answers the following questions:

- What is a secure IC and what types of secure ICs are used in smart cards?
- What security features are designed into secure memory ICs and secure microcontrollers that protect data and thwart attempted attacks?

- What is the impact of contact and contactless interfaces on security?
- What are the advantages of hardware vs. software in implementing cryptography on smart cards? How do the operating system and IC hardware countermeasures function together to enhance the overall security of the smart card IC? What levels of cryptographic algorithms are currently used in smart card deployments?
- How do smart cards fit into overall system security? How is the financial industry using smart cards to improve the security of credit and debit payments?
- What industry certifications and evaluations are available that organizations can use to gain confidence in the security implemented in various smart card products and in the interoperability of the technology among various component suppliers?

While the white paper focuses on the financial payments industry when discussing overall system security, the discussion of secure ICs, interfaces and cryptography applies to all industries and applications. Examples from other industries are mentioned, with references provided for additional detail.

2. Secure Integrated Circuits and Smart Cards

Integrated circuits go by many names: IC, microcircuit, microchip, silicon chip, or just plain chip. An IC is simply a miniaturized electronic circuit that is manufactured in the surface of a thin substrate semiconductor material. In a smart card, the IC provides the logic for executing applications specific to that card. The ICs used in smart cards are "secure" ICs – meaning that they have been designed and manufactured with features that are used to protect the data and enable secure transactions with smart card applications. Applications contained on smart cards vary in complexity, memory requirements, and the security required to protect the information stored and processed in the IC. Depending on the requirements, the ICs used for smart card programs are either secure memory ICs or secure microcontrollers.

2.1 Secure Memory ICs

Memory ICs are used for smart card applications that need data storage, but that have minimal requirements for data protection. The data can be any information required by the specific smart card application. For example, the following information can be stored on a memory IC to support an identification application:

- Card issuer
- Card serial number
- Other user information (depending on the card application)

Memory smart cards use non-volatile memory (NVM) which allows the card to hold data even after its power source is removed. The NVM in a memory smart card can incorporate different memory technologies but typically uses erasable programmable read-only memory (EPROM) or electrically erasable programmable read-only memory (EEPROM). EPROM can only be changed once and is often used in prepaid service cards such as telephone calling cards that count off the minutes used and are then discarded. EEPROM can be changed up to 500,000 times. Logic that can be used to update a counter in prepaid service cards is built in.

Every secure memory IC is identified by a unique serial number. Optional fields on the memory IC include authentication logic, counter logic, error counter, data, and secret codes or keys. Application developers have options for several different memory card structures to meet design requirements. Figure 1 shows the block diagram of a typical secure memory IC.

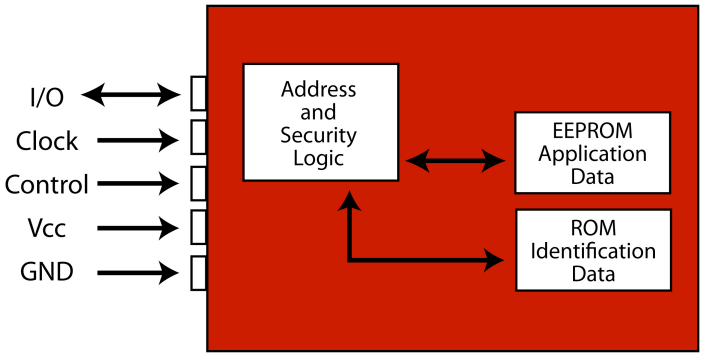

Figure 1. Secure Memory IC Block Diagram

Of the two types of secure ICs – memory and microcontroller – used in smart cards, the secure memory IC is the less secure. In the simplest designs, secure memory ICs have logic that prevents writing or erasing data. More complex designs also restrict memory read access. Security for the memory card is managed by static logic that allows for the execution of symmetric cryptographic algorithms, which are used to encrypt the data to be transmitted from the card. Symmetric algorithms can have key lengths of up to 128 bits.

2.2 Secure Microcontrollers

The secure microcontroller is a more sophisticated smart card IC. Microcontrollers consist of non-volatile memory, user memory, RAM, ROM, and an I/O unit. (See Figure 2 in Section 3.2.1 for a block diagram of a typical secure microcontroller IC.) Secure microcontroller ICs are programmed to execute applications, and functionality can be performed dynamically. Depending on what security functions the microcontroller is required to perform in a particular application, the controller may also have a cryptographic engine to more quickly and securely process asymmetric and/or symmetric algorithms.

Program code is written into the microcontroller's ROM during the IC manufacturing process. This program code, which is often referred to as the IC's operating system (OS), supports the execution of the applications that the microcontroller is intended to perform. Data and application program codes are stored in NVM, which can be modified under the control of the OS after the IC has been manufactured and embedded into the smart card. The NVM in a secure microcontroller IC can be one or a combination of memory technologies: EPROM, EEPROM, flash memory and ferroelectric random access memory (FRAM). Flash memory is a specific type of EEPROM that is erased and programmed in large blocks. FRAM is a fast and low power technology that uses the material to hold and change polarity for data storage over 100 trillion times.

One of the primary features of a secure microcontroller is dynamic active security. Microcontrollers have been adopted in smart cards mainly for secure data transactions. If a user or system cannot successfully authenticate to the microcontroller, the data stored on the card cannot be retrieved. Therefore, even if a smart card is lost, the data stored on the card will not be exposed. In addition, as a portable computer, a microcontroller smart card can process internal data securely and output the calculated result to a terminal for further processing. The integrity of the stored data is protected by a suite of countermeasures that are invoked when the microcontroller senses an attempted attack. These countermeasures are discussed in Section 3.

Secure microcontrollers offer on-chip security features that protect against physical and logical attacks. External clock frequency and voltages are monitored. Memory access rights are controlled by the memory management and protection unit. An active shield layer can detect attempts to probe or force internal components or signal lines. Random generation of current noise on idle buses (bus confusion) protects against attackers who analyze the bus. When someone tries to analyze the IC with various techniques, the built-in sensors are activated and trigger a special security reset, which immediately overwrites the RAM area. A functional current scrambling engine, in conjunction with the true random number generator and random wait state feature, protect against power and timing analyses.

Secure microcontrollers have begun to replace secure memory ICs as semiconductor technology has evolved to offer more functionality on less silicon area (i.e., lower cost). Secure microcontrollers are available with 8KB or less NVM and provide basic file system card capabilities or traditional paged/banked storage space structured similarly to the NVM of secure memory ICs. Such low cost and fixed ROM devices provide the security features of secure microcontrollers presented in this paper, but can be confused or mis-identified as secure memory ICs.

2.3 Protection of Sensitive Data

The main goal for a secure smart card product is to protect embedded assets and achieve the security objectives defined by the application designer. A secure product therefore has to be developed to protect sensitive data (the assets) from identified threats that could compromise any of the following:

- Confidentiality. All data classified as sensitive by the OS and application developers must be kept confidential. This protection includes, at a minimum, controlling access to IC memory.
- Integrity. The integrity of all sensitive (and any related) data or code must be controlled, including the integrity of the security functions.

- Availability. The data required by the IC must always be available, and the security functions must always be controlled and accessible.

Smart card applications vary in their requirements for data storage, processing and security. These requirements will dictate the choice of secure IC to be used and the types of security measures that will be implemented in the application.

2.4 Standards for Smart Cards

Both secure memory and secure microcontroller ICs need to conform to standards in order to achieve interoperability. Smart cards follow the ISO/IEC 7816 and ISO/IEC 14443 standards.

Contact secure ICs must comply with the standards defined in ISO/IEC 7816 parts 1, 2, and 3 for smart cards. Part 1 describes the physical characteristics of integrated circuit cards. This part of the standard addresses the accommodation of exposure limits for a number of electromagnetic phenomena such as X-rays, UV light, electromagnetic fields, static electrical fields, and ambient temperature of the card. Part 2 defines the dimensions and location of the contacts. It also includes standards about number, function and position of the electrical contacts. Part 3 describes electronic signals and transmission protocols of integrated circuit cards.

Secure contactless ICs comply with an additional set of standards defined by ISO/IEC 14443. ISO/IEC 14443 consists of four parts and describes two methods of modulation by which the cards communicate with readers. The modulations are referred to as type A and type B. Part 1 describes physical characteristics. Part 2 specifies the radio frequency power and signal interface Part 3 defines initialization and anti-collision. The transmission protocol is described in part 4. The transmission protocol specifies data block exchange and related mechanisms: data block chaining, waiting time extension, and multi-activation.

The standards for both contact and contactless secure ICs will be referenced throughout this white paper.

The detailed specifications documents for ISO/IEC 7816 and ISO/IEC 14443 can be found at http://www.iso.org.

3. Secure Microcontroller IC Attacks and Countermeasures

Although a smart card IC can be either a secure memory IC or a secure microcontroller, the remainder of this paper focuses on the secure microcontroller. Secure microcontrollers support the confidentiality, authentication, and integrity of stored data while still allowing the data to be accessible for applications. Applications requiring the most security use microcontroller-based smart cards; examples of deployed applications include the ePassport, the FIPS 201 Personal Identity Verification (PIV) card, EMV[1] credit/debit cards, and contactless credit/debit cards.

3.1 Goals for IC Security

Acceptable security exists when the cost of a successful attack is an order of magnitude higher than the potential profit. Achieving security is an ongoing race. Given enough time, effort, and money, any security solution can be compromised.

The level of security implemented must be balanced appropriately for the data any given transaction uses. The value of the data being protected determines the level of security measures that should be deployed and the robustness of the cryptography that should be used. As the number of applications that are developed for secure ICs grow, the more attackers' attention is focused on the technology.

3.1.1 Types of Attackers

Attackers typically fall into one of three areas:

- Amateur. Amateurs are curious individuals who carry out attacks just to "see if it can be done."
- Expert. Experts attack under the auspices of scientific institutions and universities studying the technology.
- Professional. Professionals attack for financial reward or to obtain sensitive data and compromise a system.

3.1.2 Types of Attacks

Attacks are techniques implemented to compromise the security of a smart card IC by discovering what information it holds. Attacks can be categorized as fault attacks, side-channel attacks, or invasive attacks.

Fault attacks alter the IC's internal workings to induce an error in the operation of the IC. Erroneous operation reveals information about the chip. The IC has a set of sensors that control IC operation (described in Section 3.2.1), as well as redundant logical operations. If the IC is manipulated to function outside the established sensor parameters, the IC goes into alarm mode or prevents operation completely.

Side-channel attacks are attacks based on information gained from the physical implementation of a cryptosystem. For example, timing information, power consumption, electromagnetic leaks, or even sound can provide a source of information that can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented.

Certain countermeasures in an IC can deter side-channel attacks (see Section 3.2.1):

- Random wait state insertion
- Bus confusion and memory encryption
- Continuous check of random characteristics

[1] Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment smart cards and terminals.

- Current scrambling/stabilizing
- Voltage regulation
- Dual bus rails, where the transmission of data is passed from one rail of the bus to the other to confuse the attacker

Invasive attacks, also known as **hardware attacks**, use more intrusive means to access the information on the IC. Examples of invasive attacks are probing the IC with a microprobe or focused ion beam (FIB), reverse engineering, and circuit modification.

Certain countermeasures implemented in an IC can deter invasive attacks (see Section 3.2.1):

- Flexible and user-defined memory encryption of user memory, RAM, and ROM
- Use of a memory management unit to prohibit one application from accessing the code of another application
- Active shielding that renders the IC inactive when triggered
- Small IC geometry (0.22 µm as a maximum feature size) to deter microprobing
- Bus confusion and encryption of data travelling on the bus
- Continuous checking of the random characteristics of the IC
- Proprietary timing and IC layout.

3.2 Achieving IC Security

The most comprehensive IC security is multi-dimensional. No single security mechanism protects completely against the broad spectrum of possible attacks. Therefore, the design of a secure IC and its use in a system must incorporate hardware, software, and system countermeasures to protect data and transactions.

Security should be an integral part of every smart card solution deployed. It is important to consider the security strength of the IC platform selected for any smart card application. Overall system security would also be enhanced by other measures implemented at the system level.

Secure smart card microcontrollers are commercially available that are designed to function in hostile environments. These ICs are fortified with mechanisms that are designed to withstand attempts to extract the confidential data the IC is protecting.

3.2.1 Secure Microcontroller Architecture

To defend against attacks, a secure IC should have an architecture that allows the IC to withstand all known attack types. Each IC manufacturer incorporates its own features and security modules into its IC architecture. The manufacturer may utilize its own nomenclature for the modules, but the modules perform similarly or identically while providing varying levels of protection. This section describes security features generically, recognizing that each manufacturer may have different terminology and varying levels of protection.

As described later in this paper (Section 7), independent third party test laboratories can verify that each specific secure IC platform adequately protects itself from known/defined threats. Many IC manufacturers use feedback from these third party labs to improve and invent new countermeasures that they would never willingly share with their competition. Therefore, it is better to specify which threats the IC must be capable of resisting (and to what degree) than to specify the countermeasure, as described in the section below. Specifying the countermeasures might needlessly restrict selection of ICs or add cost while providing no benefit.

Figure 2 is a block diagram of the components of a typical secure smart card microcontroller.

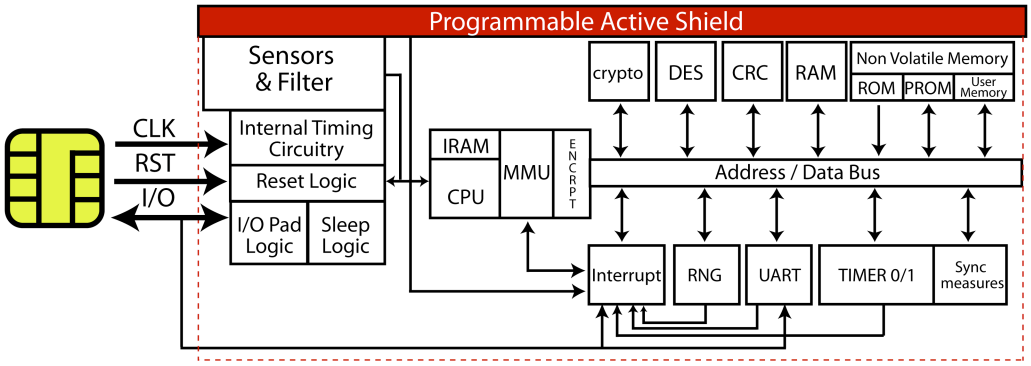

Figure 2. Components of a Typical Secure Smart Card Microcontroller

All IC components provide some aspect of protection against attacks. The following describes how the different components contribute to the security of the IC.

- A **programmable active shield** covers the entire IC and is equipped with signal layers that detect attempts to probe or force internal modules or signal lines.
- A number of **sensors** are built into secure microcontrollers to thwart fault or invasive attacks, including:
  - Low and high frequency sensors for the internal clock
  - Sensors and filters for the external clock
  - External high and low voltage sensors
  - Internal voltage sensors
  - Temperature sensors
  - Peak voltage sensors
  - Glitch sensors on internal voltage
  - Light sensors on the IC surface
- Inaccessible **internal timing circuitry** is used for cryptographic and security operations.
- The **central processing unit** (**CPU**) should have proprietary timing to make it difficult for an attacker to determine the operations that the IC is performing.
- The **memory management unit (MMU)** is an optional module that creates a true hardware firewall within the IC, enhancing the security of multi-application smart card operating systems. It does this by preventing applets from accessing important chip resources that should only be controlled by the card operating system. While this feature adds security for multi-application smart card platforms, it may not necessarily provide value for single application cards running either a single fixed application, nor fixed/configurable file system-oriented card operating systems.
- The **memory and processor bus encryption module (ENCRPT)** encrypts and decrypts stored data using specific keys stored in ROM, RAM, and NVM and a proprietary symmetric algorithm. In addition, the RAM bus (connecting the RAM to the processor) can also be encrypted after each chip reset. These measures prevent an attacker from seeing any IC calculations in the clear if the internal operations of the IC are exposed. Critical registers, the crypto module, and other peripherals are also encrypted.
- **The crypto coprocessors (crypto)** are additional processors that execute either symmetric or asymmetric algorithms such as 3DES, AES, RSA and Elliptic Curve Cryptography (ECC). These engines offload the more intensive cryptographic processing from the CPU, and increase security

by implementing hardware security countermeasures. Thus, these countermeasures allow the chip to operate more efficiently and more securely.

- The **Data Encryption Standard (DES)** module performs the calculation of DES and triple DES algorithms.
- The **cyclical redundancy check (CRC)** module verifies data integrity by checking the data to see whether an error has occurred during transmission, reading, or writing. CRC calculations are standardized in the protocol layer; ISO/IEC 7816 for contact smart cards, and ISO/IEC 14443 for contactless smart cards (with coding examples showing how host systems should implement them provided in their appendices).
- The **non-volatile memory (ROM, PROM and user memory)** data are encrypted to prevent an attacker from seeing data as clear text if the data is extracted from the IC.
- **Data bus encryption**. The data that is transmitted along the bus is encrypted, making it difficult for an attacker to determine what is being transported on the bus. All data transmitted to and from security-relevant, special-function registers should be encrypted across the bus. The bus can also scramble addresses being carried and transmitted, making the address scheme more obscure to an attacker.
- A high quality, true **random number generator (RNG)** is the basis of many cryptographic protocols and is also used in conjunction with software to harden cryptography against Differential Power Analysis (DPA) and Simple Power Analysis (SPA). The RNG can be used to create randomly different and false wait states that confuse the attacker when they are attempting to analyze the power consumption of the chip.

  Most importantly, high quality random numbers protect keys when appropriately used in mutual authentication and encryption. In these applications, random numbers are encrypted, exchanged and then eventually used as the basis of session keys guarding transactions. True random numbers are not feasibly guessed by attackers and therefore maximize the strength of the cryptography used.
- A **current masking device** unit scrambles current consumption by performing dummy access operations in memory (ROM, XRAM, and NVM). As a result of scrambling, the current consumption of the actual program flow is hidden. When used in conjunction with the RNG and random wait states, this feature is a powerful countermeasure against power analysis.

3.2.2 Secure Microcontroller Operating System

The secure microcontroller needs an OS to allow it to drive resident applications. The OS is embedded in the IC's ROM during the manufacturing process. The OS not only defines program operations for IC applications, it also includes software security features to counter software attacks and enhance hardware security features. As much as 50 percent of the OS code in a smart card product may be used to support security features. The software developer must be knowledgeable about the IC's architecture so that the OS can be designed to optimize the IC's security module operation.

It is important to note that the speed and performance of a given processor versus another in a specific application should always be judged with each running a secured OS and secured applet/application (independently verified by a trusted third party lab) to ensure one does not have the advantage of running without security.

4. Smart Card Interfaces and the Impact on Security

The need for data protection in a secure IC or smart card product must be balanced with the need to communicate with the IC and access the data. In general, smart cards currently cannot display information or directly accept input from the user.[2] For the user to access the information a smart card contains, the card needs an interface to communicate with a reader or terminal, such as a merchant point-of-sale terminal, a bank ATM or a computer smart card reader.

Four elements are required for a smart card to communicate with the outside world:

- A power source
- Clock signal transmission
- Data transfer to the secure IC
- Data transfer from the secure IC

Data can be transferred either by physical contact, using electrical connections with the contact pads on the surface of the smart card, or without contact (i.e., contactless), using radio frequency (RF) transmission. Contactless data transmission is used by many of the newer smart cards issued for applications such as mass transit tickets, physical access control, and debit and credit payment cards (such as ExpressPay from American Express®, Discover® Network Zip℠, MasterCard® *PayPass*™, and Visa payWave™).

The two methods of data transfer give rise to three types of smart cards: contact cards with a contact interface, contactless cards with a contactless interface, and dual-interface cards, with both a contact interface and a contactless interface. The choice of interface depends on both application and business requirements, which must also include security considerations. Contact and contactless smart cards may use either secure memory or a secure microcontroller as the underlying IC.

4.1 Contact Smart Card

A contact smart card's protocol interface is standardized in ISO/IEC 7816-3, while its physical connections are standardized in ISO/IEC 7816-2. A typical smart card is assembled with an IC delivered as a sawn wafer, packaged in a module, and embedded into a plastic card.[3] The component elements are shown in Figure 3.

Interfacing with the outside world requires the card to be inserted into a smart card reader or terminal in such a way that the smart card module makes a physical connection with the contact wiper pads within the reader device.

[2] Smart cards are emerging with numeric LED displays that can display (for example) an internally generated authorization code or with an activation button that controls whether a particular function (e.g., contactless mode) is on or off. However, these cards are currently complex and costly and have yet to reach mass deployment with proven reliability. They usually contain additional circuitry, such as additional ICs, and require a battery to power any display.

[3] Secure IC-based devices (i.e., smart cards) can come in a variety of form factors, including plastic cards, key fobs, wristbands, wristwatches, PDAs, and mobile phones.

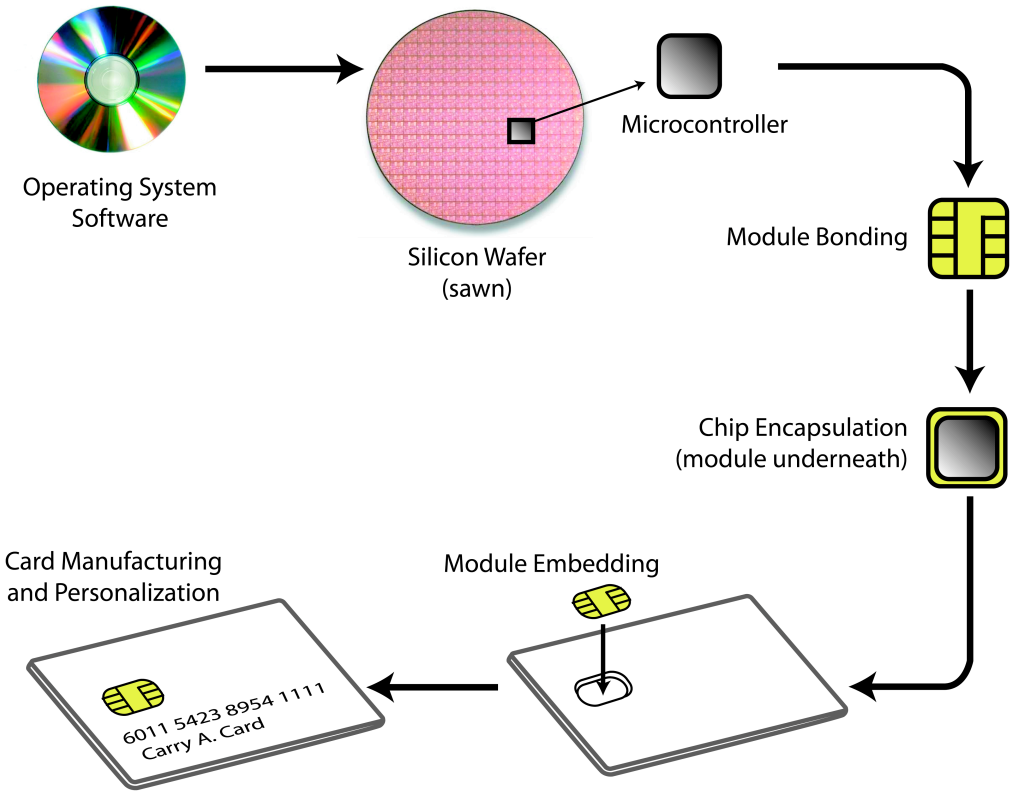

Figure 3. Component Elements of a Contact Smart Card

4.2 Contactless Smart Card

There are two main differences between a contact and contactless smart card. First, there are no physical connections between the contactless card and the reader. Second, a contactless card's power to drive the secure IC is generated from energy transferred from the reader by generating an RF field and inducing an electrical current in the IC's antenna coil when it enters the reader's RF field (Figure 4).

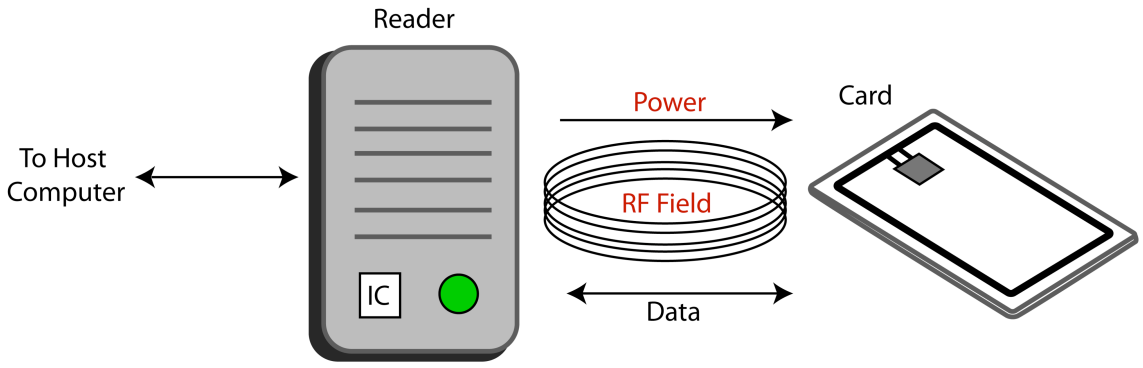

Figure 4. Contactless Smart Card in RF Field

The secure IC module is embedded in the card with no exposure to the card surface. The module has only two external contacts (whereas a contact smart card normally has five), which connect to an antenna coil that is also embedded in the card (Figure 5).

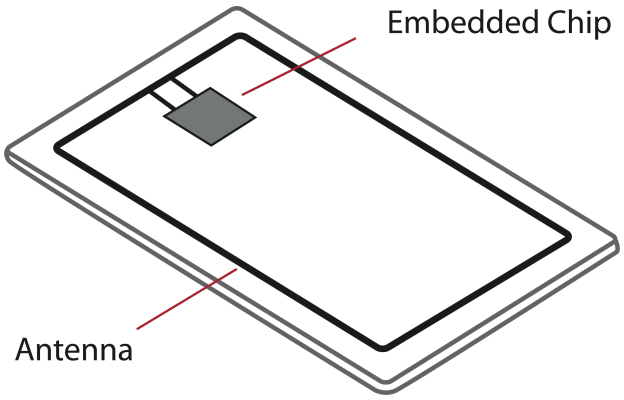

Figure 5. Contactless Card

Data transfer to and from contactless smart cards is managed by ISO/IEC 14443-compliant protocols; however, the security features and data protection features (to protect the secure IC's memory contents) are exactly the same as with a contact smart card. The only difference is the manner in which the data is transferred to the outside world.

A key point to note is that the power generated by the reader's RF field significantly decreases with distance. The further the card is from the reader, the less power is available to drive the secure IC. The limit for powering and communicating with most secure microcontrollers is in the range of 2–4 inches (5-10 cm) from the smart card reader.

Contactless mobile payment applications[4] are also now being implemented using Near Field Communication (NFC) technology, which follows universally implemented standards from ISO, Ecma International, and the European Telecommunications Standards Institute (ETSI) and is compliant with ISO/IEC 14443.

4.3 Dual-Interface Smart Card

The dual-interface smart card, as the name implies, has both a contact interface and a contactless interface. Physically the card looks like a contact card, but the IC module has two additional contact points for the antenna coil. The IC uses both ISO/IEC 7816 and ISO/IEC 14443 protocols to communicate the reader. Figure 6 shows an illustration of a dual-interface card.

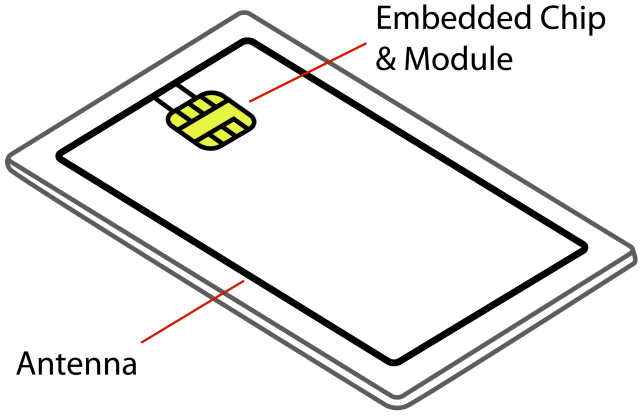

Figure 6. Dual-Interface Smart Card

[4] Also called proximity mobile payment.

A dual-interface card may be required, for example, for a transit card, which requires the contactless mode for fast transaction times and throughput at turnstiles and the contact mode to allow funds to be reloaded at an ATM or merchant POS terminal.

A hybrid smart card can be considered a type of dual-interface card. Hybrid cards operate in both contact and contactless modes by using separate secure ICs for each mode. Hybrid cards, while still in use, do not represent current technology; they were an earlier solution to allow smart cards to operate in both contact and contactless modes, which is now readily available with today's dual-interface products.

4.4 Security Implications of Different Smart Card Interfaces

For some time, the perception was that contactless cards were less secure than contact cards. However, this is not necessarily the case. A contactless card is inherently as secure as a contact card—the same security features are designed into a secure contactless microcontroller as a contact device. One comprehensive study[5] concludes that "contactless technology is not fundamentally more vulnerable than contact technology but specific constraints and threats have to be taken into account and should be solved at the application level." A position paper[6] published by Eurosmart[7] last year also concluded that: "Secure contactless smart card technology provides the same level of security as secure contact smart cards. They use smart card secure microcontrollers with physical security features to protect from tampering and cloning."

Dual-interface secure ICs must be designed so that one mode of operation cannot pose a security risk by leaking information to the other. For this reason, some applications are designed so that both modes cannot be operational at the same time. However, application requirements are emerging that require simultaneous operation so that, for example, a mobile phone can continue with voice communication while also being used to pass through a transit gate. Dual operation does not necessarily pose a security threat. However, the requirements for dual operation must be specified at the design stage.

There has been much media coverage about eavesdropping on RFID devices and contactless payment cards. Most of this coverage confuses RFID technology and secure contactless smart card technology. While both use RF, the former is designed with only limited security and can be read from a long distance, whereas the latter is designed to be secure and read only over a very short distance (a maximum of 10 cm).

Some attacks are now aimed specifically at the contactless interface:

- Eavesdropping, in which an attacker attempts to listen to a valid contactless card using an alternative reader
- Unwanted activation, which is similar to eavesdropping, in which the attacker attempts to activate a genuine contactless card without the card owner's knowledge
- Denial of service, in which the attacker tries to interfere with RF transmissions so that the system does not work and transactions cannot be completed correctly
- Man in the middle, in which a fake reader captures data by intercepting transmissions and relays the information to a fake contactless card by an alternative communication channel, such as an ultra high frequency (UHF) link, which then communicates with an alternative genuine reader

[5] Helena Handschuh, "Contactless Technology Security Issues, Smart Card Security," Information Security Bulletin, Volume 9, April 2004.

[6] "Understanding Secure Contactless Device versus RFID Tag," Eurosmart, http://www.eurosmart.com/4-Documents/PositionPapers.htm.

[7] Eurosmart is a non-profit organization located in Brussels that is committed to expanding the world's smart card market, developing smart card standards and continuously improving quality and security applications. Additional information can be found at http://www.eurosmart.com.

Such attacks can be thwarted with good system design that uses strong authentication and dynamic cryptography. As concluded by Eurosmart, "The use of smart card contactless technology allows secure management of stored and transmitted data using strong encryption, random challenge, access control through authentication and therefore provides countermeasures to defend against the attacks described."[8]

Good security design takes into account the security requirements and limitations of an application at the outset and identifies what risks are acceptable. As is true for all attacks and threats, countermeasures can be implemented, some of which may incur additional costs or be less convenient for users. For example, a contactless card can be protected by enclosing it in a protective metal sleeve, but then the card must be removed from the sleeve for use. Many countermeasures ultimately involve a tradeoff.

In both contact and contactless environments, it is important to remember that the smart card is only one part of the system. Just as the software within the card can compensate for limitations in hardware (and vice versa), system security measures external to the card can strengthen the security of the overall application.

[8] Eurosmart, op.cit.

5. Hardware Cryptographic Security vs. Software Security

In today's digital world, access to voice, video, and high value data over wired and wireless connections is fast becoming the norm. Electronic wallets, cell phone applications, and the increasing use of digital rights management (DRM) in connection with audio, video, and online streaming services are examples of this trend, which is introducing a whole new set of security concerns. Today, a properly-designed security architecture creates a high integrity solution in which security is enforced by both hardware and software. Companies must understand the threats specific to their systems, so that they can develop solutions providing the right level of security. It is not only banks and government databases that are at risk; non-commercial entities that store sensitive information that can be sold or incorporated into competitive, revenue-producing products are also affected. Compromised authentication can also enable illegal access to private networks and private data.

Both software and hardware security systems make use of cryptography and therefore cryptographic keys. Applying keys in software running on open platforms (such as PCs or servers) leaves them open to discovery using reverse engineering. They can then be used to compromise the system. Adding secure hardware, such as a secure microcontroller, to a software security system provides a means to deploy, protect and apply root system keys within a secured environment. The protected user memory holding the keys is part of the same hardware as the main core (which includes the crypto coprocessors) that is protected from attack and reverse engineering as previously described. System keys protected within a secure microcontroller can be used to derive temporary session keys deployed in their open host systems having much higher processing capability. In this way, a chain of trust is built upon the root keys guarded in the secure microcontroller but eventually implemented at the processing speed of today's cutting-edge computing platforms.

The combination of hardware security and software security must balance communication bus speeds, processing capacity, and key use/deployment to satisfy all application requirements. For example, deploying financial point-of-sale (POS) system keys and cryptography as a secure access module (SAM) works well to quickly and securely process transactions using small amounts of data. In this case the SAM processes all of the transaction side cryptography such as static data authentication (SDA) or dynamic data authentication (DDA) (see Section 6.2.2) using on-board DES/RSA crypto-coprocessors. Another good example is in the cable and satellite TV industry's use of smart cards to manage customer access to paid programming. In this case the smart card does not process the bulk encryption/decryption of audio and video, but rather acts as the keeper/deployer of root system keys, enabling secure cryptography to run in software on the host set-top box. Smart cards not only simplify the deployment of the keys enabling both of these very different applications, but do so while managing cost. The secure microcontroller provides system-level security in less costly ICs that do not require higher speed buses (such as serial peripheral interface (SPI) and universal serial bus (USB)), and replaces costly software/hardware security countermeasures otherwise required to secure complete electronic systems and devices.

The customers for these controllers determine which cryptography routines to use based on the application requirements and will implement the security features using their own OS and application software. Figure 7 illustrates how security can be achieved by a range of symmetric and asymmetric cryptography choices.

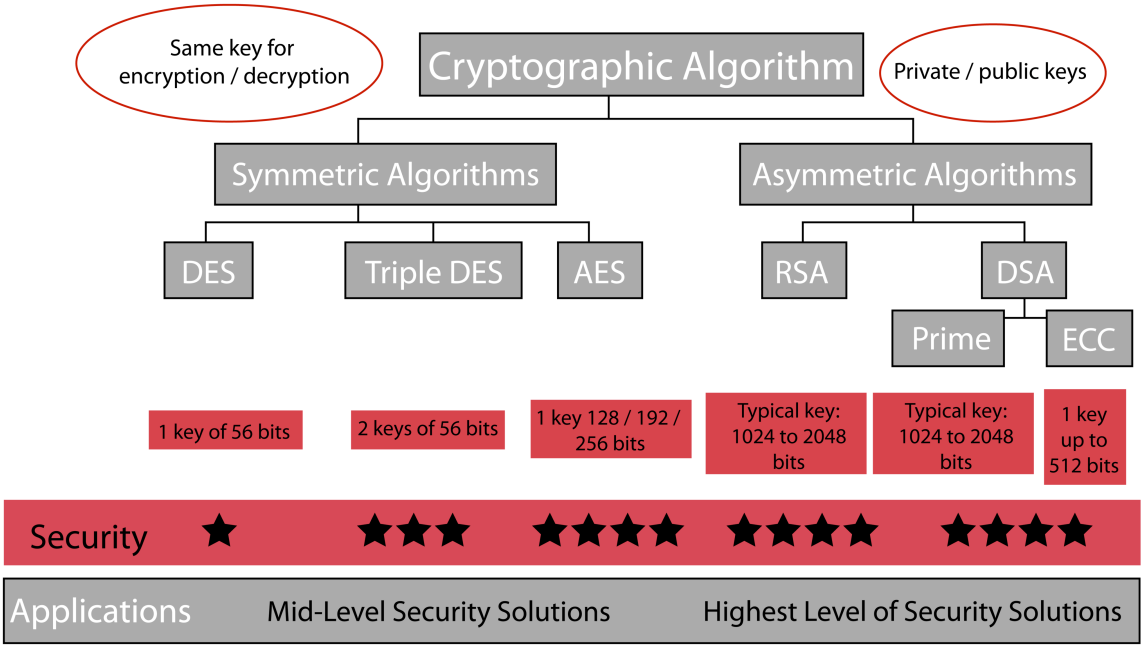

Figure 7. Cryptographic Algorithm Requirements

6. Layers of Security in Smart Card Implementations

The smart card itself is only one component in a smart card-based system implementation. Security mechanisms can be implemented in the card and at the OS, software, and system levels. This section takes a holistic view of security for an application.

As stated in Section 3, no single mechanism provides complete security. Indeed, complete security is not possible. The objective must be to ensure that the time and effort required to compromise a system yield no gain to the attacker. Risk to the system must be matched with security countermeasures to reduce exposure to a level where the risk can be tolerated. When a smart card-based system is being developed, the countermeasures that will protect the data must incorporate hardware, software, and system security features. This combination of security mechanisms is often referred to as "layers of security."

An issuer's decision on the level of security and type of security measures that should be implemented for an application in a smart card-based system must balance the risks or threats that the issuer expects to encounter, the cost of implementing the security features, and the impact that those features may have on use of the smart card. Not all applications require the same level of security. Application security requirements must be defined when a system is being designed so that the issuer can select the appropriate technology and approach for implementation.

6.1 Security Overview

Security mechanisms are implemented across an entire system. Advances in IC technology allow many security features to be implemented at the IC level. These features are designed to protect the memory contents of the IC and prevent or counter any attacks. Many of the more common features are described in Section 3. Additional countermeasures are also available that are proprietary to individual manufacturers and remain confidential.

Some attacks are designed to exploit the physical characteristics of the silicon IC, relying on the limitations of physics. An example of such an attack is a power analysis attack (DPA or SPA). IC manufacturers have implemented many different features to confuse an attacker and prevent critical data from being obtained. However, by adding a layer of security with software in the OS, physical operations can be masked even further, strengthening such countermeasures significantly.

Close cooperation between hardware and software developers can result in additional security layers that can strengthen any given secure IC feature. Software strengthens hardware and vice versa. The end result is a much more secure product.

To design a secure smart card system, designers must look beyond the secure IC itself. In the event that a card is compromised, the system designer must ensure that the security of the whole system is not at risk. For example, accessing the contents of a secure IC's memory should not reveal any master keys that are used throughout the system. Breaking into one card should not provide the opportunity for breaking into many cards.[9] Several mechanisms can be incorporated within the system that will allow additional security enhancements while the cards are deployed in the field. One methodology is to populate the IC's firmware with multiple cryptographic keys. The keys could be changed randomly or at defined intervals based on a number of transactions or a time interval criteria. Another way to update the security of the system is to enable the operating system to accept secure software downloads that would allow for new security features to be added to the IC's software as the need arises. The system could also have a suite of security features that are controlled by the issuer's back office system.

[9] This is one of the key benefits of well-designed smart card systems today. The high costs involved in breaking one card must be repeated for every card, making the process financially unviable for the would-be attacker.

One good example of how to build additional layers of security into such a system can be found in the global payment systems implemented by the financial industry (described in the next section).

6.2 The Financial Payments Industry

The financial payments industry has designed multiple layers of security into the traditional credit and debit payment systems to protect all parties involved in a payment transaction. Most of these protective measures are independent of the technology used to transfer payment account information from the payment card or device to the merchant POS terminal and are used for both magnetic stripe and contactless smart card transactions. For example, online authorization, risk management, and fraud detection systems are used to detect potential fraudulent activity for credit or debit card payment transactions. In addition, the payment brands have liability policies that protect consumers using traditional consumer credit and debit accounts.

6.2.1 Security and Contactless Payments

The financial industry has added security technology to payment systems to prevent fraud for contactless payments; these security measures are implemented both on the contactless device and in the processing network and system.[10] While implementations differ among issuers, examples of security measures that are being used include:

- At the card level, each contactless card can have its own unique built-in secret "key" that uses standard 128-bit encryption technology to generate a unique card verification value (e.g., CVV or CVC) or a cryptogram that exclusively identifies each transaction. No two cards share the same key, and the key is never transmitted.
- At the system level, payment networks have the ability to automatically detect and reject any attempt to use the same transaction information more than once. Thus, even if someone should “read” information from a contactless transaction or even multiple transactions from the same card, the information would be useless.
- Contactless payment does not require the cardholder’s name to be exchanged between the card and the terminal. In fact, best practices within the industry do not include storing the cardholder’s name in the contactless IC.
- Some contactless payment cards and devices do not include the cardholder's account number but use an alternate number that is associated with a payment account by the issuer's back-end processing system. This alternate number cannot be used in other payment transactions (e.g., with a magnetic stripe card or over the Internet).

6.2.2 Security and EMV Payments[11]

When discussing smart card security and financial payment, it is appropriate to consider the impact that the introduction of EMV payment cards has had around the world. EMV smart cards have been introduced in Europe, Asia, Latin America and Canada, with the objective of reducing fraud.

The secure microcontroller used in EMV credit and debit cards has allowed the payment industry to implement security features in addition to those available on magnetic stripe cards, such as the following:

- Card authentication, allowing a POS terminal to use cryptography to determine that a card is genuine. Three techniques are used: static data authentication (SDA), dynamic data authentication (DDA), and combined dynamic data authentication/application cryptogram generation (CDA).

[10] Additional information on contactless payments can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org/pages/activities-councils-contactless-payments-resources.

[11] Additional information on EMV specifications can be found on the EMVCo web site, http://www.emvco.com/.

- Cardholder verification, allowing the cardholder to use a personal identification number (PIN) (if not compromised) to confirm that the valid cardholder is present.

The features of the secure microcontroller in an EMV card can also enhance control over transaction authorization based on the cardholder's spending behavior. The microcontroller can support offline transactions and decide itself whether to go online, instead of having to rely strictly on merchant floor limits. In addition:

- The IC can be locked against future use by an online message from the issuer.
- 1-in-N counters can decide how many transactions can occur without online authorization. This feature can limit the number of transactions occurring below the cardholder's credit limit.
- A value counter can track the cumulative amount spent between online authorizations, trigger an online authorization, and return control to the issuer.

If the secure microcontroller in the EMV card is used to verify both the cardholder and the card itself, most "face to face" fraud can be eliminated, including fraud related to lost/stolen cards, cards never received by mail, and counterfeit cards. The card can be authenticated by checking that it has not been altered using an issuer-programmed algorithm encrypted in the IC. This process can be carried out offline between the card and the terminal.

The identity of the cardholder can also be validated by requiring the use of a PIN or other methods as set forth in the EMV specification. For PIN validation, the process checks that the PIN entered by the cardholder matches the PIN encrypted on EMV card's secure IC. Counters can prevent repeated attempts to guess a PIN and block use of the card.

By using a secure microcontroller, EMV smart cards prevent fraud caused by criminals skimming cardholder information from the credit or debit card's magnetic stripe or by embossing numbers on counterfeit cards.

The availability of transaction certificates and digital signatures with EMV payment cards can reduce merchant fraud through the use of cryptography (as described above) for non-repudiation and certified transactions.

EMV also allows issuers to use scripts to modify data elements (such as the PIN or risk parameters) on an EMV smart card during online transactions.

To support online transactions, issuers are required to receive extra IC-related data in the online message and reply to the acquirer, and therefore to the device, with additional response data. This includes authentication using the authorization request cryptogram (ARQC) and authorization response cryptogram (ARPC) in a process known as online mutual authentication (OMA).

6.3 Other Smart Card Implementations

In addition to credit and debit payments, smart cards are used for other payment applications (e.g., transit) and for secure identity implementations. For any smart card system implementation, the layers of security to be implemented and the approaches for implementation must be defined either by the issuer or at the industry level.

- ePassports are being issued with contactless secure microcontroller smart card ICs. The International Civil Aviation Organization (ICAO)[12] defines the specifications for machine-readable travel documents (MRTDs), including the ePassport, with issuing countries implementing the levels of security that they feel are appropriate for their citizens.

[12] ICAO MRTD specifications are available at http://www2.icao.int/en/MRTD/Pages/default.aspx

- The transit industry is using contactless smart cards worldwide as fare payment media in automatic fare collection systems. Security practices typically used in transit payment systems are determined by the issuing transit authority.[13]
- The U.S. Federal government is issuing smart ID cards to all employees and contractors that are based on National Institute of Standards and Technology (NIST) standards: Federal Information Processing Standard 201 (FIPS 201) Personal Identity Verification (PIV) of Federal Employees and Contractors and FIPS 140-2 Security Requirements for Cryptographic Modules.[14] These standards are discussed in more detail in Sections 7.2 and 7.4.

Smart card applications can also implement additional authentication factors (e.g., a PIN or biometric) to further bind the cardholder to the card and ensure that only the authorized cardholder can use the card.

Another important industry organization is GlobalPlatform[15]. The primary objective of GlobalPlatform is to establish, maintain and drive adoption of specifications to enable an open and interoperable infrastructure for smart cards, devices and systems to simplify and accelerate the development, deployment and management of applications across industries and geographies. GlobalPlatform develops models and conventions needed to facilitate cross-industry application loading and management, such as back-end card systems, security, key management and application deployment.

[13] For a discussion of typical security practices for transit payment systems, see the Smart Card Alliance Transportation Council white paper, *Transit Payment System Security*, available at http://www.smartcardalliance.org/pages/publications-transit-payment-system-security.

[14] Additional information about FIPS 201 and FIPS 140-2 can be found on the NIST web site at http://csrc.nist.gov/.

[15] Additional information about GlobalPlatform can be found at http://www.globalplatform.org.

7. Security Evaluations and Certifications

The government and financial payments industries have led the way in establishing security evaluation and certification programs for the various layers of smart card security. This section describes the industry-specific security evaluations for secure ICs, operating systems, and application software, as well as the entities that either require or perform these evaluations.

These standardized evaluations and certifications use a very few trusted third party labs to empirically verify that specific threats (that are state-of-the-art at the time) are prevented to a defined level of effectiveness. Measures of effectiveness encompassed in these standards include expertise, time, and cost of equipment required to achieve the specific attack. Equally important to the verification function, such standardized evaluations and certifications provide a framework to publish results of testing without disclosing details of the countermeasures that are used and verified. The resulting confidentiality allows smart cards to have their most effective security countermeasures tested without attackers knowing specifically what these countermeasures are. Best of all, those applying or specifying smart cards need not consider the specific hardware countermeasures (such as those described in this paper), but need only require that their card meet the required level of certification.

Smart cards are also subject to rigorous functional and interoperability testing, which is outside the scope of this white paper.

7.1 Proprietary versus ISO Standardized Security Evaluations/Certifications

Certification/evaluation schemes for smart cards can use an industry standardized and layered approach which is stepwise applied to the IC, then operating system (or fixed mask), and then application/applet; or a proprietary scheme which must be verified on each end product to be deployed. Openly created and published methodologies facilitate the security industry working together to define how each piece of a smart card value chain works together to deliver a complete and secure solution withstanding defined threats. Each piece of the value chain can reuse the prior step's certification/evaluation to achieve their own. For example, the IC supplier has had their secure microcontroller IC evaluated and it has received a Common Criteria (CC) EAL5+ certification. The IC manufacturer prepares a specification instructing their customers on how to make use of the IC's security features to code an operating system (or fixed function mask) that is also CC certifiable. The card operating system vendor submits the finished product to a verification lab for CC EAL4+ certification. Upon receiving a certification for their OS/mask, the supplier provides a specification guiding customers to apply the product as necessary to achieve a certifiable application of the finished card.

The differences in cost and change management for each of these approaches are both obvious and great. The standardized approach allows reuse of the prior step's work with verifiers checking to ensure the OS provider (or application user) has correctly used the features which have already been verified. A change required to the applet would only require the applet on the verified IC and OS to be rechecked using the standardized approach; this would require a full resubmission using the proprietary approach. As expected, the costs of rechecking the entire platform are significant and being able to reuse parts of the verification process greatly reduces the cost and time to complete the evaluation/certification process.

7.2 FIPS 140-2 and 140-3 for Cryptographic Modules

FIPS 140-2 is the U.S. government security standard for cryptographic modules. It applies to the entire smart card, including the secure IC, the operating system, and the application software. This standard is the benchmark for implementing cryptographic software and hardware and specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and securely working with the operating system. In the late 1990s, smart card manufacturers began submitting

smart cards for FIPS 140-1 certification. In 2001, FIPS 140-1 was replaced by FIPS 140-2, and FIPS 140-3 will soon replace FIPS 140-2.

FIPS 140-2 specifies the requirements for cryptographic modules in the areas of secure design and implementation, including module specification, ports and interfaces, roles, services, and authentication, finite state model, physical security, operational environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self-tests, design assurance, and mitigation of other attacks.

FIPS 140-2 specifies four levels of security. The standard does not specify what level is required by any particular application.

- Level 1 imposes very limited requirements; all components must be "production-grade" and obvious security functions must be present. Level 1 restricts the machine on which the module runs to operating in single-user mode.
- Level 2 adds requirements for physical tamper-evidence and role-based authentication. It is noticeably harder to obtain. The difficulty is not necessarily with the cryptographic module code, but rather with the formalities required and the fact that Level 2 modules must run on validated hardware under validated operating systems.
- Level 3 adds requirements for physical tamper-resistance and identity-based authentication. Level 3 also requires physical or logical separation between the interfaces by which certain security parameters enter and leave the module.
- Level 4 imposes much more onerous physical security requirements and requires more robust security features to defend against various environmental attacks.

Cryptographic modules receive security level ratings that reflect the requirements they meet. Most smart cards (secure IC plus OS plus application software) that are certified by FIPS 140-2 are certified to either Level 2 or Level 3. These certifications are granted according to the Cryptographic Module Validation Program (CMVP), a joint American and Canadian security accreditation program for evaluating and certifying cryptographic modules. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

FIPS 140-3 is the proposed revision to FIPS 140-2. The draft specifies five security levels instead of four, provides a separate section for software security, requires mitigation of non-invasive attacks when validating at higher security levels, introduces the concept of public security parameters, allows certain self-tests to be deferred until specific conditions are met, and strengthens the requirements for user authentication and integrity testing. The additional security level specified by FIPS 140-3 incorporates extended and new security features that reflect recent advances in technology.[16]

7.3 ISO/IEC 15408—Common Criteria

Common Criteria (CC) is an internationally approved security evaluation framework providing a clear and reliable evaluation of the security capabilities of IT products, including secure ICs, smart card operating systems, and application software. CC provides an independent assessment of a product's ability to meet security standards, with the goal of giving customers confidence in the security of IT products and leading to better decisions about security. Security-conscious customers, such as national governments, are increasingly requiring CC certification in making purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings.

CC has been adopted and is recognized by 14 countries, which allows customers in any of these countries to purchase products with the same level of confidence. Evaluating a product with respect to

[16] For more information on FIPS 140-2, FIPS 140-3, and the CMVP, see http://csrc.nist.gov/groups/STM/index.html.

security requires identification of the customer's security needs and an assessment of the capabilities of the product. CC helps customers complete both of these processes using two key tools: protection profiles and evaluation assurance levels.

7.3.1 Protection Profiles

A protection profile defines a standard set of security requirements for a specific type of product. Protection profiles are the basis for the CC evaluation. By listing required security features for specific product families, CC enables products to achieve conformity to a relevant protection profile. During CC evaluation, each product is tested against a specific protection profile, providing reliable verification of the security capabilities of the product.

For smart cards, the protection profile covers secure ICs, smart card operating systems, and application software. These components can be evaluated as separate entities or combined into a secure smart card. More than 25 protection profiles for secure ICs, smart card operating systems, application software, and other smart card related devices and systems are listed on the CC portal.[17] Customers can compile a list of critical security features by examining the details of the relevant protection profiles. The CC certification verifies that a product meets the requirements of that protection profile. Using a CC certification, customers can rapidly assess a product's ability to meet their security needs and compare the security capabilities of different validated products.

The most popular protection profile for secure ICs is the Security IC Platform Protection Profile Version 1.0, known as CC-PP-0035-2007. This protection profile is established by Eurosmart and the smart card IC industry and is an update of the Smartcard IC Platform Protection Profile CC-PP-0002-2001.[18] Both contact and contactless smart cards use this protection profile.

Multi-application smart card operating systems also use CC for security evaluations. For example, the Java Card Protection Profile is available as a collection of four separate protection profiles. One profile defines a set of security requirements for the Java Card Runtime Environment, another the Java Card Virtual Machine, a third the Java Card API Framework, and the fourth the on-card installer components. The profile provides guidelines for developing a secure Java Card platform and defines a security target that must be met to obtain high-level security certifications. The Java Card Protection Profile is intended to complement other protection profiles currently available for smart cards based on Java Card technology.[19]

In the past, MULTOS implementations have been evaluated against the Smart Card Security User Group (SCSUG) Smart Card Protection Profile v2.0.[20]

Proprietary operating systems are usually evaluated against a specific protection profile in conjunction with a specific application. For example, the CC portal lists protection profiles for healthcare cards, ePassports, contactless cards, and electronic purses.

7.3.2 Evaluation Assurance Levels

An evaluation assurance level (EAL) measures the depth of engineering review and evaluation of the product lifecycle. Unlike a protection profile, the EAL does not indicate the actual security capabilities of the product but independently stipulates the level of evidence reviewed and tested against the vendor's claims. Figure 7 shows the seven CC EALs (EAL1–EAL7) and the level of testing required to achieve the different levels. Vendors can choose an EAL.

[17] http://www.commoncriteriaportal.org/pp_IC.html#IC
[18] http://www.commoncriteriaportal.org/files/ppfiles/pp0035a.pdf
[19] http://java.sun.com/javacard/pp.html
[20] http://www.multos.com/downloads/marketing/Whitepaper_MULTOS_Security.pdf

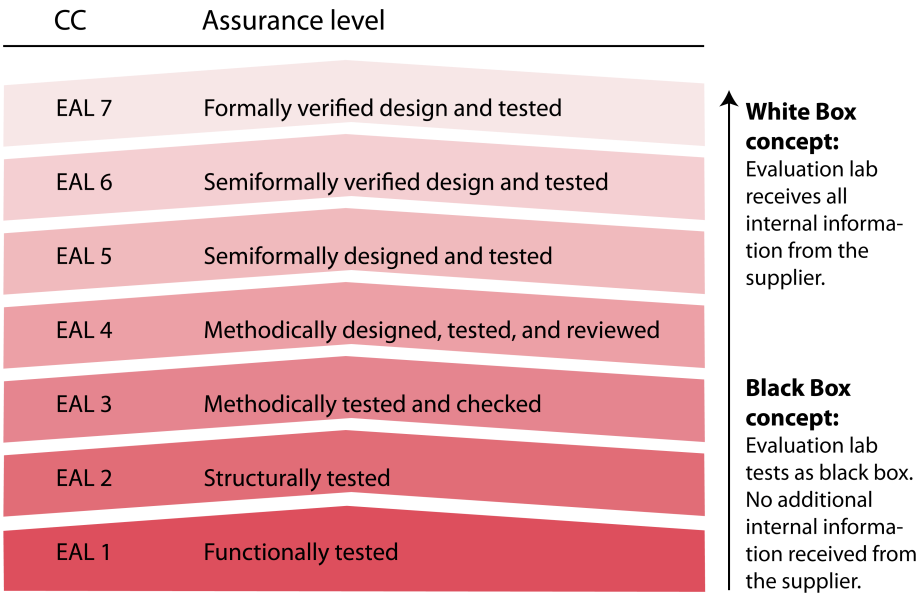

Figure 8. Common Criteria Evaluation Assurance Levels

7.3.3 Certification Process

The purpose of product certification is to provide customers with a high level of trust, which requires a thorough, reliable, objective, and globally accepted process. To submit a product for certification, the vendor must first specify a security target (ST). The ST description includes an overview of the product, potential security threats, detailed information on the implementation of all security features included in the product, and any claims of conformity against a protection profile at a specified EAL. The vendor must submit the ST to an accredited testing laboratory for evaluation. The laboratory then tests the product to verify the described security features and evaluate the product against the specified protection profile. A successful evaluation results in official certification of the product against a specific protection profile at a specific EAL. Most smart card components are currently certified to EAL 4+ and are moving to EAL 5+, as indicated in the CC portal.[21]

7.3.4 FIPS 140-2 Compared to Common Criteria

The FIPS 140 standard was initially developed in 1994, before the development of CC and with a different goal. FIPS 140-2 evaluates a defined cryptographic module and provides a suite of conformance tests with up to four security levels to determine whether the module meets certain security requirements. FIPS 140-2 prescribes basic requirements for cryptographic modules, including requirements in areas such as physical security, key management, self tests, and roles and services. A FIPS140-2 certification/evaluation applies only to the finshed cryptographic module and does not allow a composite approach on the various pieces comprising the module (such as hardware/IC, operating system, and applet).

CC evaluates a security target against an industry-defined protection profile. A protection profile typically applies to a broad range of products, while FIPS 140-2 certification applies to only a single product. A CC evaluation does not supersede or replace FIPS 140-2 validation. The four security levels in FIPS 140-2 do not map directly to specific CC EALs or to CC functional requirements. A CC certificate cannot be substituted for a FIPS 140-1, FIPS 140-2, or FIPS 140-3 certificate. CC has been designed/planned to use composite evaluations, as described in Section 7.1.

[21] For an overview of the portal, see http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf. For an introduction and general model, see http://www.commoncriteria.org/docs/pdf/CCPART1V21.PDF

7.4 Industry Evaluations of Security and Applications

Different industries have additional requirements for testing and certifying smart card products, either at the security or application level or both. Two examples are discussed in this section – FIPS 201 evaluation which is use by the U.S. Federal government and the payments industry's evaluation.

7.4.1 FIPS 201 for Application Software

Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, mandated the establishment of a standard for identification of Federal government employees and contractors. HSPD-12 requires the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems.

The Department of Commerce and the National Institute of Standards and Technology (NIST) were tasked with producing a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, initially issued on February 25, 2005 and updated to FIPS 201-1 in March 2006. The FIPS 201 PIV card is a dual-interface smart card that is to be used for both physical and logical access control and other applications as determined by the individual agencies.

FIPS 201 consists of two parts: PIV I and PIV II. The standards in PIV I support the objectives for identity assurance and requirements for determining trustworthiness described in HSPD-12. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II also specifies standards for implementing identity credentials on IC cards (i.e., smart cards) for use in a Federal PIV system.

All cryptographic functions on a FIPS 201 PIV card must be evaluated and certified under the FIPS 140-2 and FIPS 140-3 specifications.

In addition, NIST has established the NIST Personal Identity Verification Program (NPIVP)[22] to validate the PIV components required by FIPS 201. The two objectives of the NPIVP program are

1. To validate the compliance/conformance of two PIV components, PIV middleware and PIV card application, with the specifications in NIST SP 800-73-1 *Interfaces for Personal Identity Verification*.
2. To provide assurance that the set of PIV middleware and PIV card applications that have been validated by NPIVP are interoperable

The General Services Administration (GSA) has also established the FIPS 201 Evaluation Program[23] to evaluate products and services offered for use in HSPD-12 and to ensure that products and services are compliant with established FIPS 201 requirements. Products or services that are evaluated and comply with FIPS 201 specifications are added to the GSA Approved FIPS 201 Products and Services List.[24]

7.4.2 Financial Payment Industry: EMVCo Security Evaluations

In the past, individual payment brands had been solely responsible for defining security requirements and establishing evaluation procedures for secure ICs and for smart cards (also known as integrated circuit cards (ICCs)). Beginning in 2007, the EMVCo[25] Security Evaluation Working Group (SEWG)

[22] http://csrc.nist.gov/groups/SNS/piv/npivp/index.html
[23] http://fips201ep.cio.gov/
[24] http://fips201ep.cio.gov/apl.php
[25] EMVCo LLC was formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002 and with JCB joining the

assumed responsibility for evaluating all EMV-based contact smart card ICs. In 2008, this responsibility was extended to contactless smart card ICs as well. In addition, the SEWG is responsible for evaluating the security of any implementations of the EMVCo Common Payment Application (CPA). The individual payment brands (American Express, Discover, JCB, MasterCard, Visa) still maintain responsibility for evaluating the security of their individual payment applications, regardless of whether these applications are contact or contactless.

The primary objective of the EMVCo security evaluation process is to ensure that ICs and CPA smart cards conform to EMVCo security guidelines. The IC security evaluation includes the firmware and software routines required to access the security functions of the IC. The CPA smart card security evaluation includes the IC, the operating system, and all common payment applications that reside on the smart card.

The EMVCo Security Evaluation Secretariat is responsible for administering the EMVCo security evaluation process. By common agreement, MasterCard Worldwide performs the functions of the EMVCo Security Evaluation Secretariat, using the resources of the MasterCard Analysis Laboratory (MCAL).

The methodology used in the evaluation process leverages a program of research targeted at attack methodology. In addition, EMVCo supports the work of the International Security Certification Initiative (ISCI) and will support ongoing security initiatives under proposed Joint Interpretation Library (JIL) leadership, to maintain a common set of threats and attacks.

7.4.2.1 IC Security Evaluation

The IC security evaluation considers the security of the IC product used in the smart card and is intended to provide a high level of confidence in the security functions that are designed to deal with known attack methods (see Section 3). The EMVCo security evaluation process also takes into account the security of the design, development, and delivery processes. The IC security evaluation is performed by recognized external security evaluation laboratories and funded by the product provider.

7.4.2.2 CPA Smart Card Security Evaluation

The CPA smart card security evaluation considers the security of the product providers who develop operating systems and payment applications and evaluates how these applications and operating systems follow the relevant security guidelines. An important factor is how the product providers build upon the security of the IC and the OS to provide overall security for a payment application on the smart card.

7.4.2.3 Certification Process

The EMVCo security evaluation process has been conceived to provide a "high" level of assurance, as defined in the document *Application of Attack Potential to Smartcards*[26] for IC and CPA smart card products at all stages of the development process. At the device level, the evaluation methodology tries to balance so-called "black box" and "white box" testing. This balance is achieved by carrying out a security analysis that considers all viable attacks on a product and derives a set of penetration tests based on individual device characteristics.

Recognized external evaluation laboratories perform security evaluations using the relevant EMV Security Guidelines and externally developed testing tools. EMVCo recognizes the methodology used by some formal evaluation schemes (e.g., Common Criteria) but will only accept full evaluation reports as evidence.

---

organization in 2004, EMVCo is currently operated by JCB International, MasterCard Worldwide, and Visa, Inc.

[26] Joint Interpretation Library, "Application of Attack Potential to Smartcard," version 2.5, November 2007, http://www.ssi.gouv.fr/site_documents/JIL/JIL-Application-of-Attack-Potential-to-Smartcards-V2-5.pdf

The output from the EMVCo security evaluation process is an EMVCo Compliance Certificate which includes:

- A number that identifies a single approval path from product provider through manufacturer to issuer
- A date that reflects the status of the EMVCo security guidelines at the time of evaluation

Product providers must present their EMVCo Compliance Certificate number to issuers as proof that their product has been evaluated by the EMVCo security evaluation process.[27]

7.4.3 Financial Payment Industry: Other Product Security Evaluations

In addition to EMVCo security evalutions for EMV credit and debit cards, the different international payment brands (American Express, Discover, JCB, MasterCard and Visa) have specific security evaluations for their unique payment applications for both magnetic stripe cards and smart cards.

In addition to these international payment brand credit and debit cards, certain countries have proprietary debit and stored value payment cards. Typically, the issuers of these cards will require a CC security evaluation prior to card issuance.

7.5 Operating System Evaluation

In addition to IC and application level evaluation and certification, card operating systems are also evaluated.

Most of the major card manufacturers have developed proprietary operating systems that have been certified to Common Criteria and/or FIPS 140-2. In addition to proprietary operating systems, both Java Card and MULTOS offer security evaluation resources.

The Java Card Protection Profile[28] is available as a collection of four protection profiles. A profile defines a set of security requirements for the Java Card runtime environment, the Java Card virtual machine, the Java Card API framework, and the on-card installer components. The profile provides guidelines to develop a secure Java Card platform and define a security target in order to obtain high-level security certifications. The Java Card Protection Profile is intended to complement existing protection profiles available for Java Card technology-based smart cards.

MULTOS has a standard security assurance target which all implementations of the MULTOS operating system must be evaluated against.[29] Specific implementations have been given an ITSEC E6 accreditation (EAL 7 Common Criteria) by the UK and Australian Governments.

7.6 Comparison of Security Evaluations

Table 1 summarizes the types of security evaluations described in this document and corresponding certifications.

[27] A list of approved ICs can be found at http://www.emvco.com/securityevaluation.asp?show=97.
[28] http://java.sun.com/javacard/pp.html
[29] http://www.multos.com/downloads/marketing/Whitepaper_MULTOS_Security.pdf

Table 1. Currently Available Security Evaluations and Certifications

	Integrated Circuit Evaluation	Operating System Evaluation	Operating System and Application Evaluation	Notes
FIPS 140-2 / FIPS 140-3	✓	✓	✓	U.S. government standards; applies to cryptographic module only
FIPS 201			✓	U.S government standard
ISO/IEC 15408 Common Criteria	✓	✓	✓	Cross industry
EMVCo	✓		✓	Payments industry
Payment Brands			✓	Payments industry

8. Conclusions

Security is a core element of any payment and identity system; a properly-designed system is not dependent on the security of any single component. No single security mechanism provides complete security and, indeed, complete security does not exist. The objective in any secure system design must be to implement the appropriate security measures to address the expected risks and threats to the system.

Smart card technology is a critical element in most secure payment and identity system designs worldwide, enabling organizations to provide citizens, consumers and employees with a secure, portable device that protects personal information and enables secure, authenticated transactions.

Smart card technology provides security benefits at a number of levels. The secure microcontrollers used in smart cards have security features manufactured into the ICs that thwart attackers from accessing any sensitive information that is stored in the card. The secure microcontroller also enables the smart card to interact intelligently with the reader and the system, implementing cryptographic functions that authenticate the card and cardholder to the system and the reader and system to the card. With contact and contactless interfaces, increasingly powerful processors, wide range of memory options, and flexible implementation of both symmetric and asymmetric cryptographic algorithms, smart card technology is a critical component in the chain of trust in a secure system design. Organizations implementing smart card-based systems can also look to a number of industries for best practices in system design and for resources for evaluating and certifying the security of smart card products.

By placing a secure smart card in the hands of the user, organizations can implement a layered security architecture that addresses the expected risk of security breaches and implements an end-to-end chain of trust.

9. References and Resources

1. "Application of Attack Potential to Smartcard," version 2.5, Joint Interpretation Library, November 2007, http://www.ssi.gouv.fr/site_documents/JIL/JIL-Application-of-Attack-Potential-to-Smartcards-V2-5.pdf
2. Common Criteria portal, http://www.commoncriteriaportal.org/
3. *Contactless Payments: Frequently Asked Questions*, Smart Card Alliance Contactless Payments Council, February 2007, http://www.smartcardalliance.org/pages/publications-contactless-payments-faq
4. *Contactless Payments Security Q&A*, Smart Card Alliance Contactless Payments Council, December 2006, http://www.smartcardalliance.org/pages/publications-contactless-payment-security-qa
5. "Contactless Technology Security Issues, Smart Card Security," Helena Handschuh, Information Security Bulletin, Volume 9, April 2004
6. *Device Security*, Jarkko Tolvanen, University of Helsinki
7. EMVCo web site, http://www.emvco.com/
8. "Fault Attacks and Countermeasures," Martin Otto, Universitat at Paderborn, December 2004, http://deposit.ddb.de/cgi-bin/dokserv?idn=976819961&dok_var=d1&dok_ext=pdf&filename=976819961.pdf
9. GlobalPlatform web site, http://www.globalplatform.org
10. ISO/IEC-7816 and ISO/IEC-14443 interfaces:
    http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29257
    http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=28728
11. "Low Cost Attacks on Smart Cards: The Electromagnetic Side-Channel," Adam Matthews, Next Generation Security Software Ltd., http://www.ngssoftware.com/research/papers/EMA.pdf
12. National Institute of Standards and Technology Computer Security Division, http://csrc.nist.gov/
13. National Institute of Standards and Technology (NIST) publications:
    http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
    http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
14. Smart Card Alliance web site, http://www.smartcardalliance.org
15. *Smart Card Handbook*, Wolfgang Rankl and Wolfgang Effing, John Wiley & Sons, http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470856688.html
16. *Transit Payment System Security*, Smart Card Alliance Transportation Council white paper, July 2008, http://www.smartcardalliance.org/pages/publications-transit-payment-system-security
17. *The What, Who and Why of Contactless Payments*, Smart Card Alliance Contactless Payments Council, December 2006, http://www.smartcardalliance.org/pages/publications-contactless-payments-what-who-why
18. "Understanding DPA attacks and the countermeasures available to protect smart cards," Ken Warren, Cryptography Research, http://www.secureidnews.com/library/2006/01/09/understanding-dpa-attacks-and-the-countermeasures-available-to-protect-smart-cards/
19. "Understanding Secure Contactless device versus RFID tag," Eurosmart, http://www.eurosmart.com/4-Documents/PositionPapers.htm

10. Publication Acknowledgements

This report was developed by the Smart Card Alliance Contactless and Mobile Payments Council Security Work Group to provide an overview of the security features available with contactless and contact smart cards and describe the security features might apply or be important to different applications. 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 Contactless and Mobile Payments Council Security Work Group members for their contributions. Participants involved in the development of this report included: Discover Financial Services, First Data Corporation, Giesecke & Devrient, IBM, IfD Consulting, Infineon Technologies, INSIDE Contactless, JCB, NBS Technologies, NXP Semiconductors, Texas Instruments, Thales, Unisys, Venyon and ViVOtech.

Special thanks go to **Paul Legacki**, Infineon Technologies, who led the project, and to the following members of the Security Work Group who made substantial contributions to this white paper:

- **Troy Bernard**, Discover Financial Services
- **Ian Duthie**, IfD Consulting
- **Shrinath Eswarahally**, Infineon Technologies
- **Julie Krueger**, JCB
- **Paul Legacki**, Infineon Technologies
- **Cathy Medich**, Smart Card Alliance
- **Joe Pilozzi**, NXP Semiconductors
- **Rajesh Sharma**, INSIDE Contactless

Other Contactless and Mobile Payments Council and Work Group members and contributors included:

- **Patrick Comiskey**, NXP Semiconductors
- **Sunil Dewan**, Venyon
- **Gwynneth Dido**, IBM
- **Neal Goman**, NBS Technologies
- **Wendy Humphrey**, First Data Corporation
- **Mohammad Khan**, ViVOtech
- **Michael Laezza**, Thales
- **Tim Ostrem**, NBS Technologies
- **Joseph Pearson**, Texas Instruments
- **Ron Pinkus**, Giesecke & Devrient
- **Neil Ringwood**, IBM
- **Denis Scheller**, NXP Semiconductors
- **Ron Stephenson**, NBS Technologies
- **Jan van der Sluis**, Unisys
- **Charles Walton**, INSIDE Contactless

The Smart Card Alliance would also like to thank **IfD Consulting**, **Infineon Technologies** and **NXP Semiconductors** for contributing graphics for the white paper.

About the Smart Card Alliance Contactless and Mobile Payments Council

The Contactless and Mobile Payments Council is one of several Smart Card Alliance technology and industry councils. The Council was formed to focus on facilitating the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers. The group is bringing together financial payments industry leaders, merchants and suppliers. The Council's primary goal is to inform and educate the market about the value of contactless and mobile payment and work to address misconceptions about the capabilities and security of contactless technology. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Trademark Notice

10. Appendix: Glossary of Terms

AES
Advanced Encryption Standard (AES), also known as Rijndael. A block cipher adopted as an encryption standard by the U.S. government.

Asymmetric keys
Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Asymmetric cryptography
Cryptography that uses two related operations: a public operation defined by public numbers or by a public key and a private operation defined by private numbers or by a private key (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation).

Attacks
Techniques implemented to compromise the security of a smart card IC by discovering what information it holds.

Biometric
A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Chip
Electronic component that performs logic, processing and/or memory functions.

Common Criteria (CC)
An internationally approved security evaluation framework that provides a clear and reliable evaluation of the security capabilities of IT products, including secure ICs, smart card operating systems, and application software.

Contact smart card
A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader. (See ISO/IEC 7816.)

Contactless smart card
A smart card that communicates with a reader through a radio frequency interface.

DDA
Dynamic data authentication. One technique used by the EMV specification to determine that an EMV credit or debit card is authentic.

DES
Data Encryption Standard. A method for encrypting information. (See related term Triple DES.)

DPA
Differential power analysis. A class of attacks that extracts secret information from smart cards through power consumption analysis.

Dual-interface card
A smart card that has a single smart card chip with two interfaces – a contact and a contactless interface – using shared memory and chip resources.

ECC
Elliptic Curve Cryptography

EMV
Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

EMVCo
The organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002 and with JCB joining the organization in 2004, EMVCo is currently operated by JCB International, MasterCard Worldwide, and Visa, Inc.

Encryption
The process of translating information into a code that can only be read if the reader has access to the key that was used to encrypt it. There are two main types of encryption – asymmetric (or public key) and symmetric (or secret key).

ePassport
A travel document that contains an integrated circuit chip based on international standard ISO/IEC 14443 and that can securely store and communicate the ePassport holder's personal information to authorized reading devices.

Fault attack
An attack that alters the IC's internal workings to induce an error in the operation of the IC.

EPROM
Erasable programmable read-only memory. A type of memory that can only be changed once.

EEPROM
Electrically erasable programmable read-only memory. A type of memory that can be changed up to 100,000 times.

Evaluation assurance level (EAL)
A measure used with Common Criteria for the depth of engineering review and evaluation of the product lifecycle.

Federal Information Processing Standard (FIPS)
A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS publication covers some topic in information technology to achieve a minimum level of quality or interoperability.

Ferroelectric random access memory (FRAM)
A type of fast, low power memory technology that uses the material to hold and change polarity for data storage over 100 trillion times.

FIPS 140-2 / FIPS 140-3
Security Requirements for Cryptographic Modules. The U.S. government security standard for cryptographic modules.

FIPS 201
Federal Information Processing Standard Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. FIPS 201 is the standard that defines the identity vetting, enrollment, and issuance requirements for a common government identity credential and the technical specifications for a U.S. government Executive Branch employee and contractor ID card—the PIV card.

Flash memory
A type of EEPROM that is erased and programmed in large blocks.

Hybrid card
A smart card that contains two smart card chips – both contact and contactless chips – that are not interconnected.

IEC
International Electrotechnical Commission.

Integrated circuit
Electronic component designed to perform processing and/or memory functions. See also chip.

ISO
International Organization for Standardization

ISO/IEC 7816
International standard for integrated circuit cards (i.e., smart cards) with contacts as well as the command set for all smart cards.

ISO/IEC 14443
ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards." The international standard for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz.

Invasive attacks
Attacks that use intrusive means to access the information on the IC. Also known as hardware attacks.

Key
In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.

Microcontroller (MCU)
A highly integrated computer chip that contains all the components comprising a controller. Typically this includes a CPU, RAM, some form of ROM, I/O ports, and timers.

Multi-application card
A smart card that runs multiple applications – for example, physical access, logical access, data storage and electronic purse – using a single card.

NFC – Near Field Communication
A short-range wireless standard (ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they are brought close together (within 10-20 centimeters or 4-8 inches). NFC technology is compatible with ISO/IEC 14443-based technology.

NIST
National Institute of Standards and Technology.

Non-volatile memory
Memory that holds data even after its power source is removed.

PIN
Personal identification number. A numeric code that is associated with an ID card and that adds a second factor of authentication to the identity verification process.

PIV card (**Personal identity verification card**)
The dual-interface smart card that is being issued to all Executive Branch Federal employees and contractors and that will be used for both physical and logical access.

Protection profile
A standard set of security requirements for a specific type of product that is used for the CC evaluation.

RAM
Random access memory. Computer memory that can be read from and written to in arbitrary sequence and that requires power to retain its data.

Reader
Any device that communicates information or assists in communications from a card, token, or other device and transmits the information to a host such as a control panel/processor or database for further action.

ROM
Read-only memory

RSA
Public/private key encryption technology that uses an algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman and that is owned and licensed by RSA Security.

SDA
Static data authentication. One technique used by the EMV specifications to determine that an EMV credit or debit card is authentic.

Side-channel attacks
Attacks based on information gained from the physical implementation of a cryptosystem.

Smart card
A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure 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 securely 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, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens.

SPA
Simple power analysis. A class of attacks that extracts secret information from smart cards through power consumption analysis.

Symmetric cryptography
Cryptography using the same secret key for both the originator's and the recipient's operation. (Without the secret key, it is computationally infeasible to compute either operation.)

Symmetric keys
Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).

Triple DES (or 3DES)
A block cipher formed from the Data Encryption Standard (DES) cipher by using it three times.