



KEY MANAGEMENT: A VITAL ELEMENT TO A CONTACTLESS SMART CARD SYSTEM

The use of cryptography is now widespread in the technological world of smart cards and contactless or wireless security products. Large digital numbers called keys, along with cryptographic algorithms, are employed to provide secrecy and to protect the information stored on smart cards. Most contactless smart card communications are secured by a symmetric key system, in which both communicators must share a common secret (a key) as well as a common cryptographic algorithm in order to make the communication successful.

Digital Communication

A contactless smart card system can be viewed as a digital communication channel between a contactless smart card and a terminal. A contactless reader provides the translation between the RF link and the card and between the hardwired link and the terminal. These two digital links must be bidirectional to enable mutual authentication between the communicators (who must prove to each other that they all know the common secret – the key). In some cases, the contactless reader can also act as the terminal and make all the decisions locally. No one-way communication link can provide cryptographic security. For example, Wiegand is a one-way communication protocol widely used between card readers and terminals, but cannot be used to provide true security for smart card communication systems. With the exception of legacy installations/upgrades, new projects should be designed with serial or other two-way communication protocols to maximize security and system integrity.

Benefits of Cryptography

Mutual authentication between the smart card and the terminal allows communicators to positively identify each other. Pseudo random sequence generators, unique identification numbers and one-way hash functions are used in this process, along with an authentication key to prevent repeat attacks and illicit duplications of a communicator. After a successful mutual authentication, the communication between the card and the terminal is allowed. The privacy of that communication can be ensured through encryption/decryption of the data. A cipher like DES (Data Encryption Standard) or AES (Advanced Encryption Standard) and an encryption key are paired to protect the secrecy of the communication. Cryptography helps to ensure integrity and non-repudiation within a smart card system through the computation of MACs (Message Authentication Codes) accompanying the data exchanged between the communicators. Authentication keys, encryption keys, integrity keys and nonrepudiation keys are secret numbers used to protect the smart card communication system. Each type of key protects the system against various potential attacks and frauds and should therefore be managed with great care.

Using “Keys”

Keys protect a smart card system – algorithms do not. It should never be assumed that an algorithm will remain secret for a significant period of time. In fact, an algorithm that has been widely scrutinized and approved by the private and governmental scientific communities provides more strength than a secret algorithm. Most smart card systems can be used in a plugandplay fashion. Cards, readers and terminals are often factory programmed with default keys. In the real world, most systems are never updated after initial installation and operate using the same default keys. Upgrading system security by replacing default keys with truly secure keys can be inconvenient, but it should be assumed that factory default keys will eventually become known and hence compromise the security of the systems they are meant to protect. It is important to utilize the full capability of a smart card system by protecting it with secret keys.

continued

Smart card systems can be in use for years at a time. Partial information can slowly leak out of the system as cards are lost or stolen or as communications are illicitly monitored. Therefore, regularly updating keys may be beneficial to a smart card system. Keys should be difficult to remember, securely stored and frequently backed-up. Keys should look random and should not be considered weak. For example, a 56-bit key made of all zeros is very weak when used with DES. Other weak keys include those chosen from a narrow or reduced key set (such as lowercase letters in place of random 8-bit ASCII characters). Other reduced key spaces include English language phrases, dates, names and any other non-random selections. To demonstrate the weakness of a reduced key space, consider the following example: In the case of DES (or any 7-byte key algorithm), a key made of lowercase letters is 9 Million $((256/26)^7)$ times weaker than a key composed of 7 random bytes. Therefore, a brute force attack (also called an “exhaustive search”), that averages 100 years in duration, could take place in less than 6 minutes on a reduced key space made of lowercase letters. The best possible algorithms should be chosen to ensure system security. For instance, if a system offers a choice between DES and AES, the latter should be chosen without hesitation. If a smart card system is advertised to be secure, that claim should be supported with a solid study of its cryptographic algorithms (unless those algorithms are public and already well studied). Customers will feel comfortable using a system with algorithms that are known to be strong because the overall security of the system can be controlled by simply protecting system keys.

Design of the smart card system

A well-designed smart card system includes robust, upgradeable and flexible architecture and non-proprietary design features that are based on existing standards easily understood by the public. The robustness of a system is achieved through the responsible use of well-studied cryptographic techniques and algorithms. Optimal results occur when all parties involved in the design and integration of a system work openly together in the common interest of providing security. Disgruntled parties can easily introduce splits or vulnerabilities in the security of a system. For example, an angry firmware contractor could introduce a ‘Trojan Horse’ in the design to illicitly compromise the security of a system. The system should offer flexibility and upgradeability. A reader should be designed to communicate with various types of standardized terminals. Smart cards and readers should strictly adhere to communication standards in order to facilitate compatibility with future products and promote openness. Once again, the parties involved in the design of the system should be carefully selected and share the common goal of optimal security.

XceedID™, XACT™ and ISO-X™ are trademarks of XceedID Corporation. GE®, CASI® and ProxLite® are registered trademarks of General Electric Corporation. MIFARE®, I-Code® and DESFire® are registered trademarks of Philips Electronics, Inc. HID® and iCLASS® are registered trademarks of HID Corporation. my-d® and Infineon® are registered trademarks of Infineon. Other product names mentioned herein may be trademarks and / or registered trademarks of other companies.