Global Information Assurance Certification Paper

OPERATIONAL ISSUES FACED IN KEYMANAGEMENT FOR MULTINATIONAL EFT NETWORKS

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Tibor Laczko
Location: Munich Germany
Submitted on: September 13, 2004

Table of Contents

Abstract

The wide usages of Electronic Founds Transfer (EFT) network are on the rise given the demanding customer need for fast and secure access to their cash. An EFT network creates a secure channel between an Automated Teller Machine (ATM) or Point Of Sale (POS) terminal, the processing host and the issuing bank and protects this channel via cryptographic controls. This paper discusses the historical evolution of EFT networks and the protection methods used. The cryptographic key, being the bastion of the defense for the host, is further discussed. Keeping secrecy in a centralized operation is challenging enough. However, when we have to implement security solutions for numerous countries with different infrastructure, local regulations, and country specific traditional issues, even well skilled security professionals find challenges. This paper explores these operational issues and provides recommendations on the technical, physical, personnel/administrative and business issues that must work together to ensure holistic integrity of the key management network. Finally, this paper discusses the future trends in key management solutions such as remote key management and dynamic key exchange.

Introduction

Every day around the world, hundreds of millions of customers use their bank ATM and credit cards to access their accounts. The average banking customer places a blind trust in the fact that all of their financial information remains private and secure. It is the role of security professionals in the Electronic Funds Transfer (EFT) industry to make sure their trust is not compromised. Banks, merchants and retail customers rely on the integrity of the security infrastructure surrounding the industry to keep their financial lifeblood pumping.

Let us look at a small example of the extent of the financial flows going through just one industry player. According to www.atmmarketplace.com in 2003, Bank of America had an ATM fleet containing 12,000 machines. The same research paper discovered that 57% of ATM activity is cash withdrawals. Now let's assume that one ATM process only 100 transactions a day. Fifthy-seven percent of those would result in 57 pieces of cash withdrawals. If the withdrawal amount is 100 US on all the 12,000 ATMs, it will result in a **68,400.000** US dollar cash circulation daily. On a month average, the volume would be over 2 billion US dollars.

This enormous volume of financial transactions that pass through financial networks provides customers with a safe and secure way to access their money and requires special attention from security professionals. This volume of data and money also attracts criminal elements that are highly interested in using this information for their own financial gain. One of the main goals of an EFT network is to keep customers' Personal Identification Number (PIN) secure from internal and external attacks at the ATM site and throughout the entire system. Besides different protection methods, such as application specific terminal identification, cryptography is used.

This paper will address the case of operational issues faced in key management for multinational EFT networks. First, this paper will review the basics environment of EFT networks and their historical progression. After a short history of ATM networks, the paper will detail the applied cryptography that is used in the industry and the importance of the cryptographic key. In order to fully understand the operational challenges facing a security professional working in an EFT network, first one must comprehend steps of the key lifecycle. After reviewing this information, this paper will explore the operational issues that can occur when this cycle has to cover different countries, possibly on different continents. Finally, this paper will seek to discuss the future trends in key management technology.

The Evolution of Electronic Funds Transfer Networks

First of all, we should clarify what Electronic Funds Transfer (EFT) means. According to Dictionary.com, Electronic Funds Transfer is:

> "Transfer of money initiated through electronic terminal, automated teller machine, computer, telephone, or magnetic tape. In the late 1990s, this increasingly includes transfer initiated via the World-Wide Web. The term also applies to credit card and automated bill payments."[1]

In order to gain a better understanding of the dynamic growth in EFT transactions, we need to look a bit at the evolution of these networks and their future implication in consumer spending behavior.

The first Automated Teller Machine (ATM) was introduced in the late 1960s in New York-based Chemical Bank. The machine was relatively primitive compared to today's complex ATMs, but the principle was the same. Customers with a plastic card and a corresponding Personal Identification Number (PIN) were able to initiate transactions and obtain money. In the 1960's, banks built ATM networks which accepted only proprietary cards and usually covered only local geographical areas. As laws and regulations changed and people became more familiar with this style of banking experience, the need arose to expand EFT networks, and banks agreed to share their ATM network with other banks to ensure greater global convenience for their customers.

Evidence of this increase in the global numbers of ATMs is shown in figure 1. According to Financial Services Fact Book (www.financialservicesfacts.org), the total number of ATMs in 2003 is more than twice as much is it was in 1997. Furthermore, the number of off-premise ATMs (ATMs that are not situated in local bank branches) has increased almost 25%, confronting security professionals with new challenges.

[1] Dictionray.com "Electronic founds transfer"

Figure 1. OFF-PREMISE ATM DEPLOYMENT, 1997-2003)

Year	Total ATMs	Off-premise ATMs	Percent off-premise
1997	165,000	67,000	40.6%
1998	187,000	84,000	44.9
1999	227,000	117,000	51.5
2000	273,000	156,000	57.1
2001	324,000	193,000	59.6
2002	352,000	220,100	62.5
2003	371,000	238,000	64.2

(1) ATMs located away from financial institution branches.

Source: ATM & Debit News.

As the ATM networks are developed and expanded, the number of ATMs naturally increases. Conversely, networks see a decrease in the number of transactions per ATMs as the public finds it more convenient in locating an ATM in their area. Figure 2 introduces the growth in average monthly transactions per ATM, the number of terminals and the number of ATM transactions from 1993 until 2003. Even though the average monthly transactions per ATM decreased, this is due to the fact that the numbers of terminals in 2003 were four times higher than in 1993.

The real justification for the need for tight security controls is to ensure the security and integrity of all EFT transactions and the financial value they carry. Based on the data researched at Financial Services Fact Book (www.financialservicesfacts.org) and shown on figure 2 in 2003, there were over 900 million ATM transactions in the United States alone. Considering the economical value of the volume of this information, it would naturally offer a hacker a windfall of financial opportunity. It is the goal of security professionals in the industry to make sure that all valuable transactional information does not fall into the wrong hands.

Figure 2. ATM TRANSACTIONS, 1993-2003

Year	Average monthly ATM transactions	Terminals	Total transactions (2) (millions)
1993	6,772	94,822	642.1
1994	6,459	109,080	704.5
1995	6,580	122,706	807.4
1996	6,399	139,134	890.3
1997	5,515	165,000	910.0
1998	4,973	187,000	930.0
1999	3,997	227,000	907.4
2000	3,919	273,000	1,070.0
2001	3,494	324,000	1,132.0
2002	2,509	352,000	883.2 (2)
2003	2,432	371,000	902.3 (3)

(1) June data for 1993-1998, March data for 1999-2003.
(2) Total network transactions include all deposits, withdrawals, transfers, payments, and balances inquiries performed on ATMs in the network, whether or not those transactions are switched through the network data center, as well as point of sale transactions on network terminals.
(3) Adjusted to eliminate double-counting caused by two networks reporting a transaction. After 2001, transactions are reported only by the authorizing network.

Source: ATM & Debit News.

Overview of EFT security

EFT security is the cornerstone of trust between customers and their banking institutions. EFT security is a very complex issue. In EFT, all three principles of the CIA triad (Confidentiality, Integrity, and Availability) play a crucial role. Customer card information and PIN must not be disclosed (confidentiality); the message traveling through the network must not be modified (integrity); and finally, customers and business partners mandate over 99.9% uptime (availability) from an EFT network.

Implementing defense-in-depth is extremely important in EFT networks. Logical, physical and personnel security measures have to be in place and work in concert to deliver the expected level of security.

One of the main goals of EFT security is to protect the customer PIN. The PIN travels in a specific format (pinblock) from the ATM to the host, and, if needed, to the issuer bank. Introducing cryptographic controls protects the PIN within this message.

Applied Cryptography in EFT Networks

Software vs. Hardware Based Cryptography

When a security professional designs a cryptographic system, he has to decide whether to use software or hardware-based encryption techniques. In the case of a software-based cryptographic system, all the necessary secret information such as the cryptographic key is hard-coded into an either limited or non-protected memory of the given computer, thus providing insufficient protection.

In order to fulfill the necessary security requirements set for EFT networks, the best solution is to use hardware-based encryption. Where the requirements include, but are not limited to, enforcing utmost key confidentiality, restricted cryptographic functions, separation of keys, dual control, tamper detection, it is advisable to use a certified specialized device, such as a Hardware Security Module (HSM). International card organizations' proprietary standards require a certain level of security from a HSM. FIPS PUB 140-2 Security Requirements for Cryptographic Modules introduce the design and implementation requirements of a cryptographic module. The rating can be 1-4 (lowest to highest) depending on the requirements.

After having reviewed the main hardware elements, a security professional has to choose whether to use symmetric or asymmetric cryptography. EFT networks historically use symmetric cryptosystems. It means that the same key is used for encryption and for decryption. The algorithm in use is called Data Encryption Standard (DES). DES is a publicly available algorithm. Thus, the applied key makes it secure and not the algorithm itself. DES first was published 1976 in the United States and became a Federal Information Processing Standard (FIPS). DES keys are 64 bits long with 56 bits used for encryption and 8 bits used for parity check. With the fast evolution of processing power in computers, a DES key (56 bits) can be broken in less then a day using brute force attack. As technology matures, this time frame for cracking DES keys decreases. The reason the financial industry still use DES is very simple. Moving to another known algorithm would require a total change of the current hardware and software base. To bridge this problem, they have introduced TDES where the algorithm has not changed but only the operation differs.

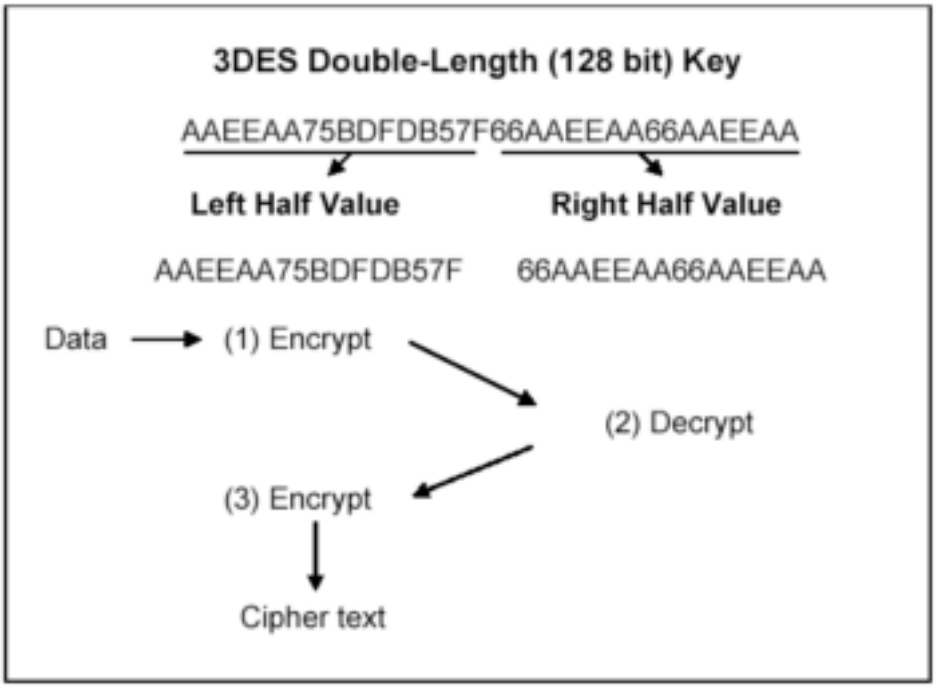
Because DES is not perfectly secure for certain areas, such as military use, the EFT community has also decided to move to a more secure solution and introduced Triple DES (TDES) as the new industry-wide standard. TDES uses a double length 128 bit DES key, which is divided into two 64 bit chunks. As for DES from the 64 bits parts, only 56 bits are used for encryption. The rest is for parity check. This results in the actual key strength of 112 bits for double length keys. The encrypting process is exactly the same as for DES, but it is repeated three times. The left chunk encrypts the data. The right chunk decrypts it. And the left chunk re-encrypts it again.

According to Edgar Danielyan, a Cisco Certified Network, Design and Security Professional: "The disadvantage of Triple DES is that it is about one-third as fast as DES when processing data. This effort just slightly extended the life of DES while a

suitable alternative could be found." [2] Until the winning solution is found, international card organizations such as Visa and MasterCard have mandated TDES for banks and processing centers as the industry wide standard.

Figure 3 from Pulse EFT shows how TDES works using double length keys.

Figure 3. TDES Key Encryption Process



http://www.pulse-eft.com/upload/EncryptionKeyWhitePaper4_2003.pdf

The Key

We have covered how key length can greatly improve the effectiveness of DES encryption. Regardless of key length, if there is no carefully designed and implemented key management solution in place, our cryptosystem faces the chance of being compromised.

In order to ensure that each and every ATM in the network is properly protected, and at the same time fulfills the requirements of international card organizations, every ATM is loaded with unique keys. For proper functioning, ATMs require two sets of cryptographic keys. It means that a network with 4000 ATMs needs 8000 keys. These keys must be securely generated, distributed, loaded, and destroyed.

The "MANTRA" Dual Control Split Knowledge

According to the National Institute of Standards and Technology (NIST) special publication 800-57 Part 1 and Part 2: General Guideline, here are the descriptions for dual control and split knowledge.

[2] Edgar Danielyan, Goodbye DES, Welcome AES

Dual control

> *"A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single entity is able to access or use the materials, e.g., cryptographic keys."*[3]

Split knowledge

> *"A procedure whereby a cryptographic key is handled as multiple key components from the time that the key or the separate key components are generated until the key components are combined for use. Each key component provides no knowledge of the ultimate key. The key may be created and then split into the key components, or may be created as separate key components The key components are output from the generating cryptographic module(s) to separate entities for individual handling, and subsequently input separately into the intended cryptographic module and combined to form the ultimate key"* [4]

This mantra follows a well-defined key management system from the beginning to the end. No single person can have access to all components of a key, and no one person can carry out sensitive functions. In the next section, the impact of the dual control/split knowledge will be more visible as we introduce each stage of a key's lifecycle.

Key lifecycle

The lifecycle of cryptographic keys includes six steps: generation, printing, storage, distribution, loading and destruction. All of these steps must have their own protection mechanism, and, when used together, they ensure the secrecy of the cryptosystem. The selected protection mechanisms might vary from organization to organization but the common goal of protecting sensitive information remains the same.

Generation

Keys used in EFT networks are generated using DES algorithm, in a random or pseudo-random process. In order to keep utmost security over the generation, the keys are generated on a Tamper Resistant Security Module (TRSM), thus minimizing the chance for the keys to be compromised. It is usually the responsibility of the Security Officer and Issuing Host to ensure proper and secure key generation. Key generation also must be compliant with EFT standards. Documentation of this process follows proprietary standards from Visa, MasterCard, and LINK, and the organization must be a member to receive these. Key generation must be performed

[3] Key Management Guideline Part 2: Best Practices for Key Management Organization p. 11
[4] Special Publication 800-57 Recommendation For Key Management Part 1: General Guideline p.21

under dual or triple control. The key generation must take place in a physically secured area such as a computer/server room. To enhance security, usually the application used for key generation is only accessible from the console of the mainframe.

Printing

The keys are printed by a dot-matrix printer into a tamper resistant paper based envelope. Each key is printed into a separate envelope. For identification purposes, the key name and a serial number is visible on the outside of the envelope. The key values are inside and only visible if the envelope is tampered with. The printer is directly connected to the console. Some of the more expensive TRSMs have direct printing capability, but international card organizations do not mandate those. It is the responsibility of the company generating the key to make sure that the key values are never shown in the system memory and that the job doesn't leave any spooled files. Detailed access control policies must be in place to control who can access the application and how. Only the designated key custodians should be able to generate keys while under the constant supervision of the security officer.

Storage

The storage media in use are mostly paper. It should be kept in mind that this key might have to travel across the continent to a local base and then to the ATM site, so using electronic storage devices might not be the best choice since the same device cannot be shared. If the cryptographic keys are to be distributed (ATM keys abroad) at a later time or until they are mailed, the left and right halves must either be placed into separate safes, or there must be dual control over the safe to ensure that no one person can access both halves of a key. A paper sign-off log is advised to keep track of all keys put in or taken out from the safe. In order to fulfill the principle of separation of duties, key custodians generating the keys cannot be the same people who are responsible for the safes.

Distribution

Transmission of keys must be conveyed or transmitted in a secure manner. An encryption key must be transferred by physically forwarding the separate key components in tamper evident packages. Each package has to travel using different courier services on different days or routes. No person should have access to the clear text of the key during the transport process. The ATM keys must remain in the tamper proof envelope until they are opened for loading at the ATM site. Upon receiving the key components, the recipients should notify the sender of the successful key delivery via e-mail or any other previously agreed communication channel.

Loading

Key loading to an ATM occurs when new ATMs are installed, taken over from one network to another, or during emergency situations where keys have to be re-entered into an ATM. ATM keys must be entered following the operating directions of the ATM manufactures in the form of at least two components using the principle of dual control and split knowledge. Key Custodians are responsible to physically safeguard the ATM key components during loading and their destruction. The key entry process must be free from monitoring or observation by unauthorized people. While loading a paper based key, the Key Custodian has to make sure that there is no visual surveillance of any kind by Closed Circuit Televisions (CCTV) or windows overlooking the ATM.

Destruction

After ATM key loading, the key components must be securely destroyed. According to international card organizations such as VISA, a secure destruction method for key components on paper consists of cross-shredding and/or burning. The key destruction process must be observed and Key Custodians must shred the key components. Finally an entry has to be created in the Key Destruction Log. In some special cases when ATM key destruction cannot take place immediately, key components must separately return to the key issuer or Third Party for secure key destruction. Dual control and split knowledge is important here as well since those keys entered are used in the production environment.

According to a company's key management policy, thorough documentation must be maintained for detailing each step of the key lifecycle. Logs and sign-off sheets must be in place in order to understand when and what happened to the keys and by whom. These logs must be continually updated and kept available for audit purposes.

While most people focus on the technical side of cryptography and the DES algorithm, there is a whole other side of cryptography that deals with the day-to-day management of keys and devices. During development and implementation of a key management system, a security professional has to face various issues. Coordination of technical, physical and personnel issues might become a complex task.

Operational Issues

Having set the basic understanding of the environment and requirements of EFT institutions to ensure that all customer financial transactions are processed in a secure manner, this paper will now seek to explore the questions concerning how security can make sure these standards are not compromised. As explained previously, any breach of these standards in day-to-day operations can lead to severe effects on the financial health of these institutions and the essential trust of their customers.

Operational issues are strongly tied to the management of the cryptographic keys and the key lifecycle. While operations at a company's central headquarters may be highly controlled and monitored, it is much harder to ensure the same level of compliance in local or regional offices. Security professionals should be aware that the further one is from the endpoint, the more chances there are for security to be compromised.

The model that will be the focus of this exploration is an international EFT network with approximately 4000 ATMs in 10 countries in Europe. Each ATM is connected to the central host through local routers. There is no PIN translation at the local offices; it is all done at the host. The key generation and printing are done at the host, and cryptographic keys are distributed to the local country operations. Once the keys are at the designated country, the local office is responsible for distributing them to the ATM site.

The challenge for a security professional is to securely generate and print the keys at the host, distribute them to the local office, and make sure that the keys reach the ATM site without tampering. Once the keys are at the ATM, they must be loaded using the principle of dual control and split knowledge. After the keys have been entered, they must be securely destroyed, and a report must be sent back to the host that the process has been completed.

EFT networks and their participating institutions must be sure to focus on four core areas which are crucial to ensuring their systems are not compromised. The four areas that can be considered fundamental operational issues of key management are the technical, physical, personnel/administrative and business requirements.

Technical

One must first clarify our definition of the technical side of operational issues. By technical, we refer only to the hardware and software requirements and support structures necessary for comprehensive key management. These devices include the HSM, the printer used for key printing, and the application used for generating the keys.

Logical access control to the Hardware Security Module (HSM)

The Host Security Module is the single most important part of a cryptographic system. The HSM performs encryption/decryption, PIN translation, key generation and many other critical functions. However, there are built-in protection mechanisms in the HSM controlling logical access to it is crucial. The security module should not be reached from a remote location but only from the management console of the machine. Sometimes even the internal network does not provide enough protection for accessing the mainframe from the LAN. Specific protection methods have to be implemented such as Secure Socket Layer (SSL) encryption between the computers on the LAN and the mainframe. There should be further restrictions such as a specific authentication to the crypto card put into place to make sure that only people

with established permissions can access the security module. Regular revision of the audit trail and the activity of the key custodians must be in place.

Redundancy/Back-up

As with all critical pieces of a system, a back-up solution must be developed and put into place. A general recommendation is that the back-up solution is situated at the company's disaster recovery site. Regular testing is required to make sure that in the event of a primary solution dysfunction or a disaster situation, the daily business functions will be able to continue.

Physical

While an EFT organization may have the technical hardware and software supporting its operations that is of the highest quality and reliability, it must ensure that its central and local facilities are designed and maintained in such a way that meet industry security standards.

Having a properly placed and configured firewall, intrusion detection/prevention systems and strict logical access control would mean little with an intruder having physical access to the server room and to the security module. That would compromise all efforts to build a secure key management system.

Central office security

The location of key generation and printing takes place has to be adequately protected. Since this is a central point of the system, the likelihood of an attack might be greater. However, we can concentrate the most effective controls here. Physical security is the step-child of information security and as such sometimes is overlooked when designing a security system. These sensitive systems are usually placed in computer rooms or processing centers. A computer room by its nature is equipped with specific security and supporting systems. Climate control, adequate power supply, UPS, diesel generator, fire detection and suppression are all required for continuous operation. At least a two-layer physical entry system must be in place, such as a biometric device and a proximity card to ensure that only authorized personnel access the premise.

No matter how well protected the central office is one has to make sure that the keys which were securely generated will remain secure even after they leave the central office and travel to the destination country.

Local office security

The local country office staff is responsible for the management of keys locally. After the keys are delivered by the courier company, storage, distribution and destruction

must be carried out / supervised by the local staff. In terms of physical security, there must be adequate protection over the local storage of the keys, and a secure channel must be used to deliver the keys to the location of the third party (Second Line Maintenance, Cash In Transit). Keys are temporarily stored at the local office. For this purpose, the local office must have a safe in which to store the keys. According to our "mantra", dual controls must be implemented here as well. There must be either two safes for storing key components separately, or if they are stored in the same safe there must be dual access control to the safe. Usually this is a physical key and a PIN which are both needed at the same time to open the safe. Of course, the safe has to be bolted into the wall or the ground to avoid theft.

As discussed earlier, a well-functioning key management system has to protect the keys from generation to destruction. There are some occasions when the control over cryptographic keys is temporarily assigned to third parties.

Third party security

One alternative is when a third party is contracted to enter keys into the ATMs. (This will be discussed in greater details in a later chapter). In this scenario, the third party has to accommodate the physical security requirements set by the organization, such as safes, sign-off sheets and the possibility of a regular security check carried out by the company.

While it is not related to physical security, here it must be emphasized that before any keying materials are handed over to third parties, a thorough risk analysis has to be carried out, and a contract has to be signed clarifying roles and responsibilities.

Now after reviewing the technical and physical issues which might possibly affect key management program, this paper will explore the biggest security risk: the human factor.

Personnel / Administrative

In the EFT industry, proper key management and entry are strongly connected to the employees hired to run these operations. A detailed key management procedure must also be provided to staff to set clear expectations and provide step-by-step instructions that can be monitored and audited.

Let us first look at the basic personnel elements that are required of all staff working in key management and involved in the key life cycle. These requirements are the same for both staff who work at a central headquarters as well as those who work in local offices.

Key custodians (background check, job description)

An important part of a key management system is the key custodians. They are responsible for any keying material through its entire lifecycle. There are designated key custodians at the host and at the local offices as well. Having a thorough background check is necessary to make sure they are trustworthy. Usually this is a part-time function only, but based on its importance, these duties and responsibilities must be included in a person's job description. Segregation of duties and conflict of interest should be taken into account when key custodians are appointed. As with all sensitive functions, job rotation is strongly advised. Back up key custodians must be appointed and trained on a regular basis as well. Background checks on key custodians must be done once per year with local police authorities.

In many cases, companies may have strongly developed training infrastructures for their central operations that cover security policies and correct practices. However, local offices or sub-contractors may not receive the appropriate level of attention or instruction. Untrained staff at the local office can pose a serious challenge to keeping the key management systems and key life cycle protected.

Staff at the local office must receive specific security awareness training. They must be fully aware of the importance of ATM key management and the consequences of non-compliance to industry standards and company policies. The training should be part of the annual corporate security awareness training, and it should be updated if there are any changes in regards to key management. The local key custodians must understand the entire process, how to store the keys locally, how to react if there is any real or suspected violation against the policy. In addition a clear reporting line should be established to the corporate security officer to ensure that any issue gets appropriate attention.

Key management policy

The key management policy defines the company's approach to the administration of cryptographic keys. The policy also contains step-by-step instructions as to how key management related tasks are expected to be carried out by the staff. It is very important to bear in mind that this document must be a "live" document and must be updated on a regular basis. It must be able to reflect to industry changes in a timely manner to make sure that the management of cryptographic keys will not result in any risk to the company.

CIT or SLM (training)

For cost-benefit considerations, sometimes Second Line Maintenance (SLM) or Cash In Transit (CIT) companies are contracted to enter keys. Both of these parties have to be present at the ATM installation for various purposes, so it seems a logical choice to have them enter the keys. This business decision sometimes can negatively affect the level of security. If a third party is contracted for key entry, it must be included in the contract, and a non-disclosure agreement has to be signed. Third party staffs also have to receive training as to how to enter keys and what are

the security considerations they must always adhere to. Finally, the company should hold the right to go and audit the process at any given time.

Business

There are cases when a security professional has to put a different hat on and think as a business person. In the worst case, he is told how to think and is placed between sometimes very tight financial constrains. We have to be able to make a business case and use concrete facts and results to be able to support our decision and win senior management's buy-in to support our idea. The following issues might become a problem between a security professional and management when they want to ensure the secure operation of our EFT network.

Cost vs. security

Unfortunately security professionals often face the problem of cost versus security. The ideal scenario usually is just too costly for senior management. There are requirements that must be implemented. One of these issues is proper key management. There are some cases where the CIT or the SLM companies do not want to enter keys. Thus, other methods must be developed. Typically, this involves local staff traveling to the ATM site which might create either overstaffing or staff shortage. To avoid this cost, too often keys are read to technicians at the ATM site over the phone or sent as a text message. In this case, not only is the key distributed via unsecured channels, but usually the same technicians enter both halves of the key. This is a typical situation when a security professional cannot settle for less. It is a security professional's duty to make sure that the keys are properly protected during the complete life cycle. A professional has to provide exact data as to what level of danger the organization faces when the ATM terminals are loaded with keys in an unsecured fashion.

Geographical considerations

Sometimes geographical challenges must be taken into account for key management. For instance, Greece with its 50 small little islands can pose a great logistical challenge. It requires careful organization that all parties are there at the same time, (CIT and SLM) and that the keys are also distributed in a secure fashion. Especially in a scenario like this, we would probably see keys read over the phone or sent as a text message.
Another geographical issue might arise with that part of these ATMs are located in little tourist villages. Often these ATMs are "winterized" for off season. Usually an ATM is placed into service and left there until it needs off-site service or it gets replaced. When these Greeks ATMs are shipped back and forth to the warehouse, they pose a possibility for breach of security. In terms of key management, we have to ensure the integrity of the keys within the ATM.

Regular key change

We have learned in the earlier sections that the secrecy of the DES cryptography relies on the secrecy of the key it is using. That brings the issue of keys being aged. Usually these keys are not the ones connecting ATMs to the host, but keys connecting two hosts or a host to the bank. International card organizations and security standards such as the British Standard (BS7799) require keys to be changed on a regular basis. This might also become a business issue to a company. If there is a processing center with over 50 host-to-host (H2H) connections, that means there are 50 keys that should be changed yearly. It involves coordination, shipping cost, and possible downtime as well. Too often companies seem to neglect this part of their key management regime.

In order to determine that the designed key management system continuously provides the required level of security, regular reviews are advised. During these reviews company standards and industry regulations should be taken into account. Most of the financial institutions and networks are required to pass periodic audits to make sure there is no significant risk to the network associated with the key management system used within.

Future trends in key management

The rapid growth of EFT networks and the incremental use of cryptography have resulted in new tools and technologies being developed. Today's procedures with all the human intervention will have to be changed in the near future. Regardless of these developments, the industry's need for adequate security will always exist. Cryptography is a fundamental part of maintaining security for electronic financial transactions, and the new progress in key management will help support this fundamental mission.

Remote key management

The sheer number of cryptographic keys used in an EFT network has naturally forced crypto-system engineers to seek other solutions. One of them is remote key management. While this new practice will relieve a heavy administrative burden from the security professional, it will trigger other technical challenges to come into the equation. To develop a secure and reliable communication protocol, a verbal communication channel from the ATM site to the central host will also be required. One of these solutions is when keys are not paired together, and they are picked randomly out of a stack at the ATM site instead of having them pre-registered at the central host. A secure communication channel must be developed to inform the central host which keys got entered at the ATM. These types of systems should ease the control over specific principles around key management such as dual control, but the energy saved there has to be put into other areas such as purchasing a new system and redesigning the company's key management system. The decision to moving forward to remote key management greatly depends on the company's business model and the level of secrecy required from the system.

Dynamic key exchange

Dynamic key exchange might not be the newest technology for EFT networks, but it has only recently own in popularity. In this scenario, the host automatically generates a new key to the ATM in predefined time intervals and sends it to the ATM encrypted with the previous key value. The exercise can be initiated even after every transaction resulting in high security over the connection. However, this solution has to have its operational procedures developed as well. Otherwise, it could result in a false sense of security. Many companies implement dynamic key exchange once the ATM is up and running. They assume that since the keys are changed so frequently the initial key is not that important after all. They use a generic initial key (0123456789ABCDEF) and change this key once the ATM operates. Based on the nature of cryptography if one knows the initial key, one can work backwards and with tapping the line, retrieve any new key getting downloaded to the ATM. Dynamic key exchange is a great tool, but it has to be used and implemented correctly. Even for dynamic key exchange, the initial key must be issued and loaded in a secure process as explained in earlier sections.

Conclusion

A carefully planned key management system is a critical aspect of today's secure EFT networks. Without a secure way of administering cryptographic keys, EFT networks would just dispense money in an unauthorized fashion, customer accounts might be compromised and debited multiple times causing great financial loss to financial institutions and customers. By implementing technical controls over these EFT networks, security professionals protect the relationship of trust between financial institutions and customers.

Purchasing and implementing state of the art cryptosystems are a great start to fighting attacks to EFT networks, but without clear operational procedures and guidelines, it will lack a holistic approach. A security professional has to walk a fine line between technology and operational effectiveness that still meets business objectives and scope.

Since only the industry can make those decisions affecting the re-engineering of security standards, infrastructures and policies, the average EFT security professional is left with the job of safeguarding their network through operational controls. This paper has stressed the need to focus on the technical, physical, personnel/administrative and business elements that define their operational approach to key management. Any compromise of a single one of these elements puts the integrity of their network in question and thus jeopardizes the bank-customer bond of trust.

Future developments in the field of key management such as remote key management and dynamic key exchange offer some benefits to EFT security professionals in terms of managing the large number of keys and the logistics

associated with the handling of these objects. However, unless they are adequately integrated into a network's operational policies and procedures, their potential benefits could be offset by the instinct of the users to see them as a holistic solution. Unless a security professional continues to think through all the possible compromise points and develops appropriate protection mechanisms, their networks might be at risk. Considering the value of financial data being processed by these networks, the financial implications of allowing this risk to be exploited would be ruinous in both dollar terms and in sacred customer trust.

References

Jim Richardson "Effective encryption key management practices" April 2003
URL:http://www.pulse-eft.com/upload/EncryptionKeyWhitePaper4_2003.pdf

KPMG "Key management policy and practice framework" January 2002
URL:http://www.ncipher.com/resources/downloads/files/white_papers/KPMG_wp.pdf

Stan Sienkiewicz "The Evolution of EFT Networks from ATMs to New On-Line Debit Payment Products" April 2002
URL: http://www.phil.frb.org/pcc/workshops/workshop8.pdf

Andrew Marshall "Applied Cryptography for Magnetic Stripe cards" 1997
URL: http://www.amarshall.com/crypt101.html

Andrew Marshall RedPay Consulting "PIN attacks on EFT networks" 28 February 2003
URL:http://www.redpay.com/White_Papers/RedpaySecurityBulletinPINAttacksOnEFTNetworks.pdf

NIST "Key Management Guidelines Part 2: Best Practices for Key Management Organization" 27 January 2003
URL: http://csrc.nist.gov/CryptoToolkit/kms/guideline-2-Jan03.pdf

NIST "Special Publication 800-57 Recommendation for key management" January 2003
URL:http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf

NIST "FIPS PUB 140-2 Security Requirements for Cryptographic Modules" 03 December 2002
URL: http://csrc.nist.gov/cryptval/140-2.htm

Financial Services Fact Book "Technology"
URL:http://www.financialservicesfacts.org/financial2/technology/atm/

Wikipedia, the free encyclopedia "Data Encryption Standard"
URL:http://en.wikipedia.org/wiki/DES

Tibor Laczko		Operational issues faced in key management for multinational EFT networks

Dictionray.com “Electronic founds transfer”
URL:http://dictionary.reference.com/search?q=electronic%20funds%20transfer

Zaxus Ltd white paper “Schemes for Electronic Funds Transfer at the Point Of Sales” 2000
URL: http://cnscenter.future.co.kr/resource/rsc-center/vendor-wp/zaxus/schemes_electronic_funds.pdf

ATM Marketplace by Staff “Remote key distribution may improve compliance rates, security” 28 Jun 2004
URL:http://www.atmmarketplace.com/futurearticles.htm?article_id=19682&pavilion=112&step=story

ATM Marketplace “Future trends / ATM Facts and Stats” 20 Aug 2003
URL:http://www.atmmarketplace.com/futurearticles.htm?article_id=16603&pavilion=112

Last Updated: April 18th, 2013

Upcoming Training

SANS CyberCon 2013	Online, VA	Apr 22, 2013 - Apr 27, 2013	Live Event
Community SANS Paris @ HSC - SEC401 - Spring	Paris, France	Apr 22, 2013 - Apr 27, 2013	Community SANS
Mentor Session - SEC 401	Minneapolis, MN	Apr 25, 2013 - Jun 27, 2013	Mentor
Community SANS SEC401 Dubai	Dubai, United Arab Emirates	Apr 27, 2013 - May 02, 2013	Community SANS
Mentor Session - TCP - SEC401	Sacramento, CA	May 01, 2013 - May 08, 2013	Mentor
SANS Security West 2013	San Diego, CA	May 07, 2013 - May 16, 2013	Live Event
Mentor Session - SEC401	Bloomington, IL	May 07, 2013 - Jun 06, 2013	Mentor
SecWest 2013 - SEC401 - Security Essentials Bootcamp Style	San Diego, CA	May 09, 2013 - May 14, 2013	vLive
SANS Brisbane 2013	Brisbane, Australia	May 13, 2013 - May 18, 2013	Live Event
SANS South Africa May 2013	Johannesburg, South Africa	May 13, 2013 - May 25, 2013	Live Event
Mentor Session - SEC 401	Greenville, SC	May 14, 2013 - Jul 16, 2013	Mentor
SANS Austin 2013	Austin, TX	May 19, 2013 - May 24, 2013	Live Event
Mentor Session - SEC401	Houston, TX	May 29, 2013 - Jul 31, 2013	Mentor
Mentor Session - SEC 401 Security Boot Camp Essentials	Alexandria, VA	May 30, 2013 - Aug 08, 2013	Mentor
Mentor Session - SEC 401	Los Angeles, CA	Jun 13, 2013 - Aug 22, 2013	Mentor
SANSFIRE 2013	Washington, DC	Jun 14, 2013 - Jun 22, 2013	Live Event
SANSFIRE 2013 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jun 17, 2013 - Jun 22, 2013	vLive
Mentor Session - SEC401	Silver Spring, MD	Jun 18, 2013 - Aug 20, 2013	Mentor
Mentor Session - SEC401	Selangor, Malaysia	Jun 24, 2013 - Jun 29, 2013	Mentor
SANS Canberra 2013	Canberra, Australia	Jul 01, 2013 - Jul 13, 2013	Live Event
SANS London Summer 2013	London, United Kingdom	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, CO	Jul 14, 2013 - Jul 20, 2013	Live Event
Community SANS Vancouver	Burnaby, BC	Jul 15, 2013 - Jul 20, 2013	Community SANS
Community SANS Augusta	Augusta, GA	Jul 16, 2013 - Jul 21, 2013	Community SANS
Mentor Session - SEC 401	Philadelphia, PA	Jul 18, 2013 - Sep 19, 2013	Mentor
Mentor Session - SEC 401	Troy, MI	Jul 18, 2013 - Aug 15, 2013	Mentor
SANS Mumbai 2013	Mumbai, India	Jul 22, 2013 - Jul 27, 2013	Live Event
Mentor Session - SEC 401	Hanover, MD	Jul 23, 2013 - Sep 24, 2013	Mentor
SANS San Francisco 2013	San Francisco, CA	Jul 29, 2013 - Aug 03, 2013	Live Event
Boston 2013 - SEC401: Security Essentials Bootcamp Style	Boston, MA	Aug 05, 2013 - Aug 10, 2013	vLive
SANS Boston 2013	Boston, MA	Aug 05, 2013 - Aug 10, 2013	Live Event