NACHA
The Electronic Payments Association®

Understanding the Value of Encryption in the ACH Network

Contributors: Juan Asenjo, *Thales e-Security*; George Bassous and Sherry Knitter, *Affirmative Technologies;* Susan Pandy, *NACHA*

This resource underscores the value of encryption as a core technology underpinning the security of the ACH Network and seeks to generate greater awareness among stakeholders over the need for robust methods to combat ubiquitous data threats and sophisticated attack scenarios. This resource introduces a discussion pertaining to encryption based on information gathered from industry experts to expand the knowledge and understanding by ACH Network participants.

What is Encryption and Why Use It?

Encryption is the process of hiding information to ensure that it is only read by its intended recipient. The process has been used for centuries to protect messages exchanged between parties. The advent of the information age has underscored the importance of encryption as a core technology to secure information exchanged across electronic means.

Encryption is characterized by two components that enable the ciphering and deciphering of information. These include the use of a mathematical formula or cycle called the algorithm, and a code or key used in conjunction with this cycle to turn the intelligible data (plain-text) into an unintelligible stream (cipher-text). Encryption can be symmetric or asymmetric depending on whether a single key or two keys are used to perform the ciphering and deciphering processes. In its simplest form, a symmetric encryption process utilizing a single key to cipher and decipher information across an exchange medium is illustrated in Figure 1 below.

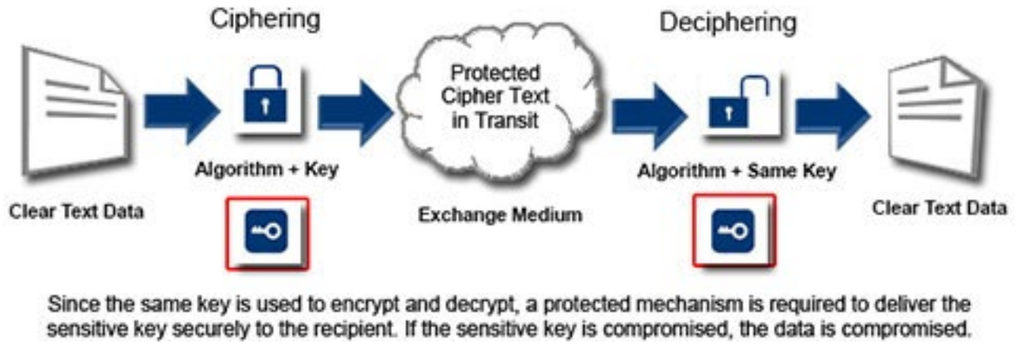

Figure 1 – Symmetric encryption utilizes a single key to cipher and decipher data

Knowledge of both the algorithm and the key are necessary to recover and transform the cipher back into intelligible information. For commercial processes, it is generally accepted that the algorithm is public knowledge, while the key is afforded a high degree of protection and only made available to the intended recipient(s).

On the other hand, asymmetric encryption — commonly referred to as public key cryptography - employs a pair of cryptographic keys instead of a single key. The key used to encrypt data is called the public key, and as the name implies, it can be made available to anyone who desires to send an encrypted message to the recipient who holds the corresponding decryption key. While the encryption key is publicly available, the decryption key or private key is always maintaned by its owner and never shared. A simplified illustration of this process is shown in the Figure 2 below.

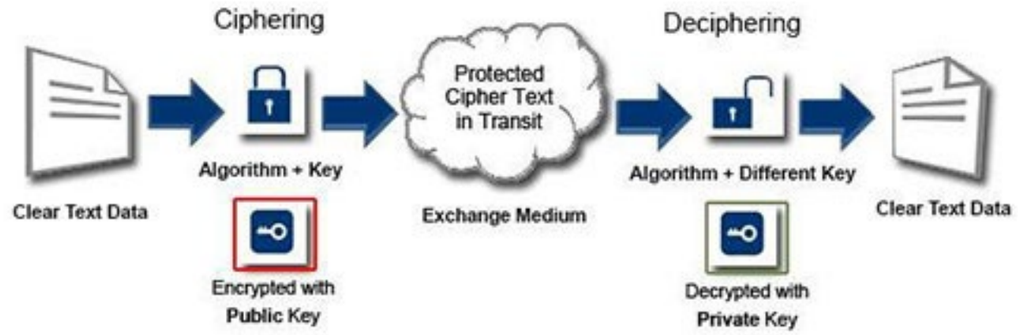

Figure 2 – Asymmetric enryption employs public key to encrypt and different private key to decrypt

Why Encrypt Data?

In the ACH Network, encryption is required for all ACH transactions that occur over Unsecured Electronic Networks using commercially reasonable technology that is at least equivalent to 128-bit RC4 encryption technology. An Unsecured Electronic Network as defined in the *NACHA Operating Rules* is a “network, public or private that (1) is not located entirely within a single, contiguous, physical facility, and (2) either (a) transmits data via circuits that are not dedicated to communication between two end-points for the duration of the communication, or (b) transmits data via wireless technology (excluding a communication that begins and ends with a wireline connection, but that is routed by a telecommunications provider for a portion of the connection over a wireless system). For clarity, the Internet is an Unsecured Electronic Network, even though secure transmissions may be made over otherwise unsecure network” (*NACHA 2012 Operating Rules & Guidelines*, OR61).

ACH Network participants that do not encrypt sensitive information and/or data expose themselves to fraud threats and data breach that can result in monetary damages, litigation, and loss of reputation.[1] Encryption is a necessary tool to protect data against malicious cyber-attacks and should form part of an organization’s overall enterprise data protection strategy. Encryption is also a requirement for compliance with a growing number of data protection and privacy regulations (state privacy laws, HIPAA, PCI, GLBA, Sarbanes-Oxley).

By understanding the role that encryption plays in the security of the ACH Network and how it protects data in its different states; whether in transit, in storage, or in use; stakeholders can gain a better appreciation for its worth as an enabling technology to protect against attacks.

How is It Used?

Within the ACH Network, transactions can be exposed to a variety of risks if not properly protected. For that reason, it is important that every participating entity in the process, from the Originator to the Receiver, be fully aware and cognizant of the vulnerabilities to which data exchanged during these transactions are exposed to, and that appropriate practices/ mechanisms to mitigate possible exploits are employed.

Figure 3 shows suggested industry practices for using encryption throughout the ACH transaction flow and among various Network participants. The practices outlined in the illustration do not represent any requirements under the *NACHA Operating Rules*. The transaction flow begins with the Originator upon obtaining consumer account data, including User IDs and authorization/authentication passwords and the illustration notes that these types of data must be protected to ensure their confidentiality and integrity. For this purpose, encryption can be employed to protect data in transit and in storage. A digital signature with time stamps (a derivative process of encryption) can also be used to ensure that transactions cannot be duplicated or replayed for fraudulent purposes.

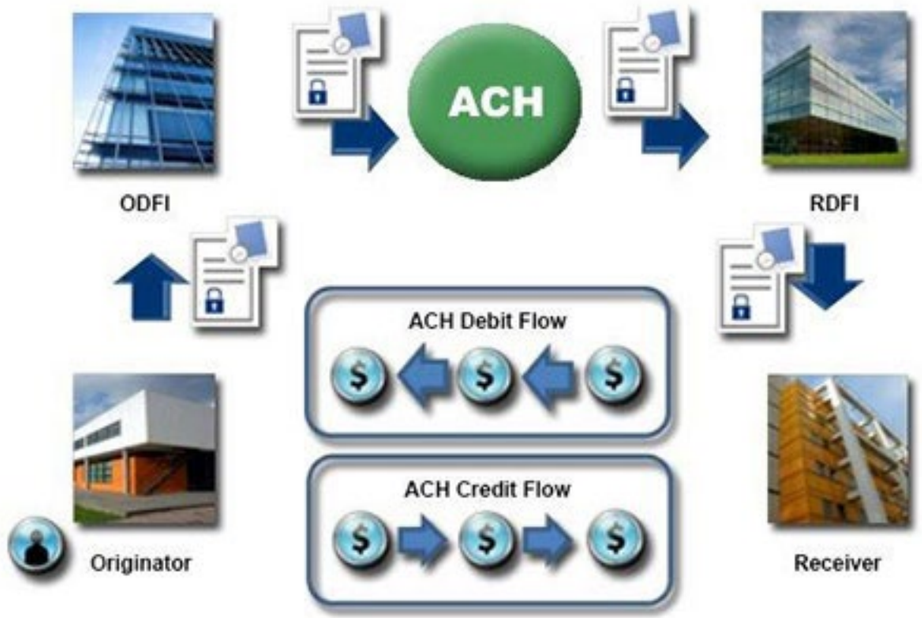

Figure 3 – ACH Network Transaction Flow and Network Participants

By using encryption mechanisms in this manner, sensitive data assets are protected, the integrity of the ACH system lifecycle is guaranteed, and proper recordkeeping can be maintained for auditing purposes.

Across the business line, typical transaction lifecycles require encryption and decryption to be performed repeatedly. As the number of encrypted segments and data assets grows, the number of encryption keys used to protect critical data such as consumer account numbers, user IDs, and passwords within these transactions can grow at an exponential rate. As shown in Figure 4, when encryption and decryption is performed at different stages of the transaction path (steps 1-7), managing the associated keys often becomes a challenge. Because encryption is only as secure as the protection afforded to the encryption keys, ensuring that these keys are always guarded and available to the authorized applications to perform the decryption process is vitally important.

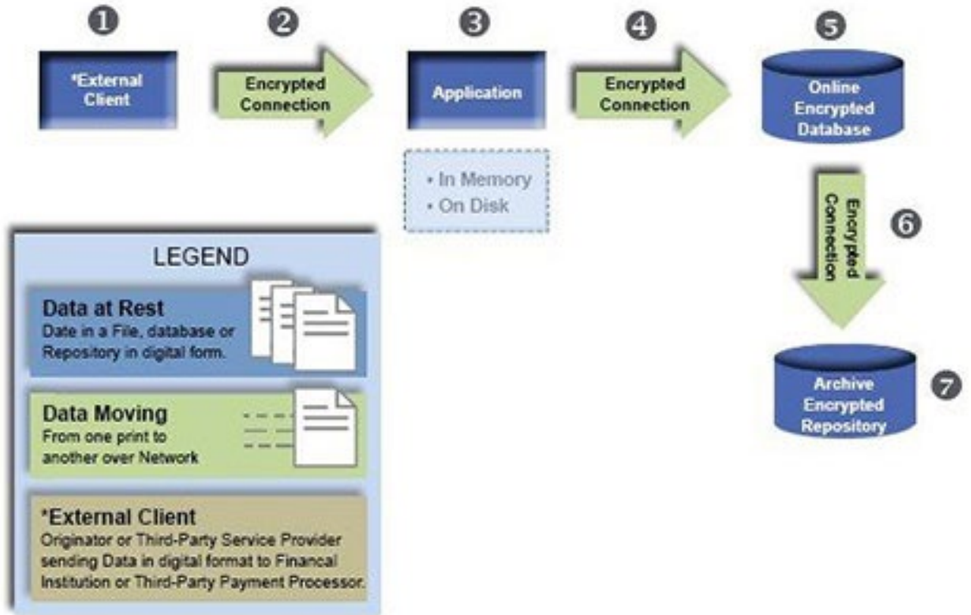

Figure 4 – Best Practices for End-to-End Encryption across Business Lines

Summary

Financial institutions, financial service providers, and corporates have a responsibility to protect the sensitive information of their clients, employees and professional partners, and the consequences of a failure to fulfill that responsibility extend far beyond the regulatory or legal penalties that may result. The short-term financial impact of fines or penalties can be significant, but the long-term financial effect resulting from a loss of consumer confidence may be far worse. A reputation hit, loss of market share and damage to a bank's brand can be as detrimental as the regulatory ramifications.[2]

Avoid those pitfalls by developing a cohesive strategy - look at what is stored, where it is stored and duration of storage, and let that structure begin to inform your strategies and solutions.

Additional Resources

1. *2012 NACHA Operating Rules & Guidelines: A Complete Guide to the Rules Governing the ACH Network.*
2. NACHA—The Electronic Payments Association. 2009. *Guidelines to Secure ACH Network Transactions.*
3. Tyson, Jeff. *How Encryption Works.* http://www.howstuffworks.com/encryption.htm
4. Data Storage Corporation. The 5 Do's and Don'ts of Choosing Data Encryption for Your Business. http://www.datastoragecorp.com/ppc/ibm/dos-donts-data-encryption/?gclid=CP_I8-OPxq0CFQXd4AodfnVHBw.
5. How-to-Geek. HTG Explains: What is Encryption and How Does It Work? http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

---

[1] Ponemon Institute. 2010 (November).*2010 Annual Study: U.S. Enterprise Encryption Trends.* Available online at: http://eval.symantec.com/mktginfo/downloads/US%20Encryption%20Trends%202010%20111510.pdf

[2] Johnson, Marc. 2012 (February). A Complete Data Security Strategy. *Bank News.* Available online at: http://www.banknews.com/Single-News-Page.51.0.html?&no_cache=1&tx_ttnews%5Bpointer%5D=5&tx_ttnews%5Btt_news%5D=16019&tx_ttnews%5BbackPid%5D=1004&cHash=53d02ab825