MAGTEK®
SECURITY FROM THE INSIDE

MagTek Response to NIST SP 800-131A
re: Two-Key TDEA Encryption

April 8, 2019

Dear MagTek Customers,

In March 2019, NIST (National Institute of Standards and Technology) released a document entitled: "***NIST Special Publication 800-131A Revision 2 – Transitioning the Use of Cryptographic Algorithms and Key Lengths***[1]". In that document, it states that the use of "Two-Key TDEA Encryption" has been listed as a "Disallowed" operational mode. This NIST document has raised concerns with our customers regarding the use of Two-Key TDEA Encryption within our products.

As a security leader, it is our intent to provide relevant information and guidance on this subject to our customers, and we can advise as follows:

At present time, "Two-Key TDEA Encryption" is currently the most widely used encryption method in the electronic payments and financial services sectors. It is used to protect both PIN and PAN payment data, and is used by most of the leading secure payment devices and payment networks deployed today.

As of this date there have been no successful attacks upon Two-Key TDEA Encryption that have resulted in the compromise of payment data encrypted under this mode. As such, Two-Key TDEA Encryption remains fully approved for use by both the ANSI X9 (American National Standards X9 - Financial Services) standards group and the PCI Security Standards Council.

MagTek customers who are currently using our products in the "Two-Key TDEA Encryption" mode can rest assured that the recent NIST announcements have no impact on security requirements within the Financial Services or Electronic Payments business sectors. As such, there is no need to make any changes to your MagTek products or encryption modes at this time.

It should be noted that the NIST recommendations only apply to Federal Agencies and their Information Systems. Commercial sector financial services are exempt from the NIST directives and are best served by following the ANSI X9 and PCI security standards organizations for recommendations on encryption requirements for payment data.

In regard to Two-Key TDEA Encryption for Transport Layer Security (TLS), PCI advised on this matter during a November 2017 blog entitled: "PCI SSC Cryptography Expert on Triple DEA[2]".

In that discussion, PCI acknowledges that the strength of Two-Key TDEA Encryption is under review and is no longer considered as "strong cryptography" by NIST. Further, PCI mentions that when NIST formally declares

Two-Key TDEA Encryption as "fully disallowed" it will no longer be considered "strong cryptography" by PCI SSC. Now that NIST has formally declared such (as of March 2019), the payment industry will need to await PCI's further guidance on this subject.

In the interim, PCI has recommended that organizations begin planning their transition towards AES-128, yet acknowledges that due to legacy considerations this transition may take place over a long period of time.

Additionally, PCI recommends the use of several mitigation techniques to reduce risk. One of those measures is to "Change TDEA keys regularly…every 256 transactions or daily, whichever is more frequent". In regard to this recommendation, MagTek can advise that our products utilize DUKPT (Derived Unique Key Per Transaction), a far more rigorous key management method. DUKPT ensures that a different key is generated for each and every transaction, taking PCI's recommendation for frequent key changes to the maximum level.

Looking ahead, both the ANSI X9 and PCI Security Standards Council are establishing standards and transition paths towards the adoption of AES-128 as the successor to TDEA for encryption of payment data.

However, due to the proven security of TDEA, legacy concerns, and logistical considerations, it is anticipated that this transition will take place over the next 4-10 years. The earliest transition milestone will be the end of PCI support for TDEA PIN encryption using fixed-key management by Jan 1, 2023.

It is important to note that this milestone does not apply to the use of TDEA PIN encryption using DUKPT (Derived Unique Key Per Transaction) key management. As such, it is very likely that there will be a long transition period where both Two-Key TDEA DUKPT and AES128 DUKPT encryption methods will be used concurrently for the foreseeable future. (See table below for upcoming security milestones.)

Security Entity	Requirement	Effective Date
VISA PCI PIN	Sunset data for SINGLE DES PIN encryption (applies to fuel dispenser environments POS only)	Oct 1, 2020
PCI PIN	FIXED Key for TDEA PIN encryption in POI devices and Host-to-Host connections is disallowed	Jan 1, 2023
PCI PIN	All hosts must support ISO PIN Block Format 4 (AES) DECRYPTION	Jan 1, 2023
PCI PIN	All hosts must support ISO PIN Block Format 4 (AES) DECRYPTION & ENCRYPTION	Jan 1, 2025

As a security leader in the electronic payments industry, MagTek is moving forward with implementation of AES-128 DUKPT into our products and security services. In the meantime, we will continue to support Two-Key TDEA DUKPT encryption in our products for however long the payments industry requests it, and/or the relevant security standards support it.

As always, MagTek will continue to keep our customers informed on these matters and provide clear guidance as new security trends and requirements emerge.

If you have any further questions, please contact your MagTek Sales Representative or me and we will be happy to answer any questions you may have.

Sincerely,

Larry Meyers
larry.meyers@magtek.com
Vice President, Qwantum Secure Media
MagTek, Inc
1710 Apollo Court
Seal Beach, CA 90740
562-546-6400

About MagTek

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission and security of cards, checks, PINs and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Its products include secure card reader/authenticators, token generators, EMV contact, contactless and NFC reading devices, encrypting check scanners, PIN pads and distributed credential personalization systems for secure magstripe and EMV enabled cards. These products are used worldwide by financial institutions, retailers, and processors to provide secure and efficient payment and identification transactions.

Today, MagTek continues to innovate. Its MagneSafe™ Security Architecture leverages strong encryption, secure tokenization, dynamic card authentication, and device/host validation enabling users to assess the trustworthiness of credentials and terminals used for online identification, payment processing, and high-value electronic transactions.

MagTek is headquartered in Seal Beach, CA. For more information, please visit www.magtek.com.

Citations

[1.] Barker, Elaine and Roginsky, Allen; March 21, 2019; NIST Special Publication (SP) 800-131A Revision 2; "Transitioning the Use of Cryptographic Algorithms and Key Lengths"

[2.] Poore, Ralph Spencer; Nov 9, 2019; PCI Security Standards; TLS/SSL and Encryption and Approved Scanning Vendors; "PCI SSC Cryptography Expert on Triple DEA"; link: https://blog.pcisecuritystandards.org/pci-ssc-cryptography-expert-on-triple-dea

###