The Critical Path from 3DES/TDEA DUKPT to AES DUKPT Encryption

DEVELOPER GUIDE: When is the right time to transition to AES DUKPT and what needs to be considered.

Initial Considerations

Understand the ever-changing risks of today's security landscape and the immediate benefits of migrating to AES DUKPT encryption and AES CMAC authentication.

Secondary Considerations

Determine what changes are required for AES DUKPT migration and how to put together a solution plan.

CONTACT US

Where hardware and services meet.

MAGTEK®

INITIAL CONSIDERATIONS

A Brief History

Since the 1970s the electronic payments and secure banking communities have strived to provide their customers with greater convenience, faster speeds, and improved security for electronic transactions. Throughout this timeline, the Open Standards Community, comprised of the International Standards Organization (ISO) and the American National Standards Institute (ANSI - X9), have led the way with the development of numerous security standards that have provided an open platform for proper implementation of accepted encryption and authentication methods. This platform was further augmented in 2007 when the PCI Security Standards council adopted these standards and provided a superset of additional guidance and requirements for PCI DSS. Collectively, the Open Standards and PCI Security Standards communities have provided a trusted foundation for guiding the global implementation of accepted security methods for Electronic Payments and Secure Banking.

Paramount amongst these security standards has been defining the use of encryption and authentication technologies for the protection of customer PINs and payment data.

TDEA ENCRYPTION WITH DUKPT KEY MANAGEMENT

Since 1998, the use of Triple DES (3DES), also known as Triple Data Encryption Algorithm (TDEA), in combination with DUKPT Key Management (Derived Unique Key Per Transaction) has been the gold-standard for protection of PINs and payment data. To its credit, the TDEA DUKPT platform continues to serve its community well and has never yet suffered a “real world” security compromise.

That said, numerous universities and security labs have conducted research and published data that suggests the security capabilities of TDEA DUKPT may soon be challenged (and surpassed) by security threats from advanced computing platforms that will brute-force calculations at ever faster speeds (e.g., quantum computers). These threats may soon provide a viable path for attackers to “crack” the TDEA DUKPT level of security. To mitigate these threats, stronger encryption and authentication methods are required.

AES DUKPT ENCRYPTION

In anticipation of increased security threats to the TDEA DUKPT platform, the Open Standards community released a new set of improved security standards in 2017 that support AES DUKPT. (Reference: ANSI X9.24-3) The AES DUKPT standards provide a pathway to improved security features that are significantly stronger and more resistant to brute-force attacks. Specifically, these standards use the AES algorithm (Advanced Encryption Standard) in conjunction with an updated DUKPT specification. AES-128 DUKPT and AES-256 DUKPT are the new standards.

AES-128 uses crypto keys that are 128-bits in length and AES-256 uses crypto keys that are 256-bits in length. Both are far more secure than the existing TDEA DUKPT implementation that uses crypto keys that provide only 112-bits of key strength.

In the world of cryptography, each additional bit represents an order-of-magnitude improvement in security. The larger AES key sizes represent a significant improvement in encryption protection from attackers. In addition, the AES algorithm itself provides numerous security improvements for faster calculation speeds and reduces the possibilities of crypto-analysis side-channel attacks.

CMAC AUTHENTICATION

In addition to stronger AES encryption, CMAC (cipher-based message authentication code) authentication enhances the security of sensitive data. In this context, CMAC authentication is the cryptographic process of validating that the encrypted sensitive data has not been manipulated or altered from its original form. The authentication process begins within the trusted hardware reader device, where prior to AES encryption, the sensitive clear-text data has a cryptographic CMAC calculation applied to it using a secret MAC key. This results in a unique 6-digit CMAC checksum that is unique to the sensitive data.

The sensitive data is then AES encrypted within the hardware reader device and the CMAC checksum is included with the encrypted data packet that is transferred to a trusted decryption host. Upon receipt at the trusted decryption host, the sensitive data is both decrypted and CMAC validated to confirm that clear-text sensitive data is still in its original form and without alteration or compromise.

Combined, the use of AES DUKPT encryption in combination with CMAC data authentication provides a powerful “one-two punch” that ensures sensitive data remains protected and intact.

Initial Decisions

Planning your Roadmap

TDEA DUKPT is in its twilight era and needs to be replaced by the more secure AES DUKPT platform. The benefits of doing so are improved security and higher confidence that financial transaction data will remain safe for now and into the future.

To stay ahead of potential threats, PCI has been encouraging the electronic payments community to begin the migration from TDEA DUKPT to AES DUKPT to protect both PIN and payment data. Although no mandates have been made, the threat landscape is expanding, and the urgency to migrate towards more secure encryption is accelerating.

What developers need to consider when creating their roadmap to AES encryption.

1. WHAT DATA DO I NEED TO PROTECT? WHAT PROTECTION SHOULD I USE?

Ideally, to meet PCI DSS requirements, it is necessary to protect sensitive PAN (Personal Account Number) payment data and/or PIN (Personal Identification Number) data so that the clear-text sensitive data is never stored, transmitted, or available within the merchant's payment systems. To do this, it is recommended to use AES DUKPT to protect this sensitive data.

2. IS THERE A REQUIREMENT TO AUTHENTICATE DATA?

No. PCI DSS only requires that sensitive data be protected/encrypted. However, this document recommends that CMAC authentication be used when available, as it provides an additional layer of security to ensure that sensitive data has not been altered from its original form. This will direct which decryption host services, card readers, and PIN entry devices are used to meet this extra level of security.

SECONDARY CONSIDERATIONS

Customer Environment and Hardware

After determining the data that needs to be protected and the best protection method, the next step is to determine how to build out the complete ecosystem including the customer environment, hardware, and services.

3. WHAT HARDWARE DO I NEED?

To move to AES DUKPT encryption, you will need a card reader / PIN entry device (PED) that is specifically rated and approved to support AES DUKPT operations. Check the data sheet of your device or speak with the product support team from your vendor. Ideally, the device should be a “PCI Approved” device rated as “PCI 6.x” (or higher) and list AES support.

4. DO I NEED NEW KEYS?

Yes, you will minimally need to have a new AES BDK generated as your Data Protection Key. If the reader device also supports PIN entry, an additional AES BDK is required as your PIN Protection Key. Regarding AES Key Size, you will need to select between 128-bits or 256-bits. Typically, the card reader / PED vendor provides key-generation and key-injection services.

5. WHAT ABOUT DECRYPTION SERVICES?

You will need to check with your existing Payment Gateway / Decryption service and validate that they can support AES DUKPT decryption for your specific reader device. Ensure they can support both AES-128 and AES-256 key sizes. Additionally, you should check if they can provide CMAC data validation services.

6. AES-128 VS AES-256 KEY SIZE? WHICH ONE SHOULD I CHOOSE?

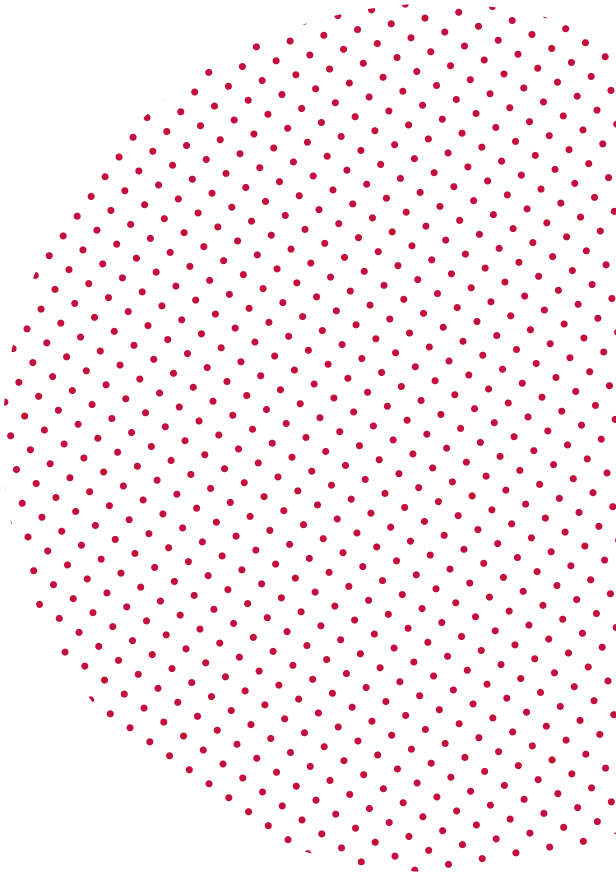
All things being equal, it is preferable to migrate to AES-256 DUKPT. Doing so ensures that you are using the maximum level of encryption protection available. However, in some cases you may discover that certain products / services only support AES-128 DUKPT. In that case, it is your preference. Although AES-256 DUKPT is strongest, AES-128 DUKPT still provides encryption that is substantially stronger than TDEA DUKPT and is fully supported by PCI.

7. HOW DO I INJECT THE NEW AES KEY(s)?

Typically, all newly ordered reader devices are injected with their AES key(s) from the factory during the initial order process. For devices already in the field, these devices can typically be updated via remote management services. Check with your reader vendor for details.

8. CAN I STILL USE MY TDEA DUKPT DEVICES DURING THE MIGRATION TO AES?

Yes. There should be no problems with operating a “mixed fleet” of both TDEA DUKPT and AES DUKPT devices. This simplifies the migration process and allows you to migrate at a pace that makes sense for your organization.



CONCLUSION

Transitioning from TDEA DUKPT to AES DUKPT requires a plan and trusted partners. MagTek and Magensa have a complete solution of integrated hardware, services, and support to make this migration simple, fast, and painless. Partner with us today and let us show you how to migrate to a higher-security AES DUKPT platform that provides maximum data protection for your customers and your business.

About MagTek

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission, and security of cards, barcodes, checks, PINs, and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Our hardware products include secure card reader/authenticators, Qwantum secure cards, token generators; EMV Contact Chip, EMV Contactless, barcode and NFC reading devices; encrypting check scanners, PIN pads, and credential personalization systems. These products all connect to Magensa, a MagTek owned gateway that offers businesses the ability to securely process transactions using authentication, encryption, tokenization, and non-static data.

MagTek is headquartered in Seal Beach, CA, please visit www.magtek.com to learn more or contact us at www.magtek.com/contactus.