Implementation of AES DUKPT in Software Point of Sale: Enhancing Security in Digital Payment Systems

Pavan Kumar Joshi

VP Information Technology, Fiserv

Abstract: ***This paper explores the implementation of the Advanced Encryption Standard (AES) with Derived Unique Key Per Transaction (DUKPT) in Software Point of Sale (SoftPOS) systems. The rapid advancement of digital payment technologies necessitates robust and efficient encryption methods to ensure secure transactions. By integrating AES DUKPT, SoftPOS systems can achieve enhanced security, scalability, and compliance with industry standards. This paper delves into the architecture, key management, encryption processes, and performance evaluation of AES DUKPT within SoftPOS environments.***

Keywords: AES, DUKPT, SoftPOS, encryption, key management, payment security, digital payments, BDK, KSN, initial key, PCI, Transaction processing.

1. Introduction

The shift towards mobile and digital payment systems has revolutionized the financial sector, offering unprecedented convenience and accessibility. However, this shift also brings significant security challenges. SoftPOS, which allows merchants to accept payments using standard over the counter mobile devices, is particularly susceptible to security threats. Implementing AES DUKPT provides a robust encryption mechanism that ensures secure transaction processing in SoftPOS systems and complies with PCI security compliance requirements.

2. Background

a) Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a highly trusted encryption algorithm used to secure data by converting it into an unreadable format without the proper key. Developed by the National Institute of Standards and Technology (NIST), AES encryption uses various key lengths (128, 192, or 256 bits) to provide strong protection against unauthorized access. This data security measure is efficient and widely implemented in securing internet communication, protecting sensitive data, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

b) Derived Unique Key Per Transaction (DUKPT)

DUKPT is a key generation method defined by the American National Standards Institute, a regulatory standard responsible for specifying the requirements for key management and the secure processing of cardholder data throughout payment transactions.

DUKPT safeguards data, such as Personal Identification Numbers (PIN) or cardholder Primary Account Numbers (PAN), by providing unique encryption keys for every transaction. Derived keys keep information safe. The process cannot be reversed to lead back to the BDK, and if one of the keys were compromised in a SoftPOS device, it would immediately be replaced by a new key in the next transaction. Through derivation, DUKPT forms a self-recycling system that promotes security, efficiency, and ease of implementation.

c) Software Point of Sale (SoftPOS)

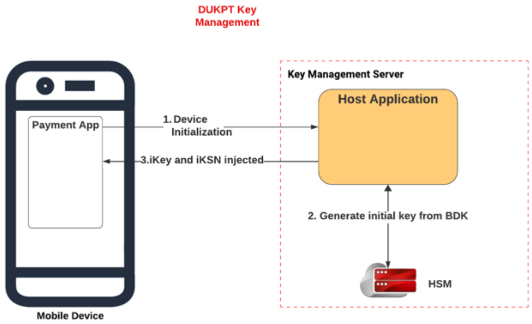
SoftPOS enables merchants to accept card payments using standard mobile devices without the need for dedicated hardware. This technology leverages the mobile device's capabilities to process transactions securely.

3. Architecture of AES DUKPT in SoftPOS

a) System Overview

The implementation of AES DUKPT in SoftPOS involves several components, including the mobile device, payment application, transaction server, and key management server. The architecture ensures secure communication and transaction processing. The process of deriving keys is two-fold; each device goes through initial configuration and then the repeated act of creating keys.

b) Key Management



c) Key Generation:

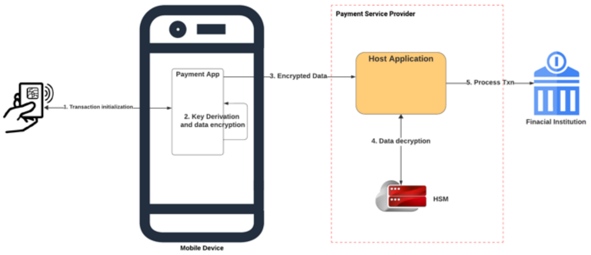
Key generation is a critical aspect of AES DUKPT implementation. One Base Derivation Key (BDK) is used to initiate the DUKPT process. The BDK itself is never exposed, but instead is used to create another key, called an initial key.

The DUKPT algorithm ensures that each transaction uses a unique key, enhancing security.

d) Key injection:
Initial key and initial KSN are injected into the devices containing identifying information for the host application by the key management server at the time of device initialization process at the time of installing the payment application. Initial key is also sent back to device under a pre-established KEK instead of sending in clear to avoid any key compromises.
Example of AES-128 iKSN and initial key:

Initial KSN	Initial Key
FFEEDDCCBBAA998 840000000	467CD68D60F8ACC44D5CFF F0BDCA8166

e) Transaction Processing



f) Transaction Initialization:
The payment application initializes a transaction by initiating NFC reader on the device. Payment application then can read the contactless/NFC enabled payment card (Credit/Debit). Once card is read by the application, it would request a unique transaction key from the list of future keys stored securely in the virtual task execution environment or chip on the phone.

g) Key Derivation:
The unique transaction key is derived using the initial key injected in the device and the transaction counter is incremented to form a unique key serial number for that transaction. Generally, it would request a set of KSNs and cache it securely to improve the performance of payment application during accepting and processing of transactions.

h) Data Encryption:
The payment application encrypts the transaction data including Personal Account Number (PAN) and optionally PIN by the future key using AES algorithm. This would create encrypted card transaction data that cannot be tempered or decrypted while transmitting the transaction to the host application.

i) Data Transmission:
The encrypted data is transmitted securely to the payment host application server for processing over TLS/https API call along with other required transaction data.

j) Decryption:
The payment host application receives the transaction data and sends the data to financial hardware security module (HSM) to decrypt it. HSM derives transaction key from BDK (stored with in HSM) by using KSN (from transaction). This step re-creates unique transaction key that can decrypt the secured card. Key Serial Numbers play an integral role in the DUKPT process by enabling the HSM to identify which initial key was used to encrypt the data.

k) Processing with Host/Bank:
After decrypting the card data within HSM, payment host application sends transaction to card associations & issuing bank (Visa, MasterCard etc) to authorize or approve transaction.

4. Security Analysis

1) Key Management Security

a) Individual device level security:
Each device is injected with an initial key (iKey) derived from the BDK and an initial key serial number (iKSN) with a unique device identifier (Terminal Identifier) and an initial transaction counter.

b) Transaction level security:
Each transaction key is unique and can't be traced back to the original key, and it's erased after use. It ensures even if a derived/unique transaction key is compromised, past and future transaction data are still protected because it's not easy to determine the previous or next keys.

c) BDK level security:
The BDK is securely stored within HSM and never exposed, minimizing the risk of key compromise.

2) Key Serial Number (KSN) format
AES DUKPT KSN is assumed to be 96-bits. Example of an AES KSN - *FFEEDDCCBBAA998840000000*

BDK ID	Device ID	Transaction Counter
In the US format BDK Id has a length of 32 bits.	It is a value which is normally unique for a terminal. It has a length of 32 bits.	Its size is always 32 bits. This value is incremented for every transaction.

3) Data Encryption Security
AES provides robust encryption, ensuring that transaction data remains confidential and tamper-proof. The use of unique keys for each transaction further enhances security. DUKPT is considered one of the most secure encryption technologies available today and helps minimize the risk of data breaches and fraud.

4) Compliance with Industry Standards
The implementation of AES DUKPT in SoftPOS complies with industry standards such as PCI-DSS, PCI-PIN ensuring that the payment system meets regulatory requirements.

5. Performance Evaluation

a) Encryption and Decryption Speed
The performance of AES DUKPT in SoftPOS is evaluated based on encryption and decryption speed. The results indicate that AES DUKPT provides efficient encryption without significant impact on transaction processing time.

b) Scalability
DUKPT's scalability aligns with transaction volume, making it ideal for large-scale payment processing environments,

effectively managing encryption keys across diverse devices and locations.

One Base Derivation Key (BDK) in AES DUKPT can be used in maximum of 4,294,967,296 devices and each device can perform 4,294,967,296 transactions before BDK need to be rotated.

c) Flexibility Adaptable and versatile, DUKPT seamlessly integrates into various payment processing systems and environments, from POS terminals to online payment gateways.

6. Conclusion

The implementation of AES DUKPT in SoftPOS offers a secure and efficient solution for digital payment processing. By leveraging the strengths of AES and DUKPT, this approach ensures robust encryption, effective key management, and compliance with industry standards. As digital payment systems continue to evolve, the integration of advanced encryption methods like AES DUKPT will be crucial in maintaining the security and integrity of financial transactions.

References

[1] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
[2] ANSI X9.24-1-2017, "Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques."
[3] Payment Card Industry Security Standards Council, "Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1," 2018.
[4] R. Rivest, "The RC5 Encryption Algorithm," Dr. Dobb's Journal, 1995.
[5] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.
[6] “ANS 24-1:2009.” American National Standards Institute. October 2009.
[7] Key Management Server – Futurex KMES Operations Guide.
[8] PKI Solutions – Futurex Public Key Infrastructure Products & Solutions