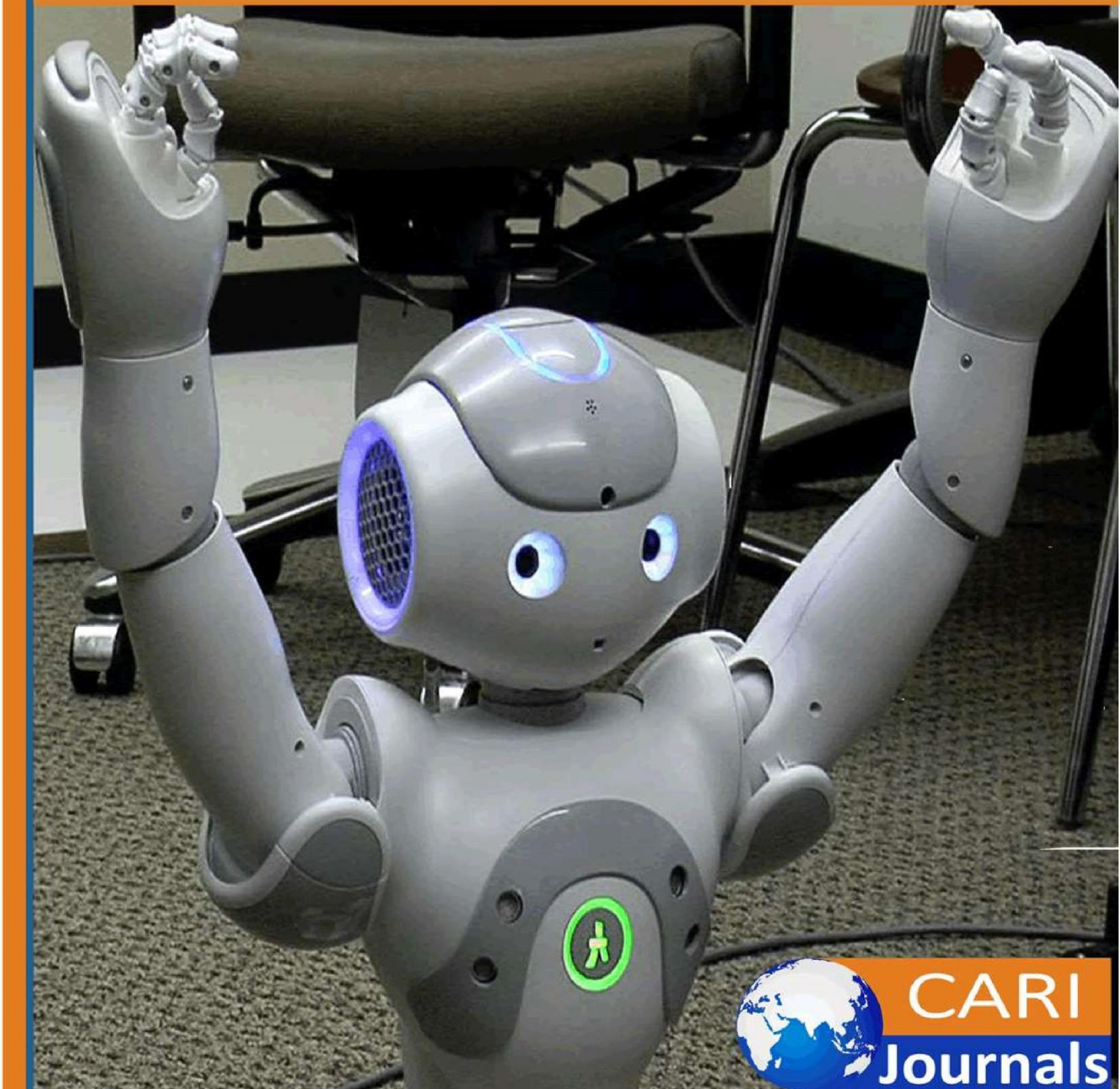
International Journal of Computing and Engineering (IJCE)

DUKPT for Software POS: A Technical Key Management Approach for Safeguarding Payment Data



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 1, pp. 16 - 29, 2025
www.carijournals

DUKPT for Software POS: A Technical Key Management Approach for Safeguarding Payment Data

Rajesh Kotha

Fiserv

https://orcid.org/0009-0004-3594-2206

Accepted: 10th Jan 2025 Received in Revised Form: 20th Jan 2025 Published: 1st Feb 2025

Abstract

Purpose: The paper explores how the Derived Unique Key per Transaction (DUKPT) encryption technique enhances the security of software-based Point of Sale (POS) systems, addressing rising cyber threats and safeguarding sensitive financial data. It aims to educate stakeholders across industries on DUKPT's implementation and long-term benefits in meeting evolving regulatory and customer demands for data security.

Methodology: A thorough literature research and a hands-on examination of DUKPT's use in software-based point-of-sale systems comprise the methodology. Existing research on key management, encryption of payment systems, and the weaknesses of conventional key management techniques are all included in the literature review. The report also provides case studies that show how DUKPT has been implemented in various industries, looking at both technical details and practical results. The examination covers network communication protocols, device security measures, secure key storage, and PCI DSS (Payment Card Industry Data Security) compliance. The conclusions are further supported by quantitative data from security breach statistics and qualitative data from interviews with industry professionals.

Findings: The findings of this paper reveal that DUKPT significantly enhances the security of software-based POS systems. Key results include: The Derived Unique Key per Transaction (DUKPT) encryption technique offers several advantages. It enhances security by generating a unique encryption key for every transaction, effectively reducing the risk of data breaches and preventing key reuse attacks. Additionally, DUKPT improves operational efficiency by allowing businesses to manage encryption keys securely without significant overhead, resulting in streamlined processes. Its implementation also demonstrates a stronger commitment to regulatory compliance, particularly with PCI DSS standards, minimizing the risk of penalties for non-compliance. Furthermore, the enhanced data security fosters greater customer trust, which ultimately strengthens client loyalty and retention

Unique Contribution to Theory, Practice, and Policy: The study makes a unique contribution to the field by providing a thorough analysis of DUKPT's benefits, enhancing theoretical discussions on cryptographic techniques, educating policymakers about the need for updated security regulations to improve cybersecurity in payment systems, and providing useful case studies and suggestions for businesses looking to successfully integrate DUKPT in software POS environments.

Keywords: *DUKPT, Key Management, Software POS Systems, Payment Security, Encryption, Cyber Threats, PCI DSS, Transaction Security, Data Protection, Payment Processing***.**

1. Introduction

The rapid evolution of digital payment systems has made securing sensitive financial data a critical priority for businesses and consumers alike. Among the various techniques developed to protect payment data, Derived Unique Key Per Transaction (DUKPT) stands out as an advanced cryptographic key management solution [1]. DUKPT generates a unique encryption key for every transaction, ensuring that even if one key is compromised, the security of other transactions remains intact. This approach has been widely adopted in hardware-based Point of Sale (POS) systems, where dedicated devices provide a controlled environment for secure key management.

However, as businesses increasingly adopt software-based POS systems for their flexibility and scalability, these systems face heightened security risks due to their reliance on general-purpose devices like smartphones and tablets. Unlike hardware POS systems, software POS solutions often operate in less secure environments, making them more vulnerable to threats such as malware, network exploits, and improper configurations. Addressing these challenges requires integrating robust key management strategies, such as DUKPT, to safeguard sensitive payment data and reduce the risk of data breaches.

This paper examines the potential of DUKPT as a key management approach to enhance payment data protection in software-based POS systems. It investigates how DUKPT's dynamic key generation and end-to-end encryption capabilities can address emerging security challenges while aligning with the need for scalable and secure payment solutions. By establishing a conceptual framework for adapting DUKPT to software POS systems, this study aims to contribute to the ongoing efforts to secure digital transactions in an increasingly cashless world.

2. Literature Survey

Due to the need for secure digital transactions, POS payment data protection research has grown. Financial data is protected by encryption and key management, especially in hardware-based POS systems. This literature evaluation covers payment security key management, software POS system difficulties, and DUKPT's solution. Financial transaction security requires key management. M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor say cryptographic systems must manage keys properly to guarantee data confidentiality, integrity, and authenticity [2]. Payment system key management involves creating, storing, distributing, and removing encryption keys to protect transaction data. Payment data security often uses symmetric encryption, where the same key encrypts and decrypts [3]. Managing these keys securely, especially for several transactions, takes time. DUKPT fixed this. DUKPT produces a unique key for each transaction, ensuring that other transactions are unaffected if one key is compromised [4]. Hardware-based POS systems use DUKPT to secure payment data by reducing encryption key exposure.

Software-based POS systems use general-purpose equipment, which increases security risks. Hardware POS systems have specific security measures which are not in mobile POS. Attackers use malware, network vulnerabilities, and software misconfigurations. The authors note that software POS solutions operate in less controlled contexts where payment data is more vulnerable to theft [5].

Software POSs need encryption key management help. Malware and network attacks can steal device static encryption keys. Without key management, software POS systems can be exploited and compromise payment data [6]. This has motivated researchers and industry specialists to examine how software can integrate DUKPT, a hardware POS security mechanism.

DUKPT protects payment data in hardware POS systems. DUKPT produces a transaction-specific encryption key from a master key [4]. One compromised key cannot decrypt other transactions, lowering security risk. DUKPT secures essential creation and delivery without POS key storage.

Several researchers have examined the benefits of DUKPT's payment system. DUKPT significantly decreases cybercriminals' attack surface [6]. DUKPT generates a unique key for each transaction, so a compromised key cannot decrypt other transactions [7]. Over unprotected networks like the internet, DUKPT is appropriate for transaction data transmission.

DUKPT adaptation for software-based POS systems has strengths and downsides. DUKPT's capacity to create unique keys for each transaction can improve software POS system security [4] but implementing it in general-purpose devices is difficult. Secure key derivation on malware—or physically tampered devices—is crucial. Software POS systems are less controllable than hardware-based ones; hence, DUKPT must be integrated.

Multiple industry efforts have integrated DUKPT into software POS systems despite these challenges. Encrypting and managing keys using DUKPT reduces data exposure in software POS setups [7]. Safeguard software development and regular security updates can help DUKPT safeguard POS payment data.

The literature emphasizes key management for payment data security and DUKPT for software POS system security. DUKPT works well with hardware; however, software POS systems must secure devices. Research reveals that DUKPT can secure software POS systems and payment data when applied

3. Problem Statement

Businesses need help safeguarding sensitive payment data as software-based POS systems become increasingly popular. Software-based POS systems use smartphones, tablets, and computers with security protocols. Dependencies expose users to viruses, network vulnerabilities, and risky program settings. Software POS systems can be hacked to steal payment data. Due to inadequate security, retail and financial data breaches have caused economic loss, legal issues, and brand damage. New laws like the Payment Card Industry Data Security Standard (PCI DSS) compel corporations to secure payment data with stringent security protocols, increasing pressure to remedy these weaknesses. Poor key management in software POS systems causes inaccurate encryption and data leaks. Software POS payment data protection demands scalable, dependable key management. DUKPT has the potential to ensure low-risk transaction data encryption.

4. Solutions

Hardware-based POS systems' Derived Unique Key Per Transaction (DUKPT) key management mechanism may secure payment data in software POS systems' increasingly vulnerable environment.

4.1 Overview of DUKPT Functions

DUKPT generates transaction-specific encryption keys with a primary master key [4]. Previous and future transaction data is protected even when a key is compromised. A unique algorithm that generates non-predictable nor reusable keys reduce significant data breaches.

DUKPT transactions never reveal Base Derivation Keys (BDKs) because they are loaded into hardware security modules (HSMs) or trusted platforms. Initial PIN encryption Keys (IPEKs) from this BDK encrypt transaction data [8]. IPEK generates unique encryption keys for each transaction to protect payment data from key-reuse attacks. This architecture works in hardware-based POS terminals with tamper-proof cryptography modules. Some software POS systems run on general-purpose computers and require higher security hardware.

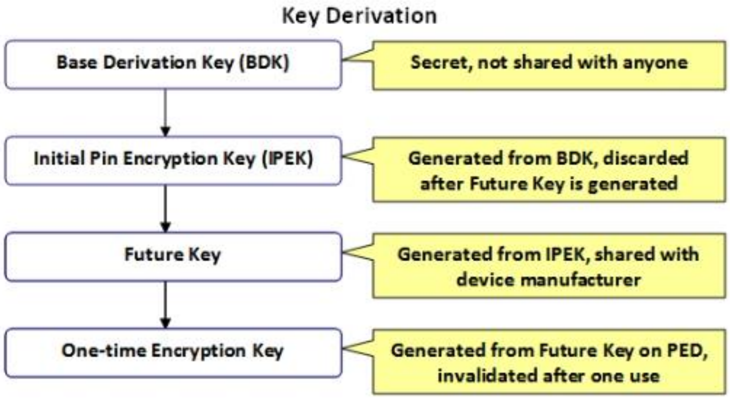

Key Derivation
Base Derivation Key (BDK)
Secret, not shared with anyone
Initial Pin Encryption Key (IPEK)
Generated from BDK, discarded after Future Key is generated
Future Key
Generated from IPEK, shared with device manufacturer
One-time Encryption Key
Generated from Future Key on PED, invalidated after one use

Fig. 1. The process of key derivation. Adapted from [9]

4.2. DUKPT Implementation Issues in Software POS Systems

4.2.1 Security Risks

Malware, keyloggers, and other security concerns are more likely on general-purpose software POS devices [10]. Malware may access encryption keys and transaction data. Unlike hardware POS systems, these devices lack hardware based cryptographic protections.

4.2.2 Security flaws

DUKPT needs a secure Base Derivation Key (BDK) or IPEK storage, even if it excludes encryption key reuse [8]. Hardware POSs store keys securely. Software POS systems leverage the device's file system or software-based security, which is vulnerable to tampering.

4.2.3 Under Uncontrolled Conditions

Public places and open networks use software POS systems. Transaction data and encryption keys can be stolen by hackers in insecure networks [11]. These conditions demand strong network encryption and communication protocols to secure DUKPT.

4.2.4 Regulations

All cardholder data systems must comply with PCI DSS [12]. DUKPT in such systems help comply with PCI DSS, it requires encryption key management and rotation to reduce vulnerability.

4.3 Software POS Secure DUKPT Implementation Options

Despite the existing restrictions, software POS systems can securely incorporate DUKPT.

4.3.1 Key Security and Storage

Any encryption uses cryptographic keys. Software POS systems must securely store the Base Derivation Key (BDK) and Initial Pin Encryption Keys for DUKPT [8]. These keys need extra protection since general-purpose devices lack tamper-proof hardware.

4.3.2 Key Management

Key management can be offloaded to an on premise or cloud-based Hardware Security Module (HSM) [14]. HSMs safeguard cryptographic key generation, storage, and management [13]. The software POS system can securely obtain the encryption keys from an HSM without exposing them to the device's memory or file system by storing the BDK and IPEKs there. Additionally, created and verified by HSMs are digital signatures [15]. Every access transaction involving an HSM logs to build an audit trail. The tools let companies migrate sensitive data and procedures from paper records into a digital version.

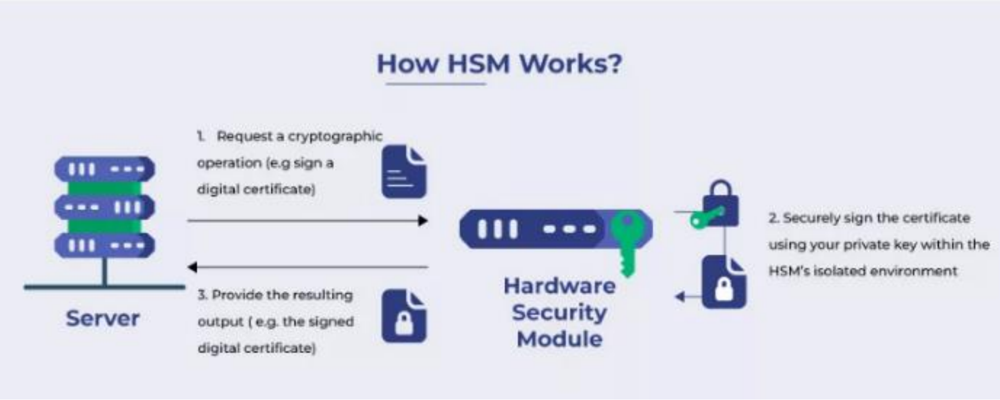

How HSM Works?
1. Request a cryptographic operation (e.g sign a digital certificate)
Server
3. Provide the resulting output (e.g. the signed digital certificate)
Hardware Security Module
2. Securely sign the certificate using your private key within the HSM's isolated environment

Fig. 2. How HSMs secure data. Adapted from [15].

4.3.3 Encryption and Tokenization

Another option is to encrypt and tokenize the BDK and IPEKs before saving them on the device. This prevents an attacker from using these keys without decryption keys. Tokenization replaces sensitive data, such as cardholder information, with a non-sensitive token that may be securely stored and delivered.

4.3.4 Key Rotation and Expiry

Regular key rotation improves security. Even with DUKPT, where unique keys are generated for each transaction, rotating keys minimizes key compromise risk [16]. Automatic key expiration reduces the danger of illegal transaction data access.

4.3.5 Device hardening and security

Securing general-purpose devices running software POS systems is essential for payment processing system integrity [17]. DUKPT protects data in transit, but the device needs further security. Software POS systems must be created with security as the first line of defense. Code audits, vulnerability testing, and secure coding are examples. Complication and tamper detection can also prevent attackers from reverse-engineering software to extract cryptographic keys or tamper with encryption.

4.3.6 Operating System and Application Hardening

Disabling superfluous services, protecting network connections, and updating the operating system and apps with security updates reduce the attack surface. A trusted execution environment (TEE) can safeguard against malware and physical manipulation by isolating sensitive cryptographic operations [18]. All assets and code associated to the TEE, including the foundational Trusted OS and the accompanying code, must be loaded and started using a technique that expects it to be in its first state as envisioned by the developers in order for the Trust to function properly in the TEE.

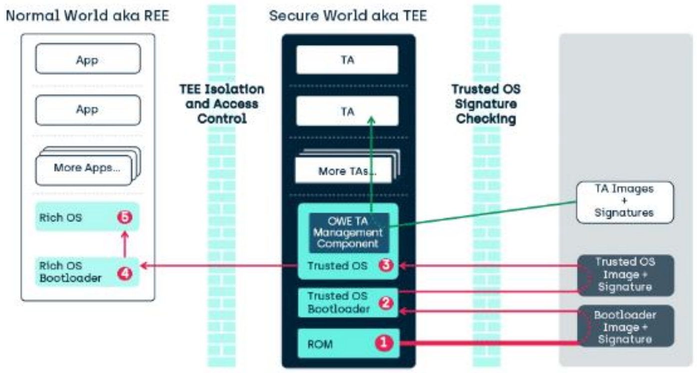


Fig. 3. Demonstrating TEE architecture. Adapted from [19].

4.3.7 Device Lockdown and User Authentication

Only authorized users should access the software POS system. Robust user authentication mechanisms, like multi-factor authentication (MFA), require two or more credentials before granting access [13]. Locking devices to prevent illegal software installation can further limit malware infection and other security breaches.

4.4 Network Communication Security

Due to their internet or other public network operation, software POS systems must secure their communication channel with the payment processor. Implementing end-to-end encryption (E2EE) protects data [13]. With the encryption keys, attackers can decipher data intercepted in transit. TLS protocols should secure communication connections to prevent data tampering and interception. VPNs can build safe, encrypted tunnels for data transmission between a device and the backend system [13]. This can prevent public or insecure networks from intercepting sensitive payment data. Software POS systems in retail organizations with inadequate network security benefit from VPNs.

4.5 Compliance with PCI DSS and Industry Requirements Industry Requirements

DUKPT-integrated software POS systems must follow PCI DSS and other industry standards to protect payment data [8]. PCI DSS requires encryption, key management, and secure data storage to protect cardholder data to protect cardholder data. PCI DSS compliance requires regular POS security audits. Unauthorized access attempts or unusual transaction patterns may reveal breaches before they expose valuable data [20]. Also, a security breach requires a response and recovery plan. DUKPT's crucial generation mechanism post-breach can allow businesses to revoke compromised keys and issue fresh ones.

4.6 Technical Implementation Steps

DUKPT deployment in a software POS system requires technical architecture and security knowledge. DUKPT deployment requires key generation, secure data transfer, key management, and in-depth monitoring in such cases.

4.6.1 Key Creation and Storage

For DUKPT, the Base Derivation Key (BDK) must be created safely. All transaction-specific keys stem from this key. A trusted platform like a Hardware Security Module (HSM) should create the BDK to prevent unauthorized access. The BDK makes IPEKs [21]. These intermediary keys generate transaction-specific encryption keys. IPEKs are essential for secure transaction encryption and must be maintained securely, preferably encrypted or in an HSM, to prevent manipulation. DUKPT implementation security depends on protecting the BDK and IPEKs.

4.6.2 Deriving Transaction Key

After securely storing IPEKs, generate transaction-specific encryption keys. POS software generates a transaction-specific key for each payment transaction [8]. This one-time-use key is derived from the IPEK and a transaction counter to avoid key reuse. This unique key generation improves security because a compromised key would not affect past or future transactions. Before transmission for processing, the transaction-specific key encrypts sensitive payment data like cardholder information. All sensitive data is safeguarded in transit and kept securely with this approach.

4.6.3 Safe Data Transmission

Encrypted data transmission over insecure networks adds another degree of security risk [11]. A VPN is needed to safeguard payment data between the POS system and the payment processor. These techniques prevent tampering with encrypted transaction data during transmission. End-to-end encryption prohibits unauthorized users from viewing or changing sensitive data even if an attacker intercepts it. System security depends on communication channel security.

4.6.4 Key Rotation and Management

Key management must be ongoing to ensure DUKPT security. DUKPT creates a new key for every transaction, although the proposed rotating keys is to reduce long-term key exposure [16]. The system rotates these keys to decrease attack time even if a key is compromised. Policies should update expired or compromised keys without disrupting transactions. Key rotation and revocation safeguard the POS system from prolonged cryptographic key use.

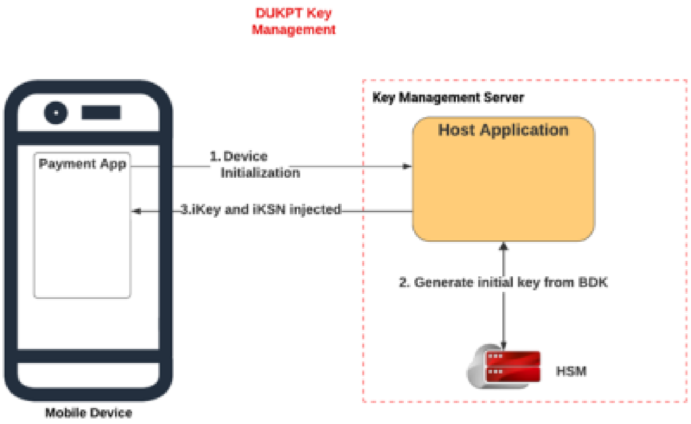


Fig. 4. Demonstrating key management. Adapted from [1]

4.6.5 Monitoring and Compliance

DUKPT must be monitored for unauthorized access and breaches after keys are safely handled. Monitoring access logs, suspicious trends, and key usage is necessary. PCI DSS and other industry laws need regular security audits. Audits ensure a software follows the best encryption, key management, and data protection practices [20]. Compliance ensures payment system integrity and data protection, building customer and stakeholder trust.

5. IMPACT

Software-based POS systems with DUKPT improve payment security. Payment security, compliance, consumer trust, and company climate are affected. Smartphone, tablet, and PC software POS systems with DUKPT address the growing threat of cyberattacks and data breaches targeting payment infrastructure

5.1. Enhanced Payment Security

DUKPT's unique encryption key for every transaction reduces key-reuse attacks, a static key system vulnerability. Only one transaction is affected by a compromised encryption key, protecting the others. This greatly decreases data breach damage, enhancing security quickly. DUKPT encrypts and secures cardholder data and other payment information during transactions [9]. Even if attackers breach POS systems, payment details are more challenging

5.2. Compliance with Regulatory Standards

Financial and payment processing requires regulatory compliance. DUKPT ensures organizations satisfy PCI DSS, General Data Protection Regulation (GDPR), and other local and global data security encryption and management regulations. With DUKPT, payment data mishandling and regulatory breaches have decreased. DUKPT protects payment-processing systems and prevents companies from incurring costly financial fines, lawsuits, and brand reputational damages

5.3. Trust and Satisfaction

DUKPT invests resources in ensuring that payment data are kept secure; this enhances customers' confidence in those businesses. In the current time of data breaches and identity theft, customers' trust in their service provider is paramount. The involvement of secure payment solutions gains them more security-conscious clients and retains the current ones; hence, DUKPT encryption payment enterprises are trusted

5.4. Risk Management and Business Continuity

DUKPT saves from expensive data leakage and security breaches for long-term stability. Further, data breaches of the payment information result in fines, legal fees, and loss of consumer trust [22]. With DUKPT, organizations may avoid these risks and survive a cyber-attack. This proactive risk management methodology lets an organization innovate without data breaches or loss of any payment data

6. USES

6.1. Retail and E-Commerce

Software-based point-of-sale systems raise customer service and payment processing for retailers and e-commerce sites. DUKPT can be employed in online payment gateways, smartphone apps, and tablet-based in-store checkout [23]. Cyberattacks are possible on retail POS systems due to their large transaction volume. DUKPT's unique key generation protects each high-volume transaction.

6.2. Hospitality

Hotels, restaurants, and travel services use POS systems to process payments from numerous devices and locations. These software POS systems use smartphones or tablets, which are vulnerable to hacking and viruses. DUKPT encrypts mobile, credit card, and digital wallet payments [23]. This is crucial in restaurants that use mobile POS systems for tableside payments and hotels that use software-based solutions to link many points of service.

6.3. Healthcare and Medical Billing

Software POS systems are increasingly used to collect healthcare fees. Cybercriminals target these systems because they handle sensitive financial and personal data. DUKPT can be integrated into healthcare payment systems to encrypt patient payment information, comply with HIPAA, and protect patients' financial data. Adding trust and security to healthcare transactions is crucial for confidentiality.

6.4. Public Transportation and Ticketing System

Many cities and transit authorities use POS software for ticketing and fare payments [24]. DUKPT secures fare transactions via kiosks, mobile ticketing apps, and in-vehicle payment systems. DUKPT prevents data breaches and preserves passenger payment information for public transportation systems that process millions of transactions daily.

7. SCOPE

7.1. Industry-Wide Global Adoption

Software POS systems are widespread, enabling DUKPT deployment. Key management and encryption help most digital payment companies [6]. DUKPT's scalability lets small and large companies make secure, standardized payments worldwide

7.2. Integration with Emerging Payment Technologies

As payment technologies evolve, DUKPT supports NFC, digital wallets, and cryptocurrency transactions. DUKPT's versatility and scalability enable secure transactions using new payment methods and protocols [1]. DUKPT's transaction-specific encryption aids Apple and Google Pay contactless payments

7.3. Regulatory Changes and Future Standards

DUKPT is tamper-proof and can adapt to global payment security laws [1]. DUKPT's inherent security will save enterprises from costly encryption system changes when PCI DSS and other industry regulations tighten

7.4. Consumer Data Privacy

DUKPT safeguards software POS and payment data [1]. These include email addresses, PINs, loyalty program data, and client data. DUKPT in POS systems can assist companies in meeting consumer privacy requirements, especially in countries with severe privacy regulations like the GDPR

7.5. Long-Term Financial Benefits

Software POS DUKPT is expensive but worth it. Avoiding payment data breaches and following best practices saves companies money, court costs, and brand [22]. Trust in security keeps clients and reduces attrition

8. Conclusion

DUKPT-enabled software-based POS systems provide a robust and reliable solution for securing digital payments. By generating a unique encryption key for each transaction, DUKPT effectively prevents data breaches and eliminates the risk of key reuse, ensuring the safety of sensitive financial information. This approach not only enhances payment security but also increases regulatory compliance and builds consumer trust. Its flexibility makes it well-suited for a wide range of industries, including retail, healthcare, hospitality, and public transportation. Additionally, DUKPT's adaptability to evolving technologies and payment methods positions it as a key component in modern payment security frameworks. Over time, its implementation reduces financial data-breach risks, strengthens operational security, and aligns with industry standards.

To maximize the benefits of DUKPT, businesses across various sectors should consider adopting this encryption technique in their software-based POS systems. Organizations must also focus on training their IT teams and stakeholders to effectively implement and manage DUKPT solutions, ensuring a deep understanding of encryption and key management. Regular updates and maintenance are crucial to address potential vulnerabilities and ensure the continued efficacy of DUKPT in mitigating emerging cyber threats.

Collaboration with regulatory bodies and industry standards organizations can further strengthen the alignment of DUKPT implementations with compliance requirements, such as PCI DSS, while preparing for future standards. Businesses should also explore integrating DUKPT with complementary security technologies, such as tokenization and biometrics, to establish a multi-layered approach to payment data security.

By adopting DUKPT, providing ongoing training, maintaining regular updates, and collaborating with industry stakeholders, businesses can create a secure environment for digital payment data. This not only enhances customer trust and loyalty but also ensures the long-term viability of secure, compliant, and efficient payment systems.

9. References

1. P. Kumar Joshi, "Implementation of AES DUKPT in Software Point of Sale: Enhancing Security in Digital Payment Systems," *International Journal of Science and Research (IJSR)*, vol. 13, no. 8, pp. 46–48, Aug. 2024, doi: https://doi.org/10.21275/sr24730131558.
2. M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, "Physical Layer Security: Authentication, Integrity, and Confidentiality," *Physical Layer Security*, pp. 129–150, 2021, doi: https://doi.org/10.1007/978-3-030-55366-1_6
3. P. Smirnoff and D. M. Turner, "Symmetric Key Encryption - why, where and how it's used in banking," *Cryptomathic*, Jan. 03, 2020. https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking.
4. Ayooluwa Olosunde, "Understanding Derived Unique Key Per Transaction (DUKPT) in Payment Security," *Medium*, Mar. 29, 2024. https://medium.com/@lovisgod/understanding-derived-unique-key-per-transaction-dukpt-in-payment-security-ab821e29964f.

5. M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," *Future Generation Computer Systems*, vol. 100, no. 1, pp. 408–427, Nov. 2019, doi: https://doi.org/10.1016/j.future.2019.03.041.
6. S. kaushik, "Key management schemes in POS : EMV Transaction Flow (Part-4)," *Medium*, Jun. 07, 2023. https://hpkaushik121.medium.com/key-management-schemes-in-pos-emv-transaction-flow-part-4-f78ad010a16e.
7. S. Gaddam, Atul Luykx, R. Sinha, and G. J. Watson, "Reducing {HSM} Reliance in Payments through Proxy Re-Encryption," pp. 4061–4078, Jan. 2021.
8. S. Perella, "Encryption Hierarchies to Simplify Your PIN & P2PE Solutions | Schellman," *Schellman Compliance*, Jan. 14, 2022. https://www.schellman.com/blog/pci-compliance/pci-p2pe-solutions-encryption-hierarchies (accessed Oct. 07, 2024)..
9. Dolo, "How ciphertext was generated in card reader using DUKPT encryption?," *Stack Overflow*, 2024. https://stackoverflow.com/questions/17362567/how-ciphertext-was-generated-in-card-reader-using-dukpt-encryption (accessed Oct. 07, 2024).
10. "POS malware: Risk factors to know | Stripe," *stripe.com*. https://stripe.com/resources/more/pos-malware-101-risk-factors-to-know-and-how-to-protect-your-business.
11. I. C. Eian, K. Y. Lim, M. X. L. Yeap, H. Q. Yeo, and F. Z, "Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges," Oct. 2020, doi: https://doi.org/10.20944/preprints202010.0018.v1.
12. M. N. M. Bhutta *et al.*, "Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1–10, Jan. 2022, doi: https://doi.org/10.1155/2022/9942270.
13. V. Mulder, Alain Mermoud, V. Lenders, and Bernhard Tellenbach, *Trends in Data Protection and Encryption Technologies*. Springer, 2023. https://library.oapen.org/bitstream/handle/20.500.12657/75398/1/978-3-031-33386-6.pdf#page=31.
14. D. Cooke, "Key Management for HSMS and post-quantum cryptography," *Cryptomathic.com*, Jun. 11, 2024. https://www.cryptomathic.com/news-events/blog/key-management-for-hosted-hardware-security-modules-and-post-quantum-readiness.
15. J. Mehta, "What is (HSM) Hardware Security Module? Role & Benefits of HSM," *SignMyCode - Blog*, Mar. 27, 2023. https://signmycode.com/blog/what-is-a-hardware-security-module-role-of-hsms-for-digital-signing.
16. "Key Rotation Strategies for Securing Sensitive Data," *www.piiano.com*. https://www.piiano.com/blog/key-rotation.

17. I. T. Moon, M. Shamsuzzaman, M. M. R. Mridha, and A. S. Md. M. Rahaman, "Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems," *Journal of Computer and Communications*, vol. 10, no. 07, pp. 103–129, 2022, doi: https://doi.org/10.4236/jcc.2022.107007.
18. U. Lee and C. Park, "SofTEE: Software-Based Trusted Execution Environment for User Applications," *IEEE Access*, vol. 8, pp. 121874–121888, 2020, doi: https://doi.org/10.1109/access.2020.3006703.
19. "Trusted Execution Environment (TEE) - What is it? Trustonic," 2019. https://www.trustonic.com/technical-articles/what-is-a-trusted-execution-environment-tee/.
20. N. Shankar and Z. Mohammed, "Surviving Data Breaches: A Multiple Case Study Analysis," *Journal of Comparative International Management*, vol. 23, no. 1, pp. 35–54, Sep. 2020, doi: https://doi.org/10.7202/1071508ar.
21. in DUKPT, "What is the point to the IPEK in DUKPT?," *Information Security Stack Exchange*, Apr. 23, 2014. https://security.stackexchange.com/questions/56414/what-is-the-point-to-the-ipek-in-dukpt
22. P. Wang, H. D'Cruze, and D. Wood, "Economic costs and impacts of business data breaches," *Issues In Information Systems*, vol. 20, no. 2, 2019, doi: https://doi.org/10.48009/2_iis_2019_162-171
23. Hectorhjure, "How are Card Payments Protected? What is DUKPT? - Hectorhjure - Medium," *Medium*, Mar. 02, 2024. https://medium.com/@hectorhjure/how-are-card-payments-protected-what-is-dukpt-89cfbbd5be94
24. "Transportation POS Systems | eMobilePOS," *eMobilePOS*, Aug. 21, 2024. https://www.emobilepos.com/industries/transportation/