ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

Review Article

Open Access

Encryption of Host-to-Host Payment Transactions Using Master-Session Key Implementation for Multi-Merchant Acquirer Integration via a Single Payment Gateway Platform

Pavan Kumar Joshi

Director Information Technology, Fiserv, USA

ABSTRACT

In the era of digital transactions, ensuring the security and scalability of a payment gateway solution is paramount. This paper explores the implementation of master-session key encryption for host-to-host payment transactions, facilitating seamless integration with multiple merchant acquirers through a single payment gateway platform. The master-session key method provides a robust framework for securing sensitive information, ensuring data integrity, protecting against unauthorized access, and improves interoperability among diverse financial entities. This paper outlines the architecture, key management, encryption process, and security benefits of this approach.

***Corresponding author**

Pavan Kumar Joshi, Director Information Technology, Fiserv, USA.

Received: July 02, 2022; **Accepted:** July 20, 2022; **Published:** July 30, 2022

Keywords: Payment Gateway, Encryption, Master-Session Key, Security, Host-to-Host Transactions, Dynamic Key Generation, Merchant Acquirers, Integration

Introduction

The proliferation of digital payment methods has necessitated robust security mechanisms to protect sensitive financial data. Traditional encryption methods often fall short in providing the required level of security and flexibility for integrating multiple merchant acquirers. This paper presents a master-session key encryption approach to address these challenges, ensuring secure host-to-host payment transactions and streamlined integration with various merchant acquirers via a single payment gateway platform.

Background

Payment Gateway and Merchant Acquirers

A payment gateway is a service that authorizes and processes payments for online and offline transactions. Merchant acquirers are financial institutions that process credit and debit card transactions on behalf of merchants. Integrating multiple merchant acquirers into a single payment gateway platform can be complex and requires robust security measures to protect transaction data [1].

Encryption in Payment Systems

Encryption is a critical component in securing payment transactions. It involves converting plaintext data into ciphertext, which can only be decrypted by authorized parties. In payment systems, encryption ensures that sensitive information such as card details, personal identification numbers (PINs), and transaction data remain confidential during transmission and storage. Traditional encryption methods, such as symmetric and asymmetric encryption, have limitations in terms of scalability and flexibility when integrating multiple merchant acquirers [2].

Master-Session Key Concept

The master-session key approach involves the use of two types of keys: a master key and session keys. The master key is a long-term key used to derive short-term session keys. Session keys are used for encrypting individual transactions and are periodically refreshed to enhance security. This method enhances security by ensuring that only subset of transactions is sharing encryption key, reducing the risk of data breaches [3].

Architecture

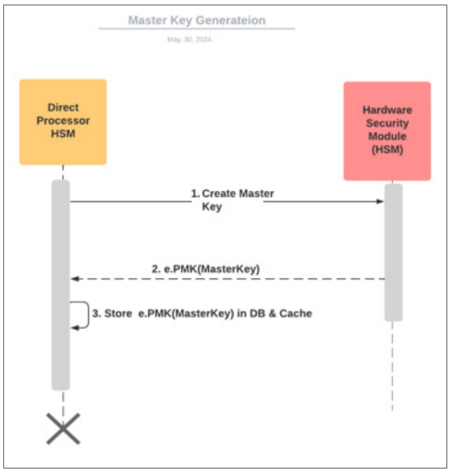
The proposed architecture involves a central payment gateway that communicates with multiple merchant acquirers using the master-session key encryption method. The merchant acquirers generate a master key. Payment gateway requests for session keys from each of the acquirers it has integrations with periodically. For each transaction that is processed by a specific merchant acquirer, acquirer's unique session key is used to encrypt the transaction data [4].

Key Management

Key management is a critical aspect of the master-session key implementation. The master key is securely generated and stored in a hardware security module (HSM). The merchant acquirer's HSM is responsible for generating session keys based on the master key. Session keys are unique for a set of transactions, ensuring that even if a session key is compromised, the impact is limited.

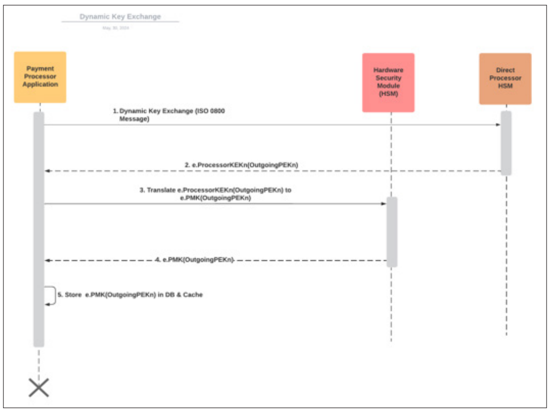
Encryption Process

Master Key Generation



The master key is generated using a secure algorithm as AES. The resulting key is encrypted under the KEK and can be stored by the host application.

Session Key Derivation and Exchange with Payment Processing Application


Dynamic Key Exchange
May, 30, 2024
Payment Processor Application
Hardware Security Module (HSM)
Direct Processor HSM
1. Dynamic Key Exchange (ISO 0800 Message)
2. e.ProcessorKEKn(OutgoingPEKn)
3. Translate e.ProcessorKEKn(OutgoingPEKn) to e.PMK(OutgoingPEKn)
4. e.PMK(OutgoingPEKn)
5. Store e.PMK(OutgoingPEKn) in DB & Cache

The merchant acquirer's HSM derives a session key from the master key using a cryptographic algorithm such as AES (Advanced Encryption Standard. This session key is requested by the payment processing application at a regular interval (typically every 24 hours or after x number of transactions whichever is lesser) to minimize the impact in case of breach/session key compromise. Session Key exchange between 2 systems must be under key exchange key (KEK) so that session key is never exposed in clear [5].

Data Encryption

Payment gateway translate the encrypted data received from the Point-of-Sale terminal from device key to the session key before transmission inside its financial HSM.

Data Decryption

Upon receipt, the encrypted data is decrypted using the corresponding session key that is recreated from the master key already present with the merchant acquirer.

Communication Protocol

The communication protocol between hosts must support the secure exchange of encrypted data. This involves establishing a secure channel using protocols such as TLS (Transport Layer Security) to protect the session key during transmission.

Security Benefits

Enhanced Confidentiality

The use of session keys ensures that set of transactions are encrypted with a unique key, making it difficult for attackers to decrypt multiple transactions even if they manage to compromise a single session key.

Data Integrity

Encryption not only protects the confidentiality of the data but also ensures its integrity. Any unauthorized modification of the encrypted data can be detected, as the decryption process will fail if the data has been tampered with.

Reduced Key Exposure

By limiting the use of the master key to the derivation of session keys, the exposure of the master key is minimized. This reduces the risk of the master key being compromised [6].

Scalability

The master-session key approach allows for seamless integration with multiple merchant acquirers without the need for complex key management systems.

This approach can be easily integrated into existing payment systems. The periodic refreshment of session keys ensures that the system remains secure over time. This method supports various encryption algorithms and can be easily adapted to different payment gateway architectures [7].

Implementation Challenges

Key Management Complexity

Managing the lifecycle of master and session keys requires robust key management practices. This includes secure key generation, storage, distribution, and destruction. Organizations must implement strict policies and procedures to manage keys effectively.

Secure Storage

The master key must be stored in a highly secure environment, such as an HSM, to prevent unauthorized access. The HSM should comply with industry standards and undergo regular security audits.

Key Distribution

Session keys must be securely distributed to the relevant parties involved in the transaction. This can be achieved through secure channels and protocols that ensure the keys are not exposed during transmission.

Performance Overhead

The encryption and decryption processes introduce computational overhead. However, with advancements in hardware and optimization techniques, this overhead can be minimized. Organizations must balance the need for security with the performance requirements of their payment systems.

Hardware Acceleration

Utilizing hardware acceleration technologies, such as dedicated encryption processors, can significantly reduce the performance impact of encryption and decryption operations.

Optimization Techniques

Implementing optimization techniques, such as parallel processing and efficient cryptographic algorithms, can further enhance the performance of the encryption process.

Compliance

Implementing encryption in payment systems must comply with industry standards and regulations such as PCI DSS (Payment Card Industry Data Security Standard) and PCI PIN (Payment Card Industry PTS PIN Security Requirements). Ensuring compliance adds an additional layer of complexity to the implementation. Organizations must stay updated with the latest regulatory requirements and ensure their encryption practices align with these standards [8].

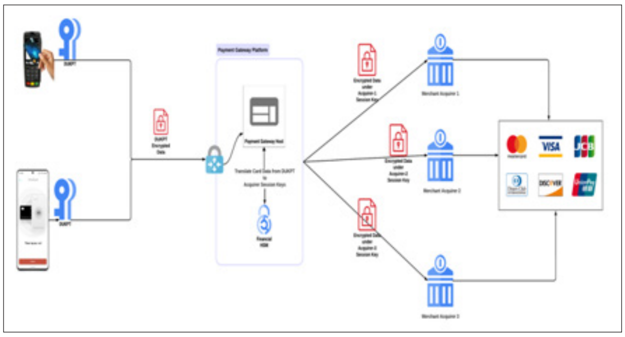
Case Study: Implementation in a Financial Institution

To illustrate the practical application of the master-session key approach in a payment gateway to support multiple merchant acquirer integrations, I present a case study of its implementation in a financial institution. The institution faced challenges in securing its host-to-host payment transactions and sought a robust encryption solution that allowed them to scale their solution for their merchant base.

Problem Statement

The financial institution's existing platform implementation only allowed a DUKPT key injection into devices by individual merchant acquirers. This limited an ability to scale the solution to be able to process merchant transactions with multiple acquiring processing platforms. Inability to integrate with multiple processing platform from a single payment gateway application stalled the merchant adoption of the platform. Merchants were left out with critical feature supported by the modern Payment gateway platform.

Solution Implementation


DUKPT
DUKPT
DUKPT Encrypted Data
Payment Gateway Platform
Payment Gateway Host
Translate Card Data from DUKPT to Acquirer Session Keys
Financial HSM
Encrypted Data under Acquirer 1 Session Key
Encrypted Data under Acquirer 2 Session Key
Encrypted Data under Acquirer 3 Session Key
Merchant Acquirer 1
Merchant Acquirer 2
Merchant Acquirer 3
VISA
JCB
DISCOVER

The institution/company implemented the master-session key approach between payment gateway application and merchant acquiring platforms (Direct Processor) to enhance the security of its payment transactions while following PCI-DSS and PCI-PIN compliance guidelines. This allowed payment gateway platform to connect multiple merchant acquirers from one application [8].

The following steps were taken:

Master Key Generation

A secure master key was generated by the individual merchant acquiring platforms using its their own HSM and stored in encrypted format within their application secure storage. Master keys were generated using AES-128.

Session Key Derivation

For set of transactions, a unique session key was derived/requested from the master key of the acquiring platform. Dynamic Session key exchanges were done for 50 thousand transactions or every day whichever is lesser upon which a new session key was requested from the merchant acquiring systems via ISO-8583 financial transaction card messaging specification [9].

Data Encryption

Encrypted transaction data received by Payment Gateway platform was encrypted under the device DUKPT. Payment Gateway application translated card data that is encrypted under DUKPT session key to acquirer's current session key before transmitting the transaction request to merchant acquiring platform. Data encryption/translation was done securely within financial HSM which is compliant per PCI-DSS standards [8].

Data Decryption

The merchant acquiring platform received the encrypted data. Card data then was decrypted using the corresponding session/master key by the acquiring platform's HSM.

Transaction Processing

Transaction was then sent to card association/issuing platforms to authorize.

Results

The implementation of the master-session key approach significantly improved the security of the institution's payment transactions. It allowed the single payment gateway to integrate with multiple merchant processors with only one set of DUKPT keys injected on the POS device. This enabled company to roll out the solution to enterprise level merchants that required connecting to multiple direct processing hosts as they were able to negotiate processing fees with the acquirers by transaction types and risk levels.

References

1. Smith J (2020) Payment Gateway Integration: Challenges and Solutions. Journal of Financial Technology 12: 45-56.
2. Brown A (2019) Encryption Methods in Digital Payments. International Journal of Cyber Security 8: 78-89.
3. Johnson M (2021) Master-Session Key Encryption for Secure Transactions. IEEE Transactions on Information Forensics and Security 15: 1234-1245.
4. Davis R (2018) Architectural Considerations for Multi-Merchant Acquirer Integration. Journal of Payment Systems 10: 67-75.
5. (2001) Advanced Encryption Standard (AES), FIPS PUB 197. National Institute of Standards and Technology (NIST).
6. Lee S (2021) Security Analysis of Master-Session Key Encryption. International Journal of Information Security 14: 567-578.
7. Wang L (2020) Scalable Encryption Solutions for Payment Gateways. Proceedings of the IEEE Conference on Cyber Security 234-239.
8. (2018) Payment Card Industry Data Security Standard (PCI DSS). Payment Card Industry Security Standards Council.
9. (2003) Financial transaction card originated messages. ISO https://www.iso.org/standard/31628.html#:~:text=ISO%208583%2D1%3A2003%20specifies,and%20values%20for%20data%20elements.