CSP(CUSTOMER SELECTED PIN)

Overview:

CSP (Customer Selected PIN) is a crucial service in online banking that enables users to set or change their card PINs securely. It involves interactions between the user's device, the bank's web server, the CSP server, HSM, and the P1C system, with strong encryption and secure communication channels to ensure the safety of sensitive data. CSP is integrated into the MPMS system, providing specialized services for mobile payment management.

What is CSP?

CSP stands for **Customer Selected PIN**. It is a service within an application that allows users to set or change the PIN (Personal Identification Number) for their bank cards. This service is particularly useful in online banking, enabling customers to select their own PIN without needing to remember their old one.

How CSP Works

1. **User Interaction:**
    - The user logs into their Internet Banking application.
    - They navigate to the page where they can set a new PIN for their card.
    - The user enters the new PIN twice to avoid errors.
2. **Request Transmission:**
    - The entered PIN and card information are sent from the user's browser to the bank's web server over a secure HTTPS connection.
    - The bank's web server then creates a request and sends it to the CSP server via a secure line, such as VPN or mutual TLS.
3. **Processing by CSP Server:**
    - The CSP server validates the request parameters.
    - It sends the new PIN to the Hardware Security Module (HSM) to be encrypted.
    - The encrypted PIN block is then sent to the PaymentOne Cards (P1C) system.
    - P1C updates the PIN offset for the specified card and confirms the update back to the CSP server.
    - The CSP server then sends a success response back to the user's browser.

Components Involved

1. **User's Device:**
    - Uses a web browser to interact with the Internet Banking application.
2. **Bank's Web Server:**
    - Hosts the Internet Banking application and processes requests from the user's browser.

3. **CSP Server:**
    - A Linux virtual machine running a Spring Boot Java application within the FIS data center.
    - Processes PIN change requests and communicates with HSM and P1C.
4. **HSM (Hardware Security Module):**
    - Encrypts the PIN using cryptographic keys.
    - Ensures the security of PINs during transmission and storage.
5. **P1C (PaymentOne Cards):**
    - A backend system that manages card operations.
    - Updates the PIN offset for the card.

Security Measures

- **Encryption:** PINs and other sensitive data are encrypted using AES (Advanced Encryption Standard) while in transit between the client's system and the CSP server.
- **Secure Connections:** Data transmission uses secure lines such as VPN or mutual TLS to prevent unauthorized access.
- **Validation:** Requests are validated for correct parameters to ensure they originate from authenticated users.

How CSP is Related to MPMS

CSP is part of the broader MPMS (Mobile Payment Management System) suite. Specific services within CSP, such as `MpmsSetPIN` and `MpmsGetPIN`, are customized for MPMS, allowing secure fetching and setting of PINs for cards managed within the MPMS system. This integration ensures that users of MPMS can securely manage their card PINs directly through the CSP application.

Key Components and Services

1. **SetCSP**:
    - This service allows users to set a new PIN for their card without needing the old PIN.
    - Process:
        1. The user accesses the Internet Banking application.
        2. They enter a new PIN, which is sent to the client's server and then to the CSP server via a secure line.
        3. The CSP server encrypts the PIN and sends it to the PaymentOne Cards (P1C) system.
2. **MpmsSetPIN**:
    - This service sets the PIN for a given card.
    - Process:
        1. The client's application sends an encrypted PIN and card information to the CSP server.

        2. The CSP server decrypts the PIN, interacts with the HSM to create an encrypted PIN block, and sends this block to P1C to set the PIN.
    - The request must include an operator ID, PAN (Primary Account Number), and encrypted PIN.
3. **MpmsGetPIN**:
    - This service retrieves the PIN for a given card.
    - Process:
        1. The client's application sends a request with an encrypted AES key, operator ID, and PAN to the CSP server.
        2. The CSP server decrypts the AES key, retrieves the encrypted PIN block from P1C, decrypts it using the HSM, and returns the encrypted PIN.
4. **CryptSetPIN** and **CryptGetPIN**:
    - These services allow the secure setting and fetching of a PIN, respectively.
    - Sensitive fields in the request and response are encrypted using AES to ensure security during transit.
5. **Vericode**:
    - This service provides an authorization code for end users to make secure PIN-related requests via mobile applications.

Communication and Security

- **Secure Lines**:
    - Most communication occurs through secure lines such as VPN or TLS, secured by client certificates (mutual TLS).
    - Some services are accessible over the public internet, but only with proper authentication (e.g., one-time verification codes).
- **Hardware Security Module (HSM)**:
    - The HSM is crucial for cryptographic operations like PIN encryption and decryption.
    - CSP uses the HSM to create and manage encrypted PIN blocks, ensuring that PINs are never exposed in plaintext.

Connection to MPMS

- **Integration**:
    - The CSP services like MpmsSetPIN and MpmsGetPIN are tailored specifically for the MPMS, ensuring secure PIN management.
    - CSP acts as a middleware, securely handling requests and responses between the client's application and the MPMS.

Detailed Functions

1. **MpmsSetPIN**:
    - **Request**: Contains operator ID, PAN, and an encrypted PIN.
    - **Process**: Validates the request, decrypts the PIN, creates an encrypted PIN block using the HSM, and sends it to P1C.
    - **Response**: Indicates success or failure.

2. **MpmsGetPIN**:
    - **Request**: Contains an encrypted AES key, operator ID, and PAN.
    - **Process**: Decrypts the AES key, retrieves and decrypts the PIN block, encrypts the PIN with the AES key, and returns it.
    - **Response**: Contains the encrypted PIN and possibly a new IV (initialization vector) if needed.

Hardware Security Module (HSM)

What is an HSM?

A **Hardware Security Module (HSM)** is a physical device that provides a highly secure environment for generating, storing, and managing cryptographic keys and performing encryption and decryption operations. It is designed to protect sensitive data and ensure that cryptographic processes are executed in a secure manner, preventing unauthorized access and tampering.

Key Functions of an HSM:

1. **Key Management**:
    - **Generation**: HSMs generate cryptographic keys using secure algorithms.
    - **Storage**: Keys are stored securely within the HSM, protecting them from exposure.
    - **Distribution**: HSMs manage the secure distribution of keys to authorized entities.
2. **Encryption and Decryption**:
    - HSMs perform encryption and decryption operations, ensuring that sensitive data remains confidential during transmission and storage.
3. **Cryptographic Operations**:
    - HSMs support various cryptographic functions, including digital signatures, authentication, and hashing.
4. **Secure Execution**:
    - All cryptographic operations are performed within the secure environment of the HSM, ensuring that sensitive data never leaves the protected boundaries of the device.

How HSM Works in the Context of CSP and MPMS

1. **PIN Encryption and Decryption**:
    - When a customer selects or changes their PIN, the new PIN is sent to the CSP server.
    - The CSP server sends the PIN to the HSM, where it is encrypted using a secure cryptographic key.
    - The encrypted PIN block is then sent to the P1C (PaymentOne Cards) system for storage and future use.
2. **Creating Encrypted PIN Blocks**:

    - **Process**:
        - The CSP server sends the plaintext PIN to the HSM.
        - The HSM uses its cryptographic keys to encrypt the PIN.
        - The encrypted PIN block is returned to the CSP server, which then forwards it to the P1C system.
3. **Validating PINs**:
    - When a PIN needs to be validated (e.g., during a transaction), the encrypted PIN block is retrieved from the P1C system and sent to the HSM.
    - The HSM decrypts the PIN block and verifies it against the entered PIN.
4. **Securing Communication**:
    - All communications between the CSP server and the HSM are conducted over secure channels to prevent interception and tampering.
    - The HSM ensures that cryptographic keys and sensitive data remain protected at all times.

Technical Aspects of HSM:

1. **Tamper-Resistance**:
    - HSMs are designed to be tamper-resistant. Any attempt to physically interfere with the device triggers protective mechanisms that zeroize (erase) the cryptographic keys and sensitive data.
2. **High Assurance**:
    - HSMs comply with stringent security standards (such as FIPS 140-2 or 140-3) to ensure high levels of security and trustworthiness.
3. **Performance**:
    - HSMs are optimized for high performance, capable of handling a large volume of cryptographic operations efficiently, which is crucial for applications like payment processing.
4. **Isolation**:
    - The secure environment of the HSM isolates cryptographic operations from the rest of the system, reducing the risk of data breaches.

Types of Keys Used in HSM

1. ZPK (Zone PIN Key)

- **Purpose**: ZPK is used to encrypt and decrypt PINs (Personal Identification Numbers) during their transmission between different zones, such as from an ATM to the central server.
- **Function**: Ensures that PINs remain secure while being transmitted across various parts of the banking network.
- **Operation**:
    - When a customer enters their PIN at an ATM, the PIN is encrypted using the ZPK before being sent to the central server.

    - The central server uses the corresponding ZPK to decrypt the PIN and verify it against the stored value.

2. PVK (PIN Verification Key)

- **Purpose**: PVK is used to generate and verify PINs. It plays a critical role in ensuring that the PIN entered by the user matches the PIN on record.
- **Function**: Enables the secure creation and verification of PINs without exposing the actual PIN.
- **Operation**:
    - When a new card is issued, a PIN is generated using the PVK and stored securely.
    - During a transaction, the entered PIN is encrypted and compared to the stored PIN. The PVK helps in verifying the match without revealing the actual PIN.

Other Common Keys in HSMs

3. KEK (Key Encryption Key)

- **Purpose**: KEK is used to encrypt other cryptographic keys, ensuring that they can be securely stored and transmitted.
- **Function**: Protects keys during key exchange processes, making sure that only authorized entities can access them.
- **Operation**:
    - When a new key is generated, it is encrypted with a KEK before being stored or sent to another HSM.

4. DEK (Data Encryption Key)

- **Purpose**: DEK is used to encrypt and decrypt sensitive data.
- **Function**: Ensures that data remains secure both at rest and in transit.
- **Operation**:
    - Sensitive data, such as transaction details or personal information, is encrypted using a DEK before being stored in a database.

How These Keys Work Together

In a payment processing system, these keys are used in conjunction to provide a secure environment for handling sensitive information. Here's an example scenario involving ZPK and PVK:

1. **PIN Entry and Encryption**:
    - A customer enters their PIN at an ATM.
    - The ATM uses the ZPK to encrypt the entered PIN and sends it to the central server.
2. **PIN Decryption and Verification**:
    - The central server receives the encrypted PIN and decrypts it using the ZPK.

    - The server then uses the PVK to verify that the decrypted PIN matches the stored PIN.
3. **Transaction Processing**:
    - If the PIN is verified, the transaction proceeds.
    - The DEK may be used to encrypt sensitive transaction details before storing them in the database.
4. **Key Management**:
    - The KEK is used to securely store and transmit the ZPK, PVK, and DEK, ensuring that these keys remain protected.

Summary of CSP, HSM, and Key Functions in MPMS

Customer Selected PIN (CSP)

- **Definition**: CSP stands for Customer Selected PIN, a service that allows users to set or change their card PIN securely.
- **Process**:
    1. Users log into their banking application and navigate to the PIN management section.
    2. The new PIN is entered and transmitted securely to the CSP server.
    3. The CSP server processes the request, encrypts the PIN using HSM, and updates the card's PIN in the PaymentOne Cards (P1C) system.

Hardware Security Module (HSM)

- **Definition**: An HSM is a physical device designed to manage cryptographic keys and perform encryption and decryption operations securely.
- **Functions**:
    1. **Key Management**: Generates, stores, and manages cryptographic keys.
    2. **Encryption and Decryption**: Performs secure cryptographic operations.
    3. **Secure Execution**: Ensures all cryptographic processes occur within a protected environment to prevent unauthorized access.

Key Types in HSM

1. **ZPK (Zone PIN Key)**:
    - Used for encrypting and decrypting PINs during transmission between different zones.
    - Ensures PINs remain secure while being transferred.
2. **PVK (PIN Verification Key)**:
    - Used for generating and verifying PINs.
    - Ensures that the entered PIN matches the stored PIN securely.
3. **KEK (Key Encryption Key)**:
    - Used to encrypt other cryptographic keys.
    - Protects keys during storage and transmission.

4. **DEK (Data Encryption Key)**:
    - Used to encrypt and decrypt sensitive data.
    - Ensures data security both at rest and in transit.

How CSP and HSM Work Together in MPMS

- **Integration**:
    - CSP services like `MpmsSetPIN` and `MpmsGetPIN` are integrated with MPMS to manage card PINs securely.
    - The CSP server communicates with the HSM to encrypt/decrypt PINs and with P1C to update or retrieve the PINs.
- **Security Measures**:
    - **Encryption**: All sensitive data and keys are encrypted using secure algorithms.
    - **Secure Communication**: Data transmission uses secure channels like VPN or TLS to prevent unauthorized access.
    - **Validation**: Requests are validated to ensure they originate from authenticated users.

Detailed Functionality of CSP Services

1. **MpmsSetPIN**:
    - Sets a new PIN for a given card.
    - Validates request parameters, encrypts the PIN using HSM, and updates P1C.
2. **MpmsGetPIN**:
    - Retrieves the encrypted PIN for a given card.
    - Decrypts the PIN using HSM and returns it securely.

Overall Summary

CSP (Customer Selected PIN) allows customers to securely set or change their card PINs, leveraging HSM (Hardware Security Module) to ensure cryptographic operations are performed in a secure environment. HSM manages various types of keys like ZPK, PVK, KEK, and DEK to protect sensitive information during storage and transmission. Integrated with MPMS, CSP services use secure communication and encryption to handle PIN management tasks efficiently and securely, providing robust security for online banking and payment systems.