Host Card Emulation (HCE) Issuer Owned Wallets

An alternative way to implement digital wallets.

Digital wallets are a mobile-based payment capability that allows Card Members to tap-and-pay with their mobile devices or wearables at contactless-enabled Point-of-Sale (POS) terminals or within a Merchant's online payment app.

Mobile payments are used for both high-and low-value transactions. It's a more secure payment tool for Card Members and Merchants than legacy mag-stripe acceptance, with the expected security of EMV® chip transactions plus the added protection of tokens and CDCVM* at the device level, all working together to reduce the risk of fraud.

American Express can help Issuers deploy their own wallet beyond the third-party wallet solutions. Issuers can integrate the HCE functionality into their existing bank app or create a standalone HCE wallet. In both solutions, the payment credentials are sent securely from the cloud to the device.

*Consumer Device Cardholder Verification Method (CDCVM)

Here's How It Works

1

Card Members can download the Issuer's payment app, enroll, and then upload their American Express® Card in the Issuer's mobile wallet.

2

Card Members can use their HCE Issuer Mobile Wallet whenever they see the Contactless Symbol and American Express logo.

3

Card Members can tap their device in front of the card terminal to pay.

4

After secure radio frequencies transfer the data between the Card Member's device and the contactless terminal, the purchase is complete.

HCE: Architecture and Security

HCE Architecture:

HCE-based payments use cloud servers to store payment credentials (vs. on the Card Member's device), helping to make transactions fast, secure and touch free.

- **Account Data** – Stored on a secure cloud server.
- **Payment Application** – Once the Card Member adds their Card to the wallet, tokenized account data from the secure cloud will be obtained. The token data will then be permanently added to the wallet for future payments.
- **Near Field Communication (NFC) Controller** – Transmits the payment information to the contactless Point-of-Sale terminal.

HCE Security:

Security against unauthorized account access in HCE relies on three provisions:

- **Limited Use Keys (LUKs)** – Each transaction is assigned a LUK with an expiry date; these can be managed according to the Issuer's risk parameters.
- **Tokenization** – A unique surrogate value will be used to conduct payment transactions. The token is restricted in how it can be used with specific devices, Merchants, transaction types or under other conditions.
- **Cardholder Verification Method (CVM)** – In addition to PIN or Signature, digital wallets also allow Card Members to use their biometric logins (e.g., fingerprint, facial recognition) or a passcode on their phone to unlock the mobile wallet; the CVM helps ensure transactions are initiated only by authorized user devices.

Getting Started: The Enablement Journey*

1. INVITATION

4–5 Weeks

- Kickoff Meeting
- Documentation shared with Issuer
- Data Collection Forms/ Requirement Gathering
- Agreements: Between Issuer & Wallet Provider/Issuer & AMEX
- Engage Project Teams

2. SET-UP AND ENABLEMENT

6–8 Weeks

- Token Bin Request* (~ 3 weeks)
- Operational and Technical Setup (including Issuer's Internal Tech Development)
- API Connectivity Setup
- Network Servicing Portal (NSP) & SSO setup
- Card Assets (Art and Terms & Conditions)

3. TESTING AND ROLLOUT

6–8 Weeks

- API Certification
- In-App Provisioning testing (If Applicable)
- ISO Messages and Batch File Certification
- Production Implementation
- In-App provisioning Key Exchange (If Applicable)
- Security Evaluation (with External Labs)
- Function Certification (with External Labs)

4. BETA TESTING AND LAUNCH

2–3 Weeks

- Production Beta
- Card Personalization Testing (internal to American Express)

*Please note this schedule is a sample; timelines are dependent on partner readiness and engagement.

Additional Services

Guides and Specifications

Guides, specifications, and a Software Developer Kit (SDK) are available to assist in enabling payment functionality on an HCE app.

Certification and Approval

Access documentation required to certify products and services for use on the American Express Global Network.

Technical Assistance

American Express is available to assist with technical queries and provide best practices acquired from previous HCE solutions and wallet projects launched across the globe.

Assistance with Commercial Launch

Assistance in marketing efforts to accelerate adoption of products or services.

Implementation and Investment: Considerations for the Issuer

- Evaluate the maturity of the region's mobile device landscape and the contactless acceptance coverage.
- Determine a project plan for integrating existing Issuer payment apps or the mobile wallet and include the development of the user interface that meets the security requirements.
- Decide whether to utilize American Express' On Behalf Of (OBO) services or Issuer solutions.
- Explore integration of the Issuer back-end to support the mobile wallet functions.
- Define the customer care and servicing model. Plan and develop Card Member communication.
- Consider certification requirements:
  - A mobile application where a payment method is included will require certification via approved labs both for functionality and security.
  - Payment applications must be EMVCo® approved.

Learn More and Go Mobile

To learn more about HCE and mobile wallet payments go to amexglobalnetwork.com or contact your American Express representative.

DON'T do business WITHOUT IT℠