Fact Sheet

Host Card Emulation

Secure and manage your host card emulation-based mobile wallet with a single, end-to-end software solution

Secure Element in the Cloud (SEiTC) for host card emulation (HCE) gives issuers control and exclusivity over customer relationships with their own-label mobile wallets. Managing tokenization in-house removes the need for intermediaries to issue payment credentials. SEiTC eliminates domain fees and simplifies partner integration to provide value-added services, such as loyalty and couponing, more easily. Utilizing the cloud, roll-out of new payment flows such as peer-to-peer, contactless and digital payments are quicker and more secure.

Potential benefits

Tailor your solution

Choose whether to integrate with Token Gateway Service (TGS) in line with business and technical requirements.

Simplify partner integration

The single, unified TGS API removes integration complexity with multiple token service providers (TSPs).

Plug-in to payment schemes

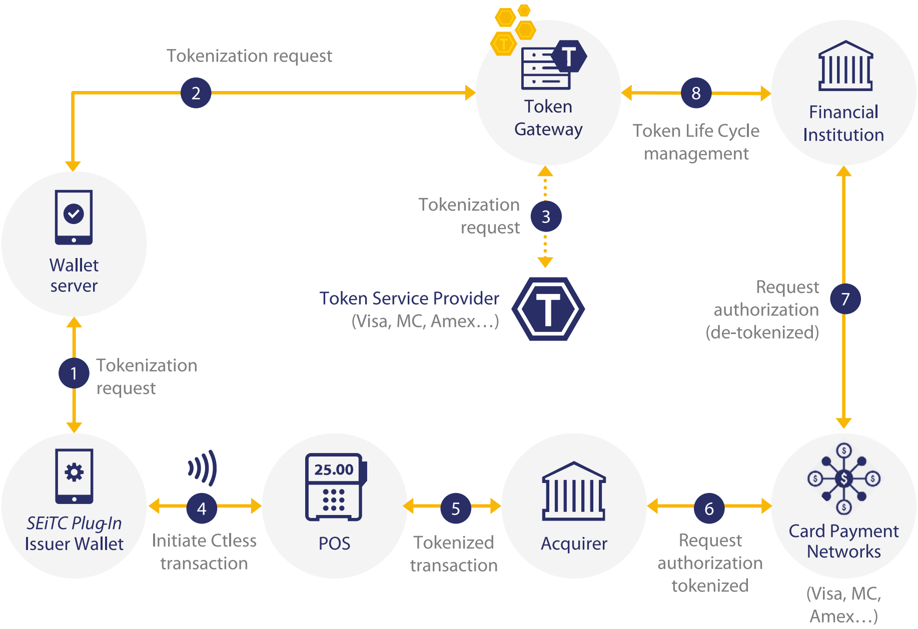
Support multiple international payment schemes instantly with a scheme-agnostic and certified platform.

Enhance digital payments

Protect and enrich the customer payment experience with tokenization while retaining full brand visibility and relationship control.

How it works

Unlock the benefits of SEiTC for HCE in-house or with TGS which provides a single, unified point of connection to multiple TSPs. TGS for HCE enables issuers to manage the role of Token Requestor and deploy contactless payment credentials to their customers.



1. The first step shows the initial token request from a token requestor such as an issuer mobile wallet to the wallet server
2. The tokenization request is routed to TGS which then requests a token from the appropriate TSP
3. The TSP generates and issues the payment token(s), which are routed back to the issuer wallet via TGS and the wallet server
4. As a contactless transaction is performed, a token is passed to the merchant POS
5. The tokenized transaction is passed from the merchant to the acquirer
6. The acquirer passes a tokenized authorization request to the payment network
7. The payment network sends a de-tokenized authorization request to the issuer
8. The issuer sends a detokenization request to the TSP and performs payment processing and approval authorization. The authorization is passed back along the transaction flow to the merchant and the payment is completed

Features

End-to-end solution

A two-part solution: a server where virtual cards are managed, and a plug-in to provision payloads to the mobile device.

Legacy system interoperability

Support international and domestic payment schemes without upgrading existing payment acceptance infrastructure.

Integration with Token Gateway Service

Provision HCE payment credentials for all leading network TSPs via a single, simplified integration.

Certified solution

Align instantly with payment network and global body requirements to perform compliant cloud-based mobile payments.

Offline transaction support

Provision payloads in advance to enable payments when the consumer device cannot connect to the server.

Learn more

For more information, contact your Visa Account Executive or **click here to fill out our online enquiry form**

Please note, all diagrams are presented for illustrative purposes only.