ACI TOKEN MANAGER™ FOR MOBILE: TOKEN SERVICE PROVISION, HCE AND EMBEDDED SECURE ELEMENT IN THE CLOUD

- Enable full support of the mobile payments process for embedded secure element, host cloud emulation or both
- Increase security of mobile payments through tokenization
- Manage the entire lifecycle of payment credentials

Mobile cloud payments using host card emulation (HCE) technology have become an attractive alternative to the traditional secure element (SE) near-field-communication (NFC) model for delivering mobile services. While the hardware-based (SE) model is currently recognized as more secure, it is also more complex and expensive. For this reason, additional security measures have been introduced to the cloud model to reduce risk. Tokenization technology has been brought forward to keep card data safe during transactions.
Tokenization reduces the value of payment credentials by replacing the need for merchants or digital wallet operators to store primary account numbers (PANs). Instead, a unique identifier called a “payment token” is provided, reducing the value of the credentials to hackers. These payment tokens can only be used in a specific domain (such as a merchant’s website) or a channel (a mobile device to make an NFC payment, for example).

Secure token vault with a link between the PAN and the token value

WHAT IS A TOKEN SERVICE PROVIDER?

A token service provider is an entity within the payments ecosystem that is able to provide registered token requestors — such as merchants holding card credentials — with “surrogate” PAN values, known as payment tokens.

A token service provider stores PAN values in a token vault, replaces these with tokens and issues these for token requestors.

The token service provider can be independent from the payments network or payments processor, or alternatively can be integrated with one or both of these entities. Token service providers are responsible for a number of functions. They oversee the ongoing operation and maintenance of the token vault, deployment of security measures and controls, and the registration process of allowed token requestors.

In this new age of mobile payments, a token service provider solution must enable the implementer to issue and manage the entire lifecycle of payment credentials, implement tokenization to reduce payment card fraud and manage transactions to integrate with the existing authorization host by validating cryptograms as well as performing functions like processing checks.
The issuance and remote management of the payment credentials provided by token service providers must comply with specifications defined by the global payment schemes; this can take place in the cloud using HCE or on a smartphone inside a secure element.

WHY BECOME A TOKEN SERVICE PROVIDER?

There are a number of reasons why entities like issuing banks would consider becoming a token service provider and issue their own tokens. The most important are outlined below.

REDUCED PAYMENT NETWORK SERVICE FEES
Issuing and managing tokens internally means the provider will not have to request tokens from a third party, saving service fees.

INCREASED SECURITY
Since providers won’t have to integrate with any third parties to perform this service, security is increased. They keep full control of the original PAN number, do not have to share it and don’t need to integrate with external systems.

REDUCED TIME TO MARKET
Controlling their own token vault means that providers can determine when and where to launch their tokenized services.

FLEXIBILITY TO EXPAND TO OTHER USES
Being a token service provider ensures that organizations can further strengthen security by deploying tokens within other use cases. This includes embedded secure elements in mobile devices, the cloud, eCommerce or card on-file scenarios.

ACI SOLUTION OVERVIEW

ACI Worldwide, in partnership with Bell ID, offers one software platform that enables organizations to perform the responsibilities of a token service provider, as outlined by EMVCo. The role includes the generation and issuance of payment tokens, as well as the operation and maintenance of a token vault. ACI Token Service Provider is a modular platform that can also enable organizations to perform a wide range of other roles in the payments process, such as loading and managing credentials on mobile devices, as well as into the cloud. It also enables the use of tokenization in other scenarios such as eCommerce transactions. The next page shows some of the key capabilities provided by ACI’s platform, with individual modular functionality outlined in more detail.
TRANSACTION MANAGEMENT

Transaction management enables issuers to perform transactions without making major changes to the authorization host. It calculates cryptogram version numbers (CVNs) on behalf of the authorization host.

ACI’s transaction management component calculates cryptogram version numbers on behalf of the authorization host.

- **Cryptogram validation**: Validates the cryptogram as part of the authorization request
- **Assurance level validation**: Provides assurance levels, e.g., account verification, risk score and card issuer authentication
- **PAN processing**: Provides the issuer with the PAN in case tokens are used
- **Messaging**: Supports different types of messaging interfaces (ISO 8583, SOAP and JMS)

TOKENIZATION MANAGEMENT

This process helps organizations reduce fraud by removing confidential consumer card data from the payments network, replacing it with unique tokens which are limited in how they can be used.

- **Tokenization**: Replaces the PAN with a surrogate value, includes both card-present and card-not-present tokens for e.g., card on-file scenarios
- **Token vault**: Establishes/maintains payment token-to-PAN mapping
- **De-tokenization**: Converts the token back to the PAN via the token vault
- **Domain management**: Adds additional security by restricting tokens to use within specific (retail) channels or domains
- **Clearing and settlement support**: Provides ad-hoc de-tokenization for the clearing and settlement processes
- **Identification and verification support**: Ensures that the payment token is replacing a PAN that was legitimately used by the token requestor
The tokenization management component by ACI offers the functionality to issue and manage an organization’s own tokens.

**PHYSICAL SECURE ELEMENT MANAGEMENT**

Banks and service providers can issue contactless payment cards and provision static card data and dynamic key material to a physical SE on a mobile device. The platform is compliant with all trusted service manager standards.

Managing physical secure elements is needed on mobile operating systems where cloud-based mobile payments are not (yet) supported.

- **Service delivery**: Provide over-the-air (OTA) personalization of secure elements, such as UICC/SIM, smart microSD or embedded; protocols supported are SMS-PP, CATP-TP and RAM over HTTP
- **Messaging**: Provides integration with other TSM actors using messaging-based communication protocols such as GlobalPlatform Messaging and AFSCM
- **Service management**: Provides full management of the services deployed on the physical SE

---

**CLOUD-BASED MOBILE PAYMENTS MANAGEMENT**

By issuing and managing cloud-based payment cards, organizations can allow end users to perform NFC transactions based on HCE. This module aligns with the cloud-based specifications by American Express, MasterCard and Visa. It also includes a plug-in to the mobile wallet.

- **HCE payments**: Implements the cloud-based payment specifications from all major payment schemes
- **Credential management**: Manages the system credentials by replenishing static and dynamic card data (payloads)
- **Consumer enrollment**: Enrolls cards on the mobile device using a secure channel
- **Lifecycle management**: Manages the lifecycle of cards and cryptographic keys
- **Notification services**: Enables push notifications to the mobile devices to trigger the connection
- **Wallet integration**: Provides integration services for wallet providers

---

1. Real-time and/or batch file import of card and personalization data
2. EMV command and cryptogram generation (key management/HSM)
3. Secure connection
4. An ACI client API SDK allows for a smooth integration to existing (mobile wallet) applications
ACI Worldwide, the Universal Payments company, powers electronic payments and banking for more than 5,600 financial institutions, retailers, billers and processors around the world. ACI software processes $13 trillion each day in payments and securities transactions for more than 300 of the leading global retailers, and 18 of the world’s 20 largest banks. Universal Payments — UP — is ACI’s strategy to deliver the industry’s broadest, most unified end-to-end enterprise payment solutions. Through our comprehensive suite of software products and hosted services, we deliver solutions for payments processing; card and merchant management; online banking; mobile, branch and voice banking; fraud detection; trade finance; and electronic bill presentment and payment. To learn more about ACI, please visit www.aciworldwide.com. You can also find us on Twitter @ACI_Worldwide.