Making Cloud-Based Mobile Payments a Reality with Digital Issuance, Tokenization, and HCE
Why Cloud-Based Mobile Payments?

The promise of mobile payments has captured the imagination of banks, mobile operators, merchants, and consumers for over a decade. Yet time and time again initiatives have failed or fallen short because of business and technological hurdles that impede the innovation and collaboration that is necessary for real success.

To date, mobile payments have depended on the secure element (SE) to store secure credentials on mobile phones. Secure elements themselves have been contentious in mobile payment deployments since they force issuers to work on a single platform usually owned by another entity in a business relationship that may or may be beneficial to the credential issuer.

A Game Changing Innovation

Google’s announcement of NFC Host Card Emulation (HCE) support in Android is being called a game changing innovation. HCE enables a normal Android app to perform the application functions of a secure element by relying on secure cloud storage for the account credentials instead of a secure chip in the phone. Today any NFC-enabled Android 4.4 and Blackberry 10 phone can perform HCE. More announcements about HCE support from other OEMs are expected in the coming months.

The significance of HCE is the independence from secure elements it gives issuers that want to enable apps for mobile payments. Instead, apps use cloud-based digital cards to make EMV-compliant payments at the point of sale. This new technology opens a number of opportunities for issuers to enable mobile payments and wallet services to their customers. HCE returns control over payment issuance and user experience back to the card issuers.

Cloud Digital Issuance is the Key

To make secure cloud-based mobile payments possible, there has to be digital issuance systems capable of securely storing credentials in the cloud, issuing them to mobile apps, and providing secure access to those credentials to trusted apps in the phone. Digital issuance systems must manage tokens downloaded to mobile phones in lieu of real card data for payment transactions.
The Benefits of Cloud-based Mobile Payments

Cloud-based mobile payments bring a number of benefits to credential issuers.

- **Open and flexible**: Cloud-based mobile payments open multiple opportunities to deploy services to consumers using flexible business models.

- **Unlock issuer brand value**: Issuers have direct control over branding and user experience.

- **No ecosystem dependency**: Cloud-based mobile payments require fewer intermediaries, speeding time to market and giving issuers more control of the launch and project.

- **Security**: By relying on approved vendors that provide completely secure environments and advanced tokenization methods, issuers can achieve high security levels for card data.

- **Visa and MasterCard endorsed**: Cloud-based mobile payments have been endorsed by both major card associations. Standards, requirements and program approval processes are being defined to enable financial institutions to securely host digital cards in the cloud.
The Challenges

Cloud and HCE promise to unlock the benefits of mobile payments for multiple stakeholders. However, the implementation of a secure system for cloud-based payments has the potential for major liabilities for issuers if not handled properly.

- **Security in smart phone memory:** In order for transactions to be performed at merchant POS systems, even without network coverage, the issuing bank must provision digital card details to the phone’s memory. Details such as a card holder’s name and account number must be stored in unsecure phone memory. Tokenization only partly addresses this problem.

- **Generic tokenization standards:** Common tokenization solutions create their own issues if not done properly. By replacing the real card data with randomized account details these tokens represent actual account details stored in the cloud. The actual cardholder data is never stored in phone memory, not even in encrypted form. The problem is that in most available tokenization schemes the card data becomes so generic that processors can’t identify if card accounts are linked to rewards programs.

- **Security and standards compliance:** Digital Issuance vendors handle the same sensitive data as plastic issuer providers. Banks and other issuers should be working with approved vendors by the main card associations that are compliant with EMV, PCI and other major payments standards.

- **Risk and fraud management:** Using mobile devices and cloud to perform transactions creates both challenges and opportunities for issuers on risk management. Mobile payment using connected devices gives a new meaning to fraud and risk management. On the one hand, there are challenges with mobile devices that have limited security against threats such as malware sniffing card data while on the other hand, rich contextual data creates new risk management opportunities for issuers. Legacy risk management systems are not designed to handle dynamic, contextual data from connected devices.

- **App and user experience:** Consumers want the choice to pay using a bank app, a merchant app, or other favorite app. This expectation by consumers requires a management platform to enforce configuration and business rules. Rules and procedures must define which apps can access which credentials so that the right apps can perform transactions at the point of sale and user experience is seamless across multiple apps.
Sequent Digital Issuance

Sequent Digital Issuance solution for edge issuance (secure element based) has been in the market for over three years, deployed in commercial and pre-commercial environments at large banks and perso bureaus globally.

Extending Secure Digital Issuance to the Cloud

Sequent is now extending its PCI-compliant and Visa approved Digital Issuance solution for cloud. Sequent’s Digital Issuance solution for the cloud enables financial institutions, hospitality providers, merchants, and other card issuers to issue digital cards securely from cloud-based servers to any mobile device. The Sequent Digital Issuance for the cloud provides advanced HCE-based account issuance with features that address the biggest issues related to cloud-based mobile payments:

Features:

- **Tokenization and on-device middleware for secured phone memory:** Sequent’s Tokenization Service supports the mapping of tokenized credentials to real cardholder data, in real-time, during authorization and settlement. Not relying on tokenization alone, Sequent’s on-device software manages security of card data, one-time use keys, and other confidential user data in the phone.

- **Issuer-specific token formats:** Sequent tokenization strategy works with genuine card data. Our tokenization system replaces a portion of the account data with randomized details, but works with the issuer so that tokenized accounts remain recognizable to acquiring systems, gateways, networks, and issuer processors.

- **Advanced risk management:** Sequent’s patent-pending risk scoring solution further reduces issuer’s risk of fraud from lost, stolen, compromised devices, or stolen transaction data. As part of a comprehensive risk-management strategy, these tools strengthen the issuer’s confidence and ability to compartmentalize mobile payment risk without burdening the cardholder.

- **Built-in app and user experience:** Sequent’s innovative and patented Wallet Wizard combined with SDK allows banks, merchants, and other developers to turn their existing mobile apps into wallets. It creates a policy-driven link between bank-issued payment credentials and trusted mobile applications.

- **Bank-level security on all products:** Sequent designs, builds, and operates its products and services to the highest level of commercial security. Sequent production environment is PCI DSS and EMV compliant, and is a compliant and approved over-the-air (OTA) perso bureau.
Sequent Digital Issuance supports card issuance to mobile devices using Cloud with HCE or Secure Element for flexible deployment options in different environments, with different partners and with all technologies.

- **In the cloud, on the phone, everywhere:** Securely issue digital cards to the cloud using tokenization and HCE or to mobile phones with secure elements.

- **All card types:** Provision any card or credential including credit, debit, prepaid, transit, access control, loyalty, coupons, and offers.

- **All standards:** Sequent Digital Issuance systems are compatible with EMVCo, Visa, MasterCard, and non-payment standards such as Mifare 4 Mobile.

- **All redemption technologies:** Broad set of redemption options such as NFC, QR code, or bar code.
Why Sequent?

Sequent is the world’s leading provider of digital issuance and open wallet platform-as-a-service that delivers secure mobile payments and value-added services to banks, mobile operators, merchants and access control providers. With Sequent, customers can offer wallet services open to an ecosystem of partners and developers, while meeting the requirements of highly secure and regulated industries. Sequent products include: Sequent Open Wallet Platform, Digital Issuance and Trust Authority. Sequent is endorsed and used by major customers on four continents.