Samsung Pay Will Transform the Mobile Wallet Experience

What You Need to Know

Gartner Research: Market Trends: Cloud Solutions and Digital Commerce will Drive Mobile Payment Adoption

Gartner Research: Innovation Insight: Issuer Tokenization Secures and Enhances Future Payment Services

About Samsung Electronics Co., Ltd.
Samsung Pay Will Transform the Mobile Wallet Experience: What You Need to Know

This summer, Samsung will launch Samsung Pay, a mobile payment service for Samsung Galaxy S6 and Galaxy S6 edge. Samsung’s entry into the nascent but increasingly crowded mobile payment space is poised to make a splash given its global reach and strong line-up of financial and retail vendors. Here’s what you need to know about the service, and the changes in store for both consumers and businesses.

When it launches, Samsung Pay will have the potential to be a point-of-sale payment option at approximately 30 million merchant locations worldwide, making it the only mobile payment solution with near universal acceptance. Samsung has already announced a strong partnership list that includes MasterCard, Visa, American Express, Bank of America, Citibank, JPMorgan Chase, and U.S. Bank. Samsung Pay users will have access to more merchants than other competing mobile payment services, utilizing near field communication (NFC) and Samsung’s secure Magnetic Secure Transmission (MST) technologies to support both legacy and modern payment card options.

Mobile Payment Trends

Samsung’s entry into the mobile payment/smart wallet space comes at a significant point in the adoption of mobile payment and commerce. More people than ever are participating in the global economy, in large part due to new digital tools that are available through mobile devices. The rise of digital banking, finance and payments represents a major trend which, over the next several years, will transform economies worldwide.

On April of this year, the World Bank announced that 700 million unbanked adults worldwide became account holders between 2011 and 2014; a 20 percent drop in the number of unbanked. This continuing progress toward a more-inclusive global economy is due in large part to the availability of mobile money accounts.

To meet the needs and challenges that accompany the rapid rise of mobile finance, financial institutions, mobile carriers and policy makers are working to put the necessary structures and practices in place that will enable people to participate actively in a digital economy. According to MasterCard’s Hemant Baijal, these include a legal and regulatory framework; a robust business case for large-scale investments in mobile money services; global standards to help establish vibrant mobile ecosystems; and mature B2C program management practices.

Samsung has long been a leader in creating the conditions necessary for mobile innovation to flourish, and enabling consumers to actively take full advantage of these innovations. The same is true as it enters the world of mobile payments and commerce.

How Samsung Pay Works

Samsung announced Samsung Pay at the GSMA Mobile World Congress 2015 in Barcelona, Spain. It will initially be available this summer on Samsung Galaxy S6 and Galaxy S6 edge mobile devices in the United States and Korea, and will expand to other regions including Europe and China.

When a consumer activates the app, they will first add their credit and debit cards to the app. Then, when they are at a point of sale, they will swipe up from the bezel to invoke the Samsung Pay app, choose the desired payment card, and authenticate. Tapping the device to the point-of-sale (POS) terminals allows for a fast, secure, and easy purchase.
New Technology

Consumers who use Samsung Pay can make secure mobile payments at nearly all merchant locations, via existing point-of-sale terminals. This compatibility with existing terminals is a key feature, made possible through Magnetic Secure Transmission (MST): a new, proprietary technology that makes Samsung Pay usable in merchant locations regardless of whether the terminals support NFC or traditional magstripe (the vast majority of existing terminals.)

Samsung Galaxy S6 and Galaxy S6 edge smartphones in the United States and South Korea have built-in MST technology to enable contactless payment over existing payment infrastructures. This enables Samsung Pay to emulate a card swipe by sending tokenized payment credentials from the device to a payment terminal via an electromagnetic field, within a 5cm distance from the card reader.

MST technology also enables Samsung Pay to support a wide range of payment cards, including private label credit cards. These cards, which give owners access to a line of credit at specific retailers, can be added to Samsung Pay and processed at the point of sale in the same manner as other cards, providing consumers with a seamless shopping experience.

Security and Fraud Prevention

Security is a major concern for mobile payments, particularly at the point of sale. Samsung Pay provides enhanced security with the Samsung KNOX™ mobile security platform and ARM TrustZone®, both of which help protect transaction information from fraud and data attacks. In addition, Samsung’s Find My Mobile feature enables users to locate, lock and wipe lost devices remotely, before their data falls into the hands of fraudsters.

Issuer Tokenization

Samsung Pay’s security is further reinforced with tokenization: a fraud-prevention technology which replaces sensitive card data with a unique, secure token. According to Gartner’s 2015 Innovation Insight report on the topic states that, “Issuer tokenization will be one of the most important technologies to impact the payment industry in coming years.” By taking advantage of the benefits issuer tokenization offers, Samsung is an early adopter in supporting new use cases and form factors in mobile payments.

Among its benefits, issuer tokenization:

- Enhances transaction security regardless of the underlying payment methods or technology
- Gives issuers greater control and flexibility in risk management
- Provides users with an easy registration process in which tokens can be provisioned quickly over the air, with no need to download new software or plug-ins
- Allows users to continue to pay with the same plastic card, and use other devices if one device is lost or stolen.

The Potential Impact of Samsung Pay

In a recent Market Trends report on mobile payment adoption, Gartner stated, “Enabling digital commerce in the physical world is conducive to mobile payment adoption when delivering good value and user experience... We expect merchandise purchase using mobile devices to reach more than $400 billion in 2018, accounting for 44% of total mobile payment transaction, up from 35% in 2013.”

However, in the same report Gartner also noted, “Consumers won’t use mobile payment just because it is mobile. They need a reason to make the switch. The service should bring good enough benefits to show value in the form of convenience, low cost, better security or new capabilities.”

Samsung has focused heavily on providing user value through Samsung Pay, a strategy which is expected to dramatically accelerate the adoption of mobile payments and e-commerce once the service is launched. The advantages of Samsung Pay to both consumers and businesses are evident in benefits such as:
• Providing a native mobile payment solution leveraging both NFC and MST at nearly all merchant locations.

• Reducing the barrier to entry for merchants by working with existing POS terminals - making it easier for their customers to pay with Samsung Pay.

• Bringing easy, secure mobile payments to private label credit card companies and their retailers – for example, Synchrony Financial, a company with 60 million active accounts.

• Creating new global opportunities through its extensive ecosystem, enabling future collaboration with financial technology companies.

**Summary**

When Samsung Pay was announced, Jong-Kyun Shin, CEO and Head of IT & Mobile Communications Division at Samsung Electronics, said, “Samsung Pay will reinvent how people pay for goods and services and transform how they use their smartphones. The secure and simple payment process, coupled with our robust partner network, makes Samsung Pay a truly game-changing service that will bring value to consumers and our partners in the ecosystem.”

Samsung is an important new player in the mobile payment and e-commerce space. It has laid the groundwork for success through the security, broad terminal compatibility and ease of use of its technology; as well as its powerful slate of global partnerships. All eyes will be on the company this summer when Samsung Pay debuts, and a new era of mobile payments begins.

*Source: Samsung*

---

Digital commerce will lead to use cases that are conducive for mobile payment adoption, while cloud solutions remove some adoption hurdles by making the service ride on existing infrastructure. Mobile payment solution provider product managers need to make payment frictionless to make it successful.

Key Findings

- Enabling digital commerce in the physical world is conducive to mobile payment adoption when delivering good value and user experience.
- No single standard will emerge in the foreseeable future, and multiple technologies will coexist to serve a variety of use cases in commerce and engagement where they can best fit.
- Cloud-based mobile payment solutions using SMS and mobile apps will capture the majority of the market share while NFC goes through prolonged evolution cycles.
- Payment alone is not enough to move NFC forward. Nonpayment services such as personal ID, loyalty, access control and transportation should all present on a single device to give consumers a reason to adopt NFC.

Recommendations

- Make payment frictionless to users when they enjoy other services that are enabled by payment such as food and dining, taxi hailing, ticket and travel, and local services.
- Design the solution for specific use cases that bring value to users and merchants in the form of convenience, location-based offers, higher sales and customer engagement for merchants.
- Keep the solution open to new technologies, including but not limited to NFC/HCE, quick response code and Bluetooth Low Energy, to make it future-proof as well as open to third-party solutions to make it versatile.
- Be prepared for dirty work in integrating your solutions with various payment infrastructure such as retail POS systems and terminals, personalization systems, prepaid card networks, and the payment switches and card networks in different markets.

Strategic Planning Assumptions

Mobile payment transactions will grow at a 30% compound annual growth rate (CAGR) in 2013 through 2018 and reach more than $900 billion in 2018.

Mobile commerce will become the second-largest driver of mobile payment, following money transfer, and contribute to about 45% of total transaction value in 2018.

Near Field Communication (NFC) payment will remain a minority factor throughout 2018, accounting for less than 6% of total transaction value in 2018.

Introduction

Gartner defines mobile payment as the service where users make a payment using a mobile device that manages the account and the transaction. The mobile device can be directly or indirectly involved in the payment process such as pay from a mobile app, or pay from an accessory such as a sticker or key fob that is connected to and managed from the mobile device.

Mobile payment remains a high-interest topic for mobile payment technology and service providers (TSPs) where fast-pacing innovation and competition pulls the market in all directions. This brings new opportunities as new services and products deliver benefits to consumers and merchants. At the same time, the market is still in the early stage and needs to cross many hurdles for mass adoption. We expect mobile payment to grow at an annual rate of 30% from 2013 to reach more than $900 billion in 2018.

This report looks at the latest trends in mobile payment, opportunities and challenges, and advises product managers of mobile payment solution providers on product development and market positioning.
Market Trend

Digital Commerce and Engagement Are Key to Mobile Payment Adoption

Consumers won’t use mobile payment just because it is mobile. They need a reason to make the switch. The service should bring good enough benefits to show value in the form of convenience, low cost, better security or new capabilities.

Digital commerce and engagement can lead to new use cases that are conducive for mobile payment adoption. We expect merchandise purchase using mobile devices to reach more than $400 billion in 2018, accounting for 44% of total mobile payment transactions, up from 35% in 2013. Already, many consumers are using mobile devices for online shopping, and merchants are seeing fast growth of their mobile sales. According to eMarketer, mobile retail commerce in the U.S. grew from $25 billion in 2012 to $42 billion in 2013, a growth of 70% year over year. Besides online shopping, more consumers now rely on mobile phones when they shop in the physical world, and this brings new opportunities to merchants and payment providers to engage their customers. Amazon’s recent introduction of a mobile wallet that stores only loyalty and gift cards indicates the importance of these engagement functions.

Discover Catalyst Use Cases of Digital Commerce

Digital commerce is the creation of revenue opportunities by blurring the digital and the physical worlds. Examples include scanning a bar code to get a coupon, checking into a store to get an offer, placing an order from a mobile app and picking up the item in the store, or hailing a taxi and paying from an app. These use cases greatly improve the discoverability of merchants and deals around when consumers are on the go, and consumers can use mobile phones to pay for offline consumptions such as a taxi ride, an in-store purchase and restaurant dining. Digital commerce offers a fertile ground for mobile payment adoption when designed properly to offer good user value and experience. Here are a few examples.

Order in Advance

A number of quick-service restaurants (QSRs) have launched mobile apps to enable people to order and pay in advance, and pick up the order from the store. They include McDonald’s, KFC, Subway, Burger King, Wendy’s and Dunkin Donuts. Starbucks also announced it will introduce this feature in the U.S. in late 2014.

In addition, some fine dining restaurants are also joining the pack and enabling customers to make reservations and preorder from the app before they arrive. Once the customer confirms the order on arrival, food can be served in a shorter time since the order is already in the system. Customers can also use the mobile app to pay when they finish dining. Taobao has launched the service in some major cities in China and MyOrder (owned by Rabobank) in Netherlands will launch a similar service in partnership with PayPal.

In both cases, customers get the convenience of ordering from the mobile device and avoiding waiting in the store. Merchants can increase turnover by shortening the time to serve without much investment in store expansion.

Taxi Hailing

Uber enables people to easily get a taxi and pay electronically. This has seen good adoption worldwide. Didi Taxi and Kuaidi Taxi, owned by Alibaba and Tencent, respectively, saw huge adoption in the beginning of 2014 when the two companies ran promotions to entice passengers and drivers to pay using mobile apps. These apps are not positioned as payment apps but more as utility apps, and payment is just the last step to conclude the service.

Ticket and Travel

This includes tickets for public transportation, flights, movies, sporting events, theme parks and even hotel reservations. These tend to be dedicated apps such as those offered by the transport authority to enable mobile ticket purchase on the go, and people can use e-tickets to enter the gate. These apps are available for cities such as Boston, Chicago, New York and London. Some can be travel-related apps that enable users to book flights, hotels, admission tickets and vacation packages, sometimes at the last minute to take advantage of flash deals. These apps offer the convenience of ordering on the go and sometimes at the last minute, and no need to print or carry paper tickets.

Local Services

There are apps that help people find local services such as cleaners, plumbers, repair personnel, dog walkers and baby sitters. Those services usually have a group of qualified service providers and guidelines for service delivery to ensure transparency of pricing and service quality. Users can pay via the app after the service is delivered.
Money Transfer

This has been the top use case in many emerging markets where unbanked consumers use mobile devices to pay. It has since expanded to mature markets and to banked users where the service is positioned as a catalyst for adoption. For example, Barclays launched Pingit in February 2012 as a money transfer app, and later added purchase and gift card functions. Venmo in the U.S. has created some buzz among young people as a money transfer app, thus generating some adoption. WeChat makes a further push of its payment service by positioning person-to-person (P2P) money transfer as a prominent service in its latest version, after increasing user adoption with a taxi-hailing service and red-packet function.

Money transfer helps remove the adoption hurdle by encouraging users to link their payment accounts to the service, a big obstacle for new service providers. We expect mobile money transfer to reach more than $420 billion in 2018, accounting for more than 45% of total mobile payment transactions, an annual growth of 25% from 2013.

All the above examples are use cases that can drive mobile payment adoption. Except for money transfer, many services are not known as payment services. But they win consumers by offering good value and user experience, and payment just becomes a natural step when users are ready to make a purchase. For mobile payment to be successful, the experience should be frictionless while consumers enjoy other services that will lead to payment.

Technology Trend

Multiple Technologies Will Coexist in the Next Five Years

Mobile payment makes use of various technologies to serve the local markets and use cases, and multiple technologies will likely coexist in the next five years since there is no single standard that can suit all use cases. Table 1 shows technologies at play in mobile payment, and is a nonexhaustive list as new technologies keep coming into the market.

### Table 1. Mobile Payment Technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMS</strong></td>
<td>• Emerging market mobile money service</td>
</tr>
<tr>
<td></td>
<td>• Text alerts/responses</td>
</tr>
<tr>
<td><strong>USSD</strong></td>
<td>• Emerging market mobile money service (Global System for Mobile Communications [GSM] networks only)</td>
</tr>
<tr>
<td><strong>Mobile Apps/Browser</strong></td>
<td><strong>Remote Payment</strong></td>
</tr>
<tr>
<td></td>
<td>• Online shopping</td>
</tr>
<tr>
<td></td>
<td>• Bill payment</td>
</tr>
<tr>
<td></td>
<td>• Money transfer</td>
</tr>
<tr>
<td></td>
<td>• Airtime top-up</td>
</tr>
<tr>
<td><strong>F2F/In-Store Payment</strong></td>
<td>• Bar code</td>
</tr>
<tr>
<td></td>
<td>• Audio</td>
</tr>
<tr>
<td></td>
<td>• Location-based</td>
</tr>
<tr>
<td><strong>Contactless Technology</strong></td>
<td>• Electromagnetic induction</td>
</tr>
<tr>
<td><strong>Requiring New Hardware</strong></td>
<td>• NFC</td>
</tr>
</tbody>
</table>

USSD = Unstructured Supplementary Service Data; F2F = friend-to-friend
Source: Gartner (September 2014)
SMS is a basic technology but currently accounts for a larger portion of mobile payment transactions, driven by mobile money services in emerging markets where many use SMS as the transaction channel. Mature markets also make extensive use of SMS in sending text alerts and letting customers give payment authorization with a text response. Some e-commerce sites also direct payment requests to mobile devices for purchase confirmation and password entry so as to enhance security.

Unstructured Supplementary Service Data (USSD) is a signaling technology in the GSM network, and works on most GSM phones. It enables users to access a service menu by dialing a short code, and it usually takes multiple rounds of menu choices to complete a transaction. It is often free to use, and is mostly used in emerging markets.

Mobile apps and browsers is the second-largest technology for mobile payment, and will eclipse SMS in 2016 to become the largest one, accounting for more than 45% of the mobile payment volume. This is propelled by mobile commerce-related transactions in mature markets and some emerging markets, such as China, where consumers use mobile apps and browsers to shop online. We see mobile apps to be more popular than browsers due to its richer user interface and functionality. Besides remote online payment, mobile apps are increasingly being used for friend-to-friend (F2F) and in-store payment, and this is an area that sees a lot of innovation in both technology and services.

Bar Code

Users can scan a bar code at a point of sale (POS) station, or show their account bar code to the cashier to be scanned. The easy and inexpensive integration of bar code versus other new technologies makes bar code adoption faster among merchants. Many have used it for marketing and advertising. The increasing user awareness and usage for nonpayment of services will have a ripple effect on payment. A bar code makes it easier to link the user account with the product item or merchant account, but on the other hand it may have performance issues due to the reflection on the phone display, dark lights or a damaged bar code. It can also have security issues should fraudsters use the bar code image for unintended transactions. There are, of course, countermeasures.

Audio

Acknowledging the challenges of a bar code, audio is used to improve security and performance. Users can place the phone close to a POS terminal or vending machine and the phone will send a beep to make the payment. Or the user can place it near another phone to transfer the money to a user. Alipay has deployed the solution in some vending machines and retail stores. Audio sound is generated by the mobile payment app, unique for each transaction, and linked to the payer’s account so it cannot be reused when recorded. Audio can be used interchangeably with bar codes, and has advantages in speed of transaction with no need of ambient light. The drawback is the need of additional hardware of a sound-receiving module on POS terminals, which costs about $8.3 each.

Location-Based Payment

We want to make it clear that the technologies mentioned below are location technologies and not payment technologies. These location technologies are used to support payment by recognizing the location of a user. Popular location technologies include Bluetooth Low Energy (BLE), Wi-Fi and GPS. Square Wallet (now Square Order) was the first service that enabled users to be recognized by the merchant via their GPS location as they walk into the store. The username and profile picture can be shown on the merchant POS, and users can say their names to pay. PayPal Beacon uses a similar mechanism, except that it uses BLE as the location technology and users need to check into a store before the account profile shows on the merchant POS. Groupon recently launched Gnome, a mobile POS product that uses a same approach but only works on Gnome merchant devices.

The benefit of location-based payment is that it combines user engagement with payment, and makes payment a natural step to take when the user is ready to pay. Merchants can send coupons and promotional messages when users enter the geofence, and can learn their preferences if they have shopped there multiple times.

Electromagnetic Induction

The technology was invented to enable contactless payment over the existing payment infrastructure, such as a mag stripe, so that merchants don’t need to invest in new POS terminals. It can come with a dynamic card verification value (CVV) code so that issuers can offer enhanced security for their cardholders. Users need to purchase an accessory in the form factor of a key fob or phone case that sends payment credentials to the POS terminal over an electromagnetic field, emulating a card swipe. Users can store an unlimited number of mag stripe cards in the mobile app, and manage the cards from there, such as loading a default card onto the accessory.
Loop, the company behind the technology, claims the technology works at more than 90% of retail locations worldwide, and is working to use the technology for e-commerce transactions. It is working with device OEMs to embed the technology into mobile devices so that users don’t need to carry the accessory. However, this can increase the adoption hurdle since people need to purchase new phones. This is the same hurdle that has haunted NFC for years. In addition, as the U.S. is rapidly migrating to EMV, this can be an interim technology unless it supports EMV down the road.

**NFC**

NFC enables contactless payment by mobile devices within 10 centimeters. When designed properly, it can speed up transactions to less than 500 milliseconds. It can also make use of chip-based architecture that makes it more secure than other mobile technologies and is on par with card-based payment. The downside is that it is an expensive and complicated technology to deploy because it requires NFC-enabled mobile phones and readers, and additional participants such as mobile carriers and trusted service managers (TSMs), thus leading to higher fees.

Apple Pay is good news for the industry. It will help increase user awareness of NFC and encourage adoption by offering a frictionless payment experience. However, Apple faces the same challenges that have been haunting the industry for years. It failed to address the value proposition question as to why NFC mobile payment is better than cash and card payments, including debit and credit cards that are accepted everywhere. Also payment alone is not enough to move NFC forward as nonpayment services such as personal ID, loyalty, access control and transportation should all be present on a single device to give consumers a reason to switch. At the same time, benefits for merchants remain elusive as it is not clear whether they will see increased turnover, foot traffic or a lowered transaction fee as a result of the service.

Apple Pay will be launched initially in the U.S., followed by other markets. But gaining the support of issuers, merchants and other partners in various markets is not an easy task, nor is the change of user behavior as not all payment markets are the same. Therefore, we maintain our prediction that NFC will account for less than 6% of total mobile payment transactions throughout 2018. As Apple continues to include more card issuers, merchants and other NFC services, NFC payment will slowly evolve to a larger user base. This will take years to happen.

The list above is only exemplary of what is available for mobile payment, and new technologies keep coming into the market. In each case above, the technology and service are designed to serve a particular use case in a target market. There is no single technology that can satisfy the needs of all users in all markets. We don’t expect there to be a single standard for mobile payment in the foreseeable future, and it is likely that multiple technologies will coexist to serve various segments.

**Cloud-Based Solutions Will Capture Majority Share**

Cloud-based solutions store most payment credentials in the cloud instead of on mobile devices. There are rarely pure cloud-based solutions as most services do store some information, such as login names or mobile phone numbers in the mobile device for a better user experience. This is as opposed to NFC payment using the secure element (SE) option where the majority of credentials, such as card numbers, are stored in the local chip on the device.

Cloud-based solutions require little investment in the hardware of user and merchant devices, and rely mostly on software upgrades. Thus, this can be more cost-efficient and have a shorter time to market. However, depending on the service, architecture and number of parties involved, sometimes it may entail significant investment of software integration into the existing POS and payment systems. This will counter the benefits of no-hardware investment of the cloud solution. Examples of cloud-based solutions include Starbucks’ Mobile Card App, McDonald’s mobile ordering app, KFC’s Fast Track, Subway’s app, MXC’s wallet (to be deployed) and Barclays’ Pingit. Although some are fairly new, such as Subway’s app, and McDonald’s app, which is still low in volume, these apps account for the majority of mobile payment deployments and transaction volumes in mature markets today.

In contrast, NFC payment requires upgrades of users’ mobile phones and merchants’ POS terminals, making it more expensive and time-consuming to deploy. It also adds complexity by bringing in a TSM role into the ecosystem, thus taking longer to deploy. Although host card emulation (HCE) simplifies the business model by taking out the TSM role, HCE itself is going through standardization and testing processes, so will take time to commercialize.
Therefore, cloud-based solutions will capture the majority of market opportunities while NFC payment goes through longer development cycles. Even when NFC enters the mass market in the future, we expect cloud-based solutions to maintain the majority share as it can well serve a large variety of use cases while NFC is better suited for services that require fast speed and are of small value.

**HCE Will Speed NFC Deployments**

HCE is a software-based approach that moves the credentials to the cloud, thus avoiding the complexity associated with the SE-based approach. It enables NFC services to be provisioned by the service provider — such as banks and merchants — directly to their customers without partnering with mobile carriers or TSMS. This greatly simplifies the architecture and business model, and can speed time to market and reduce deployment costs. Already, several banks and retailers such as RBC, Bankinter, The PrivateBank and Tim Hortons have either deployed their own branded NFC wallet using HCE, or are in pilot. Currently, the technology works on devices running Android 4.4 and BlackBerry.

As HCE moves user credentials from the SE to the cloud, it faces security and performance challenges, and tokenization is introduced to address those. Tokenization is the service where a surrogate value is used instead of the card number, and a limited-use token is generated for each transaction so that risks are contained. Each card network is developing its own specification for tokenization that has been or is in the process of being finalized. For more details on HCE and tokenization, please see “Innovation Insight: Host Card Emulation Will Speed NFC Deployment.” We expect a number of commercial deployments to start near the end of 2014 or in early 2015, with a larger scale rollout taking place from 2016.

While HCE can speed NFC deployments, it doesn’t solve the issue of the need of NFC-enabled mobile devices and POS terminals, nor does it create additional value for users or merchants. It takes time for consumers and merchants to be convinced of the value of NFC payments before upgrading their devices.

**Buyer Trend**

**Banks Have Not Succeeded in Extending From Mobile Banking to Mobile Commerce**

Some banks are leveraging their position in banking and payment to offer mobile commerce. Examples include branded malls in their mobile banking apps, along with ticketing, lottery, gift card and airtime top-up services. Others have launched separate apps that move from mobile banking into mobile commerce. For example, Barclays launched its Pingit mobile app in February 2012 to enable free money transfers among bank users in the U.K. Later, in September 2013, it added the purchase function to enable users to buy from print ads (by scanning a bar code) or online websites. In August 2014, Barclays further added a gift card function so that users can send and redeem gift cards from the app.

U.S. Bank is also deploying a mobile shopping platform that it intends to offer to retailers and brands. Many Chinese banks have either built their own online malls or integrated with third-party services for travel, ticketing and commerce. On a global level, this is the minority and most other banks choose to focus on the mature mobile banking offerings.

So far, the banks’ commerce entry hasn’t been successful as it is losing money and struggling to ramp up the volume. It remains to see whether banks can successfully transfer their position in banking and payment into commerce.

**Retailers Engage Customers With Mobile Commerce Apps**

Retailers are another active player in mobile commerce as it directly benefits their businesses. QSR is the leading sector in launching mobile apps for advance ordering. The value proposition is that it can save time and offers convenience to customers by enabling them to order in advance and pick up an item from the store, thus avoid waiting in line. Retailers can also engage customers by allowing them to track loyalty points, redeem rewards and receive marketing messages.

At the same time, retailers also benefit from increased revenue without investing in store expansion, and may be able to lower the transaction fee by using a close-loop payment mechanism such as a store card, gift card or cross-merchant schemes.
MCX, the alliance of more than 50 retailers in the U.S., is in the process of launching its own mobile wallet. It aims to offer a consistent user experience across merchants, as well as lower fees to banks by enabling on-network payment. We expect to see a large number of retailers launching their own apps within the next two years, offering opportunities to solution providers.

Telcos Find Sweet Spot in Emerging Markets but Struggle in Mature Markets

It is clear that emerging markets have pent-up demand for mobile financial services, especially for the unbanked and underbanked population, which has limited access to modern financial services. Mobile offers a safe and efficient way for them to transact. Telcos are a driving force of mobile money services in emerging markets, where they use their brands, distribution networks and customer relations to promote the service to the unbanked population. Such efforts have paid off in some countries, such as countries in sub-Sahara Africa and Southeast Asia. But it is not a done deal that telcos in emerging markets can all be as successful as Safaricom in Kenya because they need to find the right business model, sometimes through trial and error, which works in the local market and satisfies the user demand. It usually takes 15 to 24 months for a service to show signs of promise, so it is a long-term commitment to launch such a service.

Telcos are not so lucky in mature markets where the demand for mobile payment isn’t very strong since people already have a lot of means to pay. It takes innovative thinking to find the use case where mobile payment can deliver good user value, often related to commerce and engagement, to drive adoption. Telcos don’t have an obvious advantage in those services, nor do their brands and customer relations. As a result, telcos in mature markets have focused their resources on promoting NFC services where they think they can add value by offering and controlling the SIM card as the SE. But with the availability of HCE technology, such an opportunity may also evaporate. As of today, we haven’t seen any telcos in mature markets succeeding in their mobile payment initiative.

Technology Providers Are Driving Innovation

Technology providers are an important force in mobile payment in that they drive a lot of innovations that make it convenient or secure to use mobile payment. For example, Square came up with the pay-by-name feature to make payment as frictionless as possible. PayPal has developed features for mobile wallet to be used in the physical world, such as in retail stores and stadiums using technologies such as a bar code and BLE. Alipay uses audio for payment to vending machines and POS terminals to enhance security and performance. Tencent has included commerce and payment into its social chatting app to enable payment for taxis, airtime, ticketing and other commerce. TabbedOut enables easy payment from the mobile app for bars and restaurants. Seamless enhances security for POS payment by linking a user’s payment account with the merchant account and POS. Braintree and Stripe make it easy for merchants to integrate with mobile payment. The list goes on. The industry wouldn’t have progressed this far had we not had the contributions from technology providers.

Vendors to Watch

CorFire is the mobile commerce business of SK C&C, the IT solution subsidiary of SK Group in South Korea. CorFire offers a white-label solution that includes wallet software development kit (SDK) and management, NFC SE and TSM capability, and mobile marketing that includes gift cards, loyalty and offers. It offers comprehensive Web consoles to manage all payment and loyalty instruments. It has a number of live projects, including Vodafone’s mobile wallet and E-Plus’ NFC wallet in Germany.

Gemalto has a full range of mobile payment solutions that works in both emerging markets and mature markets. Its mobile financial services suite includes Gemalto’s mobile payment platform, mobile wallet application and management server, and NFC and TSM services, with an upcoming tokenization solution for HCE. It is one of the providers to MCX mobile wallet service.

Monitise offers mobile banking and payment solutions primarily to financial institutions. Its Bank Anywhere, Pay Anyone and Buy Anything are the three core modules for mobile banking, payment and commerce. It also has a mobile app design practice that it acquired. It has a strategic partnership with Visa Europe that is a major shareholder in the company.

Paydiant focuses on providing a cloud-based white-label mobile wallet platform to retailers and financial institutions, among others. It has partnered with payment processors, and POS application and equipment vendors to make the mobile wallet work with existing retail and e-commerce infrastructure. It has won the deal
to offer a mobile wallet platform to MCX, and counts Bank of America, Capital One, Barclays, Harris Teeter and Subway among its clients. **PayPal** offers mobile SDK for app developers to integrate its payment services. It has been focusing on cloud-based services and shunning NFC projects, and has launched several initiatives to push PayPal usage in the store. It has a Bluetooth Beacon product that can enable users to check out with their names after they have checked into a store. PayPal also announced a One Touch feature that enables consumers to easily check out from a mobile shopping page. Neither solution has been commercially deployed yet.

**Sequent** started as a TSM solution provider for the SE-based architecture and later expanded to include HCE and tokenization solutions. It offers SE management to Sprint in the U.S., and is in a pilot project with Sberbank in Russia for both SE and HCE solutions. It also has an Open Wallet solution that manages secure access to credentials and value-added services that can be shared across a range of NFC apps.

Gartner RAS Core Research Note G00264792, Sandy Shen, 23 September 2014
Research from Gartner

Innovation Insight: Issuer Tokenization Secures and Enhances Future Payment Services

Issuer tokenization will be one of the most important technologies to impact the payment industry in coming years. IT managers of token requesters should consider embracing it to address the increasing security risks brought by connected devices.

Key Findings

• Issuer tokenization applies to all new form factors, enables new use cases, works across multiple channels, and supports both mag stripe and EMV cards as the payment method.

• Issuer tokenization employs a number of security control mechanisms that protect real card data while giving card issuers control over how the payment is made, such as in which channel and for how much.

• Weakness in the issuer verification process allows fraudsters to use stolen card data over mobile devices, as happened to Apple Pay, which compromises the integrity of the service. This risk is not specific to, and is outside the scope of, issuer tokenization but needs to be addressed.

• Issuer tokenization standards are evolving, and confusion exists about the definition, implementation and common practices, as well as the scope and responsibility of the token service provider (TSP).

Recommendations

IT managers at token requesters (such as card issuers, processors, merchants and other wallet providers) should:

• Embrace issuer tokenization today if you want to be an early adopter that supports new form factors and use cases, or wait for the market and standards to mature if you want to avoid uncertainties.

• Select TSPs that can connect with multiple card schemes and issuers, that have streamlined implementation practices, and that offer flexibility in swapping service modules from different providers when required.

Strategic Planning Assumption

By 2020, issuer tokenization will penetrate 20% of the digital wallet installed base worldwide.

Analysis

Innovation Description/Definition

Issuer tokenization is a new trend in the payment industry that aims to address the increasing security risks brought by connected devices and new use cases. It allows payment providers to enhance security, offer a better user experience, and enable new services across channels and devices. This is one of the most important technologies impacting the payment industry in coming years because it applies to all new form factors and works over both the mag stripe and EMV rails. Apple Pay and Samsung Pay already use issuer tokenization, and other mobile wallet providers are likely to adopt it in the future.

What Is Issuer Tokenization?

A token is a surrogate value of the primary account number (PAN) to ensure that the real card number is not revealed, and the cardholder account data is protected. Issuer tokenization is a process to replace the PAN with payment tokens to be used for payment processing. In theory, the service can be used for any card that needs the underlying PAN to be protected, and the card is used for payment, such as bank-issued cards, merchant-issued cards, gift cards or prepaid cards. Today, it is mostly focusing on bank-issued cards, such as debit and credit cards. The service works for both mag stripe and EMV cards.

Card issuers are intimately involved in issuer tokenization because they set the rules and parameters of the token service, conduct account verification and authorization during the token request stage, and authorize transactions. This differs from merchant/acquirer tokenization, in that these are nonpayment tokens and are not used for payment processing, so they are not passed through the entire payment ecosystem. Merchants/acquirers use their own systems to tokenize PANs and store tokens in their own databases for future reference.
This report is based on EMVCo tokenization specifications, a standard supported by major payment networks, such as Visa, MasterCard and Amex, and it is likely to be a dominant standard adopted by the market. At the same time, there are other tokenization standards, such as from The Clearing House (TCH), that may complement the EMVCo specification.

**Token Request and Issuance**

Before a token is issued, the wallet provider first needs to register with a TSP as a token requester. Anyone that wants to offer a payment service, such as merchants, wallet providers, device OEMs, technology providers, processors, acquirers and issuers, can be a token requester. The TSP offers services such as token requester registration, token life cycle management, security and controls, and processing management.

Once registered with the TSP, the token requester can request a token on behalf of the consumer. When the consumer registers a card in the wallet app, the request will be sent via the token requester to the TSP. The TSP will perform a series of security controls and verification processes with the card issuer before issuing the token (see Figure 1).

**Payment Flows With Tokens**

A typical payment process with tokens is shown in Figure 2.

The payment process with tokens looks very much like a traditional card payment, except for the following:

- A token is used instead of a PAN.
- New data fields are included, such as token assurance level and token requester ID.
- The TSP is a new role between the payment network and the card issuer. The TSP manages the token life cycle and security controls. The TSP role can be assumed by one of the existing ecosystem players, such as card issuers, payment networks, processors or third parties.
- The TSP conducts a PAN recovery process before it passes the data for issuer authorization.

There is not much difference between an in-app payment (a type of e-commerce transaction within a mobile app) and a POS payment in terms of transaction flows, and the POS entry mode and token requester ID can be used to indicate the channel where payment is initiated.

**Security and Control Mechanisms**

A key purpose of payment tokens is to enhance transaction security. There are several security mechanisms included in the issuer tokenization.

**Tokens**

Payment tokens are issued per card account, per device. So, if cardholders use the same card on two devices, they will receive two different tokens. Or, if cardholders use two different accounts over the same device, they also get two different tokens. This creates a binding between the card token and the device being used, so the token cannot be used on other devices.

---

**FIGURE 1** Token Request and Issuance

![Token Request and Issuance Diagram](image)

Notes:
1. User registers a card to the mobile wallet that triggers a token request.
2. Token requester passes the token request to the TSP, based on the process and technologies specified.
3. TSP conducts security controls based on the defined process, such as verify the cardholder, account and device information, and assign assurance level and domain restrictions to the token.
4. TSP issues and provisions the token to the token requester and notifies the card issuers of the token issuance.

Source: Gartner (March 2015)
A static token remains the same for the lifetime of the card account until the card expires, the user changes the device, or the card or device is lost or stolen. A dynamic token changes from time to time and can be used for a limited number of times or limited value based on the rules set by the issuer. Both types of tokens can be used for POS and e-commerce/in-app transactions.

A static token offers the convenience of user tracking, so merchants can use that information for loyalty programs, and a static token requires less data exchange between the user device and the TSP. Dynamic tokens can trace the original transaction but cannot uniquely identify the paying customer, which can be a problem for merchants that rely on a static PAN/token to track their customers.

The choice of static or dynamic tokens is at the discretion of card issuers. Of the limited deployments and implementations of token services today, most issuers have chosen static tokens as the preferred token type.

**Cryptographic Key**

The cryptographic key is another important element to ensure the transaction’s integrity. When making a payment, the user device sends the payment token, along with a cryptogram, via the merchant POS or app to the payment network for approval. The cryptogram is generated by the mobile device using a cryptographic key and the algorithm embedded in the mobile app, encrypting data such as token, time stamp, counter and token expiry date.

Card issuers hold the master key to a card product that is used to generate a unique derived key (UDK) for each cardholder that remains unchanged for the lifetime of the card (static key). If the UDK is lost or stolen, it can be replaced over the air without replacing the physical card. The UDK can be used to generate transaction keys that are valid for only a single transaction or a limited number of transactions, and it needs to be replenished from time to time (dynamic key).
The rules of the key are set by the card issuer in accordance with the specifications of the payment networks, such as the number of transactions, value, channel and valid time frame that the key can be used. To ensure transaction performance, the user device needs to obtain dynamic transaction keys ahead of time, and multiple keys can be downloaded at the same time. Once these keys are used or expire, users need to connect online to obtain new keys for future transactions.

The choice of static or dynamic keys is also at the discretion of card issuers and is independent from the token choice. That is, a static token can work with either a static key or a dynamic key. The choice of key types is dependent on the storage media (see Note 1) available on the user device. If hardware-based secure storage is available, such as on the iPhone 6/6 Plus and Samsung Galaxy S6, static keys may be used and are stored in the local device. If secure local storage is not available and a cloud-based delivery mechanism is used, such as in hosted card emulation (HCE) deployments over Android devices, dynamic keys have to be used.

Both tokens and keys are needed to successfully process a payment. If one is lost or stolen, it is useless to the party that gets it. If both are lost or stolen — but used on other devices from other channels or merchants than what the token is issued for, or at a time outside the validity period of the token — the transaction won’t go through. This is how tokenization enhances transaction security.

The EMVCo specification doesn’t include key management in the scope of tokenization, and this is subject to the customization of each card network. The function of key management can be undertaken by the TSP or a third party.

**Token Domain Restrictions**

Domain restrictions ensure the token is used for the intended cases it is approved for, and they specify the use case, channel and merchant of the token from a specific token requester. So, if the token is lost or stolen, the transaction won’t go through unless it is used on the device from the channel or merchant, from the token requester and for the use case the token is intended for. Token domain restrictions are defined by the TSP during the token requester registration process.

**Token Assurance Level**

The token assurance level indicates the confidence level of the payment token to PAN/cardholder binding. It brings transparency in payment processing, so that merchants, acquirers and processors understand the assurance level of a token; it also supports card issuers in making authorization decisions.

The assurance level is determined as a result of identification and verification (ID&V) steps conducted at the time of token issuance. EMV specifications define a number of ID&V methods — from no ID&V conducted to card issuer verification of the cardholder using a combination of token requester data, such as billing address, device ID and location, and various communications channels, such as 3D secure, mobile banking, federated login and one-time password.

The EMV specification hasn’t defined the value of ID&V methods to indicate the steps taken by an issuer. Without this, the payment ecosystem cannot fully embrace the mechanism. In addition, not all payment networks, acquirers and processors support the new data fields, so the assurance level hasn’t been adopted on a large scale. Nevertheless, tokens can be processed over the existing payment infrastructure without including the new data fields, and some implementations have repurposed the unused data fields in the existing message to contain information about the assurance level as an interim solution.

**Business Impact**

Issuer tokenization is a new way to enhance transaction security across new devices, new channels and new use cases, regardless of the underlying payment methods or technology. It gives issuers much more control and flexibility in risk management. Compared with including the PAN in the user device and issuers needing to replace new cards if the device is lost or stolen, tokens give issuers more controls and choices. Switching off one token won’t impact other tokens being used, and no card replacement needs to take place either. Users also have an easier registration process whereby tokens can be provisioned quickly over the air. No download of new software or plug-ins is needed. They can also continue to pay with the same plastic card and other devices if one device is lost or stolen. This helps issuers to reduce costs and enhance customer satisfaction.

New benefits come with new fees, as TSP service comes with a price tag. MasterCard announced a fee structure of its TSP service; it charges a token provision fee per card, per device and a monthly fee for life cycle management. Visa hasn’t published a fee
structure and only says it will waive the fee for 2015. Many payment players are competing for this new role or at least want to perform some TSP functions so that they get new revenue streams. Since tokenization is still in its early days, the fee practice hasn’t been established. This means some strong wallet providers may even be able to extract revenue from the service. Apple is one example of a provider charging card issuers a fee for each transaction. So, the rule of the game isn’t cast in stone and depends on the market power of each player.

Besides the payment industry, issuer tokenization also impacts retail, e-commerce, consumer products and technology players since they are involved in the payment process, and some also aspire to offer their own wallet service. However, tokenization by itself will not solve fraud issues, as evidenced by recent reports on the discovery of fraud over Apple Pay (see the Risks section).

Figure 3 shows whether the impact is heavy, mixed or weightless, depending on the industry.

**IT Impact**

Tokenization impacts the entire value chain of the payment industry, and each player needs to make certain system changes to support the service. The extent of the IT impact depends on the role they play in the ecosystem; the token functions they use; and their delivery model, existing systems and available resources.

![FIGURE 3 Innovation Window](image)

Impact is categorized according to industry, for example:
- **Heavy**: Mining, engineering, construction, energy and utilities, military, automobile, and manufacturing
- **Mixed**: Consumer packaged goods (CPG), logistics, retail, pharmaceuticals, local government, education and healthcare
- **Weightless**: Insurance, media, banking, advertising and intelligence

Source: Gartner (March 2015)
Card Issuers
Card issuers can outsource the TSP function to a third party or do this in-house. If outsourced, relatively fewer integration efforts are required, as TSPs usually offer Web APIs, and issuers need to decide only what functions they want to use and configure the rules for those functions. Sometimes no integration is needed if the TSP (such as card networks) offers online tools for issuers to configure. This can normally be done within a few weeks. If implemented in-house — that is, the issuer works as a TSP itself — the task requires much more intense development efforts that impact issuing, processing and back-office operations and can take between three and six months before the system can reach full production.

Issuer Processors
Issuers need to make incremental changes to ensure they support the new data elements required to process a tokenized transaction. If the issuer has integrated with a TSP or becomes a TSP itself, there is little change to the processor. If the issuer delegates certain functions to the processor and uses it as an interface to the TSP, the processor needs to integrate with the TSP and offer services such as issuer onboarding, training and ongoing support.

Merchants/Acquirers
If the merchants/acquirers have enabled technology such as Near Field Communication (NFC) used by the consumer device, no change is required at their ends, where they process the token payment as a normal transaction. If they have set up their own tokenization systems, they need to work with the vendor to make sure their system is compatible with the issuer tokenization. However, merchants tracking customers using static tokens will encounter problems in identifying customers using dynamic tokens, thus, they want to work with issuers, payment networks and acquirers to influence the use of static tokens when possible.

EMV specifications have included card-on-file use cases for merchants to replace the stored customer PAN data. Merchants need to follow the industry’s best practices to secure these tokens.

Wallet Providers
Wallet providers are the token requesters that request tokens for their customers. They need to register with the TSP to get the token requester ID and integrate with the TSP to receive tokens and keys. Wallet providers also need to embed the cryptography algorithm into the wallet app that is required for cryptogram generation. Many vendors offer wallet software development kits (SDKs) with the algorithm that has been certified by payment networks, so limited development efforts are required as related to tokens.

Adoption Rate
We expect issuer tokenization to reach 2%, 20% and 40% of digital wallet users worldwide as of 2015, 2020 and 2025, respectively.

Drivers of the service include:

- Payment ecosystem players all want to improve the user experience while maintaining security. Card issuers, payment networks, merchants and wallet providers all want to enable new use cases and promote a better user experience while maintaining security.

- HCE deployments have been including tokenization. Financial institutions and other players deploying mobile wallet services using HCE have included tokenization by using pre-EMV specifications. HCE is in the early stages, but the number of deployments is on the rise worldwide, especially in markets with established contactless infrastructure.

- Issuer tokenization is versatile in risk management. There are alternative risk and fraud management tools that are often optimized for some form factors or use cases, but not all. Issuer tokenization covers many form factors, channels and use cases, including those that may emerge in the future. The tools can be used in combination with tokenization for additional controls.

Inhibitors of the service include:

- The standard is immature and evolving. EMVCo released the first version of specifications in March 2014, and major card networks have also published their own specifications based on the EMVCo standard. However, further clarifications are needed in certain areas, such as token assurance level and ID&V methods; hopefully, these clarifications will be available in the next release, planned for April 2015. Card networks will update their specifications to incorporate new changes. This may cause some players to wait on the sidelines for the standards to mature.
• Local payment scheme support can vary. Major card networks have launched the service in the U.S. in support of Apple Pay and expect to roll out the service to other markets in the coming months. However, local payment schemes may not support the EMV standard, or networks may introduce their own version of the service, which would require modifications during implementation. Even in the U.S., there are other credit and debit networks whose support of tokenization is not pronounced.

• Service practices and processes are confusing and not transparent. Today, major card networks are playing the TSP role, but in theory, TSP functions can be assumed by different players, so we will see multiple TSPs, such as issuers and processors, emerge. It is not clear how token requesters register with various TSPs to reach all issuers. The TSP function can also be modularized and offered by different parties. This will cause confusion about how the service works and what the related processes are. In addition, major card networks haven’t released Bank Identification Number (BIN) ranges, so this creates a lack of transparency at the merchant acquirers.

• Cost can be quite substantial with the increasing number of devices. Issuers need to pay for the tokens provisioned and for token life cycle management. If they are large issuers and their customers use those cards on multiple devices, service fees can be significant. Some issuers may consider implementing TSP functions in-house to avoid the fee, while others may not adopt them at all.

Risks
Issuer Verification Is a Weak Link
This is not a risk specific to issuer tokenization but applies to all payment services where account verification needs to be done before provisioning the card to a device. Nevertheless, it impacts the whole experience and security of the service.

There are recent fraud reports on Apple Pay. Although we doubt the actual fraud rate is as high as claimed, the weakness in an issuer’s verification process is a real risk. If issuers verify only some basic account information, they increase the fraud risk, since personal identify information is readily available on the black market. Once a stolen card is registered as a legitimate card and provisioned with tokens, fraudsters can use this card with no problem and with the protection of tokenization. There is no 100% correct user verification, so issuers need to share more information to increase the rigor of the verification process; see “The Four Layers of Identity Proofing Lead to Stronger Identity” for best practices.

Standards Confusion
Besides the EMVCo specification, TCH also published a tokenization standard in 2013 to address the proliferation of payment credentials with the increasing use of mobile devices. TCH is a banking association and payment company owned by more than 20 banks in the U.S., and it offers payment, clearing and settlement services for its member banks. There are some similarities and differences between TCH and EMVCo specifications, and the two bodies are considering adjustments to their specifications to accommodate interest and suggestions by ecosystem players. This will impact those implementations carried out according to the existing specifications, but we expect the impact will be limited.

Performance and Integration Risks Are Low
Issuer tokenization has limited risks on performance, as the payment process is almost the same as using the PAN. Integration risks are low for issuers because TSPs usually publish Web APIs and provide hand-holding for integrating with various services. Payback risks vary by issuers and depend on how much value issuers place on enabling new use cases and a better user experience.

Key Technology and Service Providers
Bell ID Tokenization Manager offers token issuance, detokenization, domain management, and ID&V and processing support, and it can be used independently as a token vault or in combination with other token life cycle management products. Bell ID offers the solution for on-premises deployment. The company is also involved in a number of HCE projects, such as RBC’s Secure Cloud deployment.

Carta Worldwide offers tokenization service as part of its digital enablement platform and includes a digital credentials management and provisioning service, a token transaction processing service, and a mobile payment application SDK. It offers both a managed service on behalf of an issuer and in-house deployment on-premises. Carta’s background in card issuance, transaction processing, value-added services and mobile apps helps it offer a comprehensive package for service providers. It provided the HCE and tokenization solution to Banco Sabadell in Spain.
First Data is a major processor serving financial institutions and merchants in about 70 countries. Its TransArmor solution is a merchant-side tokenization service that reduces the scope of PCI compliance for merchants. It is a launch partner for Apple Pay in the U.S., assisting card issuers to authorize payment and connecting with the card networks. It offers issuers with onboarding, training and ongoing support for issuer tokenization.

MasterCard Digital Enablement Service (MDES) offers token issuance and provisioning, life cycle management, ID&V, domain controls, and key management. MDES charges 50 cents per card, per device for token provisioning and a 10 cent monthly fee per token/PAN for life cycle management, with a 2.5 cent fee for calls to its alternate network API. These fees kicked in from 1 September 2014. MasterCard is a launch partner of Apple Pay in the U.S.

Visa Token Service includes three turnkey components: token management tools, Token Vault and Visa Risk Manager. The token management tools offer service enrollment, token provisioning, life cycle management and card metadata management. Token Vault offers token mapping, detokenization, domain control and processing support. Visa Risk Manager is a risk management tool that supports issuers making risk decisions during provisioning. Issuers can fully integrate Visa Token Service or use its On-Behalf-Of service, whereby issuers use Visa online tools and functions to manage the deployment. Visa is a launch partner of Apple Pay in the U.S.

Evidence
1 “Visa CEO Confirms Tokens as New Network Revenue Stream,” PYMNTS.com, 13 November 2014.
Note 1. Storage Media

The security of the storage location on the mobile device impacts whether static or dynamic keys are used. When highly secure hardware-protected storage is available, static keys can be used. In general, hardware-based storage is regarded as more secure than software-based storage. The following are identified options for storage location.

Hardware-based storage:

- **Secure Element (SE):** This is a physical, tamper-resistant chip on the mobile device in the form factor of embedded chip, SIM card or microSD card. The chip is an isolated storage location from the rest of the device and requires special keys and authorization rights to access. Apple Pay and Google Wallet use an embedded chip as the SE, and Softcard uses the SIM card as the SE.

- **Trusted Hardware:** One example is Trust Execution Environment (TEE), a secure environment that runs on its own OS and is separated from the main OS all the way from the hardware layer. It is invisible to normal apps, and secure apps need to obtain the TEE API to access the secure OS. Even when the main OS is compromised, the secure OS remains intact. Since TEE standards have not been finalized, very few devices shipping today have an integrated TEE API, such as Samsung Galaxy S3, S4 and S5. This is therefore not a mass-market option for secure storage.

- **Remote Hardware Storage:** Use a Hardware Security Module (HSM) to store and manage cryptography keys for authentication and processing. HCE implementation of NFC services relies on HSM to provide the SE function from the cloud.

Software-based storage:

- **Mobile App Host Memory:** This is generally an unsecure place to store sensitive information because compromised devices give hackers full access to the app binary, although techniques such as obfuscation can enhance the security of an app. Obfuscation is a technique to dissolve sensitive information, such as cryptography keys and algorithms, into the app binary by renaming or rearranging the code blocks, so it is much more difficult to retrieve the original information. It is also called app hardening or white-box cryptography. In HCE implementations, where hardware-based storage isn’t available, tokens and keys are distributed differently. For example, a static token may reside in the app memory while keys need to be refreshed from time to time.

- **Remote Database:** It resides in regular storage media with no additional hardware for enhanced security. It is usually managed by merchants to store PANs or tokens for customer identification.
Samsung Electronics Co., Ltd. inspires the world and shapes the future with transformative ideas and technologies, redefining the worlds of TVs, smartphones, wearable devices, tablets, cameras, digital appliances, printers, medical equipment, network systems and semiconductors, and LED solutions. We are also leading in the Internet of Things space through, among others, our Smart Home and Digital Health initiatives. We employ 319,000 people across 84 countries with annual sales of US $196 billion. To discover more, please visit our official website at www.samsung.com and our official blog at global.samsungtomorrow.com.