A First Data White Paper

# NFC-Enabled Payments and the Role of the Trusted Service Manager

**By:**
**Christopher Cox**
Vice President, Product Development

**Roger Musfeldt**
Director, Product Management

# Introduction

Tech-savvy and time-challenged consumers are driving rapid changes in commerce in the 21st Century, and they expect to use the technology already at their fingertips to transact their business anytime and anywhere. From a consumer's perspective, shopping, payments, marketing (i.e., offers and coupons), loyalty, money management and social sharing should all blend together — and it should occur on demand, in both offline and online experiences. This is Universal Commerce, and it is seamlessly integrating in-store commerce, eCommerce and mobile commerce into one cohesive experience.

Consumers' purchasing patterns are shifting, enabled by the broad availability of self-selected, timely and relevant information. Today's savvy shoppers are online, they are mobile, they go to stores, they socialize, they solicit and share opinions, and they compare before they make decisions.  They also want convenience and choice, and they expect incentives, rewards and value for their money. To many people, particularly Millennials who have always utilized the Internet and mobile devices, this is not just a way of commerce—it is a way of life.

The Universal Commerce lifestyle is not limited to a few developed countries. At this writing, 3.2 billion people–more than half of the world's total adult population–have at least one mobile access subscription, and many have multiple subscriptions.[1] Selling at a pace of more than a billion units a year, smartphones now outsell feature phones.[2] These devices and the sophisticated mobile wallet applications they can run are a fundamental building block of Universal Commerce. They are the access point for consumers to transact their business, make payments electronically, and keep track of their financial records.

> “NFC is on the verge of broad adoption worldwide, as the NFC controllers and SEs are now commonplace components in many models of smartphones and point-of-sale devices currently available in the market.”

When mobile NFC wallets were first envisioned, the blueprint called for a mobile device equipped with a near field communication (NFC) controller and a secure element (SE). The SE would be the secure storage location for payment and other kinds of applications, as well as individualized customer account information. NFC would be the means of establishing communication and exchanging data with other devices like point-of-sale (POS) terminals and transit fare gates. This model has taken some time to catch on, but there have been several significant pilot programs as well as actual implementations that have provided many industry players with experience and useful insight for optimizing this business model going forward.

The outlook for mobile wallets based on NFC + SE technology is good. NFC is on the verge of broad adoption worldwide, as the NFC controllers and SEs are now commonplace components in many models of smartphones and point-of-sale devices currently available in the market. In addition, secure elements are a critical component to support a wide range of applications for Universal Commerce and other needs. This paper shares insights on lessons learned and how the market has evolved to support the NFC + SE model for mobile commerce. These lessons have important implications for mobile network operators (MNOs), financial institutions, payment associations, and other service providers that want to secure their position in the Universal Commerce ecosystem.

[1] Wireless Intelligence research, October 2012
[2] Gartner press release, "Gartner Says Worldwide Mobile Phone Sales Declined 1.7 Percent in 2012," February 13, 2013

# An Overview of NFC and Where the Technology Fits in the Mobile Commerce Marketplace

NFC is a technology that uses an embedded NFC controller and a radio frequency (RF) antenna to establish radio communication between NFC-capable devices by touching them together or bringing them into close proximity (usually no more than a few centimeters). Industry standards cover communication protocols and data exchange formats, and are based on existing ISO standards. NFC builds upon RF systems by allowing for multiple communication methods, including card emulation using an SE, reader emulation, and peer-to-peer mode (two-way communication between endpoints)—whereas earlier systems such as contactless smart cards were card emulation mode only. These multiple communication methods facilitate the ability to support a host of value-added capabilities.

## A wide range of uses for NFC

NFC is a broad term for a technology that can be used in many different ways. For example, a secure element embedded or inserted in a device such as a phone or a key fob can allow that device to emulate a credit card so that it can replace the plastic card. An NFC controller can emulate a reader so it can become a point-of-sale device at a retail store, or a fare reader on a transit system. NFC can also support peer-to-peer communication so that "bumping" two handsets together can complete a transaction like exchanging business cards or music play lists. It can be used for pairing devices such as a Bluetooth headset to a phone. And, unpowered RF chips can be embedded into posters, menus, etc. to activate more content or applications on a consumer's NFC smartphone; for example, an application to buy tickets to a play advertised on a poster.

The remarkably versatile NFC technology can be applied to myriad applications, including:

- Mobile wallets/mobile payments
- Affinity/loyalty cards
- Building access cards
- Personal identification cards
- Health cards
- Transportation ticketing
- Parking meters
- Advertising and marketing promotions
- URL shortcuts
- Contactless logins and authentication on computers
- Social networking "check-in" (e.g., Foursquare) and data sharing
- Connection to headphones, speakers and other wireless devices
- And more…

In "An Explanation of NFC," Steve Gurley writes: "There is a tremendous amount of buzz focused on NFC. Most of the excitement has been directed at turning the smartphone into a platform for enabling a broad range of new NFC-enabled experiences that provide added value to the consumer as well as the venues with which the consumer does business."[3]

[3] Steve Gurley, Symon Communications, "An Explanation of NFC," 2012

## The market outlook for NFC in mobile commerce

Admittedly, the uptake of NFC for mobile commerce has been slower than many experts predicted, but the market is looking brighter for the next two to five years. Research firm IDC predicts that NFC will grow rapidly in the next five years, fueled by the influx of mobile devices into the market and also by upgrades in point-of-sale terminals.[4]

The research firm Forrester concurs with that timeframe, saying that mainstream use of the technology is still three to five years away for most countries. According to Forrester Analyst Thomas Husson, "Turning adoption into mass-market usage among consumers will require not only a lot of market education but also, more importantly, the construction of a value proposition for consumers and merchants that goes well beyond convenience and speed to adding value to the entire commerce process."[5]

> "Admittedly, the uptake of NFC for mobile commerce has been slower than many experts predicted, but the market is looking brighter for the next two to five years."

The foundation for a broad NFC ecosystem is underway. Consider the following indications that NFC will be hitting its stride soon:

- As of March 2013, there were at least 127 models of mobile phones worldwide that support NFC, and another 35 that are planned or "rumored" to be coming onto the market soon.[6] Many manufacturers of Android phones—Android being the dominant mobile platform worldwide—have embraced NFC.
- One of the world's leading mobile phone and tablet manufacturers, Samsung, has at least 30 NFC-enabled devices on the market. What's more, Visa and Samsung recently announced a partnership that includes plans to embed Visa's Mobile payWave technology directly into Samsung devices.
- According to Berg Insight, a firm specializing in telecom industry business intelligence, a total of 3.9 million contactless enabled POS terminals were installed globally by the end of 2011, and the number is due to grow at a compound annual growth rate of 49.4 percent to reach 43.4 million units in 2017. This corresponds to an increase in the global penetration rate from 8 percent in 2011 to 53 percent in 2017. The penetration rate is projected to be highest in North America where an estimated 86 percent of the terminals will be NFC-ready by 2017. The penetration rate in Europe and the rest of the world will be 78 percent and 38 percent respectively." This means that consumers will be able to use their NFC-enabled mobile devices to make purchases at millions of merchant locations around the world.
- 2013 is set to be a breakout year for mobile contactless payments and digital wallets, according to Visa Europe. Across Europe in 2013, there will be 40 issuers offering mobile contactless payment services to consumers, and by the end of 2013 around 80 types of smartphones will be certified by Visa Europe to carry out contactless payments.

[4] www.nfcme.com, "Bright Future Ahead for NFC?" June 2012
[5] Mobile Payments Today, "Forrester: NFC adoption still a few years off," August 6, 2012
[6] NFC World, "NFC phones: The definitive list," updated march 19, 2013

## Components of the NFC ecosystem and where a TSM fits in

> “Relationships are vital in this ecosystem, as no single company has what is needed to serve the entire market.”

Certainly the momentum for NFC-enabled commerce is building, and now is the time for MNOs, card issuers and other service providers to solidify a strategy and establish relationships in order to be ready to serve the mobile wallet market. Relationships are vital in this ecosystem, as no single company has what is needed to serve the entire market.

Consider the traditional business model where NFC is included in a mobile device and we want to use this device to conduct Universal Commerce transactions. There is an ecosystem of companies that control different components of the total solution, and they must work together to enable the Universal Commerce experience for the consumer. Many of the businesses in this ecosystem have never worked together before and have no existing relationships; for example, MNOs on one side of the solution, and financial entities such as banks, credit unions and card associations on the other side. Prior to mobile payments and mobile commerce, companies from the telecommunications and financial services industries had no reason to interface with each other. Now their interaction, either directly or indirectly through a third party, is crucial.

Following is a look at the technology components of the NFC ecosystem, which players own or control them, and why a new business entity called a Trusted Service Manager (TSM) is needed to bring critical players together.

### The NFC device

This is the mobile phone—or a tablet, ebook reader, etc., that has Internet access and/or carrier service. It is increasingly likely that the device will have an NFC chipset for the purpose of communicating with other devices such as card readers, Bluetooth headsets, speakers and other devices.

In order to make the device an attractive and valuable purchase for consumers, they come enabled to support as many applications as possible from a wide variety of service providers. This includes mobile wallet applications.

### The secure element (SE)

According to GlobalPlatform, an industry association pertaining to secure chip technology, a secure element is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. SEs are an evolution of existing secure technology. The chip that resides in many credit and debit cards has been adapted to suit the needs of the mobile world. With multiple applications now being stored and their processes executed in the same device, it is essential to be able to house trusted applications and their associated credentials in a secure environment.

The secure element is separate from the NFC controller chip. There are currently three SE implementations: a secure element embedded in the mobile device, usually soldered to the motherboard; a removable universal subscriber identification module (USIM) card; and a removable (micro) secure digital (SD) card. The SE functions in card emulation mode to securely store sensitive applications and data. Example applications might be a payment card, a transit card, or an identity card. The types of data stored on an SE could include cardholder account information, a transit credential, consumer loyalty points, etc.

It is important to note that the SE is completely separate from the regular storage area of the device that holds personal contact information, photographs and other user-generated data. Because it is associated with the mobile device, access to the secure element chip—but not the actual applications or data on the chip—is often controlled by the secure element owner (such as an MNO) or, more commonly, by a designated representative. How applications and data get provisioned to the SE is discussed later in this paper.

## Applications and data

Applications run on the secure element, similar to programs running on a personal computer. The applications on the secure element give the device a special purpose or use. For example, an electronic payment application such as MasterCard Mobile *PayPass*™ or Visa Mobile payWave allows the consumer to use the device for making payments. A personal identity application may give the consumer access to a building in which he works. Each application has its own data associated with the consumer's personal account or identity.

> “The mobile wallet provides a user interface (UI) on the mobile device that allows the consumer to manage multiple accounts and initiate contactless payments, and allows interaction with the applications stored on the secure element.”

Though these types of applications and their associated data are stored on the secure element, they both are owned or controlled by the service provider that provides the application to the consumer; i.e., the bank, the transit company, the building management company, and so on. In most cases, the company with the application would like as many of its customers as possible to have the application on their respective devices, regardless of which SE owners' services they use.

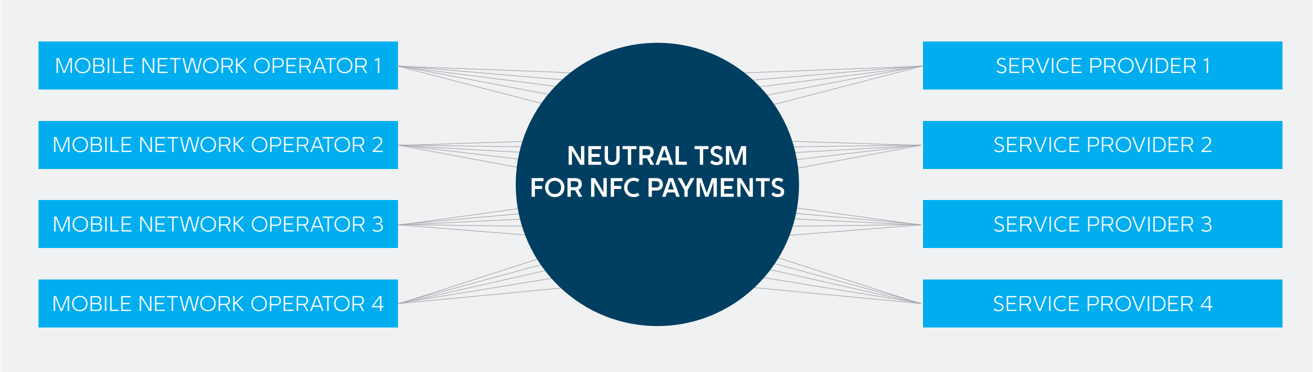
In terms of Universal Commerce, the mobile wallet is a most important application. The mobile wallet provides a user interface (UI) on the mobile device that allows the consumer to manage multiple accounts and initiate contactless payments, and allows interaction with the applications stored on the secure element. The UI application turns a mobile device into something like a wallet full of cards because a mobile device can contain many "cards" (credit, debit, prepaid gift card, other special stored-value accounts, public transit tickets and merchant-specific loyalty cards, to name a few). The mobile wallet allows the user to select the card or application when making a purchase. Examples of a mobile wallet application are Google Wallet, Isis Mobile Wallet™, Samsung Wallet and the Valyou mobile wallet.

## The role of the Trusted Service Manager

If the goal is to allow a consumer to replace his physical wallet, then the MNO (or whatever entity owns the SE) must have relationships with many service providers, and each service provider must have relationships with many MNOs, in order to replace consumers' most popular credit cards, loyalty cards, transit cards, etc. with applications on the device. A much more practical approach for this vast ecosystem is to have a neutral third party to bring the secure element owners and the service providers (application owners) together. Called the Trusted Service Manager, or TSM, this entity's role is to integrate as many MNOs/devices as it can with as many service providers' applications as it can, and to safeguard the applications and the data associated with the user accounts.

For instance, if a large merchant wants to issue a loyalty application to its customers or a bank wants to issue a payment card application to its customers, this makes sense only if the merchant or bank can reach most or all the potential users of these applications, regardless of what MNOs these consumers use. It is not practical for every merchant and bank to maintain its own contractual relationships with each MNO or other secure element owner; this is a logical role for a TSM.

The Trusted Service Manager resides between the secure element owners and the service providers and allows them to integrate applications–lots of them–onto NFC devices controlled by various telecommunications carriers. More importantly, the TSM is the entity that is trusted to provision and maintain personal accounts (i.e., consumer data) on the secure element of the mobile devices. For example, if the secure element of an NFC device is effectively a replacement for a plastic credit card, the consumer's account information has to be securely provisioned to the SE. The best way to send this data to the SE is over-the-air (OTA) via the mobile operator's network. The TSM also performs lifecycle maintenance on the virtual card on behalf of the card issuer, renewing the account when the "card" expires, decommissioning the "card" if the account is closed or the device is lost, and so on. Because an SE can host multiple applications from various service providers, the TSM can be responsible for provisioning and maintaining accounts for many service providers. The TSM ensures isolation and security of data across multiple, unaffiliated service providers.


MOBILE NETWORK OPERATOR 1
MOBILE NETWORK OPERATOR 2
MOBILE NETWORK OPERATOR 3
MOBILE NETWORK OPERATOR 4
NEUTRAL TSM FOR NFC PAYMENTS
SERVICE PROVIDER 1
SERVICE PROVIDER 2
SERVICE PROVIDER 3
SERVICE PROVIDER 4

# The Evolving Role of the Trusted Service Manager

For the purpose of brevity, the above description of the TSM role has been greatly oversimplified. In reality, the activities performed by the Trusted Service Manager are quite complex, especially given the vast size of the potential market, the transient nature of consumers' mobile subscriptions, the highly sensitive data involved, and a dearth of global standards.

And then there is the biggest challenge of all: consumers want to be the ones to decide what device they use, on what mobile network, and which personalized applications they want to run on their device. They do not want to be told that in order to have a mobile wallet, they must have "X" brand of device, subscribe to "Y" brand of mobile network coverage, and have a credit card from financial institution "Z" associated with card association "A" and shop at a merchant who uses payment processor "B." In many of the mobile wallet pilot programs–which were conducted for proof of concept more than anything–the ecosystem players were intentionally limited, but this isn't likely to be accepted in the open market. The mobile wallet ecosystem has to be more open in order to provide more value to consumers and in turn gain their acceptance. As more consumers embrace a mobile wallet solution, more merchants will want to accept payments via the mobile wallet, creating a cycle that spirals upward to broad acceptance.

In consideration of these challenges, the role of the Trusted Service Manager is evolving to adapt to market needs.

# Just what is a TSM?

Simply stated, a TSM is a neutral third party whose primary role is to load, or provision, personal account information onto the secure element of a consumer's mobile device. Although the concept is the same as provisioning a plastic credit or debit card, the actual process is quite a bit more complicated. Looking at this process gives a better feel for what a TSM really is and the crucial role it plays in setting up and maintaining mobile accounts.

When a consumer receives a plastic credit or debit card, the card comes with his personal account information already imprinted on the magnetic stripe or stored on an embedded chip, and with his name and account number embossed on the front of the card. There are a few companies, like First Data, that provide plastic card fulfillment services to card issuers. These services involve storing personal account information in accordance with Payment Card Industry Data Security Standards (PCI DSS), and transmitting that data during the card-issuing process.

> "Simply stated, a TSM is a neutral third party whose primary role is to load, or provision, personal account information onto the secure element of a consumer's mobile device."

Now think about a leather wallet full of various credit and debit cards. Perhaps the consumer has a credit card carrying the MasterCard® logo, a debit card with the Visa® logo, a merchant's proprietary credit card, and a credit card from American Express®. There is a separate provisioning process for each card involving different financial or merchant entities. Companies that provide provisioning services typically maintain contractual relationships with many such entities in order to collect the essential personal account information needed to complete the card provisioning process.  For the most part, consumers are unaware of these relationships.

In the case of a mobile wallet, it is the consumer that decides which accounts he wants to have in his wallet. The consumer will want the flexibility of adding new accounts to his device at any time in the same way he might want to sign up for a new payment card or a merchant loyalty account. Therefore, provisioning a mobile NFC device with personal account information is fundamentally different from card provisioning in two important ways:

1. A commerce-enabled device can contain many accounts, such as credit accounts, debit accounts, merchant-specific accounts, transit pass accounts, loyalty accounts and others. Each of these accounts can come with its own personal identity, financial and security information. Putting these accounts into one mobile device brings together account information from many different entities (service providers), some of which could even be competitors.
2. The only practical way to get personal account information onto the secure element of an individual's device is through the MNO's wireless network or via Wi-Fi. Account information is transmitted on demand by a process called over the air (OTA) provisioning. This transaction can be difficult to accomplish without the active participation of MNOs, or others who control the secure element on their device. Even with their cooperation, the OTA provisioning process can be challenged by technical glitches such as interruptions to the transmission (i.e., think "dropped calls"). The TSM is responsible for ensuring the data has been successfully installed on the secure element so that the consumer can use his account for uCommerce purposes.

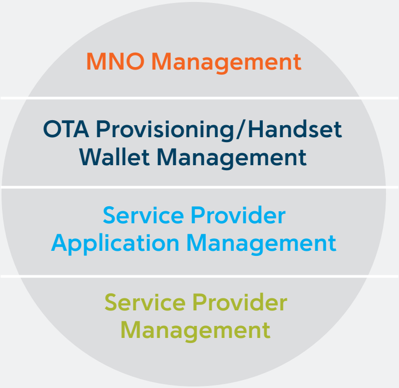
The core function of the TSM is to securely OTA provision and manage the lifecycle of NFC virtual cards on behalf of service providers to the customer base belonging to various MNOs or secure element owners. However the TSM role is much broader than providing only the technical capability to provision and personalize NFC virtual cards OTA. The TSM also manages contractual relationships between many MNOs and many service providers. And the TSM provides many supporting business services, including customer service, data center hosting and quality assurance.

Critically, the TSM is the one entity in the mobile commerce ecosystem that has a view of the intersection of the customer base of the MNOs or secure element owners and the service providers. This view enables the TSM to provide customer support from both the MNO perspective and the service provider perspective and enables the management of customer lifecycle events such as exchanged, damaged, lost or stolen devices (and associated impact on service provider accounts previously provisioned). Related to this is the TSM's responsibility for managing the lifecycles of NFC applications, electronic wallet applications and mobile devices/secure elements.

In the First Data white paper Trusted Service Manager: The Key to Accelerating Mobile Commerce, the many essential tasks the TSM performs in the areas of MNO management, service provider management, service provider application management, OTA provisioning/device management, and various other areas are outlined. Some of those tasks are represented in the following chart.

### MNO Management

- Contractual relationship
- Secure connection
- Business rules and authentication
- Billing, reporting and reconciliation
- User registration


MNO Management
OTA Provisioning/Handset Wallet Management
Service Provider Application Management
Service Provider Management

### OTA Provisioning/ Handset Management

- OTA provisioning
- OTA post-issuance/content delivery
- Chip management
- Wallet management
- Handset management
- Secure element key management
- MNO, handset and end-customer lifecycle management
- Fraud/security management
- End-customer support

### Service Provider Application Management

- Chip data preparation
- Application key management
- Service Provider, application and end-customer lifecycle management
- Fraud/security management
- End-customer support

### Additional TSM Services

- Call center
- Data center hosting
- Application testing and certification

### Service Provider Management

- Contractual relationship
- Secure connection
- Data preparation/data staging
- Business rules and authentication
- Billing, reporting and reconciliation
- User registration

## How the market has evolved from a single TSM model to a multi TSM model

The concept of the TSM was initially introduced in 2007 by the Global System for Mobile Communications (GSM) Association (GSMA) to facilitate adoption of NFC services.[9] The TSM role addresses the biggest challenge to realizing simple, transparent mobile payments within the mobile commerce ecosystem: bringing multi-account services to different mobile NFC devices accessed through a variety of proprietary networks.

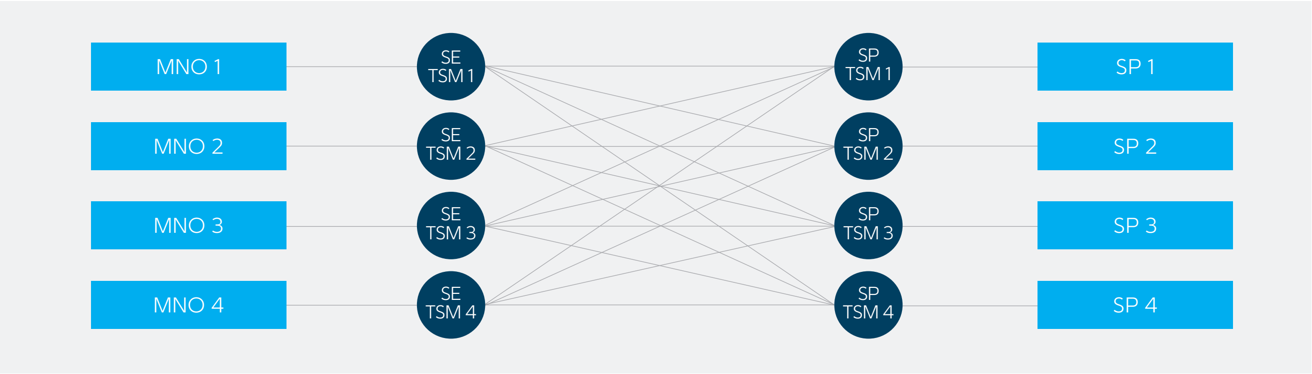
A key element of the TSM role as envisioned by the GSMA is that it is an independent entity serving MNOs or secure element owners and any account-issuing entities such as banks, card associations, transit authorities, merchants and

[9] The GSMA is a trade association representing nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organizations in industry sectors such as financial services, healthcare, media, transport and utilities.

marketing companies, to name a few potential service providers. An independent TSM is key to the provisioning of applications to NFC-enabled devices such that they have the broadest possible array of uses for the consumer.

Given the scope of the worldwide mobile commerce ecosystem, as well as markets that vary from one global region to another, the role of TSM is too large and complex to be met by a single entity. Numerous companies, including First Data, have stepped forward to assume different aspects of the TSM role. In fact, there has been an evolution toward two distinct sides of the market.

On the one side there is the service provider TSMs (SP-TSMs) which cater to the entities that have applications and content to deliver and provision to the secure element of consumers' mobile devices. The SP-TSMs typically represent banks, card associations, transit authorities, merchants, marketing companies, and so on. On the other side there are SE-TSMs (also called MNO TSMs) that have taken on responsibility for managing access and allocation of space and privileges on secure elements on behalf of MNOs or other secure element owners. Some TSMs play both roles. Nevertheless, in most markets this split of the TSM roles and responsibilities results in each TSM participating in multiple relationships with other TSMs. This is illustrated by the graphic below.



SP-TSMs ensure that useful applications and data are securely delivered to and maintained on consumers' mobile devices.

### The SE-TSM and why this role came about

As noted earlier, a secure element is typically—but not always—controlled by the MNO, largely because it is embedded or inserted (in the case of a USIM- or microSD-based version) into a mobile device. Controlling the SE may allow an MNO to earn additional revenue by renting or allocating space on the chip for various applications. However, MNOs typically don't want the complication of managing SEs or the content on them due to the complexity of maintaining encryption keys and the liability of having access to secure data. For example, having contact with credit card data on the SE chip puts a company in scope for PCI DSS compliance. Instead, an MNO can contract with an SE-TSM that manages access to the SE by managing the chip (i.e., the encryption keys). In turn, the SE-TSM establishes relationships with SP-TSMs and provides them with the keys for loading and personalization on the secure element. In this scenario, it's the SP-TSM that has access to and liability for sensitive data that may require PCI compliance.

In this emerging business model, it is the TSMs–and not the secure element owners and service providers–that establish relationships with each other and perform any necessary system integration in order to load as many commerce applications as possible onto as broad a distribution of NFC-enabled mobile devices as possible. In essence, the secure element is becoming a space that can be open for any application provider that wants to use it. Often, the MNO or secure element owner and the service provider are helping facilitate relationships between SE-TSMs and SP-TSMs as needed to meet market requirements.

## The complex work of the Service Provider TSM

There are many more service providers (i.e., card issuers, loyalty program providers, transit agencies, etc.) than there are MNOs, and the application and data provisioning needs of these service providers are varied. Consider the complexity of lifecycle events. For example, say that John Doe has a leather wallet full of payment and loyalty cards and he wants to put them all on his mobile wallet. The SP-TSMs that work with the card issuers have to ask and answer questions such as:

- How do we put "the plastic" that John has today on his mobile device when he wants it there? Unlike plastic cards that are pre-provisioned before being given to account holders, accounts must be provisioned on demand in the mobile wallet world, with data being sent OTA.
- How is John properly authenticated by the card issuers before his card is provisioned OTA?
- John has numerous cards: credit, debit, loyalty, prepaid. Though they come from different card issuers, he wants all of his cards in one digital wallet. Can the issuers' SP-TSM work with the SE- TSM that manages the SE on John's mobile device to get the card accounts and their respective applications onto the wallet?
- How can John delete a card from his mobile wallet if he no longer wants it there? If the card were plastic, he could simply cut it up. Since the account is digital, what does John need to do to have the card removed?
- What happens if John loses his mobile device that now has multiple cards on it? Who should he notify about lost cards? What is his liability for the accounts on the lost mobile device?
- What happens when John wants to get a new mobile device? How does he move his card accounts from the old mobile device to the new one? What if the two mobile devices come from different MNOs? How does he move his entire mobile wallet from, say, an AT&T device to his new Verizon device? Who will help him do this?
- What happens when a card account on a mobile device reaches its expiration date? How does the account get renewed?
- John is attempting to put another of his accounts on his mobile wallet, and the carrier connection is dropped during the provisioning process. What does the SP-TSM need to do to restart the process to make sure the account is provisioned properly?

> "There are many more service providers (i.e., card issuers, loyalty program providers, transit agencies, etc.) than there are MNOs, and the application and data provisioning needs of these service providers are varied."

The issues above illustrate provisioning and lifecycle events from a consumer's perspective. Now let's look at it from a card issuer's viewpoint. Let's say that Bank XYZ wants to enable its customers to put their bank-issued credit and debit cards on mobile wallets.

- Bank XYZ's credit cards carry a MasterCard brand and its debit cards are Visa-branded. There are two distinct processes for provisioning the plastics. Can Bank XYZ find one SP-TSM that can service all of their provisioning needs?
- Bank XYZ's customers use a wide variety of devices hosted by different carriers. How can the bank ensure that its cards can be deployed to as many devices as possible in order to support its full customer base?
- What is necessary to set up the card management system in order to set up mobile payments?
- What happens if a customer has both a plastic card and a mobile device-based card for the same account, and the customer loses the device? Does the physical card need to be canceled or replaced? What should the bank do for lost/stolen cards if one of the devices (called a "presentation instrument") is lost?

The fact of the matter is that provisioning cards to chip-based devices–whether an EMV card, a contactless card, or a mobile device–is much more complicated than provisioning an old fashioned magnetic stripe card.

# Considerations for choosing a TSM provider

MNOs and service providers of all types should be developing their strategies for participating in the NFC-enabled uCommerce ecosystem. Certainly one aspect of the strategy is deciding which Trusted Service Manager(s) to select as a partner. Here are some considerations when choosing a TSM provider.

## Ecosystem neutrality

A key element of the TSM role as envisioned by the GSMA is that of an independent entity serving MNOs and/or any account-issuing entities. An independent TSM is key to the provisioning of applications to NFC-enabled devices to ensure they have the broadest possible usage for the consumer. Moreover, neutrality gives the MNO or issuer the ability to choose among multiple TSMs and select the one that provides the most value to the organization.

In contrast, some very large card manufacturers and card associations act as their own TSM, and thus they would be likely to favor their own services if conflicts arise between competing vendors. On the NFC device side, some MNOs are tied to a specific SE-TSM because that particular company manufactures or provides the secure element chipset that is used in the device. Such cases of bias will only serve to limit the potential usefulness of the service to consumers by locking out applications that consumers may want.

## Secure technology that enables OTA provisioning

Consumers' accounts on mobile devices are going to be provisioned and maintained OTA. An SP-TSM must have the knowledge and experience to ensure that this activity can be done securely. This is largely a factor of the TSM's expertise with the technology specifications published by GlobalPlatform.

The secure element used in a mobile device can be the exact same secure element that is used in a plastic payment card, such as an EMV or contactless card. Therefore, the same security that is associated with an EMV card–a plastic–can be associated with a mobile secure element. Part of it is related to the secure element operating system. Different types of chip operating systems have different levels of security that can be invoked, so when a TSM is pushing data out OTA, it can ensure that the data is not only encrypted for confidentiality but also encrypted for integrity. In other words, the TSM can validate that the data cannot be read by thieves and it also can validate that no one changed the data when it was going OTA.

## Breadth of support for mobile devices, chips and carriers

In the ecosystem, there will be numerous SE-TSMs and SP-TSMs. They need to establish business relationships and develop technical integrations with each other to create, in essence, a network that can support a wide variety of mobile devices supported by numerous carriers, and the SE chipsets of those devices. From a service provider's standpoint, it's better to choose an SP-TSM with a wide network, because this will ensure that the service provider can "reach" more consumers. The questions to ask the SP-TSM are, "What is your range of participation in the ecosystem?

## Economies of scale

The ability to provision applications and accounts to secure elements on mobile devices is really a matter of having developed software that is coded to specific sets of application programming interfaces (APIs) for the various platforms. Once the software is developed, the SP-TSM can achieve economies of scale because the integration work is already done. So, for example, once an SP-TSM has integrated toa particular wallet, the TSM can easily help other issuers provision their accounts to the same wallet. The TSM can use the same process again and again once it has done the initial integration.

A service provider that is looking to engage a TSM should consider how much of the wallet integration work the TSM has already done in order to get its accounts onto as many SEs as possible without funding the development effort.

## Provisioning experience

NFC-based payments are still a relatively small percentage of all electronic payments. However, there are companies that have years of experience in this area from pilot programs and full blown implementations. From a chip technology standpoint, they understand not only the chips and the operating systems, but also the payment applications that go on a secure element. They understand how to prepare and personalize data; how to do key management and encryption of data; how to integrate to host systems where issuers' applications reside; and how to integrate to other host systems. This expertise is invaluable for avoiding pitfalls, managing costs, and getting the best value from having a presence on a mobile commerce platform.

## End-to-end solution

OTA card provisioning to a secure element on a mobile device starts at the source--the card management system where the service provider's card data is stored.  Often, modifications are required to card management systems to enable one-at-a-time, real-time requests for OTA card provisioning from a mobile wallet.  And card management systems must be tightly integrated to SP-TSM systems to support card lifecycle management.   A single company that both hosts card data and provides SP-TSM services can proactively integrate systems to ensure its issuing customers are ready to participate in NFC payments.  And these companies are set up to provide end-to-end customer support for cardholders who participate in mobile wallet programs.

# Conclusion

NFC-enabled commerce is here to stay. It has been slow on the uptake to date, but is poised for mass appeal now that NFC devices are widely available worldwide, merchants can accept NFC transactions, and mobile wallets and other important applications are readily available.

MNOs and service providers such as card issuers cannot afford not to play in the NFC-enabled payments space. The convenience of mobile wallets will likely help determine which devices and carrier services people use, as well as which payment cards they choose to use. For MNOs and card issuers alike, significant revenue could be at stake as NFC-enabled payments become mainstream.

Getting account credentials securely onto a mobile device is a complicated process. It is not an activity for novice companies with little experience in the account provisioning space. A Trusted Service Manager is expected to have the technical expertise, business relationships and experience to get accounts and applications onto the device on behalf of service providers and MNOs.

> “A Trusted Service Manager is expected to have the technical expertise, business relationships and experience to get accounts and applications onto the device on behalf of service providers and MNOs.”

Companies seeking to join the mobile payments ecosystem need a TSM partner that can maximize their presence on mobile devices (for service providers) or fill their SE space with applications and accounts (for MNOs and other secure element owners). When customers find significant value in Universal Commerce, the whole ecosystem will win.

# The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

**For more information, contact your First Data Representative or visit firstdata.com**