Smart Card Alliance

The Mobile Payments and NFC Landscape: A U.S. Perspective

A Smart Card Alliance Payments Council White Paper

Publication Date: September 2011

Publication Number: PC-11002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

TABLE OF CONTENTS

1 Introduction

Man's desire to communicate is as old as man himself, and even today, very few needs are stronger. The invention of communication devices such as the telegraph, the telephone, and particularly the mobile phone have affected how people live in ways that almost no one could have anticipated.

Another requirement almost as old as the need to communicate is the need to exchange things of value—commerce. Just as methods of communication have evolved over time, so have the methods and tools of commerce, from the development of commonly accepted currencies and the establishment of banks, to the evolution of today's complex and robust payment networks that can validate and authorize transactions across thousands of miles in seconds.

The communication and commerce industries and their supporting technologies have evolved over the past century, changing most dramatically in the last 40 years. Combining the most recent technologies from both industries—mobile phones and e-commerce—results in a product that provides new capabilities and the freedom to conduct commerce in ways that would otherwise not be possible. This product is known as *mobile payments*.

The Smart Card Alliance has developed this white paper to provide a snapshot of the mobile payments and NFC landscape in the United States, including:[1]

- A description of the different types of mobile financial applications in use today
- Discussion of the different mobile payments approaches with implementation examples
- A summary of the merchant, consumer, issuer, and mobile operator requirements for NFC mobile contactless payments and the attendant benefits
- An update on the status of Near-Field Communications (NFC) mobile contactless payments
- Evaluation of how different mobile payment approaches fulfill overall market requirements

Technology changes rapidly, and how it is ultimately applied is not always predictable. The goal of this white paper is simple: to provide a holistic view of mobile payments and the ecosystem currently supporting NFC mobile contactless payments. The hope is that this paper can help players in the industries directly involved, as well as observers and participants in secondary markets, understand the current mobile payments landscape, anticipate how mobile payments are likely to change, and appreciate the opportunities that mobile payments present.

[1] This white paper does not endorse any specific company, product or service. Company, product or service references are provided to illustrate the points being made.

2 The Mobile Financial Application Landscape

The numbers of mobile commerce applications (apps) and app types have grown at rates matching the rate at which Web sites were launched during the early days of the Internet commerce boom. A wide array of financial apps can provide value to the mobile phone owner, regardless of whether the owner is a business or a consumer.

Currently, merchants or small business owners can run their entire businesses directly from a smartphone, providing a new level of freedom and convenience. Consumers also use their mobile phones for a wide variety of financial functions, including checking various account balances, performing bank transactions, making payments, and completing credit applications. Technology and business solutions are merging to provide powerful value propositions.

This section summarizes the mobile financial apps: mobile banking, mobile commerce, mobile point-of-sale (POS), and mobile payments, including person-to-person payment, remote payment, and mobile proximity payment.

2.1 Mobile Banking

Mobile banking can be defined as the use of a mobile device by a consumer to access and manage financial services provided by a bank, credit union, brokerage, or other financial services provider.

A recent commercial shows a woman receiving a text message on her mobile phone while hanging from the side of a mountain. Her bank is telling her that her account is about to be overdrawn. With a few clicks on her phone, she transfers funds from her savings account to her checking account to cover the overdraft. This commercial suggests that the future of banking is mobile banking, enabling mobile phone users to access basic financial services even when they are miles away from their nearest bank branch or home computer. In some parts of the world, such as the Philippines, Brazil, and Africa, mobile banking based on person-to-person remittance services is already flourishing. According to the Nielsen Company, mobile Web banking in the United States has grown to more than 13 million mobile subscribers—up 129 percent in just 2 years—and is now poised to level the playing field for customers of all kinds—banked, unbanked, young, old, rich, poor, downtown, uptown, and out-of-town.[2]

The following factors point to the growth in mobile banking. First, banks are rolling out mobile banking solutions that reduce the need for branch visits while providing an increased level of services available anywhere, at any time. At the same time, mobile network operators (MNOs) are upgrading their networks to deliver data more quickly. Consumers are acquiring advanced, Internet-ready phones. Finally, consumer awareness and consumer confidence are increasing while the convenience of such solutions becomes more appealing.

2.2 Mobile Commerce

Mobile commerce (also known as *m-commerce*) refers to the use of a mobile phone, smartphone, or other mobile device to support a commercial transaction. Mobile commerce can be defined as any transaction that involves searching or paying for goods or services using a mobile phone's Web browser, a specialized app, or a text message. Like Internet-based e-commerce, m-commerce activities include both shopping and paying for products using the mobile phone. For example:

- A retailer's Web site may be optimized for mobile devices, allowing consumers to shop on the Web site using a mobile phone's Web browser.
- Retailer applications can run on a mobile device, allowing consumers to use a downloaded application to shop and pay for products from the retailer.

[2] Nielsenwire, *Mobile Banking in U.S. Grows 129% in Last Two Years*, October 19, 2010, http://blog.nielsen.com/nielsenwire/consumer/mobile-banking-in-u-s-grows-129-in-last-two-years/.

M-commerce is already one of the major trends affecting small business owners. As of January 2011, the number of Americans who owned smartphones was 65.8 million[3], up from 45.5 million the previous year.[4] According to a ComScore survey, 48 percent of these people, or more than 31 million, are using their phones to shop.[5]

In addition, people can use mobile devices to research products, recommend products to friends on social network sites, and compare online product prices to the prices in brick-and-mortar stores. That is, m-commerce is not restricted to selling and paying for products; it encompasses many of the activities involved in shopping and in establishing relationships between retailers and customers.

2.3 Mobile POS

Mobile POS is defined as the use of a mobile device to replace a traditional merchant POS terminal or system and is typically used for inventory management, electronic payment, and queue busting. Smartphones and mobile commerce have made a significant impact on mobile POS. Mobile technology can deliver a restaurant order to the kitchen in an instant, allow riders to pay a taxi fare by credit card, and let shoppers scan their groceries as they place them in their carts. Mobile POS can support different types of payment devices – from traditional magnetic stripe cards to contactless bank cards to mobile proximity payment with a smartphone – and can also be an NFC-enabled device configured for POS acceptance.

Some retailers are replacing centralized checkout facilities with smartphones, providing store associates with the ability to roam the store. Apple stores have removed cash registers and equipped each representative with an iPhone or iPad to answer customer questions, check stock, and finalize sales. The Hampton Jitney bus service, which carries passengers from New York to the Long Island beach communities, uses a smartphone-based system that allows attendants to check reservations, take payments, and print out receipts.[6]

A wide variety of systems are available for merchants. One example is the offering from Square that enables small merchants (such as flea market vendors and bake sale operators) to accept credit cards and process transactions using an iPhone, iPad, or Android device. Another small merchant payment solution, Quicken® Mobile POS, allows a merchant to process any major credit card, send receipts by e-mail, and export transactions to QuickBooks Financial software. For direct marketing merchants and those merchants who need inventory control, gateway providers, such as USAePay, offer mobile POS solution applications that can be securely routed to the appropriate financial processor.

Although there is some concern in the payments industry about the security of wireless transactions, both consumers and merchants can benefit from the freedom and convenience of mobile POS. Retailers and service companies who invested in mobile have realized improved employee productivity and lower labor costs while improving customer service and ensuring quicker payment for goods and services rendered.

[3] comScore, *comScore Reports January 2011 U.S. Mobile Subscriber Market Share*, March 7, 2011 http://www.comscore.com/Press_Events/Press_Releases/2011/3/comScore_Reports_January_2011_U.S._Mobile_Subscriber_Market_Share

[4] Small Business Computer, *Is Small Business Ready for Mobile Commerce?* , March 16, 2011, http://www.smallbusinesscomputing.com/news/article.php/3928386/Is-Small-Business-Ready-for-Mobile-Commerce.htm

[5] Ibid.

[6] Howstuffworks, *How are point-of-sale systems going mobile?*, http://communication.howstuffworks.com/convergence/point-of-sale-mobile.htm

2.4 Mobile Payment

Mobile payment is a transfer of funds in return for goods or services in which a mobile device is functionally involved in executing and confirming payment. The payer can be standing at a POS or be interacting with a merchant located somewhere else.[7]

Consumers can use a mobile device to pay for goods and services such as:

- Music, videos, ringtones, online game subscriptions, wallpapers, and other digital goods
- Transportation-related items, such as bus, subway, or train fares and parking at meters
- Any merchandise in a physical merchant location

2.4.1 Characteristics of Mobile Payments

As shown in Figure 1, mobile payments are typically differentiated by technology, transaction size, location (remote or proximity), and funding mechanism.

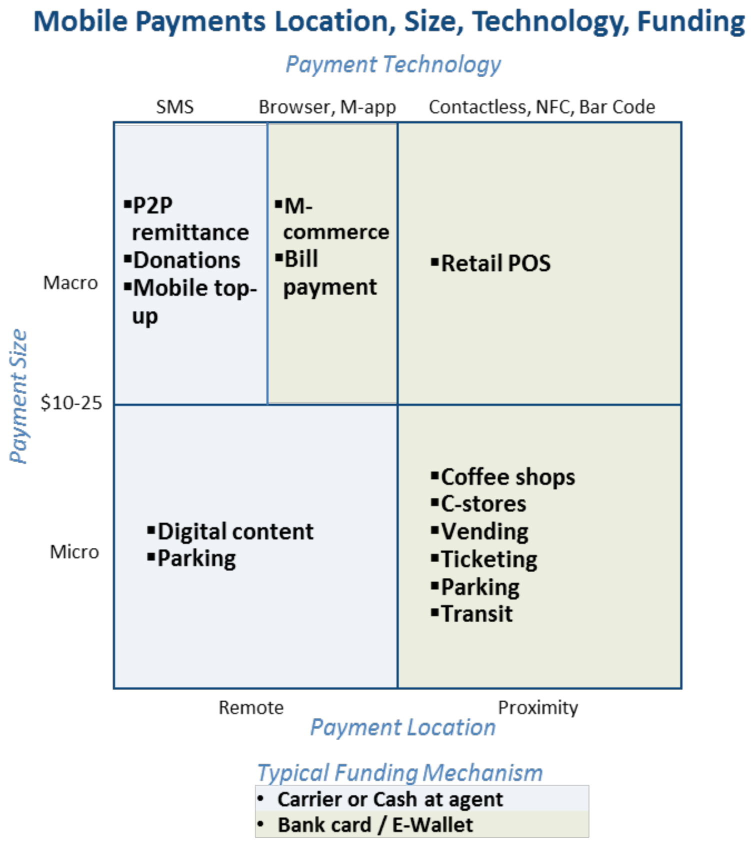

Figure 1: Mobile Payment Differentiators[8]

[7] Innopay, *Mobile Payments 2010*, http://admin.nacha.org/userfiles/File/The_Internet_Council/Resources/Mobile%20payments%202010%20-%20Innopay.pdf

[8] Adapted from Mercator Advisory Group, "US Mobile Banking and Mobile Payments: Finding the Seams, Accelerating the Pace" and Smart Card Alliance, *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure,* September, 2007, http://www.smartcardalliance.org/resources/lib/Proximity_Mobile_Payments_200709.pdf

2.4.1.1 Technology

Mobile payments can use a number of different technologies to perform a transaction. Remote payments typically rely on text messaging (short message service, or SMS), a mobile browser, or a mobile app. Proximity payments rely on either bar codes or a contactless interface to chip-enabled payment technology, such as NFC-enabled mobile phones, contactless stickers, tags, or fobs.

2.4.1.2 Transaction Size

Transaction size affects the choice of mobile payment technology and approach. Mobile payments typically fit into one of two transaction size categories. Micropayments (less than $10-$25) are typical for paying for ring tones, music, parking, transit, coffee, and items in convenience stores. Macropayments (over $25) are typical for all other transactions, such as person-to-person domestic and international remittances, charitable donations, Web site purchases, bill payment and retail POS.

2.4.1.3 Location

Remote mobile payments and proximity mobile payments are distinguished by the location of the mobile handset in relation to the merchant's POS, as well as by payment account information and the payment acceptance device or service. A remote mobile payment is a payment in which the payer does not interact directly with the merchant's physical POS system (for example, transferring funds through a mobile phone app to a merchant's PayPal account). A proximity payment is a payment in which the mobile phone interacts in some way with a physical POS device to transfer the consumer's payment information and perform the transaction.

2.4.1.4 Funding Mechanism

Mobile payments can rely on multiple funding mechanisms.

Transactions can be included on a telephone bill or funded by a prepaid account associated with the phone (typically used for text-message-based payments). Alternatively, cash can be loaded into a virtual account at an agent location that is then used for payment.

Another source of funds is a traditional bank account or credit, debit, or prepaid card, accessed through a virtual wallet (a wallet that is accessed using the mobile phone's browser or a mobile application). The wallet may provide access to one or more of the above funding sources, which are loaded into the wallet.

2.4.2 P2P Mobile Payment

Person-to-person or peer-to-peer (P2P) payment allows individuals to pay one another through a third party. P2P payment services, which are offered by many banks and third parties, can also allow business owners to transfer money to a customer or supplier account (and vice versa) using an e-mail address or mobile phone number. Users can conduct transactions using funds from a bank, credit, debit or prepaid account, or the payment can be funded through the mobile phone bill.

According to Javelin Research, nearly 44%, or 38 million, of the 86 million online households completed at least one online P2P fund transfer in 2009, up from 27% in 2008. Javelin is forecasting that 60 million American households will use P2P transfers by 2014.[9]

PayPal is the leader in the P2P category, with the largest global Internet-based payment network (approximately 94.4 million customers). In June 2000, PayPal diversified to support payments between businesses and consumers (B2C). PayPal offers a mobile phone app that allows consumers to send and request money using an e-mail address or phone number[10] and a service based on SMS. PayPal has

[9] Fox Business Small Business Center, *Peer-to Peer Payments Gain Momentum*, June, 17, 2010, http://smallbusiness.foxbusiness.com/sbc/2010/06/17/say-goodbye-checks-peer-peer-payments-gain-momentum/

[10] PayPal web site, http:www.paypal.com

just announced a P2P payments solution for Android NFC phones that allows money to be transferred by tapping two NFC phones together.[11]

Other examples of P2P mobile payment solutions include the following:

- In 2010, Visa announced a new P2P payment service that gives its U.S. customers the ability to receive and send money from their Visa accounts. Visa's service includes a partnership with CashEdge and Fiserv, two P2P financial transaction companies that now have access to VisaNet, the company's payment processing network.[12]
- MasterCard MoneySend uses the mobile browser, SMS, or a mobile app to enable customers to transfer money from person to person using a mobile phone.[13]
- ZashPay, a service provided by Fiserv, offers a public Web site that allows people to transfer money using e-mail addresses or mobile phone numbers. The banks involved determine the sender's fee, with a suggested fee of 50 cents.[14]

2.4.3 Remote Mobile Payment

Remote mobile payment refers to transactions in which consumers use a smartphone or mobile phone to make purchases without interacting with a physical POS. Most mobile phones deployed over the last five years are equipped with the functionality required to support remote mobile payments, including SMS, secure mobile browser sessions, and mobile apps.

Practical use cases for remote mobile payments include making purchases from a Web merchant, paying a merchant who does not have traditional acceptance capabilities for physical goods, paying a merchant for the purchase of digital goods, or sending money to another individual. Remote mobile payments can be implemented using the existing financial payments infrastructure (e.g., for payment at a Web merchant) or a closed loop mobile payments system.

One example of the remote mobile payment process is as follows:

1. The consumer and merchant set up an account with a trusted third party or mobile payment service provider.
2. When a transaction is initiated, an SMS message is sent to the mobile payment service provider. Authentication can be accomplished using a variety of mechanisms, such as entering a secret password, validating handset hardware information, or verifying other sender personal information.
3. After the transaction request is received and authenticated, the mobile payment service provider transfers funds from the consumer's account into the merchant's account and notifies the merchant that the funds have been transferred.
4. In a closed loop system, the merchant may then move the funds into a standard bank account.

Remote mobile payments are ideal for use in markets that require P2P payments and for underbanked consumers and merchants who are not part of the normal POS acquirer payment process, such as flea market vendors and seasonal outside vendors.[15]

One major retailer who has taken advantage of remote mobile payment is Foot Locker, Inc., a specialty athletic retailer with more than 3,400 stores in North America, Europe, and Australia. Using a smartphone, Foot Locker customers can access any of Foot Locker's sites anywhere. They can then

[11] Near Field Communications World, *PayPal announces NFC peer-to-peer payments*, Juley 13, 2011, http://www.nearfieldcommunicationsworld.com/2011/07/13/38574/paypal-announces-nfc-peer-to-peer-payments/

[12] Watters, Audrey, *Visa Announces P2P Payment Service for U.S. Customers*, March 16, 2011, http://www.readwriteweb.com/archives/author/audrey-watters.php

[13] https://www.mastercardmoneysend.com/consumer/welcome.shtml

[14] http://www.zashpay.fiserv.com

[15] Smart Card Alliance, *Proximity Mobile Payments: Leveraging NFC and the Contactless Infrastructure*, op. cit.

view and purchase products, find the nearest store, look at inventory, and check model, size, and color availability. Customers can also use the sites to monitor their Foot Locker loyalty account status and sign up for mobile alerts about new products and offerings.[16]

Remote mobile payment represents a convenience for consumers as well as merchants. For example, PayByPhone, a brand owned by Verrus, features consumer payment options in several transportation categories, including car parking, taxi fare payment, and bicycle rental. Over 2 million people have signed up to use the PayByPhone service globally, and PayByPhone processes 2–3 transactions per second all day.[17]

2.4.4 Proximity Mobile Payment

Proximity mobile payment refers to a transaction in which a consumer uses a phone to pay for goods or services at a physical POS or with a mobile POS device. Proximity mobile payments can be used at both attended POS locations, such as stores, and unattended locations, such as vending machines. The consumer uses a mobile phone to interact with the merchant's POS system.

Proximity mobile payments can rely on the financial industry's payment infrastructure or a closed loop payment infrastructure. Merchants can implement proximity mobile payments using NFC technology or other contactless technology and bar codes.

2.4.4.1 NFC-Enabled Proximity Mobile Payment

One implementation of proximity mobile payment uses NFC technology (also referred to as mobile contactless payment). An NFC-enabled phone is provisioned with a version of a payment application (e.g., American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa payWave) and personalized with a payment account (i.e., credit, debit or prepaid) issued by the consumer's financial institution. The phone can then use NFC technology to communicate with a merchant's contactless payment-capable POS system. To pay, the consumer holds or taps the phone close to the merchant's reader.[18] The consumer's account information is sent to the contactless POS reader via radio frequency (RF). The payment and settlement processes are the same processes used when a consumer pays with a traditional contactless or magnetic stripe credit or debit card. NFC technology can be built in and integrated with new mobile devices (see Section 4.5) or can be added to existing mobile devices using a bridging technology (e.g., microSD or sticker).

Numerous NFC-enabled payment and mobile marketing applications have been piloted and implemented globally (see Appendix B: Examples of NFC Mobile Payments Deployment). In the United States, Isis and Google have announced NFC-based mobile contactless payment services to be piloted within the next 12 months.

Isis, the mobile carrier joint venture that includes AT&T, Verizon, and T-Mobile, will be piloting its service in Salt Lake City, UT, and Austin, TX. Users will be able to tap their phones to pay for fares on Utah Transit Authority buses and trams and make purchases at merchant outlets that accept contactless payment in both Salt Lake City and Austin. The pilot projects will begin in the first half of 2012. Isis will work with American Express, Discover, MasterCard, and Visa for its NFC rollouts.[19]

Google announced Google Wallet in May 2011, with general availability planned during October 2011, in New York and San Francisco. Using the Google wallet, consumers can use a Sprint NFC-enabled phone and a MasterCard PayPass or Google prepaid card to pay for purchases at merchants who accept

[16] Tsirulnik, Giselle, *Foot Locker upgrades mcommerce strategy to more complete experience*, Mobile Commerce Daily, May 10, 2011, http://www.mobilecommercedaily.com/2011/05/04/foot-locker-upgrades-mcommerce-strategy-to-more-complete-experience

[17] http://paybyphone.com/

[18] Smart Card Alliance, *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*, op. cit.

[19] http://www.paywithisis.com/#/news/

MasterCard PayPass. Google is also working with POS system companies and top retail brands to allow consumers to be able to redeem promotions, and earn loyalty points.[20]

2.4.4.2 Bar Code-Enabled Proximity Mobile Payment

Another form of proximity mobile payment is based on the use of bar codes. A two-dimensional (2D) bar code is displayed on a smartphone screen and read by an optical scanner at a retail POS, or the smartphone's camera is used as an optical scanner to read a bar code displayed on a POS terminal.[21]

Starbucks has rolled out mobile payment using 2D bar code technology to its nearly 6,800 company-owned stores in the United States. Consumers can download the Starbucks Card mobile app to an iPhone or iPod Touch, a variety of BlackBerry models, and select models of Android phones. The app displays a bar code that the customer uses as a Starbucks Card to make purchases. When the bar code is scanned at the POS, Starbucks deducts the amount of the purchase from the customer's Starbucks Card account. The app also lets a cardholder track the card balance, add to it with a major credit card, check the status of rewards points, and locate nearby Starbucks outlets.[22]

[20] Google, *Google, Citi, MasterCard, First Data and Sprint team up to make your phone your wallet*, May 25, 2011, http://gw-press.appspot.com/index.html

[21] National Retail Federation, *Mobile Retailing Blueprint: A Comprehensive Guide for Navigating the Mobile Landscape*, January 2011, http://www.nrf.com/modules.php?name=Pages&op=viewlive&sp_id=1268

[22] Balaban, Dan, *Starbucks Rolls Out Bar-Code Mobile Payment Nationwide*, NFC Times, Jan. 19, 2011, http://www.nfctimes.com/news/starbucks-roll-out-bar-code-mobile-payment-nationwide

3 Key Requirements and Benefits of NFC Mobile Proximity Payments

New payment methods typically face an uphill battle. The new method must be faster, more convenient, less expensive, or more secure than the current method, or it must provide some new benefit, such as rewards, enhanced record-keeping, or even a "coolness" factor. The benefits must be great enough to overcome barriers to adoption, which include upgrade costs, training and support requirements, the pain of changing behaviors, or the value of any business being replaced, also known as cannibalization. In fact, some technologies seem not to work as well as established technologies when first introduced but are driven to the forefront by an explosion of utility and new uses. This was the case when mobile phones were first introduced.

This section describes the requirements and benefits of NFC mobile proximity payments for the key stakeholders in a mobile payments transaction: consumers, merchants, issuers, and mobile operators. The requirements outlined below establish a baseline for each stakeholder, a set of "must haves," while the benefits are those things which will drive the stakeholder over the "finish line."

Stakeholder requirements for NFC mobile proximity payments fall into the following seven attribute categories:

- **Reliability at POS**: transactions that work every time with fast, robust, reliable performance
- **Security**: secure storage and processing of payment credentials and transaction data, and ability to suspend payment apps in case of fraud or customer request
- **Ease-of-use and convenience**: convenient transactions with an easy, intuitive interface for consumers and store staff, with no training required
- **Wallet functionality**[23]: ability to reliably and easily load payment cards into the wallet, transfer the wallet to a replacement phone, vary payment defaults by merchant, encourage preferred payment instruments, and establish branding
- **Acceptance**: broad merchant acceptance, particularly at every-day venues, with no significant POS or business process changes and coexistence with the existing systems
- **Device deployment/availability**: support in a wide variety of handsets with broad customer availability
- **Value-add applications**: ability to support value-add applications and services – for example, automatically linking retail loyalty accounts, supporting retail promotions and couponing, presenting customer offers in-store, and sending secure payment messages

3.1 Consumer Benefits

Increasingly, people say they cannot live without their mobile phones. NFC mobile proximity payment can offer consumers increased convenience, and personalized assistance with their shopping and payment needs. A wide range of additional applications can also be enabled using NFC technology.

Table 1 summarizes examples of benefits of NFC mobile proximity payment for consumers.

[23] Wallet functionality is not part of the NFC specification and would depend on product features offered by the wallet supplier and capabilities of the POS terminal (e.g., returning receipt to the phone).

Table 1. Consumer Benefits of NFC Mobile Proximity Payment

Attribute	Benefits
Reliability at POS	• NFC contactless transactions are reliable, with certified terminals providing greater first-time read reliability than standard magnetic stripe readers.
Security	• Payment credentials are stored securely in the NFC-enabled mobile device's secure element, protecting the credentials from skimming and account compromise. • The card and transaction authentication process used in contactless transactions leverages dynamic cryptogram technology, which is significantly more secure than current magnetic stripe technology.
Ease-of-use and convenience	• Mobile phones provide an easy and intuitive interface allowing the consumer fast and convenient access to payment accounts. • Payment and loyalty accounts are managed in the mobile wallet, eliminating the consumer's "fat wallet." • Mobile phones provide new convenience features, for example, storing payment records on the phone and integrating with other value-add programs (e.g., loyalty and promotions). • New contactless transaction acceptance points (e.g., NFC-enabled vending machines) increase consumer convenience by reducing the need for carrying cash and coins.
Wallet functionality	• Mobile wallets provide consumers with the ability to use a single device to support multiple payment brand options. • Wallets can also provide additional functionality, including: storing and providing access to merchant-specific payment products; supporting payment, loyalty and merchant promotions (e.g., coupons); storing receipts; and providing organized tracking of offers and promotions.
Acceptance	• Mobile wallets provide consumers with the ability to use a single device to support multiple payment brand options, without carrying multiple form factors. • New contactless transaction acceptance points (e.g., NFC-enabled vending machines and other unstaffed acceptance points) increase consumer convenience by reducing the need for carrying cash and coins. • Recent payment brand announcements providing incentives for merchants to move to contactless and contact POS terminals to support EMV will drive ubiquity of contactless POS acceptance over the next five years.[24]
Device deployment/ availability	• A wide variety of handsets are expected to support NFC in the next two years (see Section 4.5), providing consumers with a choice of mobile device. • MicroSD or other bridging technologies provide the consumer with the potential to add NFC to an existing handset, providing flexibility and choice.
Additional value-add applications	• Mobile devices and wallets provide consumers with the potential for additional value-add applications – for example, providing savings from instant/specialized offers tailored to shopping patterns or tied to consumer location, or supporting additional value-added functions such as key entry to clubs.

[24] Visa, *Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments*, August 9, 2011, http://corporate.visa.com/media-center/press-releases/press1142.jsp

3.2 Merchant Benefits

Merchants require a robust, secure, reliable payment method that they can leverage to enhance loyalty and promotional effectiveness.

Table 2 summarizes examples of benefits of NFC mobile proximity payment for merchants.

Table 2. Merchant Benefits of NFC Mobile Proximity Payment

Attribute	Benefits
Reliability at POS	• NFC contactless transactions are reliable, with certified terminals providing greater first-time read reliability than standard magnetic stripe readers. • Contactless readers require less maintenance, providing cost savings to merchants.
Security	• The card and transaction authentication process used in contactless transactions leverages dynamic cryptogram technology which is significantly more secure than current magnetic stripe technology, reducing fraud. • Increased security and reduced fraud can significantly reduce costly compromises and potential bad PR.
Ease-of-use and convenience	• Mobile payment technology should reduce the frequency that cards are passed to the clerk to perform a transaction, simplifying the transaction. • NFC-enabled vending machines will reduce cash collection costs and stimulate sales. • Contactless POS systems facilitate customer-facing payments. • Customer familiarity with the mobile phone and its ease of use will improve checkout throughput.
Wallet functionality	• The mobile wallet provides opportunities for integration with other merchant value-add applications (e.g., supporting loyalty programs and merchant promotions). • The mobile wallet can encourage a preferred payment instrument (e.g., private label or gift card), and increase store branded card usage rate by reducing wallet space competition.
Acceptance	• Contactless POS readers and terminals can integrate and coexist with merchant POS systems with minimal POS process changes, keeping operational costs in check. • Recent payment brand announcements providing incentives for merchants to move to contactless and contact POS terminals to support EMV will drive ubiquity of contactless POS acceptance over the next five years. • NFC mobile contactless transactions will leverage the EMV payment processing infrastructure • Mobile payments can help to increase electronic payment penetration into traditional cash markets such as at temporary remote locations.
Device deployment/ availability	• A wide variety of handsets are expected to support NFC in the next two years (see Section 4.5), with the ubiquity of mobile phones helping to drive payment and other mobile applications.
Additional value add applications	• Mobile devices and wallets provide merchants with the potential to offer additional value-add applications. • Loyalty program effectiveness can be enhanced – e.g., through mobile enrollment, automated accrual at POS, and special offers. • Promotion effectiveness can be enhanced using the mobile channel and smart posters. • Merchants can offer a mobile app to enhance brand presence. • Mobile devices provide merchants with the flexibility to change the layout of the store and bring checkout to the customer, instead of requiring sales and payment to be separate processes.

3.3 Issuer Benefits

Issuers require transaction and messaging security and can benefit from differentiation, growth achieved by replacing cash payments, and the ability to offer new personalized services.

Table 3 summarizes examples of benefits of NFC mobile proximity payment for issuers.

Table 3. Issuer Benefits of NFC Mobile Proximity Payment

Attribute	Benefits
Reliability	• Reliable NFC contactless transactions reduce the number of lost transactions resulting from magnetic stripe read problems, reduce cardholder calls and improve cardholder satisfaction.
Security	• Contactless transactions enhance security over magnetic stripe card transactions, leading to reduced fraud. The card and transaction authentication process incorporated in contactless transactions leverages dynamic cryptogram technology which is significantly more secure than current magnetic stripe technology. • Increased security and reduced fraud can significantly reduce costly compromises and potential bad PR. • Secure over-the-air provisioning and lifecycle management provide new capabilities for secure issuance of payment credentials and the ability to easily suspend payment applications in case of fraud or user request.
Ease-of-use and convenience	• Mobile phones provide consumers with quick access to payment accounts. Consumer ease of use and convenience can drive "top of wallet" use for the issuer's payment card.
Wallet functionality	• Issuers can establish their brand as preferred in the consumer's mobile wallet. • Issuers can offer new, differentiated payment services through new wallet functionality to increase transaction volumes and extend brand.
Acceptance	• NFC mobile payment provides issuers with new opportunities to further penetrate cash- and check-heavy merchant segments and open new acceptance channels.
Device deployment/ availability	• The ubiquity of mobile phones allows issuers to reach a larger consumer base. • NFC-enabled mobile phones and over-the-air provisioning enables instant issuance of payment credentials.
Additional value-add applications	• Issuers can offer payment-related services such as account management and tracking, instant savings and rewards, personalized loyalty programs, and e-coupons. • Mobile phones provide a personalized messaging channel to drive volumes and usage. • Over-the-air lifecycle management provides issuers with real-time capabilities for card management and issue resolution, reducing lifecycle management costs.

3.4 Mobile Operator Benefits

Mobile operators can benefit from differentiation and reduced customer churn.

Table 4 summarizes examples of benefits of NFC mobile proximity payment for mobile operators.

Table 4. Mobile Operator Benefits of NFC Mobile Proximity Payment

Attribute	Benefit
Security	• The mobile operator can minimize vulnerabilities for multiple issuers and ecosystem stakeholders through the increased security of NFC cryptographic technology and secure element management.
Wallet functionality	• Wallet applications, when incorporated into mobile operator app environments, can build brand value while introducing new opportunities for recurring revenue streams.
Acceptance	• Widespread merchant adoption of mobile payments creates new opportunities for mobile operator participation in the payments landscape.
Device deployment/ availability	• Promoting NFC technology and its array of value-added applications to an expanding base of consumers will enable the mobile operator to differentiate their brand, attract new customers and reduce customer churn, while increasing unit sales and handset upgrades.
Additional value add applications	• The continuous innovation occurring in the app market will create new revenue streams for the mobile operator and increase customer retention.

3.5 Summary

A review of the requirements and benefits for each major stakeholder—consumers, merchants, issuers, and mobile operators—can provide a roadmap for adoption. NFC mobile proximity payment must satisfy all of the stakeholders' basic requirements and offer enough benefits to drive behavioral change and overcome structural inertia.

NFC mobile proximity payment offers increased convenience, security, differentiation, and growth. Moreover, a wide range of additional applications can enhance loyalty and promotional effectiveness and provide new personalized services.

4 NFC Mobile Contactless Payments: State of the Market

This section provides a more detailed review of one specific mobile payment approach – NFC mobile contactless payments – outlining the NFC ecosystem players and roles and discussing the current state of the North American market for NFC-enabled handsets and NFC mobile contactless merchant acceptance.

4.1 NFC Basics

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices located a few centimeters apart. The technology can be used for a wide variety of mobile applications, including:

- Making payments with a wave or a touch of a device anywhere contactless POS readers have been deployed
- Reading information and picking up special offers, coupons, and discounts from posters or billboards on which an RF tag has been embedded (for example, in smart posters and billboards)
- Securely storing tickets for transportation, parking access, or events and enabling fast transactions at the point of entry/exit
- Securely storing information that allows secure building access

NFC-enabled devices are governed by standards in ISO/IEC (ISO/IEC 18092), ETSI (ETSI TS 102 10 V1.1.1 (2003-03)) and ECMA International (ECMA-340), and by specifications published by the NFC Forum. ISO/IEC 18092 allows for backward compatibility with existing contactless devices by supporting ISO/IEC 14443 (the standard used by payment network-branded contactless payment cards and devices), and the Japanese Industrial Standard (JIS) X 6319-4 (also known as FeliCa) contactless interface protocols.

An NFC-enabled device can operate in reader/writer, peer-to-peer, or card emulation mode. For mobile contactless payments, the NFC-enabled mobile device operates in card emulation mode and appears to an external reader to be a traditional contactless smart card. Payment information is stored in the mobile phone in a secure element, which is a smart card chip that protects stored data and enables secure transactions. Contactless payments and ticketing using NFC devices can be enabled without changing the existing acceptance infrastructure.

The NFC Forum[25] has developed and released implementation specifications and has also launched a certification program that checks devices for compliance with NFC Forum specifications. Compliant devices behave consistently, facilitating an interoperable infrastructure.

4.2 NFC Ecosystem

Deploying NFC mobile contactless payment applications requires an ecosystem in which stakeholders cooperate to deliver different functions and capabilities.

Figure 2 shows the stakeholders in the NFC ecosystem. As the figure illustrates, the secure element in the NFC-capable device (discussed in the following section) is provided to the consumer by one of the ecosystem stakeholders. Which secure element is chosen and who provides it has critical implications for usability, portability, ubiquity of handsets, and control.

[25] http://www.nfc-forum.org

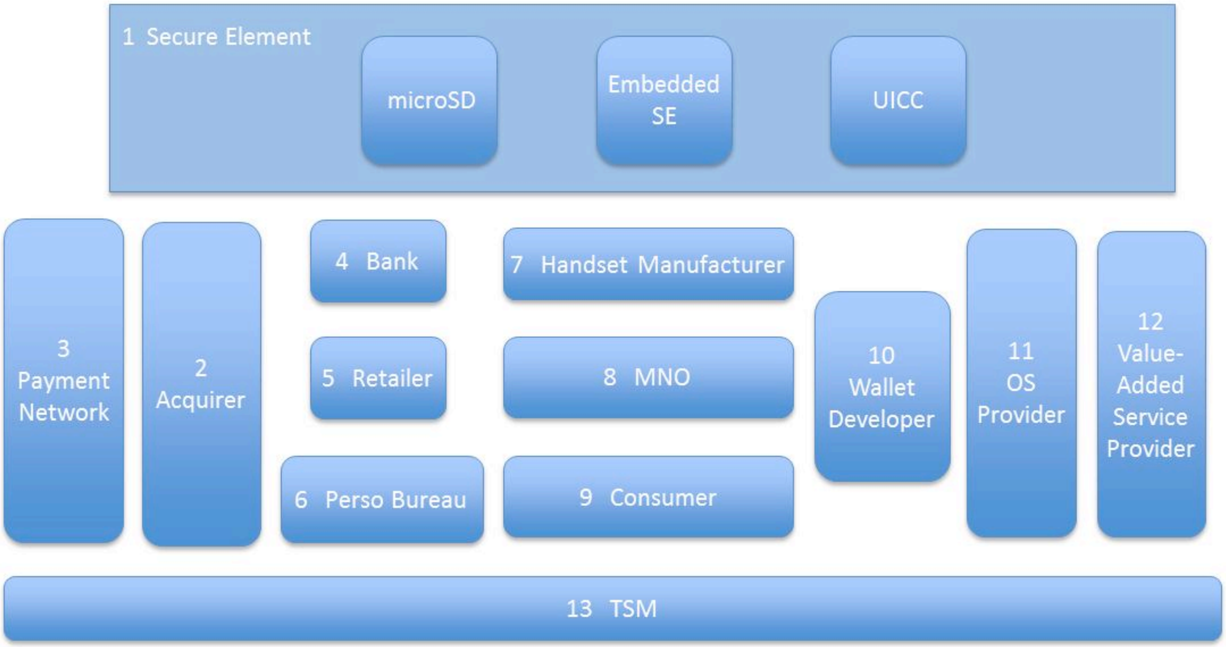

Figure 2: NFC Ecosystem

4.2.1 Secure Element (1)

The secure element (SE) is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications (e.g., American Express, Discover, MasterCard, Visa and other payment applications). SEs can also support other types of secure transactions, such as transit payment and ticketing, building access, or secure identification.

A mobile handset can implement the SE in one or more of the following ways:

- MicroSD removable SE
- Embedded SE
- UICC removable SE

MicroSD removable SE. The microSD is an SE form factor that can enable mobile contactless payment on phones that do not have inherent NFC capabilities. Many phones on the market already support microSD cards; adding a specially-equipped microSD with an SE to such a phone enables contactless payment transactions. The microSD can contain a payment application, a cryptographic coprocessor, the NFC controller and antenna, and even the user interface to a wallet for display on the phone. Mobile phones lacking embedded NFC capability can become mobile contactless payment enabled by inserting a microSD card.

Embedded SE. Another option is to embed an NFC-payment-capable SE in the phone when it is manufactured. This implementation does not provide the portability of the microSD or UICC approaches. However, it does allow the phone's manufacturer and mobile operating system providers to design, certify, and implement basic NFC payment transaction applications for a particular phone.

UICC removable SE. The third option is to include an SE in a removable UICC or SIM card. SIM cards have been used in mobile phones for years. Although the SIM slot on the phone is not designed to accommodate frequent changes, and therefore is typically not accessible from the external casing of the phone, some phones include accessible SIM slots. Consumers who buy a new phone for use with the same mobile network operator (MNO) can insert the SIM card from their old phone into their new phone, use the phone on the MNO's network, and port their contact information and phone number to the new handset.

All phones that support Global System for Mobile Communications (GSM) technology use a SIM, so adding an NFC payment application SE to the SIM is a natural extension. Unfortunately, most phones that currently incorporate SIM cards require upgrades to use a UICC that supports NFC. For this reason, UICCs have been created that also support an NFC controller and antenna. This type of UICC bridges the need to replace the phone to enable NFC payments.

A variety of stakeholder relationships are possible, depending on how the SE is implemented. Section 8 describes the possible relationships and interactions among stakeholders for the three SE approaches.

4.2.2 Acquirer (2)

Acquirers facilitate the placement of terminals at retail locations and the communication of payment transactions to the payment networks for authorization and settlement. To support NFC payment transactions, acquirer terminals at merchant customer locations must support NFC/contactless transactions.

4.2.3 Payment Network (3)

Payment networks facilitate authorization processing and the settlement of bank card transactions. To support NFC payment transactions, payment networks must support contactless messaging and authentication functions.

4.2.4 Bank (4)

In the standard card payment system model, the bank (issuer) holds the funding account for a consumer's payment card and is responsible for provisioning credit and debit cards to the bank's customers. In the emerging open NFC payment system model, the bank continues to hold the funding account but works with other parties to provision the payment application to NFC-enabled mobile phones. In most cases, issuers will deploy physical "companion cards" for customers to use at locations where NFC mobile contactless payment is not accepted. The bank card issuers' host systems will need to support mobile contactless transactions.

4.2.5 Retailer (5)

Retailers can both accept NFC payment transactions and issue NFC payment applications. To accept NFC payment transactions, retailers need NFC-enabled contactless POS terminals that are certified to process each payment brand's NFC payment application. Retailers can also choose to implement closed-loop NFC payment applications (such as gift cards or a retailer-specific payment card) or other value-added applications (e.g., coupons, loyalty).

4.2.6 Personalization Bureau (6)

The personalization (*perso*) bureau traditionally provisions credit and debit cards to consumers by mailing them. The bureaus receive files from a bank that contain information for provisioning the card's magnetic stripe and/or smart card chip, and data for embossing and mailing the card. Preprinted cards are processed through equipment that performs both card surface personalization and electronic encoding of the magnetic stripe and contact or contactless chips. The personalization process also provides for the ability to insert companion cards or tokens as well marketing inserts linked to a specific product.

To support the adoption of contact and contactless chip technology card issuers and personalization bureaus have had to implement new applications to convert the cardholder data into a format compatible with chip technology and to establish and apply cryptographic security keys that are at the core of chip technology security. These applications are generically referred to as data preparation and key management applications. These same applications can be leveraged to prepare data and establish issuer-specific security for NFC-enabled mobile proximity payment applications.

Personalization bureaus that personalize contactless chip cards for issuers may already have these applications in place and only need a payment-brand-specific script to add the ability to prepare cardholder data and application security. With some adjustments to the standard mass personalization equipment, these personalization bureaus will have the ability to electronically personalize microSD and UICC cards through the standard card issuance process. For microSD cards, contactless programming stations are required on the equipment, and for UICC cards contact programming stations are required. By leveraging the standard card personalization process, issuers have the ability to insert an NFC-enabled microSD or UICC in the same mailing envelope as the consumer's standard card.

Perso bureaus can also perform the role of creating the personalization data, setting the application security keys and passing the data to a trusted service manager (TSM) to provision the data into a consumer's NFC-capable phone. In this case, the bureau's role will change; rather than personalizing a bank card before it is issued, the bureau will be personalizing an account on a mobile phone that has already been distributed. Personalization bureaus are often considered good candidates for offering TSM capabilities to issuers.

In some cases financial institutions may want to maintain control of their data and the NFC-enabled mobile proximity payment application. This can be achieved by implementing the same data preparation and key management systems that are used by personalization bureaus. In addition, these systems can be configured to work in an online real-time environment, with an interface for over-the-air provisioning.

4.2.7 Handset Manufacturer (7)

The handset manufacturer defines which mobile phone models will be NFC-enabled based on the MNO's requirements and the level of demand projected in the market. Handset manufacturers may also have a stake in the embedded SE model (versus other SE approaches), potentially introducing additional business models.

4.2.8 Mobile Network Operator (8)

The MNO provisions wireless settings for phones provided to consumers and determines both the required handset features and functions and the service options to be provided with mobile phones sold by the operator.

4.2.9 Consumer (9)

In the context of the NFC ecosystem, the consumer is a customer of the NFC payment application issuer. How the consumer becomes aware of NFC payment options may determine how the NFC payment capability is loaded to the consumer's handset.

4.2.10 Wallet Developer (10)

A wallet developer is a value-added application provider who provides the user with an interface on the mobile phone to manage multiple NFC payment applications. To facilitate consumer demand for multiple payment options, the wallet developer provides the wallet, either directly, as part of the issuer's NFC payment solution, as an application provided by the MNO, or through another vendor or service provider.

4.2.11 OS Provider (11)

An operating system (OS) provider maintains the core OS used by various handsets, including version upgrades, and provides application programming interfaces so that application developers can provide compatible applications. The OS provider may also provide a wallet application and other value-add applications.

4.2.12 Value Added Service Provider (12)

Numerous service providers can be involved in the NFC ecosystem to provide value-added applications. The value-added service provider would provide the application and the services required to deliver the application to the NFC-enabled mobile phone. Examples of value-added services include coupons, loyalty programs, merchant promotions and offers, and location-based services.

4.2.13 Trusted Service Manager (13)

The TSM is the trusted third party who provides over-the-air (OTA) services to the NFC payment application issuer and the owner of the SE (e.g., the MNO, issuer, or retailer). The TSM handles the provisioning and management processes so that issuers do not need to deal with multiple MNOs, phone models, and operating systems, and MNOs do not need to deal with multiple issuers. The TSM role could be played by many different entities, including the MNO, the issuer, the personalization bureau, the payments processor, or some other neutral third party service provider. Multiple TSMs may be involved in the provisioning of a payment application.

The primary role of the TSM in the NFC ecosystem is to facilitate management of the NFC payment application on the consumer's phone. A few of the functions provided by the TSM are OTA activation or provisioning of the NFC payment application, life-cycle management of the NFC payment application on the consumer's phone, and bridging services for transferring the NFC application to a new phone when necessary. A core piece of the OTA provisioning process includes preparing the data and accessing the appropriate security keys required to initially provision the NFC payment application and to update it once provisioned.

4.3 NFC Provisioning

One of the first steps in enabling NFC payments is to load the payment application or wallet (or both) onto the mobile phone and personalize the application and wallet to the mobile phone owner. This process is referred to as *NFC provisioning*. Provisioning actually has a number of steps, and the provisioning method can vary, depending on the type of SE used and the channel by which the application is offered to the consumer. Because the payment application or wallet is stored in the secure element on the mobile phone, the provisioning entity must have access to security keys.

Figure 3 illustrates four methods of provisioning an NFC payment application, which are described in the following sections. A single mobile payment application issuer can use one or all of these methods; in addition, multiple methods are possible at certain channel points. For example, OTA, Internet Web page, or an instant issuance application are all possible methods for provisioning within a financial institution's branch.

4.3.1 OTA Provisioning

OTA provides a means to load, activate, and personalize an NFC payment application by leveraging the mobile phone wireless networks. A mobile phone user can initiate the OTA provisioning process from wherever the user has network access. The process is very similar to the process used today to download standard applications to a smartphone. The primary difference is that the source of the payment application requires specific authorization from an issuer and the keys required to access the secure element on the phone.

4.3.2 Internet-Based Provisioning

A mobile phone can be connected to a home computer or a Wi-Fi network and use the Internet communication infrastructure to provision a mobile payment application. Figure 3 depicts this as provisioning from a Web page.

This method enables mobile payment application issuers to provide the payment application for download and to initiate activation from a Web page. Provisioning from a Web page also enables visual guidance and user training. The underlying security required to facilitate the provisioning process is the same as for the OTA process.

4.3.3 Central Issuance

The process of provisioning through a central issuance channel mirrors the current plastic card issuance process. A mobile payment application is often the companion to a plastic card. When an application is issued through a central channel, a microSD card on which the personalized payment application is loaded can be included in the mailer with the standard plastic card. The mailer can also include inserts explaining how to use the microSD card and activate the account.

4.3.4 Instant Issuance Applications

Instant issuance applications are suitable for provisioning mobile payment applications within financial institution branch networks, MNO retail outlets, or other channel points with an internal network and a service representative available to assist consumers in the activation process. An instant issuance application can also provide local activation reporting, inventory management (if microSD cards are the carrier for the payment application), and other standard instant-issuance features, such as interfaces to authorization switches and issuer card management systems. Instant issuance could apply to any secure element form and could use the personalization systems that are currently used for instant issuance of traditional bank cards, once they have been upgraded to support NFC provisioning.

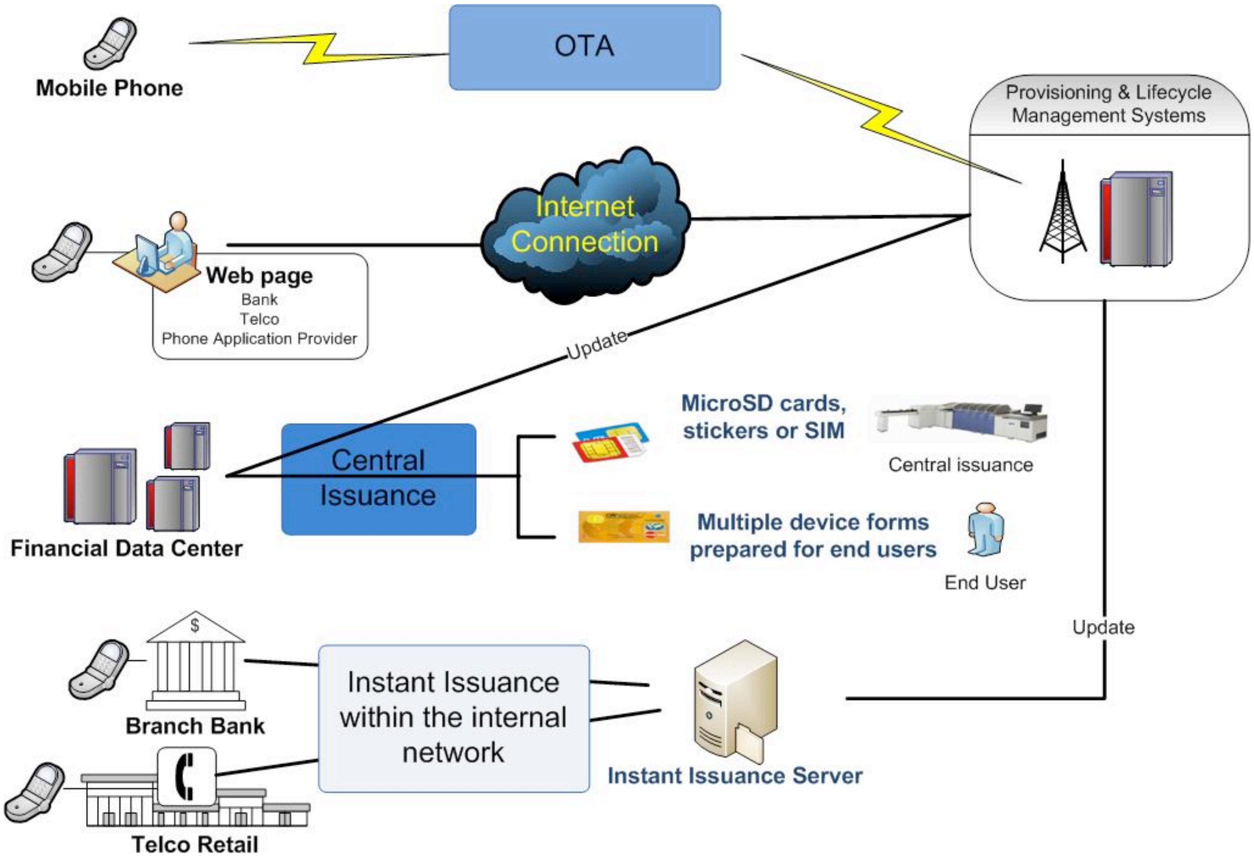
Mobile Phone
OTA
Provisioning & Lifecycle Management Systems
Internet Connection
Web page
Bank
Telco
Phone Application Provider
Update
MicroSD cards, stickers or SIM
Central issuance
Financial Data Center
Central Issuance
Multiple device forms prepared for end users
End User
Update
$
Branch Bank
Instant Issuance within the internal network
Instant Issuance Server
Telco Retail

Figure 3. NFC Provisioning

4.3.5 Provisioning and Life Cycle Management System

It is essential to maintain a record of what mobile payment applications have been activated. Figure 3 shows that each of the provisioning methods is connected to a provisioning and life cycle management system, illustrating the need to coordinate and manage activity across channels and methods. The provisioning and life cycle management system is often implemented by a TSM, but it could also be an add-on application to an issuer's card management system. The system maintains information required to reprovision wallets and mobile payment applications when consumers lose their phones or change phones and carriers.

4.4 NFC Security Approaches

Figure 4 illustrates the security mechanisms that protect the processes used in NFC mobile contactless payments.[26] Additional information on security approaches used for NFC-enabled mobile contactless payments can be found in the Smart Card Alliance white paper, *Security of Proximity Mobile Payments*.[27]

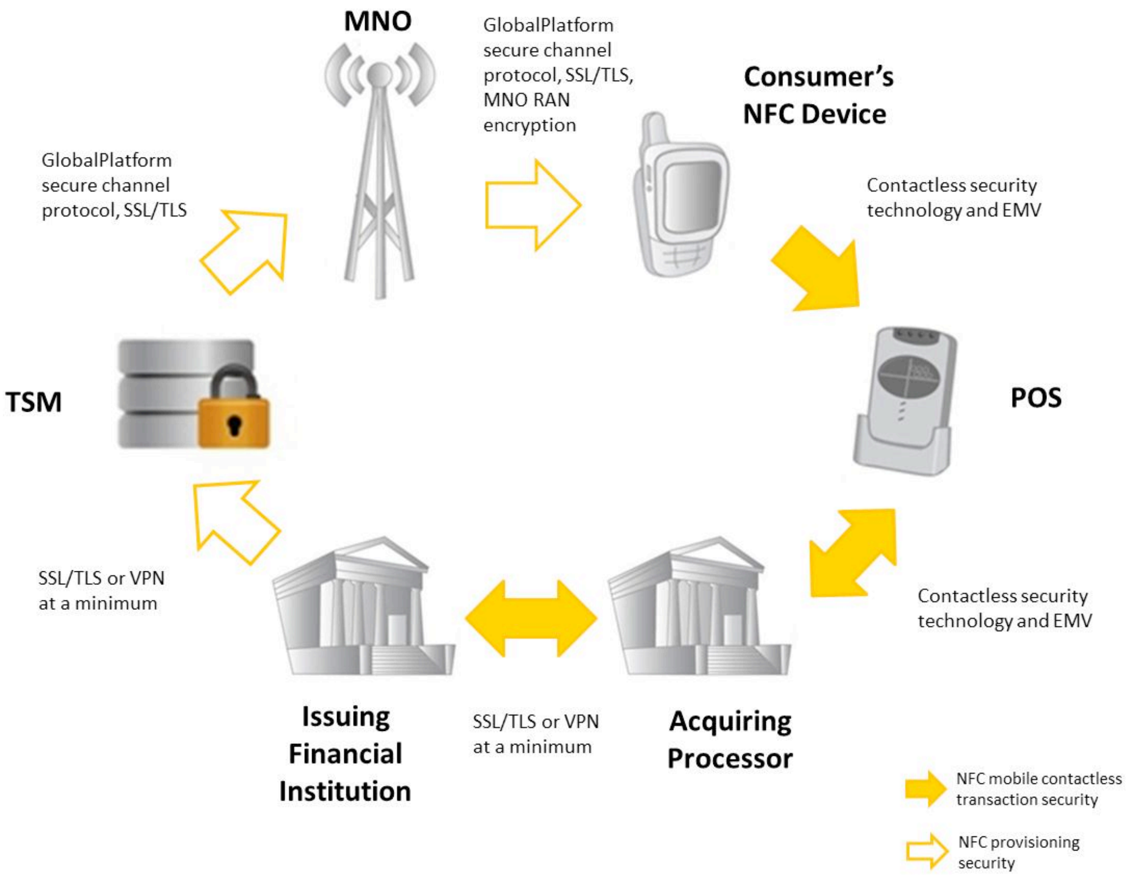
MNO
GlobalPlatform secure channel protocol, SSL/TLS, MNO RAN encryption
Consumer's NFC Device
GlobalPlatform secure channel protocol, SSL/TLS
Contactless security technology and EMV
TSM
POS
SSL/TLS or VPN at a minimum
Contactless security technology and EMV
Issuing Financial Institution
SSL/TLS or VPN at a minimum
Acquiring Processor
NFC mobile contactless transaction security
NFC provisioning security

Figure 4. NFC Mobile Contactless Payments Security Mechanisms

The transmission of payment, personalization, and life cycle management information from the issuer to the TSM is secured by standard Internet technologies, such as secure sockets layer (SSL) or virtual private networks (VPNs). GlobalPlatform's secure channel protocol provides for transmission of sensitive

[26] Canadian implementations may be different.

[27] Smart Card Alliance, *Security of Proximity Mobile Payments*, May 2009, http://www.smartcardalliance.org/pages/publications-security-of-proximity-mobile-payments

account data between the TSM and the SE in the mobile device and storage of such information in the SE. Account data is further kept secure from OTA sniffing by encryption provided by the MNO.

When the consumer uses the NFC device for payment, the transaction is protected using the dynamic cryptogram authentication technology already in place for contactless credit and debit cards.

4.4.1 Secure Delivery of Financial Data

Mobile contactless payments do not require that account data be stored on a physical card. The data is passed securely from the issuing bank through a TSM to the SE in the mobile handset. The data is protected by cryptography throughout the process; the TSM has a critical role in managing the security of the process and keeping the cryptographic keys secure through the use of both physical and logical security measures.

4.4.2 Protecting Stored Payment Application and Account Information

Within the mobile phone, both the payment application and consumer account information must be protected, and different NFC applications must be able to work securely and independently of each other. Security approaches used include:

- Storing the payment application and data in the SE (see Section 4.2.1).
- Using GlobalPlatform-specified security domains and hierarchy to provision data OTA to the SE.
- Using smart card technology inherent in the SE to authenticate all communications with the application to update or change operational parameters and to provide built-in tamper resistance security features that recognize hostile attacks and take appropriate protective measures, such as blocking the application.
- Providing a mobile wallet for accessing the payment account information in the SE during a transaction, with an optional personal identification number (PIN) authorizing access to the wallet.
- Leveraging existing and future EMV contactless card transaction authentication security technology.
- Leveraging existing issuer host system payment transaction authorization technology and account management processes.

4.5 NFC Handset Status

The availability of NFC-enabled handsets continues to grow. According to Juniper Research, at least one in five smartphones will include NFC technology by 2014. More than 20 mobile phone manufacturers are currently producing or rumored to be in preproduction of NFC-enabled handsets.[28] Since there are frequent announcements of new handset availability being made, the section provides only a snapshot of handset availability as of September 2011.

Google's Android operating system is increasing in importance in the market, and the Gingerbread and Ice Cream Sandwich versions support NFC. Google's current smartphone market share is close to 30%[29] and is expected to reach 38.5% by the end of 2011,[30] representing a larger portion of the market than Apple's iOS, which commands a 19.4% share. Google also recently released the Android NFC APIs to developers, sparking an initiative to create NFC applications. These development possibilities, combined

[28] Clark, Sarah, *List of NFC Phones*, NFC World, SJB Research, 13 June 2011, http://www.nearfieldcommunicationsworld.com/nfc-phones-list/

[29] NetMarketShare, *Mobile Holiday Winners*, May 2011, http://www.netmarketshare.com/2011/01/01/Mobile-Holiday-Winners-iOS-Gains-the-Most-Usage-Share-but-Android-Has-the-Highest-Growth-Rate

[30] Reiseinger, Don, *Android Market Share to Near 50 Percent*, CNET, April 2011, http://www.cnet.com/8301-13506_3-20051610-17.html

with Google's growth rate and market share, the acquisition of Motorola Mobility,[31] and the addition of card emulation by Google, represent perfect conditions for massive market expansion.

Currently more than 10 NFC-enabled handsets are available for purchase worldwide. Samsung leads the way with the Galaxy S II and S5230 (marketed under various names depending on the country) and has teamed with Google to produce the Nexus S and Nexus S 4G (available on T-Mobile and Sprint). Nokia has released both the C7 (Europe) and Astound (U.S.);[32] Motorola and Casio have released their respective industrial personal data assistants, the MC75A[33] and IT-800RGC-35.[34]

Smartphones on the horizon include the Samsung Wave 578, the Blackberry Bold 9900/9930 (available in mid-2011), and two other unnamed Samsung phones to be released in September 2011.[35] Other manufacturers, such as LG, Toshiba, and Fonelabs, have issued limited release/proof-of-concept NFC-enabled handsets and are expected to produce something similar.[36]

There is currently speculation that Apple, Sony Ericsson, HTC, Motorola, LG, and Blackberry are considering NFC-enabled handsets. Such speculation is mainly centered on Apple, which is sending mixed messages about whether the iPhone 4S/iPhone 5 will include NFC technology. There is persistent speculation that Apple will produce the technology themselves and NFC will be included in the iPhone 5.[37]

If Apple intends to enter the NFC market, it will face competition from Google. Google has the first mover's advantage in terms of handsets and holds that same advantage concerning payments (Google Wallet). Assuming Apple does not release an NFC-capable iPhone until 2012, Blackberry will almost certainly be the second major manufacturer to enter the NFC market with the Bold 9900/9930.[38]

Internationally, Sagem Wireless released its own handset, the Cosyphone,[39] in France in 2010, with availability in selected cities in the United Kingdom and Ireland. Chinese manufacturer Hedy[40] currently supplies NFC-enabled handsets to Chinese mobile provider giant Unicom, and Shanghai Simcom is currently producing numerous NFC-enabled handsets under the brand name East Com;[41] both manufacturers are partnering with chip manufacturer Shanghai Fudan Microelectronics.[42] Malaysian manufacturer Fifth Media, in collaboration with Garmin Asus, is currently producing specialist handsets, Axia A306 and A206, both running on Windows Mobile 6.5.3.[43] The Sky Vega Racer by Pantech, dubbed the fastest Android phone yet, is to be released in Korea in mid-2011.[44]

[31] http://www.wired.com/epicenter/2011/08/google-motorola-acquisition/

[32] Nokia USA, *Nokia Astound -- Made to Perform*, Nokia USA, http://www.nokiausa.com/find-products/phones/nokia-c7-00

[33] Motorola, *MC75A HF RFID Contactless Mobile Computer*, Motorola Solutions, http://www.motorola.com/Business/

[34] Casio, *IT-800*, CASIO-B2B, http://www.casio-b2b.com/mis/uk/products/it800/

[35] Near Field Communications World, *A definitive list of NFC phones*, http://www.nfcworld.com/nfc-phones-list/

[36] Ibid.

[37] Lowensohn, Josh, iPhone *5 Rumors Again Claim NFC, A5, Big Screen*, CNET News, 22 March 2011, http://news.cnet.com/8301-13579_3-20045918-37.html

[38] Blackberry, *Blackberry Bold Touch 9900/9930*, http://us.blackberry.com/smartphones/blackberrybold/touchbold.jsp

[39] Clark, Sarah, *Sagem Wireless' New NFC-enabled Cosyphone*, NFC World, September10, 2010, http://www.nearfieldcommunicationsworld.com/2010/09/10/34448/hands-on-sagem-wireless-new-nfc-enabled-cosyphone/

[40] Clark, Sarah, *China Unicom to Launch World's First Commerical Single Wire Protocol Based NFC Service*, NFC World, 19 February 2010, http://nearfieldcommunicationsworld.com/2010/02/19/32859/china-unicom-to-launch-worlds-first-commercial-single-wire-protocol-based-nfc-service

[41] Specific model numbers are not available.

[42] NFC Software, *List of NFC phones*, http://www.nfc-software.com/list-of-nfc-phones/

[43] Near Field Communications World, op. cit.

[44] Phandroid, *Pantech's Vega Racer Shows Up in Google Phone Gallery,* June 21, 2011, http://phandroid.com/2011/06/21/pantechs-vega-racer-shows-up-in-google-phone-gallery/

4.6 NFC POS Infrastructure Status

The NFC POS infrastructure comprises the following components:

- Contactless/NFC readers
- Payment terminals
- POS systems

4.6.1 Contactless/NFC Readers

Contactless readers provide the consumer with the touch point for exchanging data between the NFC handset and the POS system. Contactless NFC readers support the standards defined in Section 4.1. NFC standards (ISO/IEC 18092) are compatible with ISO/IEC 14443, the standard used by contactless payment card readers; as a result, contactless payment card readers can accept transactions from NFC handsets operating in card emulation mode. The newer contactless readers can also operate in peer-to-peer mode with NFC handsets for transactions other than bank card payment transactions, such as loyalty applications or coupon redemption.

Contactless readers can be part of the payment terminal or separate. Payment terminal vendors support contactless readers integrated with the payment terminals. Vendors also market separate contactless readers that can integrate with any payment terminal to enable contactless and NFC transactions.

4.6.2 Payment Terminals

Payment terminals interact with the contactless readers to obtain the payment data from the NFC device instead of from the magnetic stripe on a card and construct records to send to the POS system (if they are integrated) or directly to processors (if they are standalone).

Traditionally, payment terminals accept payment cards, gift cards, and loyalty cards. Payment terminals with contactless readers can be loaded with payment brand applications (American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa payWave) for contactless payment card and NFC mobile payment transactions. When operating with contactless readers and NFC mobile phones, payment terminals may need to accept other items, such as coupons and tickets. New terminal and reader applications are being created to support these items and to send the transactions to the POS system or directly to the processor.

Major POS terminal vendors have upgraded their payment terminals to incorporate contactless readers. They have also created a process to securely deploy applications in the payment terminals and contactless readers without requiring recertification of the payment brand applets.

4.6.3 POS Systems

The POS systems (supporting cash registers and shopping applications) provided by vendors such as IBM, NCR, and Micros (and possibly customized by retailers) must be capable of accepting new transactions from the payment terminals and returning the transaction results to the payment terminals when the response is to be returned to the NFC handset.

Some NFC/digital coupon solutions are triggered by loyalty cards to retrieve coupons stored in a backend system owned by the retailer (e.g., Safeway Copient) or operated by a third party (e.g., Zavers). These POS systems will require changes at the application level.

4.6.4 NFC and EMV

Globally, the payments industry is migrating from magnetic stripe bank cards and infrastructure to EMV chip cards and infrastructure. EMV is an open-standard set of specifications for smart card payments and acceptance devices. Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. In August 2011, Visa announced plans to accelerate chip migration and adoption of mobile payments in the United States, through retailer incentives, processing infrastructure acceptance requirements and counterfeit card liability shift.

NFC mobile contactless payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by contactless EMV credit and debit cards. NFC-enabled mobile phones will be able carry one or more payment applications and accounts from different issuers; the NFC specifications don't define or specify the payment application. NFC payment applications will follow the payment brand specifications for the region of the world where they are being issued. An EMV payment application and account would be loaded in the NFC-enabled phone and used with compatible EMV POS terminals.

EMVCo, the organization that manages, maintains and enhances the EMV specifications, has been active in defining the architecture, specifications, requirements and type approval processes for supporting EMV mobile contactless payments. This effort has been critical in supporting the launch of NFC mobile contactless payment in regions that have already migrated to an EMV-based payments infrastructure.

Since both NFC technology and EMV payment cards are being introduced into the North American market over the next few years, merchants should select and install POS terminals that support both capabilities when upgrading their POS infrastructure.

4.7 Stakeholder Activities

Within the United States, two major influences motivate stakeholders: the activities of Google[45] and its partners and of Isis[46] and its partners. A third influence is the activities of Apple, although Apple has made no formal announcements about NFC support. (Section 4.5 contains additional information on Google and Isis.)

Table 5 summarizes examples of NFC mobile contactless payments stakeholders in the United States. The list of stakeholders in the table is not inclusive of all companies offering products and services in the market; since the NFC market is emerging and changing rapidly, the listing should be viewed as providing examples to illustrate the breadth of NFC ecosystem participants.

Table 5. Example of Stakeholder Activities in the United States[47]

Stakeholder	Example Companies
MicroSD and specialized hardware solution vendors NFC device add-on vendors	DeviceFidelity Tyfone WatchData Technologies Wireless Dynamics
NFC SE and UICC suppliers	Gemalto G&D INSIDE Secure NXP Semiconductors Oberthur Technologies STMicroelectronics

[45] http://www.google.com/press/pressrel/20110526_wallet.html; http://www.youtube.com/watch?v=am8t6iZ7up0

[46] http://www.paywithisis.com/news/2011-06-21-austin-launch-press-release.html; http://www.youtube.com/watch?v=7EIyAoID2JE

[47] This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Stakeholder	Example Companies
Payment networks	ACH Network American Express Discover MasterCard Worldwide PayPal STAR Visa Inc.
Banks	Citi Barclays Bank of America
Retailer POS suppliers and acquirers/processors	Castles First Data Hypercom Ingenico VeriFone ViVOtech
Perso bureaus	First Data Gemalto G&D Oberthur Technologies
NFC handset manufacturers	HTC Huawei LG Nokia Pantech RIM Sagem Samsung
MNO/telecom related services	Isis Monitise Smart Trust Sprint Sybase 365
Specialized software solution developers and vendors: device software, apps, wallet, similar software	Cassis C-Sam Google mFoundry ViVOtech
OS providers and web-based services companies	Apple Google Microsoft RIM
TSMs	Bell ID Cassis First Data Gemalto G&D Obethur Technologies SK C&C

4.8 Regulatory Environment

The rapidly developing mobile payments market will undoubtedly raise interesting questions regarding regulatory oversight, and will bring together regulatory bodies that share an interest in different parts of the mobile ecosystem, such as the Federal Reserve (Fed), the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC). In fact, the research arms of the Boston and Atlanta Feds have been actively engaged in this space, and recently published a white paper through the Mobile Payments Industry Workgroup (MPIW), which they sponsored. The MPIW was formed in early 2010, and recently published a paper titled "Mobile Payments in the United States – Mapping Out the Road Ahead".[48] Page 9 of this report states the following:

> "Regulators must participate in the evolution of mobile as the regulatory framework for mobile payments is fragmented with respect to MNO and other third party participation in the provision of payment services. In business model examples where payment flows leverage existing value chains of networks and payment clearing and settlement systems such as the card brands and the ACH, existing regulatory oversight and consumer protections are expected to prevail. However, questions are arising about the legal liabilities and responsibilities of new parties to the payments transaction, which may be governed by agreements between the stakeholders in the value chain. Participants desire clarity of the new regulatory structure and want to know how to be proactive in addressing consumer protection issues such as identity management, cyber-security and prepaid mobile accounts. Dialogue between FI regulators, the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Department of Commerce, and with mobile industry stakeholders is necessary to ensure that emerging mobile payments."
>
> The report goes on to suggest that "…representative constituencies of all of these participant groups have asked the FED to coordinate with other regulatory agencies (such as the FCC and FTC) and provide a "regulatory road-map" of what functions, activities, and implementations would be viewed as permissible over the next three to five years. These mobile payments ecosystem players are also asking for clarity on what infrastructure can/should be shared on a non-competitive basis."

The Smart Card Alliance and its members have been active in the MPIW activities to date, and will likely remain very engaged. The approach taken by the Fed thus far has been collaborative, and this presents an encouraging scenario regarding at least a likelihood that regulatory bodies will not inhibit innovation in the mobile payments space, and may even continue to actively encourage and support such innovation. However, there remains a risk that the FTC, the Fed, and other bodies might not continue to move in lockstep with the industry or with each other, given the different constituencies involved. For this reason, and to mitigate this risk, it will continue to be critical for the Smart Card Alliance, its members and industry stakeholders to remain actively involved in trying to keep interests aligned in a way that continues to support the growth of this developing market.

[48] Federal Reserve Board of Atlanta, *Mobile Payments in the United States: Mapping Out the Road Ahead*, March 25, 2011, ww.frbatlanta.org/documents/rprf/rprf_pubs/110325_wp.pdf

5 Comparison of Mobile Payment Approaches

Currently, the following technologies are available (or have been announced) that can enable mobile payment:

- Mobile handset with integrated NFC
- Non-integrated NFC and contactless devices, such as stickers, microSD cards, key fobs, and similar form factors
- Bar codes
- Mobile phone initiated payments in the cloud
- SMS text messaging

Each technology has advantages and disadvantages, and they are not mutually exclusive. A single device can accommodate multiple types of mobile payments. At least in the short term, it is likely that no single technology will prevail. Just as consumers can currently choose whether to pay with cash, use a magnetic stripe credit card or a PIN or signature debit card, or write a check, they will be able to choose between different types of mobile payments, depending on the circumstances (e.g., using a bar code at a merchant who has adopted that technology or tapping the phone for NFC payment at a different merchant location).

5.1 Review of Mobile Payment Approaches

This section reviews and evaluates the different approaches to mobile payments. Table 6 summarizes the results.

5.1.1 Mobile Handset with Integrated NFC

The concept of implementing NFC-based mobile payments on a handset with an integrated SE continues to attract attention. Until recently, the adoption of NFC in the United States has lagged, due in part to adoption being a “chicken-and-egg” problem. While this method of payment requires a POS terminal capable of accepting contactless transactions, relatively few merchants in the United States have installed appropriate terminals. Therefore, consumers cannot use their contactless devices in many places, discouraging adoption by more consumers. The recent Visa announcement mandating that acquirers implement support for contactless transactions by 2013 should significantly increase the rate of acceptance at merchants throughout the U.S. Also critical to widespread availability is agreement among the different business partners involved (issuers and mobile carriers) on a business model. Only recently have joint ventures been formed (Isis and Google Wallet). These strategic alliances should strengthen the case for NFC, and there is a strong likelihood that NFC is poised to become the dominant mobile payments technology.

NFC-based payments are processed through a payment brand and are therefore suitable for payment over both open-loop merchant networks and restricted access networks.

NFC-based contactless payments are extremely secure; there is no empirical evidence to the contrary. However, NFC technology is new to consumers, and they require education regarding its safety and security. There is a perception by consumers that NFC may be unsafe (“What if I lose my phone?”) when in fact there are numerous ways to protect the phone’s wallet beyond the standard account management processes for rapidly blocking transactions from a specific PAN (primary account number), including the ability to protect access with a PIN and disable information on the handset remotely.

The benefits of NFC mobile contactless payments include the following:

- Handsets are more ubiquitous than credit cards; consumers are more likely to have their phones with them than a traditional wallet or purse.
- The processing power of the handset supports a robust interface and the ability to integrate core payment functionality with other applications.
- The wallet interface can support value-added applications such as loyalty programs.

- Payment credentials are stored in an integrated SE and accessible through an application that can be protected by a passcode or other means.
- Existing payment networks and the growing infrastructure for card-based contactless payments can be leveraged.

The challenges with NFC contactless payments include the following:

- A limited number of integrated NFC handsets are currently available in the market, although this situation is expected to change in the relatively near future. Regardless, new equipment will be required.
- The business relationships will continue to evolve and are probably more complex than for any other solution, presenting some risk and potential consumer inconvenience.
- Physical POS hardware upgrades are required for merchants who currently do not accept contactless payments. Installed contactless POS terminals may require application or software upgrades to accept NFC contactless payments.

5.1.2 Stickers / microSDs / Other Non-Integrated Devices

Stickers, microSDs, and similar approaches (e.g., key fobs, watches) allow a consumer to use a device other than a mobile handset to transmit payment credentials to a contactless POS terminal. While some of these approaches are more robust than others, many of them are essentially identical to the use of a contactless card in terms of data personalization, security, and functionality. In all cases, fulfillment is required, and personalization solutions other than the standard credit card personalization process may also be required. Fulfillment is often performed by the issuing bank, which delivers both a standard card and the alternate device (often referred to as a companion device).

In many cases, the peripheral device is restricted to a single payment credential. Some of these solutions are partially integrated with a mobile handset, using a microSD slot for example, that takes power from the phone. There are also standalone devices, such as key fobs, and devices that are intended to be affixed to a handset or other surface. In some cases, these devices are used as a supplemental prepaid device that is linked to another account and may be reloadable.

The benefits of using microSDs and other contactless devices include the following:

- Deployment can move more quickly, because availability of the devices is not tied to the availability of handsets and OTA provisioning services.
- Issuers can leverage the existing provisioning infrastructure for personalization and delivery of the device.
- The payment networks and the growing infrastructure for card-based contactless payments can be leveraged.
- MicroSD solutions can be integrated with the phone, provide the same level of security as integrated NFC, and provide a richer user experience than other non-integrated approaches.

The challenges with using microSDs, stickers and other contactless devices include the following:

- Non-integrated solutions can provide more options for distribution, but may add more complexity for supply chain deployment (e.g., inventory, supplier management).
- Non-integrated solutions (e.g., stickers) may not provide a user interface.
- The performance of non-integrated solutions can be affected by the physical phone design (e.g., phones with metal bodies).
- Stickers typically are from a single issuer, providing less flexibility for the consumer.
- Some mobile devices don’t allow for use of microSD without additional accessories or certifications.

5.1.3 Bar Codes

The market already uses multiple bar code technologies, and they all have the same advantages and disadvantages.

The best known example of the use of bar codes is the Starbucks implementation, which allows a consumer to have a 2D bar code sent to a mobile device for execution of a Starbucks Card transaction. The implementation is a closed system implementation; it applies to one merchant only and allows the consumer to execute a payment on a proprietary system. The bar code is scanned at the POS and the customer's Starbucks Card account is charged accordingly. The bar code does not implement any type of dynamic data technology as part of the transaction authentication process.

A more open bar code implementation would allow consumers to register accounts with a third party provider that would then deliver an e-mail or text message containing one or more bar codes. Merchants would subscribe to a service whereby the bar code would be joined with transaction data and then converted to an ACH debit or other payment type. While this solution is not currently on the market for POS purchases, a similar solution is available for bill payment transactions. The consumer takes a photo of the bar code on an e-mail message to process a utility payment from a checking account. A logical next step would be to apply the technology in an open system POS environment.

The benefits of bar codes include the following:

- The technology is proven in the store and well understood by consumers and cash register operators; most merchants already have the ability to scan a bar code.
- Bar codes can be implemented as single use to enhance security, and bar code apps can be protected with a pass code.
- Bar code-based systems may bypass the traditional bank card payment processing system, enabling different payment types and value-added applications to be implemented by the retailer.

The challenges with bar codes include the following:

- Some users have reported problems with the reliability of the scan; multiple presentations are sometimes required. If a user has lowered the brightness of the screen to conserve energy, the ability of the scanner to read the bar code may be affected.
- The device must be powered in order to access the bar code (other solutions, such as stickers, do not have this requirement).
- Merchant POS imaging reader terminals can more expensive than contactless/NFC readers.
- Presenting the bar code may require the cashier to take the device from the customer to scan the bar code.
- Bar codes may not be readable in certain environments, such as in direct sunlight or bright light.
- Bar codes implementations that are not single-use present opportunities for increased fraud.

5.1.4 Mobile Phone-Initiated Payments in the Cloud

In the payments in the cloud scenario, the consumer is able to manage payment credentials using a cloud-based application. Payment is executed using an application to which the merchant and the customer have both subscribed. Consumers access the cloud-based application through their mobile phones, using e-mail, a mobile browser, or a dedicated mobile application. Payment notification can take a number of forms (e.g., e-mail message, SMS message, sound).

Examples include PayCloud Mobile Wallet for loyalty cards and gift cards, FaceCash and PayPal. Many efforts in this area have focused on closed system applications, such as retailer gift cards, but open systems payments are certainly feasible.

The benefits of payments in the cloud include the following:

- The solution may be lower cost for the merchant, if an alternative payment type is used.
- Consumers are familiar with similar solutions (e.g., PayPal).
- Implementation can be relatively easy for merchants since new POS hardware may not be required.
- Merchants have better ability to customize and differentiate applications.
- The solution is scalable.

The challenges with payments in the cloud include the following:

- Cloud payments require a connection to the cloud. A transaction may be interrupted or not be possible due to connectivity issues.
- Transactions may be slow, depending on how the wallet is accessed, what the connection speed is, and how much data must be entered.
- Specific mobile phone capabilities may be required.
- Deployment of a peripheral POS device may be required (for example, to support the use of ultrasonic frequencies). The POS would have to be enabled to pick up audible transaction information.
- Both the merchant and the consumer must subscribe to the cloud-based service.
- There may be security issues (e.g., using SMS or email vs. secure storage and transmission).
- The merchant may need to sign up for a service or install a non-standard application for payment processing. The existing payments infrastructure is not leveraged.
- Some cloud-based transactions have been treated as card-not-present transactions, resulting in higher transaction fees.

5.1.5 SMS

The SMS approach requires consumers to register their mobile numbers with a service that manages back-end funding accounts. This same service sends text message codes to consumers in response to merchant-initiated transactions. The consumer then provides the code to the merchant as proof of payment. The transaction is completed by a processor and settled back to the merchant.

One approach to SMS-based payments aggregates small charges and bills them to a mobile phone account. SMS can also serve as a channel to other back-end settlement solutions. To execute a payment using SMS, consumers send an SMS text message from their phones to transfer funds or pay for goods and services.

The advantages of SMS include the following:

- The solution is universal. SMS works on any phone with text messaging capability and does not require a special browser. SMS works with any carrier service.
- SMS is a highly scalable technology.
- The solution is low cost, although carriers are beginning to charge issuers for SMS text messages.
- Consumers are familiar with SMS text messaging, so the learning curve is low.
- SMS works well in countries with poor Internet and POS infrastructure.

The disadvantages of SMS include the following:

- SMS is necessarily "low tech" and rudimentary, allowing for simplicity and scalability but limiting functionality.

- Mobile carriers have been averse to the risk management requirements and liability associated with extending credit under a carrier billing solution. To date, these solutions have been limited to low-value transactions.
- Knowledge of the text message recipient's telephone number is required.
- Use of SMS does not guarantee delivery. Messages may be delayed or not delivered at all.
- The solution requires mobile connectivity, so it will not work in areas without service.
- SMS-based payments lack the high degree of security inherent in a chip-based solution.
- The merchant must sign up for SMS service or install a non-standard application for payment processing. The existing payments infrastructure is not leveraged.

5.2 Evaluation Criteria

The approaches to mobile payment described in the previous sections were evaluated on the basis of the following criteria:

- Reliability at the POS
- Transaction speed
- Security
- Ease of use
- Wallet functionality
- Merchant acceptance/deployment
- Device deployment/availability
- Additional value-add applications

5.2.1 Reliability at the POS

Reliability at the POS measures the extent to which a consumer can expect that a transaction will be completed successfully. Depending on the approach, limiting factors could include (for example) the read range between devices, the ability of a scanner to accurately read a bar code, the availability and strength of any wireless networks involved, or the complexity of an application.

5.2.2 Transaction Speed

Consumers and merchants are accustomed to fast POS transactions, with payment complete within a few seconds. Each mobile payment approach has a different process for the merchant accepting payment. Factors that contribute to slower transaction speed include the amount of interaction the consumer must have with the mobile phone, the speed of the mobile connection, and the process of communicating the payment information from the phone to the POS system.

5.2.3 Security

Security measures the ability of the device or the application to protect payment credentials or other sensitive customer data.

5.2.4 Ease of Use

Ease of use measures the "user friendliness" of the customer's payment experience using an application. It considers how simple the process is and how much training the consumer and the merchant's employees need. The more a solution minimizes the introduction of new processes and leverages elements with which the consumer is already familiar, the greater the likelihood that the overall experience will be positive. A completely new customer interface or interaction incurs greater risk that the consumer will not be engaged.

5.2.5 Wallet Functionality

Many mobile payment approaches use a wallet on the mobile device to hold payment account information. Wallets can also support coupons, promotions, and loyalty programs. Wallets provide increased convenience for consumers by aggregating the payment and payment-related applications in a single user interface. Wallet functionality measures how much support the mobile payment approach provides for a wallet.

5.2.6 Merchant Acceptance/Deployment

Merchant acceptance/deployment measures the likelihood that merchants will accept and deploy the payment method. In some cases, acceptance will be nearly universal, while in others it may be initially limited with uneven prospects for acceptance. For example, if a method requires significant merchant-level system changes and POS hardware upgrades, these requirements will affect the rate of merchant deployment. This criterion examines factors such as the extent to which the payment method requires infrastructure investment and the likelihood that merchant acceptance can increase quickly.

5.2.7 Device Deployment/Availability

Device deployment/availability considers whether the payment method relies on distribution of a new device to the consumer or whether it can leverage a device the consumer already has. If a new device is required, this criterion considers whether the infrastructure and capability to distribute it are in place.

The requirement that the consumer acquire a specific mobile handset or peripheral device will affect consumer acceptance. In some cases, consumers will be able to use devices they have but will be required to download an application, register for a service, or take another action. The less a consumer has to do, both in terms of effort and cost, the greater the likelihood of broader acceptance.

5.2.8 Additional Value-Add Applications

The mobile phone provides the platform for a wide variety of applications. This criterion measures the extent to which the mobile payment approach can support additional value-add applications such as coupons, promotions, and loyalty programs.

5.3 Comparison of Approaches to Mobile Payment[49]

Table 6 presents a summary of how the alternative mobile payment approaches meet the criteria in Section 5.2based on the benefits and challenges described in Section 5.1. Over time, these ratings will undoubtedly change, based on maturity of the solutions, changes in the acceptance environment, and other developments.

[49] The ratings in this section were based on the Smart Card Alliance Payments Council's review of the different payment approaches versus the criteria discussed in Section 5.2.

Table 6. Comparison of Alternative Mobile Payment Approaches

	Integrated NFC	MicroSD	Stickers, Fobs	Bar Codes	Payments in the Cloud	SMS
Reliability	●	◑	◕	◔	◕	◔
Transaction Speed	●	●	●	◕	◑	◔
Security	●	●	◕	◔	◑	◑
Ease-of-Use	●	◕	◕	◕	◑	◑
Wallet Functionality	●	●	○	○	●	○
Acceptance	◔	◔	◔	◔	○	○
Device Availability	○	◕	◕	●	●	●
Additional Value Add Applications	●	◕	○	◑	●	○
			Legend	Worst ○ ◔ ◑ ◕ ● Best		

5.4 Summary

A review of the various mobile payment solutions in the market leads to the conclusion that the marketplace will include multiple solutions for a considerable period of time. However, it appears likely that mobile NFC handsets will grow to be a dominant mobile payment solution. Cloud-based solutions are also likely to play a significant role, given the potential for lower cost approaches with cloud-based applications.

Ultimately, the ability to leverage existing payment system assets securely, in combination with enhanced mobile solutions for loyalty and offer management, will drive significant growth in NFC handset-based mobile payments.

6 Conclusions

Mobile commerce is growing dramatically and affects every component of the retail industry. Financial apps—including mobile banking, POS, m-commerce, and payment apps—provide consumers, merchants, and small businesses with the ability to run their financial lives entirely from a smartphone. Solutions for accepting payments using a mobile phone have been introduced over the past several years but have not gained the traction or attention that they are receiving today. Accepting payments using a mobile phone is becoming more common. Solutions improve employee productivity and effectiveness and customer service, and extend the ability to accept payment cards to many new small merchants. Increasingly, consumers research, recommend, compare, and buy online or in combination with brick-and-mortar retailing.

The white paper focuses on mobile payments, defined as payments in which a mobile device is functionally involved in executing or confirming a payment. Mobile payments are classified by location, transaction size, technology used, and funding source. Certain payments are more appropriate for certain venues or payment types (for example, the use of mobile bar codes in a coffee shop).

Adoption is always an issue with a new payment type. The main stakeholders—mobile operators, merchants, bank issuers, and, most importantly, consumers—must benefit sufficiently to overcome any barriers to adoption. Benefits can include reliability at the POS, strong security, ease of use, wallet functionality, high rates of acceptance, device deployment/availability, low transaction costs, and the availability of additional value-add applications.

Currently, two key players are driving the U.S. market for mobile payments: the Isis consortium and Google Wallet partners. Standards and hardware availability are paving the way for NFC mobile payments as well. The NFC standards, specified by ISO/IEC, ETSI, ECMA International, and NFC Forum, ensure global consistency and an interoperable infrastructure. More than 20 handset manufacturers are reportedly producing NFC-enabled handsets, and 10 handset models are already available. The key manufacturers of microSDs, SIMs, SEs, and other specialized hardware are offering the accessories and services needed to support NFC.

The first step is to provision a secure payment application onto the NFC-enabled mobile phone and personalize it, whether by OTA, through the Internet, or by centralized or instant issuance. These activities require access to the SE security keys. The provisioning service, typically envisioned as being provided by a TSM, would also perform life-cycle management to enable reprovisioning to new or replacement handsets or carriers.

Mobile payments are as secure (or more secure) than payments made using plastic payment cards. Standard security technologies, such as encryption, SSL, or VPNs, and GlobalPlatform's secure channel protocol protect the personalization and life-cycle management processes. Payments are protected with tamper-resistance and cryptography in the same manner as chip-enabled payment cards, and wallets can be protected with PINs.

Many mobile payment approaches are being discussed, evaluated and tested, including integrated NFC, non-integrated contactless, bar codes, cloud-based solutions, and text messaging. As approaches evolve, some are likely to become obsolete, while others may be combined. A comparison shows that bridge technologies, text-messaging, and bar codes solve certain device availability problems, but at the expense of reliability, security, and wallet and value-add functionality. NFC approaches emerge as the top choice, despite the challenges of acceptance and device availability, because they are reliable, secure, and easy to use.

7 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to provide an overview of the current state of the market for mobile payments and NFC-enabled payment applications in the U.S. and to evaluate the advantages and disadvantages of different mobile payment approaches.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Payments Council members for their contributions. Participants involved in the development of this white paper included: Accenture; American Express; Apriva; Bank of America; Capgemini; Capital One; Connexem Consulting; CPI Card Group; Datacard Group; DeviceFidelity; Discover Financial Services; First Data Corporation; Gemalto; Giesecke & Devrient; Heartland Payment Systems; Infineon Technologies; INSIDE Secure; JPMorgan Chase; Mike Kutsch; Dale Laszig; LTK Engineering Services; MasterCard Worldwide; NACHA; NagraID Security; NBS Technologies; NXP Semiconductors; Oberthur Technologies; Quadagno & Associates; Chandra Srivastava; Thales e-Security; WatchData Technologies USA; VeriFone; Visa Inc.; ViVOtech

Special thanks go to the following Council members who contributed to the development of this white paper:

- **Scott Allan**, NXP Semiconductors
- **Debbie Bartoo**, Bank of America
- **Nancy Baunis**, Connexem Consulting
- **Deborah Baxley**, Capgemini
- **Guy Berg**, Datacard Group
- **Louis Bianchin**, WatchData Technologies
- **Jo Ann Davaris**, American Express
- **Mike Delaney**, NBS Technologies
- **Joe DeFilippo**, Capital One
- **Jason Dell**, First Data Corporation
- **Michael English**, Heartland Payment Systems
- **Brian Gendron**, MasterCard Worldwide
- **Johanna Growney**, JPMorgan Chase
- **Ian Hermon**, Thales e-Security
- **Reid Holmes**, INSIDE Secure
- **Simon Hurry**, Visa Inc.
- **Ryan Julian**, Discover Financial Services
- **Cindy Kohler**, Visa Inc.
- **Mike Kutsch**, Independent
- **Dale Laszig**, Independent
- **Paul Legacki**, Infineon Technologies
- **Michelle Lehouck**, CPI Card Group
- **James Lock**, JPMorgan Chase
- **Eddie Lopez**, Visa Inc.
- **Kim Madore**, Giesecke & Devrient
- **Jonathan Main**, MasterCard Worldwide
- **Amitaabh Malhotra**, DeviceFidelity
- **Don Malloy**, NagraID Security
- **Oliver Manahan**, MasterCard Worldwide
- **Josh Martiesian**, LTK Engineering Services
- **Kenneth Mealey**, American Express
- **Cathy Medich**, Smart Card Alliance
- **Pete Mellor**, Chase
- **Jean-Louis Meyer**, Datacard Group
- **Susan Pandy**, NACHA
- **Nick Pisarev**, Giesecke & Devrient
- **Peter Quadagno**, Quadagno & Associates
- **JC Raynon**, VeriFone
- **Ryan Reid**, First Data Corporation
- **Bill Robertson**, Apriva
- **Dori Skelding**, Chase Card Services
- **Garfield Smith**, Oberthur Technologies
- **Brian Stein**, Accenture
- **Jeffrey Stroud**, Gemalto
- **Chandra Srivastava**, Mobile Payments Consultant
- **Stuart Taylor**, ViVOtech
- **Tom Zalewski**, ViVOtech

About the Smart Card Alliance Payments Council

The Smart Card Alliance Payments Council focuses on facilitating the adoption of chip-enabled payments and payment applications in the U.S. through education programs for consumers, merchants, issuers, acquirers/processors, government regulators, mobile telecommunications providers and payments service providers. The group is bringing together payments industry stakeholders, including payments industry leaders, merchants and suppliers, and is working on projects related to implementing EMV, contactless payments, NFC-enabled payments and applications, mobile payments, and chip-enabled e-commerce. The Council's primary goal is to inform and educate the market about the value of chip-enabled payments in improving the security of the payments infrastructure and in enhancing the value of payments and payment-related applications for industry stakeholders. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

8 Appendix A: Stakeholder Relationships and the Secure Element

Using a mobile phone as a carrier for an NFC payment application creates the potential for a wide variety of relationships between the infrastructure stakeholders. The secure element (SE) chosen and the entity responsible for life-cycle management have a direct effect on the relationships among the NFC stakeholders and the approach for NFC payment application provisioning. The entity that ultimately owns and distributes the SE and the form factor chosen for the SE have a direct effect on the possible NFC payment enablement and activation paths and on stakeholder relationships. For this reason, it is valuable to examine the relationships of the stakeholders in the NFC ecosystem within the context of the SE type, the SE and payment application distribution route, and the payment application activation options. Figure 5, Figure 6, and Figure 7 illustrate three possible paths and relationships.

8.1 UICC-Centric Model

Figure 5 illustrates NFC payment application enablement and provisioning possibilities and stakeholder relationships when the SE is in the UICC.

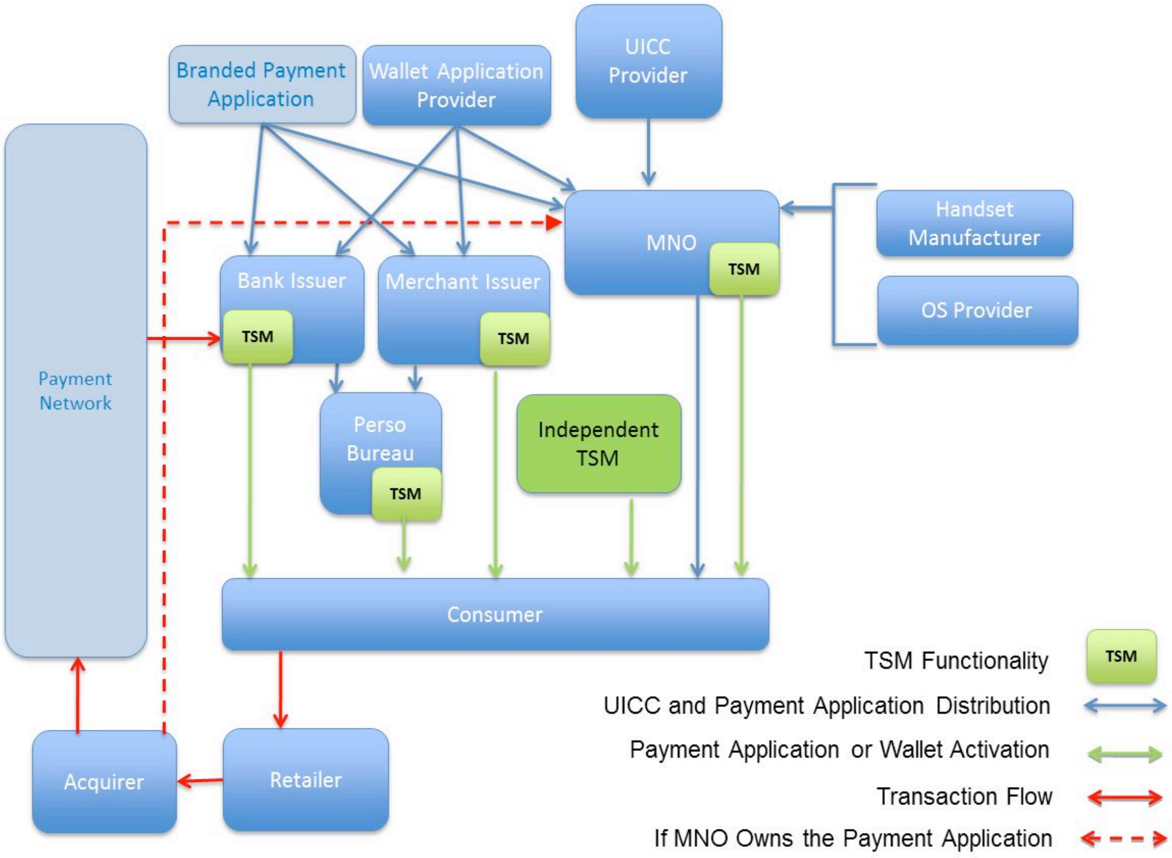

Figure 5. UICC-Centric Model

Figure 5 illustrates the following key points for a UICC-centric implementation:

- The MNO typically owns and controls the secure element and distribution of it to consumers. Accordingly, a consumer is only able to obtain NFC payment capability by purchasing a new phone from the MNO or obtaining a new USIM from the MNO. Therefore, there is only one distribution route.

- Multiple entities can provide the payment and wallet application activation, personalization, and life-cycle management functions that are typically associated with a TSM. The MNO, a bank, or a private label card merchant issuer can implement TSM functionality or outsource this functionality to a third party TSM, as illustrated by the box in the diagram labeled "Independent TSM."
- This model permits MNOs to offer their own payment applications, assuming that the acquiring networks will support the application. The dotted red line shows this payment transaction processing path.

8.2 Embedded SE Model

Figure 6 illustrates NFC payment application enablement and provisioning possibilities and stakeholder relationships when the SE is integrated into the mobile phone during the manufacturing process.

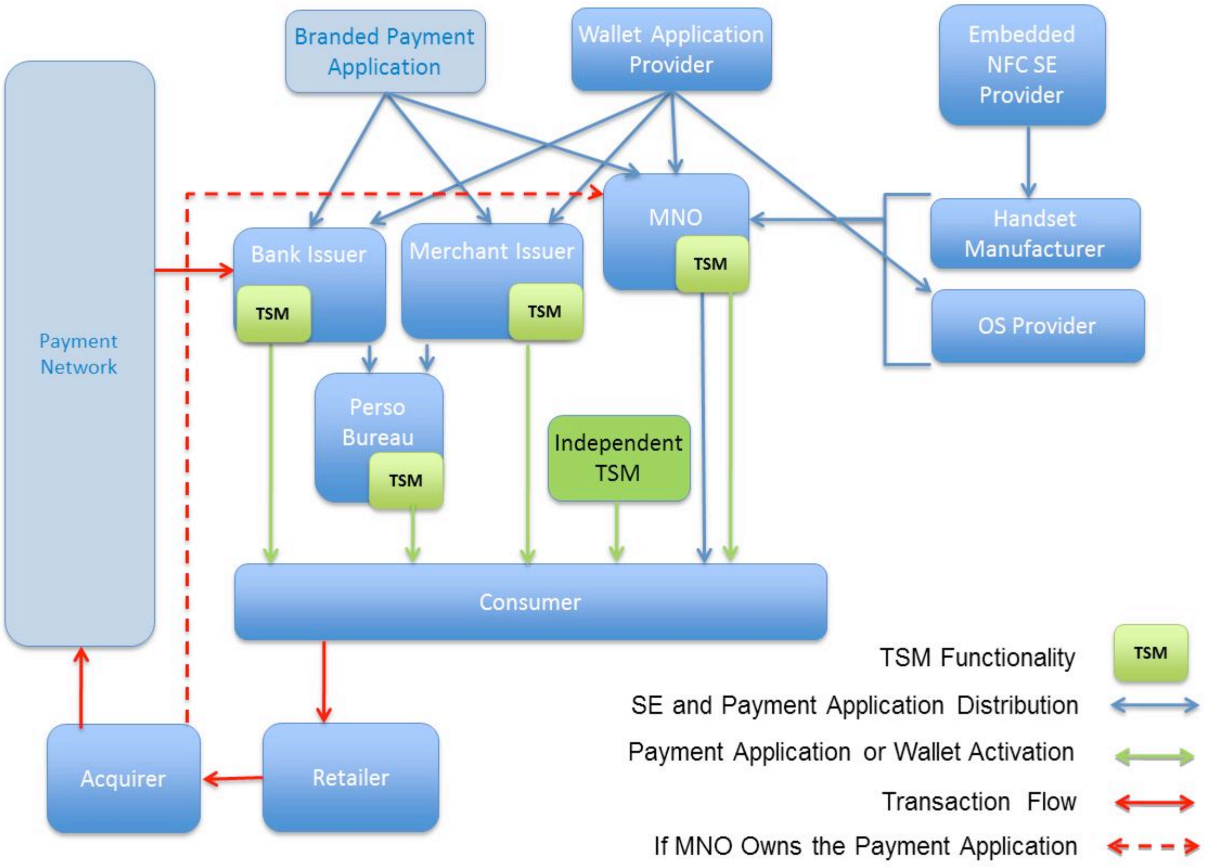

Figure 6. Embedded SE Model

Figure 6 illustrates the following key points for an implementation in which the SE is embedded in the phone:

- The MNO typically owns and controls the SE and distribution of it to consumers.
- Embedding an SE as a standard hardware feature within certain phones enables payment application providers to align with mobile OS providers to bring new applications to market (for example, Google Wallet).

- Multiple entities can provide the payment and wallet application activation, personalization, and life-cycle management functions that are typically associated with a TSM. The MNO, a bank, a private label card merchant issuer, or a third-party payment application or wallet provider can provide TSM functionality or outsource this functionality to a third party TSM, as illustrated by the box in the diagram labeled "Independent TSM." Any payment application or wallet provider can use the services of the independent TSM.
- This model permits MNOs to offer their own payment applications, assuming that the acquiring networks support the application. The dotted red line shows this payment transaction processing path.

8.3 MicroSD-Centric Model

The microSD-centric model is the most challenging to illustrate, because distribution can be handled in so many ways. In the UICC and the embedded SE models, distribution of the SE is tied tightly to distribution of the phone itself. However, in the microSD-centric model, many different entities can distribute the SE because the microSD plays a dual role. The microSD includes the SE, the NFC controller and the antenna that enable communication between the NFC-enabled phone and a contactless POS terminal. With this model, consumers don't need to change phones to have NFC functionality; they simply insert an NFC-enabled microSD card into their existing phone.

Figure 7 shows three potential distribution paths:

- Potential paths when the bank owns and distributes the microSD, labeled "1"
- Potential paths when the merchant issuer owns and distributes the microSD, labeled "2"
- Potential paths when the MNO owns and distributes the microSD, labeled "3"

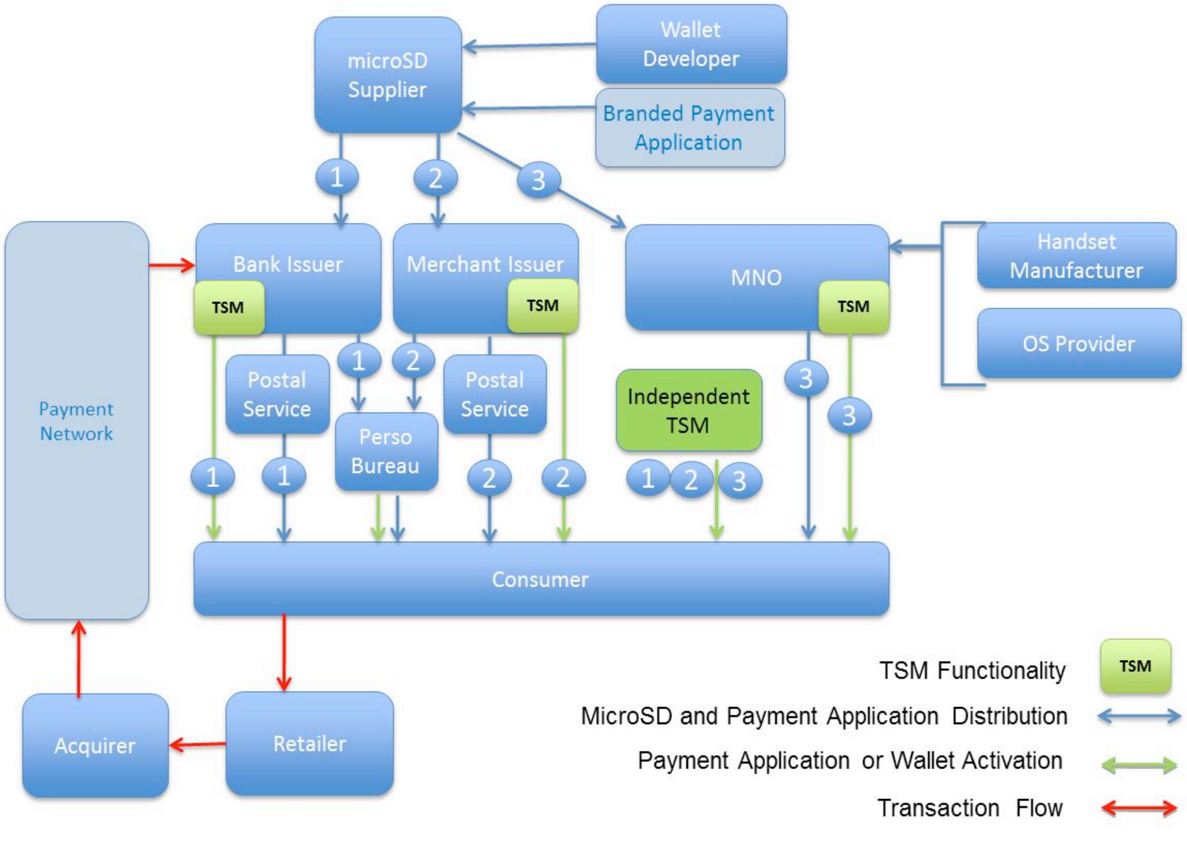

Figure 7. MicroSD-Centric Model

Figure 7 illustrates the following key points for the microSD-centric model:

- Ownership of the SE is less restricted than in the other models. A bank issuer, a merchant issuer, or the MNO can own and distribute the microSD.
- Use of a microSD opens up many more distribution paths. Banks or merchant issuers can use their current personalization bureaus to mail microSDs, either with a consumer's standard plastic credit card or alone. An MNO has the same options; to reduce the complexity of the diagram, however, Figure *7* shows the MNO distributing the microSD directly to the consumer.
- As with the other SE options, many different entities can provide the TSM functions required to activate, personalize, and manage the life cycle of a wallet or payment application stored on the microSD.

9 Appendix B: Examples of NFC Mobile Payments Deployment

NFC technology has been deployed in hundreds of pilots and commercial services worldwide, supporting mobile marketing (e.g., coupons and loyalty programs), mobile payments, mobile ticketing applications, and applications using non-mobile devices such as personal computers and printers. Table 9 lists examples of NFC mobile payments projects and announcements, illustrating the breadth of interest.

Table 9. Examples of NFC Mobile Payments Projects and Announcements[50]

Location	Participant	Status	NFC Application Deployed
		Asia Pacific	
Australia[51]	Telstra, National Australia Bank, Visa, GSMA Pay-Buy-Mobile project	Pilot completed November 2008	Payment
China[52]	China Unicom, Beijing Municipal Administration and Communications Card Co (BMAC), Watchdata	Commercial service launched January 2011	Payment for retail and transit purchases
India, Bengaluru[53]	Citi, Vodafone Essar, ViVOtech, Nokia, MasterCard	Pilot completed March 2010	Payment; smart posters with coupons and offers
Japan, Korea[54]	KDDI, Softbank Mobile, SK Telecom, with MasterCard, Credit Saison, Orient Corporation	Pilot announced February 2011; commercial services planned by end of 2011	Cross-border testing to move to NFC standard from current non-NFC mobile contactless services (payment)
Japan[55]	KDDI, Toyota, MasterCard, Orient Corp., Credit Saison, ANA, JAL, Toho Cinemas, IBM, NTT Data, Hitachi, Gemalto, Nomura Research Institute, Dai Nippon Printing, T-Engine, Japan Remote Control Co.	Pilot launched April 2010	Payment, travel services, ticketing, smart posters and other services. Compliant with GSMA PayBuyMobile specifications.

[50] Sources: National Retail Federation, *Mobile Retailing: A Comprehensive Guide for Navigating the Mobile Landscape*, July 2010; Smart Card Alliance, *Chip-Enabled Mobile Marketing*, October 2010; Near Field Communications World, http://www.nearfieldcommunicationsworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/.

[51] http://www.nearfieldcommunicationsworld.com/2009/02/24/3780/australias-first-nfc-trial-hailed-a-success/.

[52] http://www.nearfieldcommunicationsworld.com/2011/01/05/35551/china-unicom-launches-commercial-nfc-service-in-beijing/

[53] http://www.edgardunn.com/pointsOfView/showpov.cfm?instanceid=100021&type=whitepaper&popup=1, http://www.paymentssource.com/news/nfc-mobile-payments-exceed-30bn-2012-2697861-1.html.

[54] http://www.nearfieldcommunicationsworld.com/2010/07/15/34145/kddi-softbank-mobile-and-sk-telecom-to-introduce-nfc-standard-services-in-japan-and-korea/.

[55] http://www.nearfieldcommunicationsworld.com/2010/04/22/33481/kddi-to-run-multiple-nfc-tests-in-japan/.

Location	Participant	Status	NFC Application Deployed
Malaysia[56]	Maxis, Nokia, Maybank, Touch 'n Go, Visa	Commercial service launched April 2009	Payment for retail, toll, transit, parking, and theme park purchases
Singapore[57]	StarHub, DBS Bank, EZ-Link, MasterCard, Gemalto, STMicroelectronics, Watchdata	Pilot announced December 2010	Payment for retail and transit purchases
Singapore[58]	NETS, SingTel, ViVOtech, Nokia, NXP	Pilot completed February 2009	Payment; smart posters with coupons
Taiwan[59]	Taiwan Mobile, Taipei Fubon Bank, MasterCard	Pilot launched February 2008	Payment; smart posters with coupons
Europe			
Austria[60]	Orange	Commercial roll-out announced December 2010; launch in 2Q 2011	Payment
Belgium[61]	Belgacom, Mobistar, Base	Commercial roll-out announced February 2011; launch in 2011	Payment
Czech Republic[62]	Telfonica O2, Komercni bank, Citibank Europe, Globus, PDMP, Visa Europe, G&D, Oberthur, NXP	Pilot announced June 2011	Payment for retail and transit purchases
France, Bordeaux[63]	France Telecom-Orange, Moneo, Oberthur, Applicam	Pilot launched March 2011	Payment with e-purse; physical access

[56] http://www.nearfieldcommunicationsworld.com/2009/04/27/3993/first-commercial-nfc-service-launched-in-malaysia/.

[57] http://www.nfctimes.com/project/singapore-telco-bank-and-transit-purse-operator-launch-flex-antenna-trial

[58] http://www.nearfieldcommunicationsworld.com/2009/06/09/31312/dairy-queen-tests-stickers-for-targeted-mobile-coupon-campaigns/

[59] http://www.nfctimes.com/project/taiwan-taiwan-mobile-holds-trial-though-promised-rollout-delayed

[60] http://www.nearfieldcommunicationsworld.com/2010/12/16/35498/orange-to-roll-out-nfc-services-across-europe-in-2011/

[61] http://www.nearfieldcommunicationsworld.com/2011/02/10/35874/belgian-banks-and-mobile-operators-to-launch-sms-and-nfc-mobile-payments-service-in-2011/

[62] http://www.nfctimes.com/project/czech-republic-o2-launch-trial-two-banks-hypermarket , http://www.nearfieldcommunicationsworld.com/2011/03/31/36771/czech-banks-and-supermarket-to-test-nfc-with-telefonica-o2/

[63] http://www.nfctimes.com/project/france-contactless-e-purse-gets-tryout-bordeaux

Location	Participant	Status	NFC Application Deployed
France, Nice[64]	Orange-France, SFR, Bouygues Telecom, NRJ Mobile, BNP Paribas, Credit Mutuel, Veolia, Samsung, Gemalto, Oberthur	Commercial service announced May 2010	Payment for retail and transit purchases
Germany[65]	Deutsche Telekom	Commercial roll-out announced February 2011; service launch in 2011	Payment
Ireland[66]	Zapa, Irish retailers, ViVOtech	Commercial service launched August 2009	Payment, coupons, and loyalty with stickers
Poland[67]	PTK Centertel, Bank Zachodni WBK, Samsung, Gemalto, MasterCard, NXP	Pilot launched March 2011	Payment
Poland[68]	PTK, Inteligo, MasterCard, Samsung, Giesecke & Devrient, Venyon	Pilot launched June 2010	Payment
Spain[69]	Telefonica, La Caixa, BBVA, Bankinter, Autogrill, Visa Europe, Oberthur, Samsung, G&D, Sermepa, NXP	Pilot announced March 2011	Payment (with credit/debit account, prepaid, or voucher); physical access
Spain[70]	Telefonica, Visa, La Caixa, Samsung	Pilot announced, February 2010	Payment for retail purchases
UK[71]	Everything Everywhere, Barclaycard, Gemalto, MasterCard	Commercial roll-out announced 2Q 2011	Payment
UK[72]	O2, Transport for London, Barclaycard, Visa Europe, TranSys, Nokia, AEG	Pilot completed, May 2008	Payment for retail and transport purchases

[64] http://www.nfctimes.com/news/french-make-it-official-nice-nfc-launch

[65] http://www.nearfieldcommunicationsworld.com/2011/02/21/36117/deutsche-telekom-details-t-mobile-nfc-rollout-plans/

[66] http://www.vivotech.com/newsroom/press_releases/ZAPA_ViVOtech_Software_Platform.asp

[67] http://www.nfctimes.com/project/poland-orange-launches-nfc-trial-bank

[68] http://www.nearfieldcommunicationsworld.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/

[69] http://www.nfctimes.com/project/spain-telefonica-plans-big-nfc-trial-hq-staff

[70] http://www.nearfieldcommunicationsworld.com/2010/02/11/32661/telefonica-announces-nfc-trial-in-sitges-spain/

[71] http://www.nfctimes.com/project/uk-orange-and-barclaycard-announce-plans-launch-nfc-rollout

[72] http://www.mobilemarketingmagazine.co.uk/content/o2-launches-major-london-nfc-trial

Location	Participant	Status	NFC Application Deployed
Latin America			
Colombia[73]	Redeban Multicolor, Comcel	Pilot announced May 2010	Payment
North America			
Canada[74]	Bell Canada, Rogers, Telus, EnStream, Peoples Trust Bank, MasterCard, G&D, INSIDE Contactless	Pilot launched February 2010	Payment with contactless stickers
Canada[75]	Bank of Montreal, MasterCard, G&D, INSIDE Contactless, RIM Blackberry	Pilot launched November 2009	Payment with contactless stickers
Canada[76]	Rogers, Royal Bank of Canada, Visa, Gemalto, Motorola	Pilot completed September 2009	Payment
Canada[77]	Citi, Bell Canada, MasterCard, ViVOtech	Pilot completed, April 2009	Payment
USA[78]	PayPal	Service announced July 2011	Person-to-person payment service for Android phones using NFC
USA[79]	Google, Citi, MasterCard, First Data, Sprint	Pilot announced May 2011	Mobile payments and offers with Google Wallet, with pilots in New York City and San Francisco
USA[80]	ISIS: Verizon, AT&T, T-Mobile, Discover Financial Services, American Express, MasterCard, Visa, Barclaycard	Prepilot service announcement; service launch expected in 2012	Joint venture for ISIS, a national mobile commerce network, that will provide a mobile wallet that enables payment and commerce services using NFC devices. First pilots planned for Salt Lake City, UT, and Austin, TX.
USA[81]	Bank of America, Visa, Device Fidelity, MasterCard, NXP, ViVOtech	Pilot launched March 2011	Payment using MicroSD cards

[73] http://www.nearfieldcommunicationsworld.com/2010/02/11/32661/telefonica-announces-nfc-trial-in-sitges-spain/

[74] http://www.nfctimes.com/project/canada-telco-joint-venture-trials-contactless-stickers; http://blog.zoompass.com/2010/03/03/the-zoompass-tag-and-your-mobile-phone-all-you-need-to-make-purchases/

[75] http://www.nfctimes.com/project/canada-mastercard-and-bank-tests-paypass-sticker-blackberrys

[76] http://www.nfctimes.com/project/canada-royal-bank-canada-and-rogers-wireless-test-paywave

[77] http://www.newswire.ca/en/releases/archive/April2009/16/c2069.html

[78] http://www.thepaypers.com/news/mobile-payments/paypal-releases-nfc-service-for-android-based-mobile-phones/744826-16

[79] http://www.google.com/Wallet

[80] http://www.paywithisis.com

[81] http://www.nearfieldcommunicationsworld.com/2010/08/19/34339/bank-of-america-to-run-nfc-payments-trial-in-new-york/

Location	Participant	Status	NFC Application Deployed
USA[82]	Wells Fargo, Visa, DeviceFidelity	Pilot launched , December 2010	Payment using MicroSD cards
USA[83]	Discover, CPI, INSIDE Secure	Commercial launch announced November 2010	Payment with stickers
USA[84]	U.S. Bank, Visa, DeviceFidelity, FIS, Monitise	Pilot announced November 2010	Payment using microSD cards
USA[85]	JPMorgan Chase, Visa, DeviceFidelity	Pilot announced Q3/Q4 2010	Payment using microSD cards
USA[86]	Sheetz, Wright Express, ViVOtech	Pilot completed May 2009	Payment at Sheetz locations
USA[87]	Sprint, BART, Jack in the Box, ViVOtech, Samsung, Cubic, Western Union, NXP, Acumen Transit, BAH, First Data	Pilot launched January 2008	Stored value payment; smart posters with coupons and information
USA[88]	Cingular, Citi, G&D, Venyon, ViVOtech, MasterCard, NXP, Nokia, NYC Transit	Pilot completed; launched in January 2007	Payment at retailers and on the NYC Transit subway
Rest of the World			
Dubai[89]	Du, Dubai First Bank, MasterCard, ViVOtech	Pilot completed Q2 2010	Payment; smart posters with coupons
Kuwait[90]	Zain, National Bank of Kuwait, Visa, ViVOtech	Pilot completed; launched October 2009	Payment; smart posters with coupons and Visa prepaid card
Turkey[91]	Turkcell, Yapi Kredi, Gemalto, OTI, E-Kart	Commercial roll-out announced April 2011	Payment

[82] https://www.wellsfargo.com/press/2010/20101207_Mobile
[83] http://www.nfctimes.com/project/us-discover-launches-contactless-zip-stickers
[84] http://phx.corporate-ir.net/phoenix.zhtml?c=117565&p=irol-newsArticle&ID=1496802&highlight=
[85] http://www.nfctimes.com/news/chase-joins-other-big-us-banks-plans-test-contactless-microsds
[86] http://www.progressivegrocer.com/progressivegrocer/content_display/supermarket-industry-news/e3i7ee3d207fbb1fda3276468ecc9b11b2b
[87] http://www.nfctimes.com/project/us-multiapp-trial-involves-transit-agency-fast-food-restaurant
[88] http://www.nfctimes.com/project/us-citi-tests-tapping-subway-fares-nyc
[89] http://www.nfcworld.com/2009/05/19/31181/dubai-first-and-du-to-run-middle-easts-first-nfc-payments-trial/
[90] http://www.vivotech.com/newsroom/press_releases/NBK_Visa_Zain_Middle%20East.asp
[91] http://www.nearfieldcommunicationsworld.com/2011/01/31/35801/yapi-kredi-bank-and-turkcell-to-launch-nfc-payments-service-using-visa-iphone-add-on/

Location	Participant	Status	NFC Application Deployed
Turkey[92]	Avea, Garanti Bank, Gemalto, MasterCard	Commercial service announced December 2010	Payment, coupons
Turkey[93]	Akbank, Visa Europe, DeviceFidelity	Pilot announced August 2010	Payment with MicroSD cards

[92] http://www.nearfieldcommunicationsworld.com/2010/12/10/35424/avea-and-garanti-bank-launch-commercial-nfc-service-in-turkey/

[93] http://www.nearfieldcommunicationsworld.com/2010/08/09/34266/turkeys-akbank-and-visa-europe-to-test-microsd-nfc-device/

10 Appendix C: Glossary

Acquirer
The merchant's banking partner who approves and settles the card transactions.

Bar code
An optical machine-readable representation of data about the object to which the bar code is attached. Originally, bar codes represented data by varying the widths and spaces between parallel lines, referred to as linear or one-dimensional (1D) bar codes. They evolved to use rectangles, dots, hexagons, and other geometric patterns in two dimensions (2D). Mobile payments can use *QR codes* or other 2D bar codes.

Chip
An electronic component that performs logic, processing, and/or memory functions.

Cloud
A reference to using cloud computing to access services and applications. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Contactless payments
Payment transactions that require no physical contact between the consumer's payment device and the physical POS terminal. The consumer holds the contactless card or other device less than 2-4 inches from the merchant POS terminal, and the payment account information is communicated wirelessly via radio frequency (RF).

IC
Integrated circuit.

ISO (International Organization for Standardization)
An agency of the United Nations concerned with international standardization, including stored value and other bank cards. Some of the pertinent standards for contactless payment cards are ISO/IEC 7810, 7811, 7816, 9992, 10202, and 14443.

ISO/IEC 14443
ISO/IEC standard "Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards." The international standard for contactless smart chips and cards that can be read from or written to at a distance of less than 10 cm (4 in.). This standard operates at 13.56 MHz.

Issuer
The bank that provides a credit card to a cardholder.

Key
In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.

Mobile contactless payments
A payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity (within a few centimeters) of the merchant's POS equipment.

Mobile network operator (MNO)
The mobile telecommunications company that has the relationship and mobile phone account with the end user.

Mobile proximity payments
Mobile payment transaction in which a consumer uses a phone to pay for goods or services at a physical POS.

Mobile remote payments
Mobile payment transactions in which consumers use a smartphone or mobile phone to make purchases without interacting with a physical POS.

Mobile wallet
A software application that is loaded onto a mobile phone to manage payments made from the mobile phone. A mobile wallet application can also hold and control a number of other applications (for example, payment and loyalty), much as a physical wallet holds a collection of physical cards.

Near Field Communication (NFC)
A standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (called a *secure element*) that allows the phone to store the payment application and consumer account information securely and use the information as a virtual payment card. NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and U.S. contactless credit and debit cards.

OTA (Over-the-air)
The possibility to send data to and receive data from a mobile device in a distributed environment. In GSM networks, OTA can use a data connection or SMS.

Personalization
The process of incorporating the unique personal data for a user into a generic device or card.

PIN (Personal identification number)
The numeric code associated with a payment account or card that adds a second factor of authentication to the identity verification process.

POS (Point-of-sale)
The merchant's physical location where the payment transaction takes place. This term is also used to describe the equipment used by the merchant to complete the payment transaction.

QR code
Bar code that is readable by dedicated QR bar code readers and telephone cameras.

Reader
Any device that transmits data or assists in data transmission between a card, token, or other device and a host computer or database.

Smart card
A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication), and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens.

SD (secure digital memory) card[94]
A flash memory card that provides storage for digital cameras, mobile phones, and personal data assistants. Although SD cards support encryption and content protection, they are mostly used for storage due to their small size and fast transfer rate.

Secure element (SE)
The component in a mobile phone that provides security and confidentiality. A secure element can reside on the SIM, in a dedicated chip on a phone's motherboard (embedded secure element), or as an external accessory. The secure element is a smart card chip that contains a dedicated microprocessor with an

[94] Source: http://www.pcmag.com/encyclopedia_term/

operating system, memory, an application environment, and security protocols. It is used to store and execute sensitive applications on a mobile device.

SIM (Subscriber Identity Module)
A smart card that is included in GSM mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.

SMS (Short Message Service)
A system used to send text messages to and from mobile phones.

Sticker
A form factor for deploying contactless chips that can be attached to the external case of mobile phones and other devices without physical integration with the device.

Trusted service manager (TSM)
A neutral third party who provides a single integration point with mobile operators for financial institutions, transit authorities, and retailers who want to provide a payment, ticketing, or loyalty application to their customers with NFC-enabled phones.

USIM-based cards
The equivalent of a SIM card in WCDMA/UMTS (3G) phones.

WAP (Wireless Application Protocol)
A global application protocol that enables mobile phone users to access the Internet and other information services.