WHITE PAPER
Smart Card Alliance

A SMART CARD ALLIANCE MOBILE AND NFC COUNCIL WHITE PAPER

NFC Non-Payments Use Cases

Publication Date: December 2015

Publication Number: MNFCC-15002

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.

Copyright © 2015 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. 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

Contactless payment is the most prominent use case of Near Field Communication (NFC) technology in mobile devices. Apple Pay, Android Pay and Samsung Pay are three contactless payment solutions in the market that leverage NFC technology and the mobile device security infrastructure to enable convenient and secure payment.

Besides payment, NFC technology enables other non-payment use cases that are not as well known.

This white paper was developed by the Smart Card Alliance Mobile and NFC Council to highlight NFC non-payments use cases that must secure some form of user credential (e.g., a ticket, identity badge, loyalty card) and that have real-world implementations that can illustrate the benefits of the technology in different markets. The white paper includes:

- Discussion of marketing, identity and access, ticketing and gaming use cases
- Description of the use cases including implementation considerations and challenges and examples of real-world implementations
- Discussion of approaches for securing sensitive user credentials for non-payment applications
- Discussion of implementation challenges that are common to all non-payments use cases.

NFC non-payment use cases can bring the technology to hundreds of millions of new users and deliver benefits to both credential holders and credential issuers. By highlighting implementations that are breaking new ground and security approaches that can protect sensitive user credentials, the white paper provides a vision for the business cases that could drive use of NFC "beyond payments."

2 Near Field Communication—Overview

Near Field Communication (NFC) is a short-range wireless communication technology that enables data transfer between smartphones and similar mobile devices. NFC operates at 13.56 MHz and complies with ISO/IEC Standard 14443, ISO/IEC Standard 18092, and MIFARE and FeliCa specifications. NFC operates in ranges of 10 cm or less.[1]

NFC is widely available for devices running a variety of operating systems, including Android, Windows, iOS, and Blackberry. According to the NFC Forum,[2] NFC is supported in over 330 phone models, tablets, and other mobile devices, with one billion in market now and over two billion estimated to be in market by the end of 2016. In conjunction with an application, NFC can be used for a variety of purposes:

- Making payments by tapping the phone on a contactless card reader
- Reading information and picking up special offers and discounts from smart posters, smart billboards or kiosks
- Storing loyalty program information and rewards for use at retail locations
- Storing tickets that open transportation gates or access parking garages or events
- Delivering file/product updates to read/write physical contactless or dual-interface smart cards
- Storing user information that allows secure building access
- Transferring a picture to an NFC-enabled printer or monitor
- Sharing business cards with other NFC-enabled phones

The NFC Forum technical specifications define three NFC operating modes: reader/writer, peer-to-peer, and card emulation. NFC-enabled apps use one of these three modes.

- **Reader/writer mode** enables NFC devices to read and write information to NFC tags (e.g., in posters or advertisements).
- **Peer-to-peer mode** enables NFC devices to exchange data and share files.
- **Card emulation mode** enables NFC devices to function as contactless smart cards complying with ISO/IEC Standard 14443 and the FeliCa specification, allowing consumers to conduct transactions such as purchasing, ticketing, and accessing transit using the current contactless acceptance infrastructures.

Figure 1 summarizes the three NFC operating modes and identifies the underlying standards.

[1] For additional information on NFC, see the NFC Forum Web site, http://www.nfc-forum.org.

[2] "NFC: Accelerating Momentum, Expanding Opportunities," Paula Hunter, NFC Forum presentation, Smart Card Alliance 2015 NFC Solutions Summit, October 7, 2015

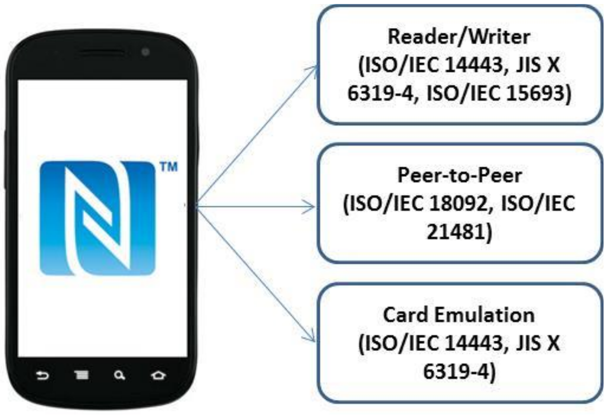
Reader/Writer (ISO/IEC 14443, JIS X 6319-4, ISO/IEC 15693)
Peer-to-Peer (ISO/IEC 18092, ISO/IEC 21481)
Card Emulation (ISO/IEC 14443, JIS X 6319-4)

Figure 1. NFC Operating Modes and Standards

The NFC specifications do not dictate a security approach for any of the three modes. How security is implemented depends on the mode and the app's requirements. (Section 4 discusses security requirements for non-payments use cases.)

Table 1 identifies the participants in the NFC application ecosystem. Which ecosystem participants are involved in implementing different NFC applications depends on the operating mode and the application.

Table 1. NFC Application Ecosystem Participants and Roles

Participant	Role
Mobile network operator (MNO)	Provides NFC-enabled mobile phones and secure element (SE) SIM cards capable of storing credentials securely. Supports secure provisioning of applications and credentials to the mobile device.
Systems integrator/infrastructure provider	Implements transport, access, ticketing, and similar systems.
Application service provider	Offers NFC application services to mobile device users.
Identity provider	Provides identifiers for users looking to interact with a system, asserts to such a system that such an identifier presented by a user is known to the provider, and possibly provides other information about the user that is known to the provider.[3]
Mobile application developer	Develops and maintains applications for NFC-enabled mobile devices.
Trusted service manager	Manages the provisioning and life cycle management of NFC applications and user credentials into secure elements (either SE SIMs or embedded secure elements), working with the application service providers and secure element issuers (either mobile network operators or handset manufacturers, respectively)
Trusted application manager	Manages the provisioning and life cycle management of trusted applications (TAs) into the Trusted Execution Environment (TEE) of certain mobile devices.
Mobile handset manufacturer/original equipment manufacturer (OEM)	Designs and produces NFC-capable mobile phones that in some cases include embedded secure elements (eSE) capable of storing credentials securely.
Mobile operating system developer	Provides support for NFC applications within the mobile device's operating system.
Chipset manufacturer	Provides the integrated circuit components needed for all NFC devices.

[3] https://en.wikipedia.org/wiki/Identity_provider

Participant	Role
NFC reader/writer and tag manufacturer	Designs and produces devices and tags to enable NFC applications.
Standards organization	Develops and publishes industry standards and specifications (e.g., the NFC Forum and GSMA).

3 Use Cases

This section describes selected use cases for NFC non-payments applications that have some form of user credential and that have been piloted or released as commercial products. Each use case defines the application, identifies the key value propositions, lists the ecosystem participants, and discusses implementation considerations.

The following use cases are described:

- Marketing
    - Loyalty
    - Coupons and offers
- Identity and access
    - Hospitality check-in
    - Travel boarding passes
    - Physical access control
    - Vehicle access control and ignition
    - Healthcare tracking and monitoring
- Ticketing
    - Transportation ticketing
    - Event ticketing
- Gaming

It is important to note that this section does not provide an exhaustive list of all possible NFC use cases. The use cases are selected to illustrate the broad applicability of NFC with user credentials.

3.1 Marketing Use Cases

3.1.1 Loyalty Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Mobile wallet (or other app) that presents loyalty cards separately or concurrently with an NFC payment tap. NFC POS terminal capable of reading value-added data separately or during an NFC payment tap.	Checkout speed User convenience--loyalty cards are always available to assure discounts Improved accuracy for customer relationship management	Merchants Handset manufacturers Loyalty programs MNOs GSMA Payment terminal and POS equipment manufacturers NFC payment solution providers	Absence of standards Low asset criticality Ecosystem and POS impact Card emulation using secure element (SE) or Host Card Emulation (HCE) Storage limit on SE Protection from modification using standard trust techniques	Softcard* Android Pay

*Softcard technology was acquired by Google and is no longer on the market.

3.1.1.1 Definition

Loyalty solutions enable a consumer to transmit data from one or several loyalty, membership or gift cards during an NFC contactless transaction made using a smartphone. A number of solutions transmit these so-called value-added credentials along with payment card information in a single tap. Softcard, Google Wallet, Android Pay are the main examples of commercially released NFC payment solutions that have implemented methods for transmitting value-added service data to a merchant's point-of-sale (POS) system to provide the user with a more integrated check-out experience.

The primary benefit of these value-added services is to simplify the checkout process for both the consumer and the merchant. Additional benefits include more reliable data transmission than using bar codes. Bar codes present one item at a time and are subject to performance issues when smartphones have scratched screens or protective covers.

One use case for NFC loyalty applications is grocery check-out, where presenting the proper loyalty card can trigger immediate discounts or "attached to card" coupons. Other use cases are transactions at convenience stores and quick service restaurants, where presenting two cards in a single tap increases checkout speed, allowing merchants to process more transactions during peak sales hours. This type of implementation can support all of the functions of common affinity programs:

- Saving save-to-card coupons
- Accumulating rewards points
- Using rewards points to pay for a transaction
- Applying product-level discounts for loyalty card members
- Implementing virtual punch cards (e.g., "get your 5th purchase for free")

Implementing NFC-based loyalty applications can benefit consumers, merchants, and brands:

- Consumers can carry fewer cards while shopping.
- Consumers always receive their affinity rewards and discounts.
- Merchants and loyalty program managers can recognize their best customers more accurately.
- The checkout process is faster, with reduced times in line.
- Sales are increased during peak business hours.
- Presentment of cards and transmission of data using NFC are more reliable than a bar code scan.

3.1.1.2 Implementation

Some of the commercial implementations to date have used NFC card emulation mode and stored the value-added data in the secure element (SE) in the phone. The SE can either be the SIM card issued by the user's mobile network or an eSE embedded in the phone by the device manufacturer. This implementation stores the loyalty credentials in the same security domain as the payment card information associated with the application's service provider. Although the value-added data does not typically need to be secure, when stored in an SE, it is protected from being erased or modified by other applications using standard trust techniques. The data is processed through an applet (Value Added Services (VAS) Applet[4]) that runs in the SE and must be addressed using an ISO-registered application identifier (AID). This implementation assures that an NFC-capable payment terminal can accurately address the data and manage communication separately

[4] As defined by GSMA.

from the payment data. NFC-capable payment terminals are programmed to execute an AID polling algorithm to scan for both standard payment cards (e.g., American Express ExpressPay, Discover Zip, MasterCard PayPass, and Visa payWave) and for AIDs for the value-added service providers.

Other implementations store the loyalty cards directly inside the mobile app running on Android OS and use Host Card Emulation (HCE) to transfer the credentials over NFC from the app to the POS.

3.1.1.3 Challenges

NFC loyalty application implementations have the following challenges:

- For implementations that use an SE, the SE data storage capacity limits the number of loyalty cards which can be stored easily.
- For implementations that use an SE, the implementation must absorb the cost of provisioning the VAS applet to the SE.
- Common industry-wide standards are lacking. However, GSMA's Digital Commerce Programme has developed Value Added Services specifications for an applet and plug-in as a proposal open to the industry.
- Payment terminals and POS systems must be updated to support the NFC loyalty applications.

3.1.1.4 Examples

The following are several examples of commercial implementations of NFC loyalty applications.

- In 2012, Softcard (then Isis Mobile Wallet) launched a mobile payment and commerce platform available on AT&T, Verizon, and T-Mobile USA smartphones. A new protocol, called SmartTap, provided loyalty card information in the same tap as payment to the merchants, which included Coke Vending, Toys R Us, and Smiths (a division of Kroger).[5]
- In 2011, Google Wallet leveraged the MIFARE protocol to transmit loyalty card information to certain merchant POS systems.[6]
- In 2014, GSMA published a series of specifications describing NFC value-added services for loyalty that leveraged work done by Telecom Italia and Orange.[7]
- In May 2015, Google announced that Android Pay will include the ability to present loyalty cards together with NFC taps and demonstrated a solution with Coke Vending. This implementation leverages the SmartTap technology, which Google acquired from Softcard in March 2015.[8]

[5] http://www.nfcworld.com/2013/09/05/325759/five-pos-providers-integrate-isis-smarttap/

[6] http://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html

[7] http://www.gsma.com/digitalcommerce/value-added-services-applet-design-proposal-version-1-0-nfc-19-march-2015

[8] https://www.youtube.com/watch?v=nioHTfqtPfU

3.1.2 Coupons and Offers Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Mobile wallet (or other app) that presents coupons separately or concurrently with an NFC payment tap. NFC POS terminals capable of reading value-added data separately or during an NFC payment tap.	Checkout speed User convenience--never leave a coupon at home Merchant benefit--highly targeted marketing and consumer engagement. Redemption tap can be tied to a specific phone, user, service provider, date, and time	Merchants OEMs MNOs GSMA Payment terminal and POS manufacturers	Absence of standards Ecosystem and POS impact Card emulation using the SE or HCE Storage limit on SE Customer notification of discounts and presence of a digital coupon stored in mobile app Protection from modification using standard trust techniques	Softcard Google Wallet Android Pay

3.1.2.1 Definition

NFC coupon and offer applications present coupon information concurrent with payment information. These applications also notify consumers about available discounts and promotions that are relevant to their buying history, stated preferences and location. The notifications and promotions can be converted into digital coupons that are stored on the consumer's phone, typically within the service provider's mobile app. A consumer who wants to take advantage of a coupon or promotion activates it within the app and then taps to redeem it. The NFC redemption tap is often concurrent with the payment tap.

Consumers benefit from having the best discounts always available and with them in digital form. Merchants benefit from the more efficient marketing programs that are made possible by leveraging mobile commerce techniques to reach a carefully targeted audience. Merchants can develop more reliable reporting and auditing techniques for their digital marketing programs because they can tie an NFC redemption tap to (for example) a specific phone, user, service provider, date, and time.

An additional benefit is that data are transmitted more quickly and reliably using NFC than using bar codes. Bar codes are limited to presenting one item at a time and are subject to performance issues when the smartphone has a scratched screen or protective cover. NFC technology supports the rapid and reliable presentation of multiple coupons or offers within milliseconds and in a single tap.

3.1.2.2 Implementation

The mobile marketing techniques used to deliver coupons and promotions to the user's mobile device are typically outside the scope of NFC and leverage technologies such as geo-fencing, consumer analytics, and Bluetooth Low Energy (BLE) beacons. The exception is the NFC tag, which can be used to deliver location-relevant information to consumers who tap an NFC phone on a tag. While the delivery mechanism may vary, the redemption method leverages NFC value-added services (for details, see Section 3.1.1.2).

3.1.2.3 Challenges

NFC coupon and offer use cases face the following challenges:

- For implementations that use an SE, the SE storage capacity limits the number of digital offers and coupons that can be stored easily.
- For implementations that use an SE, implementations must absorb the cost of provisioning the VAS applet to the SE.
- Common industry-wide standards for redemption are lacking.
- Common industry-wide standards for reconciliation and settlement are lacking.
- Payment terminals and POS systems must be updated to support NFC offer and coupon applications.

3.1.2.4 Examples

The following are several examples of commercial implementations of NFC coupon and offer applications.

- In 2012, Softcard (then Isis Mobile Wallet) launched a mobile payment and commerce platform available on AT&T, Verizon, and T-Mobile USA smart phones. A new protocol, called SmartTap, presented merchant-issued coupons in the same tap as payment to the merchants, which included Aeropostale, Jamba Juice, and Toys R Us.[9]
- In 2011, Google Wallet leveraged the MIFARE protocol to transmit discounts and offers information to certain merchant POS systems.[10]
- In 2014, GSMA published a series of specifications describing NFC value-added services for digital coupons that leveraged work done by Telecom Italia and Orange.[11]

3.2 Identity and Access Use Cases

3.2.1 Hospitality Check-In Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
The use of NFC readers and phones in hospitality settings for access and tracking	Faster service, credentialing, appropriate staffing, capacity/crowd control Limit access to hotel rooms, hospitality suites, VIP access Security countermeasures against common attacks, e.g., mutual	Hotels, amusement parks, entertainment venues, hospitality for special events OEM handset makers MNOs Trusted service managers Door access hardware providers	Need for contactless readers that are NFC compliant Need for guests to have NFC-enabled devices to store credentials Bluetooth Low Energy (BLE) as a valid alternative to NFC	Disney Choice Hotels Scandinavia Hilton Hotels

[9] http://www.mobilecommercedaily.com/jamba-juice-isis-give-away-a-million-smoothies-to-drive-mobile-payments and http://www.mobilecommercedaily.com/toys-r-us-reports-23k-isis-transactions-in-first-three-months.

[10] http://www.cnet.com/news/google-wallet-offers-make-debut-live-blog/.

[11] http://www.gsma.com/digitalcommerce/value-added-services-applet-design-proposal-version-1-0-nfc-19-march-2015.

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
	authentication, message authentication, data encryption	Physical access control system (PACS) manufacturers		

3.2.1.1 Definition

NFC has a variety of uses in a hospitality setting. Used for access control or credentialing, NFC can ensure that only the correct people have access to certain rooms or areas, such as a hotel room, a hospitality suite, an area restricted to VIP access, or any other setting where access is limited. NFC can also assist hospitality providers with crowd capacity control, tracking how many people visit a particular room or come through a line. Such information can be of benefit in anticipating appropriate amounts of staffing and forecasting inventory requirements.

Both guests and hospitality providers benefit when NFC is used in a hotel. Guests can skip the line during check-in and get into their rooms more quickly. Their room key is in their phone, which eliminates the need to carry a physical token (such as a card or key) to access their hotel rooms. Hotels benefit by allowing their staff to focus on other customer issues, providing a better customer experience. They save on the cost of room keys and reduce the environmental impact of disposing of used key cards.

When NFC is used for access control, hospitality providers can reduce costs by provisioning credentials digitally instead of issuing physical cards, badges, or tickets.

3.2.1.2 Implementation

Successful implementation of NFC in hospitality requires additional infrastructure. For NFC to be used widely, consumers must adopt mobile devices that are NFC capable and application providers will need to have access to the NFC functionality. The hospitality provider’s infrastructure must include door readers that are NFC compatible and a physical access control system (PACS) capable of managing secure distribution of credentials to the NFC mobile devices of the end users. These implementation considerations must be addressed in a timely fashion to scale the use and drive adoption of NFC technology in hospitality and not have these applications move to other technologies.

3.2.1.3 Challenges

NFC hospitality use cases face the following challenges:

- Hotels or other venues must be equipped with NFC readers.
- Implementation must absorb the cost of equipping doors with NFC capable readers and installing lobby kiosk to be used during check in or check out.
- Common industry-wide standards are lacking for provisioning and use.
- To achieve large-scale deployment, consumers need to adopt NFC-enabled handsets. Security is critical since the provisioned credential is used to authorize access to a restricted area.

3.2.1.4 Examples

The following are several examples of commercial implementations of NFC hospitality applications.

- Walt Disney World in Florida is introducing an ID tag that relies on Bluetooth and contactless NFC technology, called Disney's MagicBand. The tag replaces tickets and can be used to get on rides and enter other attractions at the park. It can also be used to access a guest's hotel room and pay in stores at the resort. In the future, the Bluetooth link will make it possible for guests to wander up to an attraction or Disney character and be greeted by name.[12]
- Choice Hotels Scandinavia and TeliaSonera piloted a program that replaces hotel room keys with NFC-enabled mobile phones. Guests make reservations as usual, and on the day of arrival they receive a text message (SMS) check-in invitation on their NFC-enabled mobile phone. The invitation provides a room number and a digital room key.[13] The keys are deactivated when guests touch the phone to a lobby kiosk during checkout.[14] The ecosystem consists of interoperable electro-mechanical locks and readers, mobile phone applications, a secure digital key delivery mechanism, and a trusted service manager for delivering and managing applications in the phone's SE.
- Hilton Hotels is rolling out technology upgrades that will allow guests to use their mobile devices to check in and choose a room on a digital floor plan. They will also roll out the use of mobile phones to replace room keys.

3.2.2 Boarding Passes Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Bag drop Self-service document check New boarding pass for cancelled or delayed flights Automated self-boarding Identification at self-service kiosks and baggage counters Lost bag report Ground transportation ticketing Access to airport lounges and priority security lanes	Faster boarding Shorter/fewer lines Flexibility Ease of use for passengers Common solution across sales channels, airlines and handsets Elimination of paper More reliable than bar codes No need for battery or connectivity*	Airlines MNOs Handset manufacturers International Air Transport Association (IATA) System integrators Trusted service managers GSMA	SE or host card emulation (HCE) for implementation Tokens stored in UICC/SIM or in app; each SD with unique encryption keys Peer-to-peer mode Collaboration required for implementation of apps for multi-modal transportation	Japan Airlines Air France SAS

3.2.2.1 Definition

In 2011, the International Air Transport Association (IATA), a global trade organization, teamed with GSMA to publish "The Benefits of Mobile NFC for Air Travel,"[15] a white paper discussing the potential uses and benefits of NFC in the airline industry. Later in 2013, IATA and NFC Forum jointly published "The NFC Reference Guide for Air Travel,"[16] a second paper designed as a guide for airlines to identify uses, benefits and implementation

[12] http://www.technologyreview.com/view/515641/disneys-electronic-wristband-illustrates-why-big-companies-push-contactless-wallets/.

[13] http://www.assaabloy.com/Global/Products/Products-old/ASSA-ABLOY-Mobile-Keys/Report-ASSA-ABLOY-Mobile-Keys-Pilot-Clarion.pdf.

[14] http://hospitalitytechnology.edgl.com/news/NFC-Enabled-Smartphones-Replace-Hotel-Room-Keys-and-Check-ins-at-Clarion-Hotel88970

[15] https://www.iata.org/whatwedo/passenger/fast-travel/Documents/iata-public-whitepaper-issue1.pdf

[16] http://www.iata.org/whatwedo/passenger/fast-travel/Documents/nfc-reference-guide-air-travel.pdf

options. The uses fall into the categories of faster travel and the ability to support and sell ancillary services (e.g., baggage fees, priority fast-track access, ground transportation). Potential applications include:

- Bag drop
- Self-service document check
- New boarding pass for cancelled or delayed flights
- Automated self-boarding
- Lost bag report

Implementing a global standard will enable the following:

- A common solution across sales channels, airlines, and handsets
- Improved flexibility for passengers
- Elimination of paper
- More reliable scanning than bar codes
- Use of credential on phone with no need for batteries or connectivity
- Reduced or eliminated lines, resulting in cost savings for airlines and time savings for passengers

3.2.2.2 Implementation

The incumbent technology adopted by airlines worldwide today and deployed in airports around the world is barcode/QR code and associated optical readers. IATA issued a now well-stablished standard for the formatting of boarding passes as a barcode – Barcoded Boarding Pass (BCBP). This standard is a good departure point to migrate to NFC: same data format, a different redemption channel.

Moving from barcodes to NFC, GSMA proposes to store tokens representing boarding pass credentials in a smartphone's UICC or SIM in specific security domains, each with unique encryption keys, thus providing security and integrity. The airline would act as a service provider. Boarding passes could also be stored in embedded secure elements in the mobile devices.

Some airlines, notably Swedish airline SAS, are taking a different approach: instead of storing tokens representing the boarding passes on a secure element, they are storing a token representing the user, namely the frequent flyer credential, on an HCE-enabled mobile app. Paired with network-connected NFC readers at the gate, the user credential can be used to retrieve the user's boarding pass from the cloud. Airlines are experimenting with an implementation that relies on HCE, to avoid the cost and complexity of provisioning to an SE.

A detailed analysis of the different implementation options can be found in the "NFC Reference Guide for Air Travel" white paper.

3.2.2.3 Challenges

Boarding pass use cases face the following challenges:

- Lack of airport infrastructure
- Lack of common industry-wide standards for NFC
- Cost of provisioning to the secure element

3.2.2.4 Examples

The following are several examples of commercial implementations of NFC boarding pass applications.

- In late 2012, Japan Airlines (JAL) became the world's first airline to offer NFC boarding passes.[17] Service was expanded to all three of Japan's major MNOs (KDDI, NTT DoCoMo, Softbank Mobile) in 2013. JAL has offered mobile boarding based on FeliCa technology since 2006 and recently introduced NFC capability as Japan's MNOs move to phones that support both FeliCa and NFC. JAL's experience with FeliCa demonstrated that very fast boarding is possible; a 500-passenger aircraft can be boarded in 10 minutes, with boarding passes being scanned 30 percent more quickly than when using bar codes.
- In July 2014, Air France and Orange France conducted a six-month pilot at Toulouse Blagnac Airport in which participating frequent flyers could use an NFC-enabled application to pass through security, access lounges, and board aircraft.[18] Boarding passes were stored on the SIM card in a phone and provisioned using SMS. The system works with phones that are turned off or have dead batteries.
- In July 2014, Scandinavian Airlines announced plans to introduce NFC boarding passes using HCE.[19]

3.2.3 Physical Access Control Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Commercial badges Corporate badges Institutional badges Universities/dormitories Homes/apartments	Convenience – no need to wait for a visitor badge Streamlined ID issuing OTA provisioning, just-in-time credentials Inventory and management cost controls Secure storage of IDs	OEM handset makers Trusted service managers Tokenization service providers Security system integrators Local distributors/servicers Door access hardware providers Physical access control system (PACS) manufacturers Commercial, industrial, residential and government PACS users	Availability of ISO/IEC 14443 readers Integration of NFC readers with existing physical access control systems Potential use of Bluetooth beacons to streamline the application selection process Application access to the SE vs. HCE User credential enrollment and privilege management NFC antenna placement in phone for optimal coupling with reader	Quinnipiac Villanova ASU

[17] http://nfctimes.com/news/two-major-airlines-diverge-initial-approach-nfc

[18] http://www.rfidjournal.com/articles/view?11964

[19] http://nfctimes.com/news/scandinavian-airlines-plans-introduce-hce-enabled-boarding-other-airlines-interested

3.2.3.1 Definition

The access control industry serves a variety of market segments, for which the credentials have historically been low frequency RFID badges used with applications that enable connected control points to read the badges and check a server in real time for access approval. During the last several years, there has been a major effort to upgrade this infrastructure and move from low frequency RFID-only support to more capable high frequency ISO/IEC 14443-compliant devices. Such an upgrade can support localized access decisions while permitting the badge or other medium to perform additional functions such as making closed loop payments, ticketing, verifying identity, and granting network permissions.

Current cloud services allow access-product vendors to port their smart card applications to smartphones, simply and securely. All the rights and functions associated with a contactless access control card can be handled by a smartphone using such services. These services are easy to integrate into current access management back-end systems, such as a physical access control system (PACS), hotel property management system, campus residence door control system, or student identity and privilege management system. Such systems typically include simple APIs for integration with other software.

Smartphones that support NFC can store and present access credentials (i.e., mobile IDs) to readers that support ISO/IEC 14443-compliant contactless access cards. Credentials can now be generated in real time or dynamically and delivered to the phone, either for storage in the SE or to an HCE app.

The ability to issue identification credentials immediately and carry them on a smartphone (i.e., as a mobile ID) has compelling advantages for both the issuer and the phone user. The smartphone with a mobile ID becomes a door opener, a mobility ticket, and a time and attendance tracker, among other functions. A guest does not have to wait for a visitor badge to open doors or pay for coffee. Operators can streamline their ID issuing processes, saving costs and increasing convenience. Users benefit because it is convenient to have all of their ID cards always at hand. And a mobile ID already works with many current reader infrastructures.

3.2.3.2 Implementation

A large number of ISO/IEC 14443-compliant contactless readers are already being used by PACS, and more are being fielded. Such an infrastructure is a prerequisite for using an NFC access credential. The key is to ensure that the credential that is provisioned to the smartphone is compatible with the reader.

A critical component of the value proposition offered by NFC is the ability of a user to obtain and use a secure credential in real time with the least possible friction (i.e., enabling a frictionless transaction). One example of a frictionless transaction is the delivery of a hotel room key or a student dorm-room key to a user as part of a check-in process. Implementation will require a secure means of generating credentials that can be registered with the PACS and provisioning such credentials to a secure environment on an NFC phone that can then be used to present them to the NFC door reader. A wallet application on the smartphone can provide the user interface through which the user can select which credential to activate. More sophisticated apps may use Bluetooth beacons to streamline the selection process, waking the app and prompting the user for some form of authentication (such as a biometric).

3.2.3.3 Challenges

Door access systems or PACs are typically designed to recognize and/or authenticate static card data. Such card data is passed to a local server, which approves or denies access. Static data on a smartphone would need to be protected (for example, stored in the SE) to prevent compromise; the solutions provider would therefore have to be able to access the SE.

The challenges of using the SE could be avoided if implementation relied on HCE and tokenization. However, door hardware would have to be upgraded to facilitate synchronization with the tokenization scheme used for dynamically changing credentials. A cost study would be required to determine feasibility.

In addition, while the software in more recent versions of door access readers is configurable, many currently installed readers are configured to support only specific contactless protocols that may not be supported by all phones or create the cross-application interoperability for which some proponents are looking. For example, the MIFARE, iCLASS, and LEGIC protocols conform substantially to ISO/IEC 14443, but they depend on unique security and application protocols that require specific reader-level support.

NFC support is not universally available to developers on smartphones. Additionally, some phones have less-than-optimal antenna placement and design. In those cases, it may make more sense to use Bluetooth as the contactless protocol. Bluetooth is available on almost all smartphones and in some cases provides a better user experience. However, Bluetooth can pose other challenges for PACS use, including read range. If the access solution does not limit transmission to a maximum of 6-8 in., the result may be that access is granted unintentionally or events are recorded inaccurately.

The primary door lock providers appear to be including Bluetooth support in addition to ISO/IEC 14443 compliance in their latest designs. Suppliers have commented that while ISO/IEC 14443 and NFC are supported in a large number of currently installed readers and door locks, inconsistent and sometimes poor positional tolerance of handset antennas, along with difficulty of accessing the SE, have turned the focus to Bluetooth. These suppliers continue to be interested in supporting NFC; however, they are waiting for these issues to be resolved.

3.2.3.4 Examples

This section reviews college/university campus use cases.

College and University Campus Use Cases[20]

Three pilot projects illustrate the benefits of using NFC smartphones to open doors on a campus. In projects at Villanova University, the University of San Francisco, and Arizona State University (ASU), groups of students and staff access campus residence halls, facilities, and selected rooms using a variety of popular NFC

[20] Information for the use cases describe in this section came from multiple sources:

- "The Buzz on NFC," College Planning and Management, Feb. 1, 2015, https://webcpm.com/Articles/2015/02/01/Near-Field-Communication.aspx?Page=1
- "Using NFC to replace campus one-cards with smartphones," University Business, March 2013, http://www.universitybusiness.com/article/using-nfc-replace-campus-one-cards-smartphones
- "Villanova pilot NFC video available on YouTube, CR80News, March 30, 2012, http://www.cr80news.com/news-item/villanova-pilot-nfc-video-available-on-youtube/
- "Villanova University Conducts Most Comprehensive NFC Access Control Trial to Date," Ingersoll Rand press release, March 21, 2012, https://investor.shareholder.com/ir/releasedetail.cfm?releaseid=658725
- "Arizona State University tests NFC," NFC World, Sept. 14, 2011, http://www.nfcworld.com/2011/09/14/39936/arizona-state-university-tests-nfc/
- "School Security: NFC Proves Itself on Campus," SecurityInfoWatch, July 17, 2013
- "NFC on Campus: Using Smart Phones as Campus Credentials," Ingersoll Rand presentations, ISC West, April 10, 2013 and NAACU, April 15, 2013, http://www.iscwest.com/RNA/RNA_ISCWest_v2/docs/2013/conference-materials/NG02_NFConCampusUsingSmartPhonesasCampusCredentials.pdf?v=635007721450876632 and http://www.naccu.org/images/2013/1-NFC_on_Campus_IngersollRand.pdf
- Arizona State University Mobile Access Pilot, HID Global case study, https://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid-asu-mobile-access-cs-en.pdf

smartphones connected to all major mobile networks. Participants use their phones to access residence halls, and some are also using them with a unique digital key and PIN to open individual dorm room doors. To open locked doors, participants present the phone to a door reader, just as they would a student ID card.

The technology can also support over-the-air provisioning and management of digital keys, which simplifies administration of the PACS. Approximately 80 percent of the student participants reported that using a smartphone to unlock a door was just as convenient as using their campus ID card. Nearly 90 percent said they would like to use their smartphones to open all doors on campus.

While these pilots are focused on physical access, nearly all participants also expressed interest in using their smartphones for other campus activities, including access to the student recreation center and laundry, transit fare payment, and meal, ticket, and merchandise purchases.

Using NFC for access control as described above offers numerous benefits to both student and faculty participants:

- A smartphone is a familiar, easy-to-carry form factor.
- Identity and identifiers are stored securely.
- Use by a non-owner is difficult.
- The phone is a powered device interoperable with ISO/IEC 14443 standards-based credentials.
- Alteration, forgery, and duplication of credentials are difficult.
- The solution is inexpensive, standardized, and accepted.
- Keyboard, PIN and biometric verification, screen, and GPS support enable strong binding of the identity credential, person and device.
- Strong authentication is supported between the reader and credential.
- Credentials are provisioned over-the-air, providing just-in-time credentials and facilitating visitor credentialing.

Combined campus NFC pilot student feedback included:

- 70%-80% of student physical keys and student access cards are lost or stolen.
- 91% of students said ease-of-use or convenience was the best part of NFC.
- Over 70% preferred using a smartphone to enter buildings over using their student ID (smart card).
- 100% of students surveyed would be interested in owning NFC technology built into their own smartphone

The main benefits identified by students and their relative importance is shown in Table 2.

Table 2. Benefits from University/Campus Implementations

Student Benefit	Percent Reporting Benefit
More convenient/easy to use	43%
Faster	15%
Less likely to lose or break credential	14%
Innovative technology	11%
Easier to replacement	6%
More secure	6%
Reduced environmental waste	5%

Villanova also reported specific institutional benefits.[21] By removing combination and key locks and using mobile phone activated doors Villanova University saved a tremendous amount of money in the annual turnover that is required to re-key dorm rooms each year. The school has also reduced the amount of lockouts because students seldom leave their mobile phone in the room. Another saving is the need to re-key if a master key is lost. Now, with a centralized room-key management system it is easy to do the annual changeover, issuing one-day permission to certain rooms as required, and enabling other key-related actions.

Kathy Gallagher, Director of the WildCard Office at Villanova University stated, "We want to provide our students the utmost in convenience and flexibility through the technology we offer. It's easier for students to use an app on their phone versus digging for their card."[22]

Laura Ploughe from ASU states, "Mobile phones are at the heart of campus life and play a major role in facilitating the students' social connections. This project has proven that a ubiquitous device can converge secure identity credentials and physical access control, and endorsed the promise that NFC technology holds within the campus environment. We were very impressed with the convenience of putting student ID credentials on NFC smartphones, as well as the enhanced security that is delivered by this next generation of advanced access control system."[23]

Table 3 summarizes the scope of the three university campus use cases.

Table 3. University Campus Use Case Scope

University	NFC Use Case Scope
Villanova University	• Phase 1: 30 students; 12 staff; 6 dormitories/offices • Phase 2: Over 100 students and staff; two major residence halls with 80 locks (with four people per room, resulting in over 200 residents) Campus-wide deployment: 4,000 doors in dormitories, offices and classrooms now implemented with locks, with 6,000 doors implemented when complete. Use has expanded to check attendance using NFC-enabled tablets; establish a loyalty points program for sports arena seating; enable POS terminals to use WildCard Bucks; NFC-enable vending machines, laundry facilities and library copier locations.
University of San Francisco	• Phase 1: 12 main doors; 3 elevators with floor control. Enable access control and laundry • Phase 2: Explore alternate student demographics and feedback; implement with executive MBA graduate students at branch campus
Arizona State University	• Phase 1: Palo Verde main hall; 32 student phones controlling 22 selected resident room doors

[21] Interview with Kathy Gallagher, Villanova, by Robert Merkert, Advanced Card Systems Ltd.

[22] http://www.cr80news.com/news-item/hid-completes-nfc-key-pilot-at-asu/

[23] http://www.hidglobal.de/press-releases/hid-global-launches-first-university-pilot-nfc-smartphones-carrying-digital-keys

3.2.4 Automotive Use Cases

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Use an app on an NFC-enabled device to transfer a user credential that can lock and unlock car doors and enable engine ignition. Such credential can also implement user-specific environmental settings, such as mirror and seat positions**.**	For privately owned cars, Improved convenience and security through fast, secure vehicle access and ignition control without physical keys or fobs Secure transfer of user data allowing customized environment settings, which improves the user experience (audio, temperature, seat and mirror presets). For car rental/car sharing, remote deployment of vehicle cars, valid only for the rental period	Auto makers Car rental/car sharing companies Automotive technology providers Trusted service managers Handset makers Mobile operators	Secure SE SIM card or embedded SE User NFC phone enrollment in vehicle access systems Integration with vehicle ignition Severe low and high temperature environmental operation range	Mercedes-Benz E-Class car Audi pilot at CES 2015

3.2.4.1 Definition

An app on an NFC-enabled device can turn the mobile device into a vehicle key, bringing a whole new meaning to the term “keyless entry and start.” Tapping a phone with NFC on the driver’s door handle can lock and unlock the vehicle. Placing the phone on a wireless charging plate inside the vehicle can enable the ignition.

3.2.4.2 Implementation

New luxury sedans are being equipped with NFC to allow keyless entry and ignition.

During preview events in Europe, automobile manufacturers revealed new technology that will be included in next-generation automobiles targeted at the executive class sedan market segment and will debut at the 2016 Detroit Auto Show. The list of new features runs the gamut, from smartphone integration to cutting-edge safety technology and autonomous driving.

According to Paul Tan’s Automotive News, “Once [the driver is] inside, placing the phone on the wireless charging plate enables the ignition. A secure SIM card is required for these functions.”[24] An eSE could also be used to store the car key credential.

High value assets require a high security standard. A secure element (SIM or eSE) likely may be required by most auto makers at least for privately owned vehicles. A tokenized solution on an app or in the trusted execution environment (TEE) may be accepted for car sharing or car rental.

[24] http://paultan.org/2015/07/08/w213-mercedes-benz-e-class-tech-revealed/

3.2.4.3 Challenges

The vehicle access use cases face the following challenges:

- Requirement of a secure element in the mobile phone (likely by many automakers considering the value of the asset the credential is protecting)
- Cost of vehicle door handle with integral NFC reader
- Enrollment of multiple user NFC phones in vehicle access control system
- Integration with vehicle locking system, ignition system, environmental control systems as well as audio, seat and mirrors presets
- Severe low and high temperature environmental operation range
- Compliance with the broad range of international driving and vehicle safety standards

3.2.4.4 Examples

The following are examples of commercial implementations of NFC automotive applications.

- The Mercedes Benz W213 E-Class car that will come to market in 2016, will incorporate NFC technology for door access and engine ignition. [25]
- At the 2015 Consumer Electronics Show (CES), Audi showcased the use of an NFC-enabled wristwatch that started the driverless Audi Prologue with a tap.[26]

3.2.5 Healthcare Use Cases

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
NFC tags on wearables or wrist bands to identify patients using a small handheld device Visit tracking to patient rooms Hospital staff and equipment check-in/check-out Tracking patient movement in hospital Tracking equipment use Tracking procedures and distribution of medicine in hospitals Registration and insurance verification Records access Home-based monitoring data collection and transmission	Faster identification Error elimination compared to manual data entry or bar codes Secure transfer of patient data Better tracking of equipment, medicine, and procedures	Hospitals Clinics Home healthcare providers	Lack of infrastructure in industry Lack of common industry-wide standards Cost of provisioning to the SE Regulations and patient privacy concerns	PatientID+ TapCheck InfoSkin Impak Health Sony–FeliCa NFC Healthcare Library Health Portal Solutions CliniCard

[25] http://www.nfcworld.com/2015/07/08/336501/mercedes-e-class-to-get-secure-nfc-keys/

[26] http://www.mirror.co.uk/news/technology-science/technology/ces-2015-audi-lg-built-4932283

3.2.5.1 Definition

Currently in a typical hospital or clinic, data is entered in electronic medical records (EMR) systems either by scanning a bar code or entering manually. Often hospital staff must wheel a heavy machine called "Computers on Wheels" into a crowded patient room to use the bar code reader to log various steps in a patient's care, such as running tests or dispensing medicine. In some cases, doctors or nurses have to keep track of every visit to a patient room. This is done by making a manual entry in the EMR system. Manual entry is inefficient and subject to errors.

NFC tags can be incorporated into wearables (such as a wristband) and read using a small, handheld scanner or similar device, enabling better control and efficiency than the current EMR system use of bar codes or manual data entry. With NFC-enabled devices, patient identity and insurance credentials can be presented at registration for speedier and more accurate registration. The patient can be identified with a small, handheld device rather than a bulky scanner. Hospital staff and equipment can check in and check out by means of small NFC devices that they carry or that are attached to equipment.

The following are examples of how NFC tags may be used in healthcare.

- Hospital applications
  - Tracking doctors' and nurses' visits to the patient
  - Tracking patient movement in the hospital
  - Tracking equipment use
  - Tracking procedures and distribution of medicine in hospitals
  - Registration and insurance verification
  - Role-based records access (for doctors, staff and family) to address HIPAA requirements
- Doctors' office applications
  - Registration and insurance verification
  - Appointment and referral scheduling
- Patients' home applications
  - Home-based condition monitoring and management. For example, diabetes, heart conditions, or blood pressure data can be collected by dedicated devices, and transmitted to the doctor using NFC on a mobile device.

3.2.5.2 Implementation

Implementation of healthcare applications requires the provisioning of NFC tags in wearables or in other form factors to enable identification and tracking applications. NFC readers must be installed that can read the NFC tags and communicate the information to other healthcare systems (e.g., the EMR system).

3.2.5.3 Challenges

Healthcare use cases face the following challenges:

- Lack of infrastructure in the industry
- Lack of common industry-wide standards
- Cost of provisioning to secure element
- Regulations and patient privacy concerns

3.2.5.4 Examples

The following are several examples of commercial implementations of NFC healthcare applications.

- Merchant360 Health Portal Solutions and CliniCard developed an app called PatientID+ that verifies patient identity and insurance quickly and reliably at hospitals and clinics using NFC tags or NFC-enabled mobile phones.[27]
- Gentag and Automated Assembly Corporation developed flexible and disposable NFC skin tags that monitor patient activity and vital signs, such as temperature and blood sugar, unobtrusively in a hospital or remotely, using NFC-enabled readers. The data can be sent automatically to healthcare providers for diagnosis and treatment.[28]
- Plus Prevention's TapCheck suite of NFC-enabled medical devices uses NFC to transmit data gathered by devices that monitor vital signs and activity monitors to an NFC-enabled reader. The data can then be processed and distributed to healthcare providers.[29]
- The Nedap trial of NFC in the Netherlands demonstrates the use of NFC readers to log the beginning and end of a healthcare provider's interaction with a patient in a hospital or at home.[30]

3.3 Ticketing Use Cases

3.3.1 Transit Ticketing Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Open and closed loop payments and ticketing in contactless fare systems	A virtualized access credential, open or closed loop, that drives down costs and improves traveler convenience Convenient access to ticketing media, lower costs to distribute media, more convenient fare product purchases, reductions in fare product sales costs, new promotional fare strategies	Transit operators Fare systems integrators Card issuers Retailers Payment networks Smart phone manufacturers Tokenization service providers or trusted service managers Transit standardization bodies	Fragmentation of approaches Cost of provisioning card or token profile into SE or HCE app State of in-place fare system: card based, account based, closed loop, open loop Supported technologies: MIFARE, Calypso, contactless MSD, contactless EMV Agency capital planning	Chicago CTA Philadelphia SEPTA JR Railway mobile Suica Seoul T-Money Transport for London

3.3.1.1 Definition

The majority of major metropolitan transit systems use contactless smart cards as the primary fare medium. In many systems, the same cards can be used at park-and-ride lots for parking fee payment and for parking

[27] http://merchant360.net/?p=491

[28] http://www.nfcworld.com/2015/02/17/334156/aac-to-mass-produce-wearable-nfc-stickers-for-healthcare/

[29] http://www.tap-check.com/?lang=en

[30] http://www.nfcworld.com/2011/09/06/39716/50000-dutch-nurses-now-using-nfc-phones/

lot access control. It is common for these systems to involve multiple agencies that offer transit services across a regional geography, accept a common card, and share processing and support services. The use of contactless smart cards for fares and parking imposes numerous non-transit functions on the part of the transit system: card acquisition, inventory management, card distribution, replacement services, and establishment and support of a revalue network that allows travelers to purchase stored value, tickets, or passes to be loaded to their cards or accounts.

While some agencies have begun to expand their systems to accept general purpose contactless payment cards directly at the point of access, network pricing models are driving these agencies to retain closed loop products, to control costs and provide options to the underbanked and underserved. In these situations, an open payment credential can be used as a non-payment access token that is tied to a closed loop account.

The promise of NFC is to virtualize both closed- and open-loop access credentials, driving down costs and enhancing traveler convenience. With an infrastructure-compatible credential, fare processing and access can be accomplished by tapping a phone on a currently installed reader. In addition, with an appropriately enabled app, the phone can provide self-service retailing and customer support functions, decreasing requirements for specialty retail networks and kiosks.

3.3.1.2 Implementation

For card-based fare systems, credentials must support read/write card emulation. Account-based systems simply require a secure token capable of mutual authentication. In either case, a card or token profile must be generated that the fare system will accept. That profile needs to be packetized and provisioned into either the SE of a handset (embedded or UICC) or into an HCE app that can facilitate presentation to fare system readers. In addition, an app will be required that allows the user to access supporting utilities and, if necessary, activate the credential prior to presentation.

One key consideration is that the design must straddle both card-based and account-based fare architectures and allow for seamless transition if an agency decides to migrate from one to the other. Ideally, the credential should be compatible with the current fare system, requiring little or no change to device and system-level software. Both the credential and the app design must consider throughput speeds and minimize the requirement for customer interaction before the tap (such as for setup).

The solution should be able to interact securely with multiple discreet transit back-office systems so that the provisioning platform does not need to be recreated for each geographic market.

For open payment credentials (e.g., a card in a mobile wallet), provisioning falls outside of the transit domain. However, for such cards to be used as transit access credentials, the issues involved in streamlining the presentation process are still germane.

3.3.1.3 Challenges

The technology and solutions for NFC-based transit applications exist and are operating in some markets today. The key challenges have been economic; the many potential stakeholders in the provisioning chain all expect some return, and there is no consensus as to what transit can reasonably be expected to pay.

As a result, NFC has been slow to move forward in many markets, resulting in a variety of approaches across product lines. In addition, UICCs and handsets may or may not incorporate SEs. It is therefore difficult to settle on a one-size-fits-the-market technical solution.

The solution may therefore need to depend on HCE as a least common denominator, but have the ability to take advantage of SEs where possible. As HCE is still evolving, transit-relevant security models and tokenization management schemes have not yet been developed. Devices that contain SEs may therefore be candidates for early market entrants for transit services.

3.3.1.4 Examples

While worldwide deployment of NFC transit ticketing has been slow to take hold due to fragmentation of the ecosystem, there are some markets where the level of control exhibited by a concentrated group of actors has allowed these solutions to flourish. Among these are:

- **Tokyo, Japan**. Starting with Japan Rail's Suica system, a national smart card scheme evolved that embraces common standards and interoperability across multiple transit brands and Sony's FeliCa smart card technology. These stored value card products have seen their acceptance extended beyond the transit environment into a variety of parking, access, and retail applications. Building on this success, NXP Semiconductors and Sony developed the NFC standard. Working in tandem with NTT DOCOMO, the trio launched large scale transit payment using NFC in 2006. NTT's market share of the mobile subscriber market coupled with a national interoperability standard created sufficient concentration for this launch to be viable.
- **Seoul, Korea**.[31] Seoul is served by a large scale integrated transit network consisting of seven rail operators, more than 20,000 buses, 120,000 taxis, and 80,000 supporting retailers. More than 50 million transit transactions are processed each day. Like Hong Kong, a national smart card interoperability standard is in place and there is substantial concentration in the mobile carrier and bank card community. Accordingly, NFC-enabled handsets and applications have been successfully launched at scale in the market. At last report more than six million mobile subscribers carried NFC smart phones enabled with the T-Money application. The application features ticketing, real time passenger information, event services, personalized information services, offers, and rewards.

While NFC is being used in both Chicago and London, it is being used for a conventional NFC-enabled contactless payment application rather than a mobile ticketing application. While the number of NFC payment transactions in these two cities is still small, valuable lessons are being learned surrounding the transit use case and how to best optimize the user experience in a demanding environment

- **London, UK**. In September of 2014, Transport for London (TfL) completed the upgrade of its contactless transit card infrastructure for the entirety of its bus and subway operations. These upgrades included the type certification and enablement of its reader fleet to support contactless EMV open payments. The system currently processes more than 14 million transactions per day with over 10 percent originating from banking contactless payment products. This continues to grow with more than 15,000 new cards seen by the system each day. Included herein are transactions originating from Apple Pay and Android Pay resident payment products on mobile phones.[32]
- **Chicago, IL, U.S.** In 2013, the Ventra system went live in Chicago thus opening CTA and PACE bus and rail lines to the acceptance of open contactless payment products. Approaching 10 percent of journeys are facilitated using open loop contactless payment products both in card and mobile (NFC) form.[33]

[31] "Mobile T-money, Services and Business," Korea Smart Card Co., Ltd. presentation, October, 2014.

[32] Source: Cubic and Transport for London, November 2015

[33] Source: Cubic and CTA, November 2015

3.3.2 Event Ticketing Use Case

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
Sales and distribution of tickets for special events, concerts, sports Identification, assessment, selection, purchase, and presentation of tickets	Self-service product ticket selection, real-time inventory access, and payment Instantaneous delivery to user device to avoid queuing Simplicity in ticket resales and reallocation of unused inventory Control of fraud associated with printed media and bar codes No dependence on battery power Fast throughput at access points Peer-to-peer transfer	Special events boards Sports teams Sports leagues Ticket sales agencies Specialty systems suppliers	State of in-place systems—complex and immature HCE vs. SE models Online vs. offline authentication/validation OTA delivery, validation, cancellation	Manchester City FC (UK)

3.3.2.1 Definition

A smartphone with a well-designed ticketing app can be a powerful tool for identification, assessment, selection, purchase, and presentation of the ticket required to access an event. Use of NFC offers a great deal of flexibility in delivery, presentation, and validation, both online and offline.

Purchased tickets can be delivered over the air to the handset and validated or canceled over the NFC interface. Advantages over alternative methods include offline cancellation, decreased dependence on battery power, a simplified presentation interface for faster throughput at access points, and the ability to transfer tickets from handset to handset using peer-to-peer or other online technology.

The ticket may be represented by data held in the phone or in a server (local or cloud), with the NFC phone either presenting the ticket itself, a token for the ticket or a user ID. The last two cases are more dependent on a real-time connection between the server and the validation service. In some cases, the validation service may be provided by the smartphone in response to a tap on an NFC tag.

An NFC phone can also be used as a validation device for a tag embedded in another phone, card, or wrist band.

3.3.2.2 Implementation

A number of models can be considered for the event ticketing use case (Figure 2), which can either return an identifier to be checked against an online database (similar to how a barcode is handled) or store verifiable data in the SE that can be checked offline.

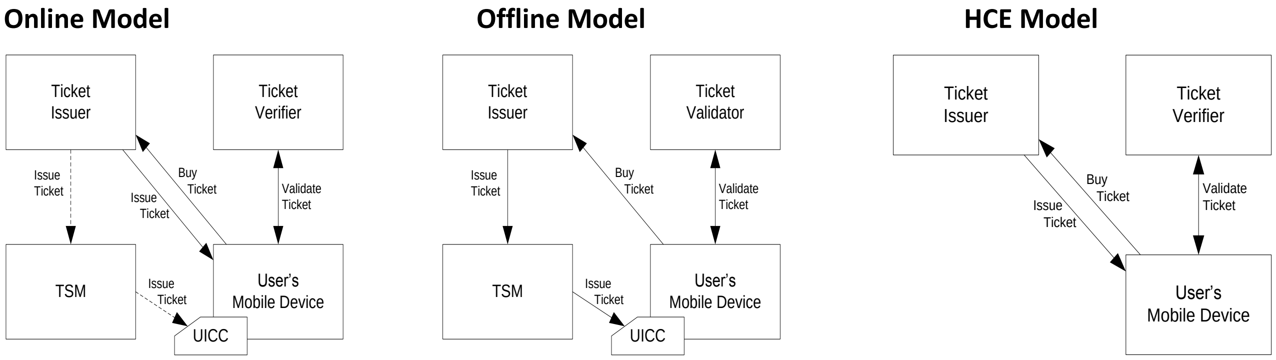

Figure 2. Event Ticketing Models

The online model can operate with a simple identifier stored in the application or on the secure element. However, this model requires an online connection to validate the identifier against a database and to ensure that duplicate tickets are not accepted. The ticket issuer could provision the identifier directly into the mobile application or use a TSM to pass the data to the UICC.

In the offline model, the ticket would need to be stored in the UICC or other SE. The ticket would need to be stored securely to guard against it being copied and distributed, but at the same time allow it to be available for the duration of the ticket validity period. The ticket can be validated without the need to communicate with a central database, which could be an advantage for temporary ticketed areas, such as festivals, for which there is no permanent communications infrastructure.

The HCE model, which is purely theoretical at this time, can use device identification to tie the ticketing credential to a specific device and prevent the ticket from being copied and distributed easily after it is provisioned. It is likely that HCE would be used only in an online environment, although there are ways to secure data within the ticketing application using advanced cryptographic techniques.

3.3.2.3 Challenges

Event ticketing use cases face the following challenges:

- Ubiquity of barcode-based solutions already in place
- Immaturity of HCE implementation approaches
- Complexity of SE infrastructure

3.3.2.4 Examples

In 2008, the Manchester (UK) City Football Club, in partnership with Orange, provided certain season ticket holders with the capability to carry a season ticket in an NFC mobile device.[34] Although few details are available, the partnership with Orange, at the time a major MNO in the UK, suggests that the ticket was downloaded and stored onto the SIM (UICC) of NFC-capable mobile devices. Similar trials are understood to be in progress with some U.S. baseball teams.

[34] http://www.itpro.co.uk/131954/manchester-city-fc-to-trial-nfc-with-orange

3.4 Gaming Use Cases

Definition	Value Proposition	Ecosystem Participants	Implementation Considerations	Real-World Examples
"Toys to Life:" A character figure in a game is placed on a device that reads the figure's tags using NFC and "imports" the character represented by the figure into the game as a playable character. Each figure remembers any points or achievements it earns, so that it can be taken to a different location and played there.*	Blurs line between virtual and physical world. Brings toys to life and makes game more enjoyable. Makes game mobile by connecting to any network or device.	Game providers (e.g., Xbox, PlayStation, Wii)	Tradeoff between open loop ubiquity and closed loop cost/security	Skylanders** Disney Infinity Amiibo U.B. Funkeys
Players can start a multiplayer game session by bringing two devices (Android phones) into close proximity.[§] "Touch to beam" attacks at another player.∞	Enables real-time, social element that gamers previously only enjoyed in a console setting		Uses peer-to-peer mode	Gun Brothers Near Field Ninja The World of Yo-Ho[#]

* The real-world collectible component is what has become so popular. Skylanders is played with a platform onto which a player can put a character, and that figure comes to life onscreen. The platform has a wired or wireless connection to the game console, and the figure.

** http://en.wikipedia.org/wiki/Skylanders.

§ http://www.nfcworld.com/2012/02/27/313930/glu-adds-android-beam-to-gun-bros-game/.

∞ https://play.google.com/store/apps/details?id=com.wolvenware.nfninja&hl=en.

# http://www.quora.com/Which-board-games-include-NFC-near-field-communications-in-the-game-mechanics.

3.4.1 Definition

Games already use NFC for payment transactions that unlock additional features. The transaction can be a direct payment or the purchase of a physical item, which signals to the platform that a certain set of features has also been purchased (e.g., Skylanders). Two more recent trends are what is called "Toys to Life" and multiplayer games played on two different NFC devices. Toys to Life imports real world objects into a game by means of an NFC interaction with a game controller. Multiplayer games can be initiated by tapping two NFC phones together.

Bringing toys to life and enabling multiplayer games make gaming more enjoyable. Blurring the line between the virtual and physical worlds adds an intuitive "cause and effect" capability that even toddlers can grasp. NFC makes games more mobile by allowing them to connect with any network or device.

3.4.2 Implementation

Gaming is facilitated by either open- or closed-loop tag technologies. Open loop allows the tag to be read on any NFC compatible device, thereby enabling more touch points for a figurine. But it also limits the game provider's ability to protect the game; a counterfeiter can copy the tag and produce a knockoff. Closed loop can employ lightweight tag-based cryptography, allowing the game provider to create an additional level of protection. However, the tag and the cryptography are not free. Closed loop solutions are mostly designed to work on portals that are attached to the leading game consoles (Xbox, PlayStation, and Wii), which allow the tagged characters to enter the game once they are placed on the portal. As long as the characters remain on the portal, they are updated with game play statistics. When they are removed, their statistics move with them.

3.4.3 Challenges

One disadvantage of open loop NFC implementation is that when a character is tapped to enter the game, it does not stay in the NFC field. To retain the statistics, the character has to be tapped again. This affects the user experience. An issue for NFC on phones or tablets is that keeping a character in the field uses power; portals are connected to a console with a constant power supply.

3.4.4 Examples

The following are examples of commercial implementations of NFC gaming applications.

- In Skylanders, Disney Infinity, and Amiibo games, the game figure is placed on the NFC-enabled “Portal of Power," which uses NFC to read the figure’s tag and "imports" the character represented by the figure into the game as a playable character. Each figure remembers any points or achievements it earns, so that it can be played anywhere
- Gun Brothers and Near Field Ninja are simple turn-based games that use NFC to connect two players, who then touch devices to compete.

4 Security Considerations

NFC in card emulation mode can be used to present any user credential or virtualize a plastic card (as mentioned in the use cases in Section 3). A key question is how to protect the cryptographic credentials and sensitive data associated with the card or credential in the inherently insecure environment of a mobile device. This section discusses the different technical possibilities and highlights the issues raised by each one. The examples in this section are mainly drawn from the transit use case (Section 3.3) but can be generalized to other use cases as well.

4.1 Using a Secure Element

One option for storing card credentials and sensitive information on a smartphone is an SE. Credentials associated with a virtual card that are stored in an SE are protected to the same extent as on a physical contactless card. However, there is one important difference. An SE is permanently connected to the smartphone and, through the smartphone, to the Internet. The potential for attacks is much higher than for an actual card, which can only be accessed if it happens to be close to a contactless reader, and then only if the contactless reader has been compromised. Therefore, it may be necessary to limit access to an application on the SE.

Whether limiting access is necessary depends on the functionality of the virtual card. For some card applications, no functionality can be used without prior authentication. However, this is not necessarily the case for certain applications. If, for example, the only requirement is a PIN, a rogue application on the phone OS can block the PIN requirement, making additional access control necessary.

GlobalPlatform has standardized an SE access control mechanism.[35] If necessary, support for this mechanism could be a prerequisite for allowing virtualization of an application in an SE on a smartphone.[36]

4.2 Using HCE Technology

The latest versions of the Android operating system support HCE. Using HCE means that NFC commands can be routed to an application running in the smartphone's operating system. Using HCE says nothing about where credentials and sensitive data are stored and processed. Nor does HCE provide or specify any security techniques. Any required security must be implemented on top of the HCE implementation.

Using HCE is perhaps the most obvious candidate for processing sensitive data, but it is by no means the only option. An application can forward NFC commands to any location reachable by the smartphone. This makes options for implementing a virtual card almost limitless, ranging from a completely cloud-based card to storing (part of) the virtual card in an SE. Because HCE does not provide security, a careful risk-benefit analysis is required to design the most appropriate security solution for each case.

For many (but not all) non-payment use cases, an attacker can obtain only limited, low value benefits from committing fraud using a virtual card. Moreover, repeating the same fraudulent transaction (e.g., traveling more in a short time on a cloned public transport card) is often not in the attacker's best interest. The potential benefit to a fraudster in payment use cases is much greater. The risk associated with using HCE

[35] GlobalPlatform Device Technology, "Secure Element Access Control," v1.0, May 2012.

[36] The SE access control mechanism must be supported by both the SE and the smartphone. Many current SEs and smartphones do in fact support this mechanism, but not all of them.

technology for virtualizing cards is consequently smaller for many non-payment schemes than it is for banks and payment networks.

Risks can also be reduced using system level countermeasures. For example, current automated fare collection systems usually include systems dedicated to mitigating the risk of travelers committing fraud using fare products. Back office systems detect fraud by aggregating transactions and looking for irregularities. In most places, inspections by an officer verify each traveler's fare product. Lost or stolen cards are put on a blacklist. These approaches or similar traditional approaches can reduce the complexity of securing credentials in a non-payment HCE implementation.

Virtual cards inside a smartphone offer additional possibilities for both preventing and detecting fraud (Figure 3).

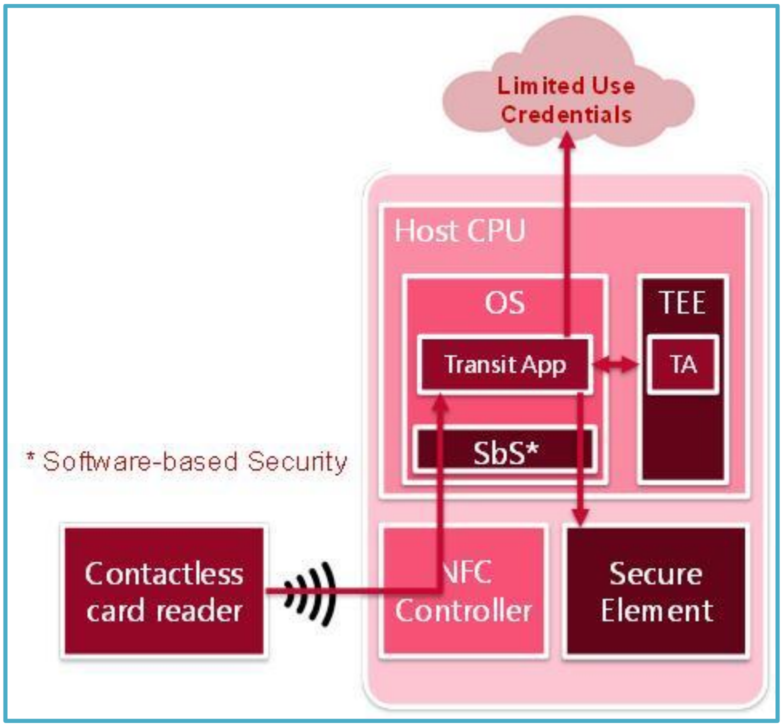

Figure 3. Possibilities for Securing HCE-based Transit Applications

One possibility is to store and run applications as trusted applications in a Trusted Execution Environment (TEE). A TEE is an execution environment that runs alongside the smartphone operating system (the rich OS). A TEE provides security services and isolates access to its hardware and software security resources from the rich OS and associated applications. In other words, a TEE is able to protect trusted peripherals such as the user interface, the NFC interface, or the SE interface from potential threats that are potentially present on the rich OS.

Another possibility is to reuse the authentication capabilities of an SE in the mobile phone. For example, a transit application could make use of an SE-based authentication solution provided by a government or bank.

Fraud can also be combatted by using tokenization, which lowers the value of the assets stored in the mobile phone OS. Typically, tokenization replaces data representing value with a limited-use credential. For example, a monthly travel subscription can be replaced by a credential that can be used for travel only a limited number of times, after which a new credential will have to be retrieved from a dedicated server managed by or on behalf of the scheme owner.[37] It is technically possible to introduce limited-use credentials that can be used in current systems without changing the current acceptance infrastructure.

Finally, the level of security of the smartphone OS and the application running on it can be increased. Although a smartphone will probably never be considered a secure environment, multiple technologies are emerging that can improve security. Such technologies include white-box cryptography, code obfuscation, OS-level integrity checking (e.g., to detect whether a smartphone is rooted or is in debug mode), and application-level checking on the authenticity of the smartphone user.

4.3 Summary

The best choice for secure implementation of a particular non-payment NFC use case (SE or HCE) depends mainly on the specific requirements of the use case and the degree to which system-level countermeasures can be effective.

Using an SE assures that the credentials can be stored securely on a mobile handset. However, several parties are typically involved in managing access to the SE.

Using HCE involves assessing security requirements as well as parameters such as cost, complexity, time-to-market, scale of interoperability, and transaction speed. Given the many possibilities for reducing risk, however, it should be possible to achieve an acceptable risk level using HCE.

[37] This raises certain questions regarding how the application can be authenticated to the server and the circumstances under which credentials can be refreshed. Moreover, the risk of stolen or cloned credentials must be considered, especially for offline transactions. Although not straightforward, these questions are expected to be satisfactorily solved in practice.

5 Implementation Challenges

The use case descriptions in Section 3 highlight the variety of benefits that can accrue from implementing NFC-enabled applications while illustrating associated implementation challenges. While some challenges are unique to a particular application, others are common and require solutions at the industry or ecosystem level before applications can truly become mainstream.

Challenges can be categorized as follows:

1. Infrastructure challenges
2. Credential security model challenges
3. Absence of consistency across device types
4. NFC accessibility or availability challenges
5. Lack of industry-wide standards

5.1 Infrastructure

The current contactless infrastructure supports a number of credential types:

- MIFARE (Classic, DESFire)
- Contactless payments (American Express ExpressPay, Discover Zip, MasterCard PayPass, Visa payWave)
- iCLASS
- LEGIC
- FeliCa

The systems that are designed to accept these credentials are typically expecting specific NFC versions of the credentials to emulate their card equivalents. It can be argued that for newer NFC implementations to be adopted rapidly, the implementations would have to emulate multiple versions of these credential types. If available and emerging NFC technologies cannot offer such emulation, systems and devices would have to be altered to support the new credential form. Such changes require a supporting business case and involve longer timelines for deployment.

The lack of maturity and consistency across the NFC ecosystem, coupled with the lifecycle lengths of current infrastructure assets, may result in refresh cycles being carried out without NFC as the primary mobile strategy. For example, barcodes and Bluetooth Low Energy (BLE) are technologies that, while perhaps not optimal from a use case perspective, are gaining traction due to their ubiquity and the resulting clearer business cases. However, much of the contactless acceptance infrastructure now supports ISO/IEC 14443 and is compatible with NFC-enabled mobile devices; this, coupled with greater NFC mobile device availability, will help to drive NFC applications.

5.2 Credential Security Model

While some applications clearly benefit from access to an SE, the lack of ecosystem consensus on SE configuration, cost, terms of access, availability, and feature set has encouraged development of HCE as an alternative. While HCE is beginning to gain traction in the payments space, support for other credential types is limited, which has impeded broad adoption. HCE implementation requires additional network level security services and changes to infrastructure and has a unique set of business model variables. A further complication is uncertainty as to whether HCE will be supported by Apple.

The market is therefore faced with potentially supporting two different security models (SE and HCE). In addition, GlobalPlatform has defined specifications for a third security model, the TEE, that can be used independently of or in combination with SE and HCE implementations. One additional complication is that it is not possible to obtain uniform business rules for SE access, given confusion about who controls access—OEMs, MNOs, or both jointly.

Solutions developers need to understand the advantages and disadvantages of the different security models to make informed decisions about how best to define their credentials and establish channels for provisioning, security management, and support services.

5.3 Consistency across Device Types

An additional challenge for solutions providers is a lack of consistency in how NFC functions behave across device types. Variations in antenna placement, read-write performance, battery life, and credential presentation (e.g., does the screen have to be lit?) create challenges in delivering a solution that performs consistently on a sufficiently broad number of handsets. As more NFC applications are deployed, it is expected that norms will be developed on how the applications and devices interact with both the user and acceptance infrastructure.

5.4 NFC Accessibility and Availability

The range of handsets supporting NFC has grown dramatically and the availability of multiple security approaches improves development flexibility for secure applications. However, different handsets have differing levels of support for NFC features and security approaches. Service providers may need to support different security frameworks in order to maximize the percentage of the user base they can reach.

5.5 Industry-wide Standards for Non-Payments Applications

NFC is supported by comprehensive technology standards and payment applications using NFC have been deployed using industry standards. However, many of the non-payment applications have no industry standards or have standards that are only just emerging. The lack of standards within each non-payment vertical (e.g., automotive, air travel) is a barrier to broad implementation of NFC applications and acceptance infrastructure.

In some of the use cases described in this white paper, standards are beginning to emerge. Industry support for and adoption of standards for non-payment applications will help to speed NFC non-payment use cases.

6 Conclusions

A wide variety of applications can take advantage of NFC to implement secure and convenient transactions at the POS, in transit, for access and for other innovative functions. This white paper has described several of these use cases and highlighted pilot or commercial use case implementations.

Common among many NFC-enabled applications is the need to provision a credential to the phone device, store the credential on the mobile device and use the credential to effect a transaction at the point of service or access. Different use cases include unique ecosystem participants and have differing requirements for security and operational performance.

As described in this white paper, NFC uses cases face several common challenges in achieving market adoption.

A requirement to support the large number of disparate handset makes, models and configurations in the market will inhibit adoption. However, a small number of manufacturers are driving the vast majority of new handset sales. Apple and Samsung both offer devices with an embedded SE, and Android mobile devices support HCE for applications. If common architectural approaches and sets of commercial parameters could be established with these leading firms, NFC use cases will be more straightforward to implement and new deployments and adoption will grow.

While there are a large variety of applications that can take advantage of NFC, those with an established compatible contactless infrastructure (e.g., transit, access) will be more straightforward to implement and those early adopters could help to drive adoption. In the past decade, contactless infrastructure has grown from access control to hotel door locks to transit access to automotive control to payments. Establishing best practices for the implementation approach for non-payments use cases that leverage this contactless infrastructure could help to drive progress with OEMs and all NFC ecosystem participants.

7 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Mobile and NFC Council to provide an educational resource that highlights the different NFC use cases beyond payments, cites commercial and pilot use case implementations, and discusses security and implementation considerations.

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 Mobile and NFC Council members for their contributions. Participants involved in the development of this white paper included: ABnote; Advanced Card Systems Ltd.; AT&T Mobility; Bell ID; Booz Allen Hamilton; Capgemini Financial Services; CH2M; Consult Hyperion; CPI Card Group; Cubic Transportation Systems; Discover Financial Services; First Data; Gemalto; Hewlett Packard Enterprise; Identification Technology Partners; Initiative for Open Authentication (OATH); IQ Devices; MasterCard; NXP Semiconductors; TSYS; Underwriters Laboratories (UL); Verifone; Visa Inc.; Wells Fargo; Xerox.

The Smart Card Alliance thanks the Council members who participated in the project team to write the document, including:

- **Deborah Baxley**, Capgemini
- **Maarten Bron**, UL
- **Rob Canterbury**, NXP Semiconductors
- **David deKozan**, Cubic
- **Frazier Evans**, Booz Allen Hamilton
- **Jeff Fonseca**, NXP Semiconductors
- **Peter Ho**, Wells Fargo
- **Jack Jania**, Gemalto
- **Simon Laker**, Consult Hyperion
- **Pedro Martinez**, Gemalto
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, Advanced Card Systems Ltd.
- **Sadiq Mohammed**, MasterCard
- **Akif Qazi**, Discover Financial Services
- **JC Raynon**, Verifone
- **Steve Rogers**, IQ Devices
- **Tony Sabetti**, CPI Card Group
- **Adam Smitherman**, TSYS
- **Brian Stein**, CH2M
- **Mike Strock**, Smart Card Alliance
- **Sridher Swaminathan**, First Data
- **Erich Tompkins**, AT&T Mobility

The Smart Card Alliance thanks the Council members who contributed to the review of the document, including:

- **Ana Egan**, Discover
- **Todd Freyman**, Bell ID
- **Scott Hagstrom**, ABnote
- **Sarah Hartman**, TSYS
- **Simon Hurry**, Visa
- **Shane Irvin**, TSYS
- **Russ Kent**, Hewlett Packard Enterprise
- **Don Malloy**, OATH
- **Jean Pare**, Xerox
- **Rob Zivney**, ID Technology Partners

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

Smart Card Alliance
Mobile & NFC Council

About the Smart Card Alliance Mobile & NFC Council

The Smart Card Alliance Mobile and NFC Council was formed to raise awareness and accelerate the adoption of payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using NFC. The Council focuses on activities that will help to accelerate the practical application of the technology, providing a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders.

The Council takes a broad industry view and brings together industry stakeholders in the different vertical markets that can benefit from mobile and NFC applications. The Council collaborates on: educating the market on the technology and the value of mobile and NFC applications; developing best practices for implementation; and working on identifying and overcoming issues inhibiting the industry.