NFC Reference Guide for Air Travel

October 30, 2013

This document is for guidance and educational purposes, and it describes sample approaches to address a variety of specific use cases. The approaches described are examples only, and they should not be assumed to be the only approaches possible or appropriate to achieve a particular result. Similarly, while the use cases selected are all feasible and should be of interest to IATA members, they do not exhaust all purposes for which NFC technology would be appropriate. IATA members are invited to bring their own innovation and creativity to applying NFC standardized technologies to the marketplace.

Table of Contents

Introduction

IATA and the NFC Forum have been working together over the last 18 months to evaluate adoption of NFC technology by the air travel industry. The outcome of this work is this *NFC Reference Guide for Air Travel*.

A number of the NFC Forum's nearly 200 member organizations and of IATA's nearly 240 airline members and technology partners have contributed to this document to help the air travel industry better understand and evaluate potential benefits and costs, use cases, and implementation options associated with adoption of NFC Technology.

It is certainly the right time for IATA members to explore adoption of NFC. The ongoing massive adoption of the technology on mobile devices from almost every relevant device manufacturer will put NFC in the hands of most travelers worldwide over the next couple of years. Throughout the document, numerous practical applications of NFC associated with the air traveler's journey are described in detail, with particular focus on core use cases related to provisioning and redemption of boarding passes. The document also shows how NFC technology compares with incumbent QR Code and Bar Code technologies.

Readers will also find detailed description about different options available to IATA members when considering implementation of NFC. The proposed implementation options differ in the exact location inside the device where the boarding passes and other possible credentials such as Frequent Flyer IDs and payment cards would be stored. All options have their merits, and it may well be that the best possible solution is one that combines them all. A comprehensive table matching core air travel requirements with each of the proposed implementation options can be found in Section 6.3.

It is not the goal of this document to advocate any particular solution, but rather to expose and explain different viable options, allowing IATA members to make their own educated choices. With the implementation of NFC technology, air travelers around the world may be able to enjoy a more seamless, reliable, uniform, fast, and overall enjoyable journey, while airports and airlines will benefit from higher customer satisfaction, reduced queues, and more efficient processes overall, with implicitly associated economies.

Key Conclusions

There are, however, two main conclusions that apply to all implementation options proposed:

1) ***These 18 months of collaboration between IATA and the NFC Forum have identified the potential need for IATA to develop industry standards around data format, access policy, and communication interfaces for storage of boarding passes inside NFC-enabled devices. A universal NFC Boarding Pass container specification could enable airlines and service providers worldwide to develop interoperable applications allowing the provisioning, management, visualization, and redemption of Boarding Passes over NFC applications.***
2) ***In order to enable a smooth transition from existing technologies to NFC, IATA will leverage the existing BCBP standard. This way, a mobile application compliant with the NFC Boarding pass container specification would allow travelers to redeem the boarding pass over NFC, and it could also present the same BP on display as a 2D barcode for redemption on existing terminals. This will allow airlines and airports to implement provisioning and redemption of NFC boarding passes independently of each other.***

1 Background

1.1 About the NFC Forum

The NFC Forum was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. This mission drives efforts to provide programs that create a highly stable framework for extensive application development, seamless interoperable solutions, and security for NFC-enabled transactions. This foundation provides an ideal environment for experts in the Near Field Communication ecosystem to collaborate on solutions across the business and technical needs of their industries and to develop NFC programs to support them.

Everyone is encouraged to read more about the Forum, and see details about its specifications, certification program, and the partners the Forum works with, in the Appendix of this document. Interested parties are also invited to join in as the NFC Forum makes NFC happen! Membership details can be found at our website, http://www.nfc-forum.org.

1.2 About IATA

The International Air Transport Association (IATA) is the trade association for the world's airlines, representing some 240 airlines in more than 115 countries. Carrying 84% of the world's air traffic, IATA's members include the world's leading passenger and cargo airlines.

IATA's mission is to represent, lead, and serve the airline industry. Its vision is to be the force for value creation and innovation driving a safe, secure, and profitable air transport industry that sustainably connects and enriches our world.

IATA was founded in Havana, Cuba, in April 1945. Its headquarters is in Montreal, Canada.

1.3 Why NFC Technology Is Important

Near Field Communication (NFC) is an intuitive wireless technology that enables a variety of use cases applicable to the air transport market. While the purchasing, storing, and redeeming of passenger tickets on a smart phone is the most obvious use case, there are many more applications unique to the air industry. Examples of applications that pertain to travelers include making purchases at the airport or in flight, obtaining lounge access, receiving frequent flyer updates, and accessing personalized schedules via smart billboards.

The International Air Transport Association (IATA) is also interested in NFC technology so that airline and airport operations and staff benefit from NFC use cases. Some of these uses include secure entry at airports and office buildings, authenticated computer logon, staff food payments, inventory controls, baggage tracking, and employee layover travel expenses.

NFC use is growing rapidly. The trend is clearly in the direction of more self-service and mobile services. While smartphones are most pertinent for the air transport market, NFC will also be widely used in consumer electronics and other devices. In addition, the growth of smart tags to transmit marketing and other information will grow exponentially over the next few years.

NFCWorld.com maintains "an exhaustive, comprehensive and accurate" list of NFC-enabled phones at this link: http://www.nfcworld.com/nfc-phones-list/. The list grows on a daily basis.

In addition:

- ABI Research reports that 125 million NFC handsets shipped in 2012 – more than were originally projected; 285 million will ship in 2013 and 500 million in 2014.
- Gartner Research predicts that half of all smartphones will have NFC capability by 2015; today, according to Strategy Analytics, one in three smartphones comes with NFC.
- Frost and Sullivan states that by 2015, NFC will be the most-used solution for mobile payment, enabling worldwide transactions totaling about $151.7 billion.
- The SIMalliance reports that SIM manufacturers shipped 30 million NFC SIM cards in 2012, 70% of them to mobile operators in South Korea and Japan, with Europe beginning to ramp up .
- The 30 million NFC SIMs were a small but high-end part of the total 5.1 billion SIMs that all vendors shipped in 2012, up by about 9% from 2011.
- The SIMalliance noted that NFC SIM shipments were up by 87% from 2011.
- 150 million NFC secure element chips were shipped in 2012 (eSE, SIM, SD Cards) according to ABI Research.
- According to 51Degrees research, NFC-enabled mobile device traffic has reached 13.32 per cent. Additionally, global web traffic from NFC-enabled devices has also increased since 2012 – growing from 3.49 per cent in January 2012 to 12.17 per cent in January of 2013.

1.4 NFC Deployment in Vertical Sectors Complementary to Air Travel

As various industries and governments deploy increasing numbers of NFC technology implementations, consumers are enjoying simplified experiences using a single device and easy-to-use technology.

- Government ID support is moving quickly:
    - European e-ID support for NFC (Russia's recent announcement)
    - Japan already supports this technology.
    - Governments are evaluating NFC adoption to simplify the process at security checkpoints.
- Companion Services adopting NFC
    - Cruise Lines
    - Hotels
    - Ground transport
        - Commercial launches of SIM-based NFC in France, South Korea, China and Russia, Japan, (NFC is compatible with existing FeliCa infrastructure), Turkey
- Retail and Payment
    - Millions of contactless terminals installed with various payment schemes
    - Banks are deploying services with MNOs in Brazil, Canada, Czech Republic, France, Japan, Republic of Korea, Poland, Singapore, UK, U.S.
    - Wider retailing: Canada, France, Japan, Republic of Korea, Singapore, UK, U.S.

2 NFC Technology Education

2.1 NFC Modes: Peer-to-peer, Card Emulation, Reader/Writer

NFC devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer. The NFC Forum technical specifications unlock the full capabilities of NFC technology for the different operating modes and are based on the ISO/IEC 18092 NFC IP-1, JIS X 6319-4 and ISO/IEC 14443 contactless smart card standards (referred to as NFC-A, NFC-B and NFC-F in NFC Forum specifications).

Card emulation mode enables NFC-enabled devices to act like smart cards, allowing users to perform transactions such as purchases, ticketing, and transit access control with just a touch. In Card Emulation mode, the NFC-enabled device communicates with an external reader much the same as a traditional contactless smart card. This enables contactless payments and ticketing by NFC-enabled devices without changing the existing infrastructure. Adding NFC to a contactless infrastructure enables two-way communications. For the air transport industry, this could mean updating seat information while boarding, adding frequent flyer points when making a payment, etc.

- **Peer-to-peer mode** enables two NFC-enabled devices to communicate with each other to exchange information and share files, so that users of NFC-enabled devices can quickly share contact information and other files with a touch. For example, users can share Bluetooth or WiFi link set-up parameters or exchange data such as virtual business cards or digital photos. Peer-to-peer mode is standardized on the ISO/IEC 18092 standard and based on NFC Forum's Logical Link Control Protocol Specification.

- **Reader/writer mode** enables NFC-enabled devices to read information stored on inexpensive NFC tags embedded in smart posters and displays, providing a great marketing tool for companies. In reader/writer mode, the NFC-enabled device is capable of reading NFC Forum-mandated tag types, such as a tag embedded in an NFC smart poster. The reader/writer mode on the RF interface is compliant with the NFC-A, NFC-B and NFC-F schemes. Examples include reading timetables, tapping for special offers, updating frequent flyer points, etc.

2.2 Mobile NFC vs. Other Contactless Forms

NFC is a short-range wireless technology. It operates within a range of few centimeters, compared to other wireless technologies that operate over larger distances.. This is a distinctive characteristic of NFC, as it requires the user to show intent of communicating over NFC by physically tapping his or her mobile device (approaching in very close proximity) on an NFC reader, NFC Tag, or other NFC-enabled device.

For the airline industry, this enables a wide variety of use cases, such as an airport kiosk sending back updated boarding passes to the device, alerts, frequent flyer updates, etc. (Readers must be upgraded to support both legacy contactless and the new NFC technologies.) NFC complements many popular consumer level wireless technologies by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS X 6319-4). NFC can be compatible with existing contactless card infrastructure, and thus it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance of a few centimeters with a maximum communication speed of 424kbps. Users can share

business cards, make transactions, access information from smart posters, or provide credentials for access control systems with a simple touch.

NFC's bidirectional communication ability is ideal for establishing connections with other technologies by the simplicity of touch. For example, if the user wants to connect a mobile device to an in-seat entertainment system, he or she can simply touch the device to the monitor's NFC touch point and the devices will negotiate the best wireless technology to use, if regulations permit such use during flight.

What does this mean for the end user? Easy connections, quick transactions, and simple data sharing.

3 Air Travel -- NFC vs. Current Technologies

3.1 Key Requirements for NFC Technology in Air Travel

IATA has defined three key requirements that must be met by any suitable implementation of NFC technology. These are:

1. Reuse current Bar Coded Boarding Pass (BCBP) Data Format, as defined in IATA Resolution 792.
2. Enable provisioning a BP into the device/reading a BP from the device even when there is no airline mobile application on the device.
3. Minimal or no user interaction with the device should be required to read/redeem a BP.

The following should also be considered:

- It should be possible to read/redeem a BP even when the device is out of battery power.
- The technology should be available and stable for a period of 10 to 20 years at least.
- The technology should be supported across multiple mobile device OS, hardware, and internationally (multi-device/OS/countries).
- It should be technically easy for an airline to manage and send NFC boarding passes to their passengers, such as through the use of a standard interface or other technologies well known by airlines.
- The technology should provide additional operational benefits compared to bar coded boarding passes, such as:
    - Higher throughput per infrastructure unit.
    - Higher level of control and reliability.
- It should enable building of premium services based on the boarding pass.
- It should enable building of premium services based on other credentials, such as frequent flyer cards or airline-issued payment credentials.
- NFC support in Airplane Mode should be available to allow usage inside the plane for payment, BP verification, etc.

3.2 Why Should IATA Members Adopt NFC?

NFC use provides a significant value proposition for the airlines. An important consideration is the potential for cost savings ("you can do more things with NFC"). Some examples:

- Airport infrastructure optimization: NFC allows faster throughput of passengers through airports, increasing opportunities for "self-service" with fewer touch points with agents at the gate, leading to less parking time of planes, fewer kiosks required (to buy and to maintain) at airports, speedier and more efficient boarding, and more efficient and safer processes.
- Reduction in paper boarding passes, moving towards "paperless travel"
- "Dematerialization" of loyalty cards: their usage via NFC becomes more efficient both for passengers (the loyalty card is present when needed via mobile device) as well as for airlines (the card can be provisioned over the air instead of via postal channel).
- NFC readers are much more affordable than optical readers. They have a much smaller form factor, and they are more reliable (98% minimum read success versus 93% for optical).
- Other efficiencies also promote savings:
    - It is possible to track the delivery of the BP to the passenger device. This gives greater control to the airlines, such as for automated check-in.
    - Fewer operations are required from staff in processing boarding passes.

NFC implementations also offer additional revenue possibilities. For example:

- Airlines can differentiate better: using NFC for boarding passes will allow IATA members to develop differentiating services later on, and create new revenue streams (e.g., sales of ancillary services, lounge access, fast track lane, couponing, etc.).
- The mobile device becomes a personalized, contextual, and cheaper direct marketing channel to the individual customer – an extremely efficient and effective means to sell and distribute transportation tickets and ancillary services, being cheaper, more secure, and faster than using physical mail service.
- NFC will boost adoption of mobile solutions for air travel services because it proposes a familiar user experience that travelers already employ for other use cases such as access, mass transit, and especially payment.

NFC technology enables better customer experience throughout the journey. Some examples:

- "Tap is the new click:" The "tap-and-go" experience that NFC provides is a much more intuitive and easy way to pass through the airport, compared to the more cumbersome paper printing, finding the right email on the device, etc. "Tap-and-go" means that no user interaction is required other than tapping the device on a reader.
- Mobile communications in combination with NFC enables a direct communication link between the airline and the passenger. More integrated and personalized messages can be sent, which can be practical, such as gate change updates, or more targeted to passengers' habits and preferences.
- NFC enables faster passing through the airport, with less standing in lines fiddling with and searching for necessary documents.
- Loyalty cards can become part of an integrated user experience at the airport.
- Some NFC implementations offer the possibility of sending Boarding Passes worldwide Over The Air (OTA) via text message, with no need of a wireless data connection. This new capability will be greatly appreciated by passengers subject to mobile roaming charges. It also enables passengers abroad to get their Boarding Passes prior to going to the airport without needing a printer; for example, by using a hotel computer.
- NFC use will provide a "peace of mind" effect to passengers who will no longer have to worry about finding their BPs, either in paper or as mobile QR codes.

Finally, NFC technology is part of the ecosystem. NFC has become a basic feature in most of the newly released smartphones, and it is no longer considered a niche technology. There are many companies that have deployed, are now deploying, or are planning to deploy NFC. This offers opportunities for airlines to find partners who can help with the implementation of NFC.

Note also that NFC is a technology foreseen to be stable in the long term (15+ years). It is a complementary solution to existing technologies, and it enables a smooth transition over time from legacy boarding pass solutions. Given the stability and long-term perspective of the technology, airlines should also consider the wider possibilities of NFC in the multi-modal context, as NFC is currently being deployed in ground transport. This provides an option to participate in end-to-end consumer journeys (plane, train, taxi, etc.) over the longer term and their associated branding and revenue possibilities.

In addition to the multi-modal travel context, NFC in the retail sector is also part of the overall ecosystem. Retailers and well-established players in the financial industries, such as banks and credit card companies, are investing in and developing NFC services.

NOTE: Some of the benefits listed above are not specific to NFC, but common to all mobile implementations.

3.3 NFC Boarding Pass vs. Bar Coded Boarding Pass

The Bar Coded Boarding Pass (BCBP) on mobile devices has limitations. It is cumbersome to manipulate at the time of reading. It needs user interaction that can be complicated (unlock device, find the right app, open the boarding pass). Then it needs to be physically positioned so that the reader can see the boarding pass and process the image. This operation sometimes creates an embarrassing handling situation between the passenger and staff when it is not clear who should hold the device on the reader. It does not work if the battery is down.

By contrast, NFC allows implementation of a "tap-and-go" user experience that solves the BCBP problems and results in greater throughput at gates. NFC offers multiple user-friendly ways to interact with the passenger, since several options to display boarding pass information are available (airline app, independent app, etc.). Also, it is possible to have mobile NFC reader devices for staff in the airport or for cabin crew.

NFC vs. Bar/QR Codes

4 Other Considerations

4.1 Common Use

The air travel industry is driven by standards and a cost-efficient model. The chosen NFC solution must leverage mutual use of the infrastructure (e.g., readers) as much as possible and maximize interoperability. The air travel industry has a model unique in the world for sharing data format and infrastructure. For details, refer to CUSS (Common Use Self Service) and to CUPPS (Common Use Passenger Processing Systems)

NFC is an ideal technology to leverage this situation. A common NFC boarding pass infrastructure, backwards-compatible with IATA resolution #792, is desired. Proposals are already available.

4.2 Security Considerations

4.2.1 Background

Many lessons can be learned from mobile software distribution through App Stores. Author registration, filtering, and code signing maintain the integrity of the OS and third-party applications. In addition, a mobile device operating system has a number of security controls, so that applications have strict control over their own memory spaces.

4.2.2 Signing the Boarding Pass

In 2009 IATA amended the bar-coded boarding pass (BCBP) standard to include a field for a digital signature to prove authenticity and validity of the bar code. IATA designed in a level of security into the specification for future needs.

The NFC Forum created data structure specifications, including the Smart Poster RTD and Signature RTD, that can be used to encapsulate the BCBP as an NDEF MIME type, and then it can be digitally signed for validity and integrity in a scalable way. Verification is very straightforward, requiring only a root certificate and software that is highly available in browsers today. Signing certificates can be distributed from already established browser roots and existing Certificate Authority (CA) hierarchies.

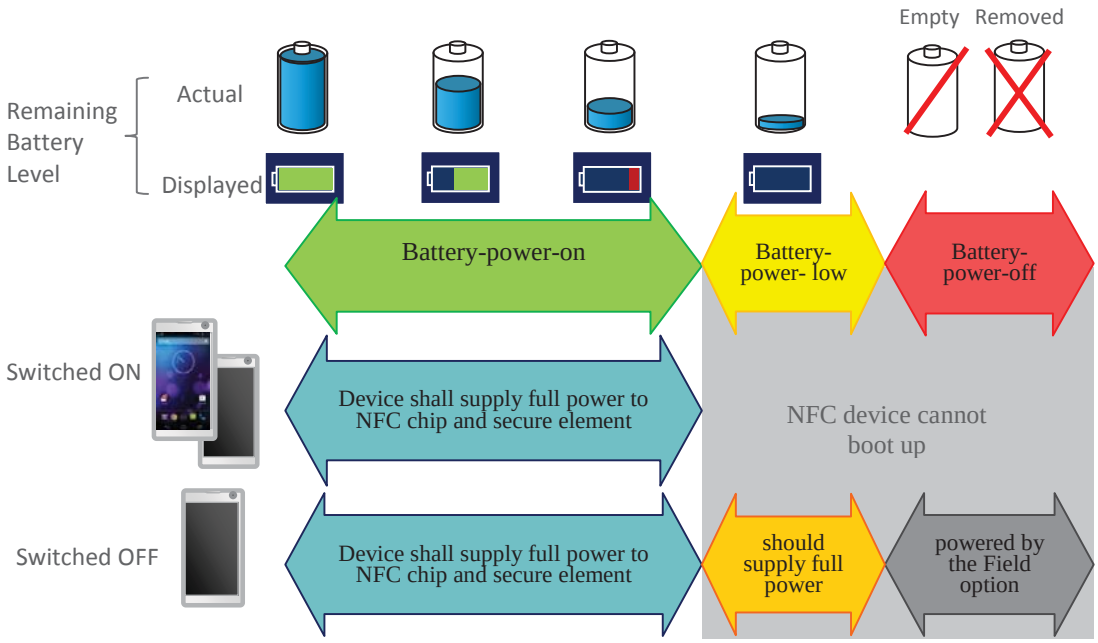
The benefits of signing the BCBP using NFC Forum specifications are numerous:

- BPs can be stored in device memory without risk of tampering.
- They can also be stored in a secure element if desired.
- Readers can operate off-line if need be, since root certificates do not need to be updated often.
- Minimal operational impact will be seen. If a root does not exist, the BCBP can still be read. A security decision could be made by exception.
- A mobile device app can present the BCBP to the screen as well as in NFC card emulation mode in a secure fashion.
- Cost is low. Signing the BCBP only requires a signing certificate fee (usually annual) from a CA, which typically is in the $300 price range, with the ability to sign an unlimited number of BCBPs. A signing hardware security module (HSM) is used to protect signing keys. These are now available as low-cost thumb drives and included in the price of the signing certificate. In addition, larger-scale HSMs can be deployed for cloud-based signing to match the airline infrastructure.
- Security will be future proof. While there is no mandated security requirement for a boarding pass, it is prudent to be able to digitally sign them if the security requirements change over time.

4.3 Power Modes

Several power modes of an NFC-enabled mobile device can be distinguished.

- **Battery-power-on mode** – The mobile device is bootable and shall supply full power to the NFC chip and the secure element even if the device is switched off.
- **Battery-power-low mode** – The mobile device is not bootable. The device has not enough power to run the operating system. The user is unable to switch on the mobile device. Screen, keyboard and other functions are not available. The mobile device, however, should supply full power to the NFC chip and secure element as long as some power from the battery is available.
- **Battery-power-off mode** – The battery is completely empty or removed. The only remaining power source is the NFC chip, harvesting power from the RF field of the reader. The NFC chip may be able to provide limited power to the secure element.



Power Modes on NFC-enabled Devices

Similar to traditional contactless cards, the NFC chip may be able to extract power from the NFC field generated by the reader to operate in battery-power-off mode. In addition, even in battery-power-low mode the battery still provides some power that can be used to power the NFC chip and a secure element.

Due to the unavailability of display, keyboard, network connection and many other essential functions, operation in both battery-power-low mode and battery-power-off mode is very limited. For example, the user may not be able to enter a PIN or even change the card that is emulated by the mobile device.

Note that some of the implementation options proposed in Section 6 may only work in battery power-on mode. For example, the implementation option “storage in device memory” will not be available in battery-power-low mode or battery-power-off mode.

4.4 Airplane Mode

In flight mode, the NFC part of the device is disabled along with radio, Wi-Fi, and Bluetooth. However, the consumer may re-activate only the NFC part for performing payment or checking a boarding pass, depending on regulatory policies by the respective authorities.

5 Use Cases

This section presents descriptions of the use cases for NFC technology in air transport that IATA desired to focus on for the purposes of this document.

5.1 Provisioning a Boarding Pass into a User's Device

5.1.1 Get New BP into the Device

5.1.1.1 Get New BP Over The Air (OTA)

A customer checks in online and wants to receive his NFC boarding pass on his phone or other mobile device over the air. Steps include:

1. Customer checks in online.
2. Customer selects boarding pass delivery mechanism (this could be optional if his preference is already known by the airline from a passenger profile).
3. Customer provides minimum information required (e.g., telephone number or email address) for airline to be able to send NFC BP over the air.
4. Information is validated by the system and boarding pass is sent to passenger's mobile device via text message or data connection. Airline is ideally notified that the BP has been received.
5. The BP is automatically stored in the “Travel” folder on the mobile device. Human-readable information of the boarding pass is available from the passenger's device.

5.1.1.2 Get New BP at a Kiosk

A customer arrives at the airport terminal and approaches a kiosk to check in for her flight. Steps include:

1. Passenger presents frequent-flyer number, name, reservation barcode, or record locator to retrieve the reservation.
2. After completing the check-in process, passenger selects how she wants her boarding pass delivered. One of the options is delivery to her mobile device over NFC.
3. She taps her device on the kiosk's NFC reader to get her BP transferred to the device.

5.1.2 Update a BP in the Mobile Device

A customer has checked in and already has an NFC-redeemable BP in his device. He needs to obtain a new BP as his flight details have changed (re-booked, seat change, etc.).

5.1.2.1 BP Update Over the Air (OTA)

Steps for this process include:

1. Customer goes online to make modifications to his reservation.
2. Customer selects delivery mechanism for the new BP.
3. The airline sends a new boarding pass to customer's device over the air.
4. The new BP is stored on customer's device and the old BP is invalidated and optionally deleted. Both passenger and the airline are notified of the update.
5. Human-readable information of the boarding pass is available from passenger's device.

5.1.2.2 BP Update at a Kiosk

Steps for this process include:

1. Customer is already at the airport and approaches a self-check-in kiosk to get a new BP.
2. Customer taps his device on the kiosk's NFC reader. The kiosk reads his old BP and retrieves user's itinerary.
3. The user makes modifications to his itinerary (different flight, different seat).
4. He selects NFC as the delivery mechanism for the new BP.
5. The user taps his device on the kiosk's NFC reader.
6. The new BP is stored on the customer's device and the old BP is invalidated and optionally deleted. The user is informed via the device's user interface that the new BP has been successfully loaded.
7. Human-readable information of the boarding pass is available from the passenger's device.

5.2 Reading a BP from a Passenger's Device

5.2.1 Presenting a BP at Boarding Gate/Airline lounge

A customer has checked in and already has an NFC boarding pass. The passenger needs to go through various processing points at the airport and validate his or her credentials.

5.2.1.1 With UI Interaction

Steps include:

1. Customer is already checked in and carrying an NFC boarding pass in her device
2. Customer opens her airline mobile application and browses through the different BPs stored in the device to select the appropriate one.
3. She taps her device at a reader (NFC gate reader) to be granted access.
4. The NFC reader identifies the BP selected by the end user.
5. The reader sends the BP data to airline application for validation.
6. Human-readable information of the boarding pass is available from the passenger's device.

5.2.1.2 With No UI interaction

Steps include:

1. Customer is already checked in and carrying an NFC boarding pass in his device.
2. Customer taps the device at a reader (NFC gate reader) to be granted access.
3. The NFC reader identifies the valid BP (as per IATA Resolution 792 - BCBP) if multiple BPs are stored in the device (selecting the right boarding pass for the right flight).
4. The reader sends the BP data to the airline application for validation.

5.2.2 Presenting a BP at a Security Checkpoint

This situation is similar to presentation of a BP at a boarding gate, but it may be subject to specific requirements depending on applicable security procedures.

5.3 Payment

A customer needs to pay for additional services at the airport and possibly receive a new boarding pass or update an existing one.

The steps include:

1. Customer is checking in or dropping a bag at the airport (via kiosk, bag drop device, or agent facing check-in counter).
2. Customer needs to pay for additional services and uses NFC to pay at the device/counter on the go, not sent back to a sales counter for that.
3. Customer pays at a payment-scheme-approved NFC reader integrated in kiosk, bag drop, or counter.
4. The airline system is capable of generating payment and receiving confirmation of a successful transaction.

5.3.1 Assumptions

- The payment use case requires the presentation of a physical payment device. In an alternative use case the payment could be made by a card on file.
- An NFC-enabled device when used for payment emulates contactless card functionality, as defined by the payment schemes.
- A customer's payment credential will be one supported by the POS/acquirer, such as:
    - Payment scheme:
        - Global schemes such as Visa, MasterCard, American Express, …
        - Regional and private schemes
    - Technology:
        - Magnetic stripe swipe
        - Contact EMV (chip & PIN)
        - Contactless

5.3.2 Cardholder Verification (Using EMVCo Scheme)

- A (PCI PED-compliant) PIN pad would be needed to accept payment devices that support online and offline PINs.
- If the payment is completed at a kiosk, the terminal would be classified as an unattended terminal. These have restrictions, including no support for signature-based transactions and possible limits to maximum transaction amounts, based on payment scheme and acquirer requirements.
- NFC payment issuers can provide products that support PIN/passcode verification into a device, removing the need for a PIN pad at the POS.

5.3.3 POS Requirements (Using EMVCo Scheme)

- The terminal/reader and payment functionality can be delivered using commercially available components.
- Custom integration will be required to support sharing the reader for NFC kiosk functionality, and to support any specific customer payment flows.
- Payment terminal/readers must comply with industry requirements, such as PCI and EMVCo.
- The POS functionality of the kiosk needs to communicate with a payment acquirer.
- The acquirer will define the requirements for the POS and payment schemes they support
- Space should be allowed around the NFC reader so that large form-factor NFC-enabled devices such as tablets can be presented.

- An airline's BP handset application can have an option to allow the consumer to select a preferred (NFC) payment card that will be the default payment option every time the app is activated.
- Support for NFC payment in Battery-power-low mode and Battery-power-off mode is subject to payment issuer and payment schemes authorizing this option in their mobile payment applications.

NOTE: PCI-compliant readers are not yet available in CUSS environments.

5.4 Other Potential Use Cases

The following presents samples from a long list of other air travel use cases identified by IATA that would benefit from implementation of NFC technology.

5.4.1 Backroom Operations

Much of this paper has focused on the needs of the passenger, but NFC also has multiple uses to improve airline and airport employee and backroom operations.

5.4.1.1 Secure Area Access

NFC-enabled devices can be programmed to work with contactless access control devices. This would allow an employee authorized to carry such a device to enter secured areas with just a tap. Also, NFC enables rapid OTA granting or revocation of access rights – far quicker and more convenient than getting a new plastic badge from the security office.

5.4.1.2 Employee Payments

Employees can use their NFC-enabled devices to pay for meals and miscellaneous expenses while on duty. Special accounts can be set up for authorized expense reports.

5.4.1.3 Employee Identification

Employee badges can be configured with NFC tags. Holding one of these tags to a contactless reader can identify the employee for access or check-in. NFC-enabled devices can also hold badge information and be used as access or identification devices.

5.4.1.4 Baggage Tracking

NFC tags can be coded and embedded in luggage tags to quickly access baggage information. A handheld contactless reader can be used to read owner, flight, and destination information.

5.4.2 Airport Operations

NFC has use cases that benefit general airport operations also, ranging from inventory control to supporting location-based services.

5.4.2.1 Parking

Travelers and guests can use their NFC-enabled devices to tap to enter a parking garage, pay at exit, or store parking details for later reference. This saves users time in locating their cars, and it speeds the exit process. It also saves money on payment-processing systems and equipment,

5.4.2.2 Onsite Purchases

NFC-enabled devices can be used to make payments for purchases and services throughout the airport. Shops can use NFC-enabled readers to accept payment and interact with passengers to send special offers or update loyalty points. Service operators such as shoeshine stands or massage sites can use handheld contactless readers to accept payment.

5.4.2.3 Logistics and Information

Passengers can tap readers to get customized information about their flight status, current loyalty updates, etc.

5.4.3 Marketing and Promotion

5.4.3.1 Smart Posters

Small and inexpensive, NFC tags can be embedded in smart posters, on product labels and on shelf displays, and easily read with a tap. These can be programmed with simple “touch and read” information or take a user to a website with a single tap. Smart posters can be used for both promotional and informational purposes. The universal “N-Mark” symbol, as described in the Appendix of this document, is used to indicate where to touch. Examples of successful use cases include downloading coupons, giving product details, launching to a website to make updates or apply for offers, etc.

5.4.3.2 Smart Billboards

This is a unique concept that can create a truly customized travel experience for the passenger. It consists of a contactless reader attached to an electronic display board and a back-end system. Passengers can customize their airline apps with personalized details such as preferred language and currency. Then, for example, when a passenger's device is presented at the reader, the back-end system can bring up customized flight details in the preferred language or show the user upgrade options in his or her preferred currency.

5.4.3.3 Loyalty Programs and Special Offers

Marketing is fast, easy, and fun using NFC technology. There are multiple “touch” opportunities to promote airline services, gain loyalty participants, and build one-to-one outreach programs. Because NFC is a two-way technology, an NFC-enabled device and an NFC-enabled reader can perform multiple actions at once. This delivers opportunities like updating loyalty points when a purchase is made or sending promotional offers when the boarding pass is redeemed. Simple “read and act” promotions enabled by smart posters and other NFC-tagged instruments also create these experiences.

5.4.3.4 Advertising

NFC can be used for effective one-to-one marketing and advertising campaigns. When combined with online tools, the advertiser has the ability to create customized campaigns with unique and specialized offers and promotions.

5.4.4 On the Plane

5.4.4.1 Device Pairing

In flight or at an airport lounge, it is possible for a traveler to pair his or her mobile device with an NFC-enabled entertainment system through a simple NFC tap. Both devices will negotiate over NFC the best way to exchange data.

5.4.4.2 In-flight Payments and Value-added Services

In-flight purchases, offers, or privileges can be pushed by the airline to consumers for redemptions when they start their journeys, reach their destinations, or return to their origin points. During a flight, payment by cash is cumbersome and expensive to handle, and payment cards might not be accepted. A potential solution can be to allow airline co-branded cards to make payment, collect points, redeem points (if applicable), and verify payments on mobile devices. This will result in faster payments, increased convenience, increased in-flight sales, and increased customer loyalty

5.4.5 Beyond the Airport

The airline can extend its offerings beyond airline ticketing by giving package deals, such as taxi access at the destination airport, hotel accommodation, or car rental, all using NFC keys delivered directly to the passenger's mobile device. Using social network channels such as Facebook and Twitter could also increase sales. The airline could track the places a passenger is visiting and use gamification to obtain more sales/conversions.

6 Implementation Options

As requested by IATA, the NFC Forum wants to present some alternatives for implementation of NFC Technology. The options presented below take into account two variables:

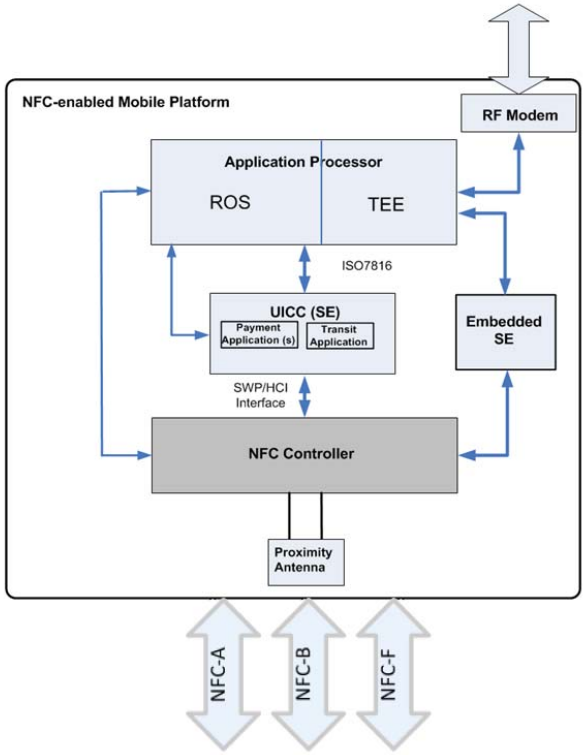
Type of Credential

- **Boarding Pass (BP)**[1] is the main credential this document focusses on, as agreed with IATA.
- **Payment credentials** have also been treated in Section 5.3 (Payment Use Case).
- ***Frequent flyer cards, lounge access cards, employee IDs…*** There are interesting use cases associated with these other credentials. They are, however, out of the scope of this document.

Location Where the Credentials are Stored

- Storage on a Secure Element (SIM Card, Embedded Secure Element or Secure Memory Card)
- Storage in the memory of the device (OS or Trusted Execution Environment)

The figure below shows how the NFC Controller in the device can manage data stored in the memory of the device or in different kinds of Secure Elements:



[1] NOTE: in order to manage BPs over NFC, an alternative to the storage of BPs in the device would be to store a passenger ID (i.e., a Frequent Flyer card). In this scenario, when the traveler tapped his or her phone at an access point or kiosk, the NFC terminal would read the Frequent Flyer card and retrieve from the airline back end the corresponding BP. Early implementations of NFC technology by airlines used a similar concept, deploying NFC stickers or plastic cards to their frequent flyers. This type of solution faces two fundamental challenges: the need for online connectivity and the lack of standards for Frequent Flyer cards. Such a solution could create a massive interoperability problem, by having multiple proprietary systems preventing the common use of infrastructure and usage by other parties not connected to the airline systems, such as airports.

It is not the goal of this document to provide a recommendation of any specific implementation option, but rather to present their merits and challenges objectively, in order to let IATA members make educated decisions.

Availability and addressable market size of each solution can vary a lot depending on the geographical regions. For targeted recommendations, advice from NFC professionals is recommended.

6.1 Storage in a Secure Element

6.1.1 Introduction to Secure Elements

A Secure Element (SE) is defined within GlobalPlatform, a standardization organization recognized by MNOs, OEMs, banks, banking organizations, and many other companies, as a tamper-resistant component that is used in a device to provide the security, confidentiality, and multiple application environments required to support various business models.

The Secure Element is generally used in the mobile device to support the emulation of physical contactless cards, such as payment cards or access cards. That is, the secure element is relevant when the device operates in Card Emulation mode, and/or when a high level of security is required.

The Secure Element is partitioned into multiple segments called Security Domains (SD), each of which can be assigned to a different external entity (Service Provider or their appointed aggregator) for the purpose of hosting "applets" to be used for contactless services. This recently standardized technology enables Services Providers (SPs) such as Airlines or Airport Authorities to have specific SDs allocated to them. Each SD has unique encryption keys, providing the right level of confidentiality, data integrity, and authentication necessary for the SP's services. This means that an airline *application* can interact securely with an *applet* containing customer-specific data, or boarding pass data, in any SD (that conforms to the standards). This provides flexibility and interoperability, as there is no need to develop a specific applet for a specific device or a specific Mobile Network Operator.

A range of implementation options is available for the storage of boarding passes. A likely example would be that a single Security Domain (SD) would be owned by a single trusted intermediary acting on behalf of all the airlines. A common application stored in a SIM card allows shared usage of the memory storage space on the SE and provides a single application that every airline can use to store its boarding passes. This applet presents the BPs to the reader, which selects the right one to use.

NOTE: The material above describes SE architecture according to GlobalPlatform. While this is a very mainstream implementation, it is not the only SE implementation available.

Mobile contactless payment is the most common use today for the secure element, driven by the need for security of the application itself as well as of the credentials associated with the customer's credit/banking account. For the airline customer to use an airline's branded or co-branded payment card in a mobile device to make a payment would require the availability of a security domain assigned to the airline for hosting the payment application and the customer's related account data.

Secure elements are essentially based on smartcard technology and can exist in several different form factors as follows:

- The SIM Card SE, also known as the Universal Integrated Circuit Card (UICC) SE
- Embedded SE
- Secure Memory Card SE

6.1.2 Common Characteristics of Secure Element Types

All SEs provide general value to the airline industry (cost reduction, operational benefits, new revenue possibilities as described in Section 3.2) and improve the ease and convenience of the customer's journey. SEs meet international security standards, which are certified and used by the financial services industry. Additionally:

- It is not a requirement to have a specific smartphone app for the passenger to receive or redeem a boarding pass. It is enough to have the BP Container applet stored in the secure element.
- No user interaction is necessary to read/redeem a boarding pass. Full "tap-and-go" experience is supported.
- The SE embodies strong physical security features (tamper-resistance).
- Flexibility: instantaneous update of BP (over the mobile network, or from a reader (via an authorized app)).

6.1.2.1 Trusted Service Manager

In order to support the provisioning and life-cycle management of applications in a secure element there must be collaboration between certain players in the mobile NFC ecosystem, based on well-defined and necessary roles.

The roles identified in the ecosystem include the Service Provider (SP), the SE Issuer (SEI), and a new role called the Trusted Service Manager (TSM) to mediate between the Service Provider and the SE Issuer. These roles are generally carried out by different players and in some instances may vary depending on the type of secure element. A summary description of each role is provided below.

Service Provider (SP): This is the entity providing the identified service to the consumer (this would be the airline in the context of this paper); what applications are hosted in the Secure Element (security domain) will be the decision of the service provider. Note that airlines do not necessarily need to implement their own SP TSM since it is possible to make use of shared infrastructure from third-party providers.

Service Provider TSM: This is the entity responsible for loading and managing the content in the Security Domain assigned to the Service Provider.

SEI TSM: This is the entity responsible to the SE Issuer for managing the Security Domain on the secure element itself. The SEI TSM does not have access to the content of the SP's security domain.

Note that TSM infrastructure does not participate in the routine transactions between the customer and the Service Provider.

Finally, it should be noted that some devices may support more than one secure element at the same time. How these multiple secure element devices will be managed from a service perspective is still being addressed within the standards/specification bodies.

6.1.2.2 Relevance of the Secure Element

In today's implementation of boarding passes (paper or 2D-Bar Code), there is little visible security and there is no express IATA requirement for additional security in a future NFC implementation. However, given the investment has to be stable and useful for the next 10-20 years, it is also important to look at NFC as a technology that enables airlines to future-proof their processes. Looking at NFC deployments in a bigger context, it is evident that other verticals such as retail, access, ground transport, and payments will require a SE for their NFC deployments. The SEs discussed in this section will exist in parallel, but will

be compatible with one infrastructure. These developments are likely to lead to a situation where airlines are required to support any and all solutions, including the different flavors of SEs.

This latter point is not an issue, since the standards allow content management across the different SE form factors to be the same. JAL is a good case in point. They are currently able to support both the UICC SE (NFC A, B, C) and the eSE (NFC F), as described in their case study in the Appendix of this document. Other examples of situations where airlines will need to use SEs are co-branded payment and physical access applications. It should also be noted that with the current work on m-identity, mobile devices will also be able to replace passports in the not-so-distant future. It will therefore make sense for the BP to serve as a secure identity for the user. The developments in m-identity will also be highly regulated going forward. Investing in NFC and being able to benefit from the SE concept ensures, therefore, that airlines are prepared for those developments.

6.1.2.3 Managing Boarding Passes in a Secure Element (SIM or eSE)

In the case of BP storage in a Secure Element, we must distinguish between the *BP Container applet*, stored inside the Secure Element itself, in charge of storing the boarding passes, and the *Mobile Application* or Apps stored in the memory of the device, that provide the user interface for the user to read and manage the BPs stored in the BP Container applet.

The NFC Forum's Air Transport Task Force would recommend that IATA define and standardize the BP Container applet, as a common use component that would in turn allow multiple mobile apps from different airlines or other third parties to access BPs following a predefined and uniform format and access policy -- in other words: one industry-wide standard BP Container, accessed by multiple Service Provider-specific mobile apps.

6.1.2.4 Using Secure Elements from a Mobile Application

The SIMalliance defined an API agnostic regarding the different mobile operating systems and providing a smooth access to any Secure Element, including UICC but also covering embedded Secure Elements or Secure microSD.

This API is called "SIMalliance Open Mobile API" and it is widely recognized by the industry. It is already used in most NFC deployments based on NFC UICC for Android devices and BlackBerry 10 OS devices.

GlobalPlatform endorsed the SIMalliance Open Mobile API and defined an Access Control mechanism – also agnostic with respect to mobile operating system – ensuring that only trusted and authorized device applications can get access to the application/information stored securely in the Secure Element.

The combination of the SIMalliance Open Mobile API with GlobalPlatform Secure Element Access Control provides a complete solution to deploy services leveraging the strong security of any Secure Element with a unique schema across different mobile platforms.

The SIMalliance Mobile Access API is also widely implemented by device manufacturers (hundreds of models from more than 15 manufacturers), especially on Android devices. It is also endorsed by BlackBerry on BB 10 OS as the reference API to provide access to Secure Elements. The specifications are public; a reference implementation "Seek for Android" with a royalty-free model is also publicly available. This implementation is covering several Secure Elements: UICC, eSE, and also microSD.

Like many other companies, airlines companies can rely on this API and associated access control mechanisms to deploy an air ticketing solution. Such a solution will be secure (based on Secure

Element), flexible (several Secure Elements can be used and the model can even be extended to TEE), and it will leverage recognized industry technology.

6.1.3 SIM Card (UICC) Secure Element Type

SIM-based NFC provides the above-mentioned benefits, which are common to all SEs. Moreover, SIM-based NFC is also characterized by the benefits the mobile industry can bring to the airline industry.

The role of mobile operators:

- Due to the existing implementations in retail and ground transport across the world, mobile operators know how to manage SIM-based NFC operationally.
- They are well positioned to market NFC services. Mobile operators can distribute NFC-enabled handsets, distribute and manage SIM cards as SEI, provide wallets to consumers, and manage services on SIM cards.
- Another core strength of mobile operators is the ability to partner with the airline industry for customer care. The passenger knows whom to call when something goes wrong: the mobile operator is a reachable and known entity for the customer with regard to technological problems when downloading the app and complementary to airline customer support.
- The SIM SE works in battery-power-low mode and offers the same customer experience worldwide, independent of the mobile device type.
- The dynamic provisioning of credentials to the SIM via the OTA channel is a familiar process for operators.
- The mobile operator is a contractual participant in the value chain – along with the TSM and hardware suppliers – ensuring security of the SE.

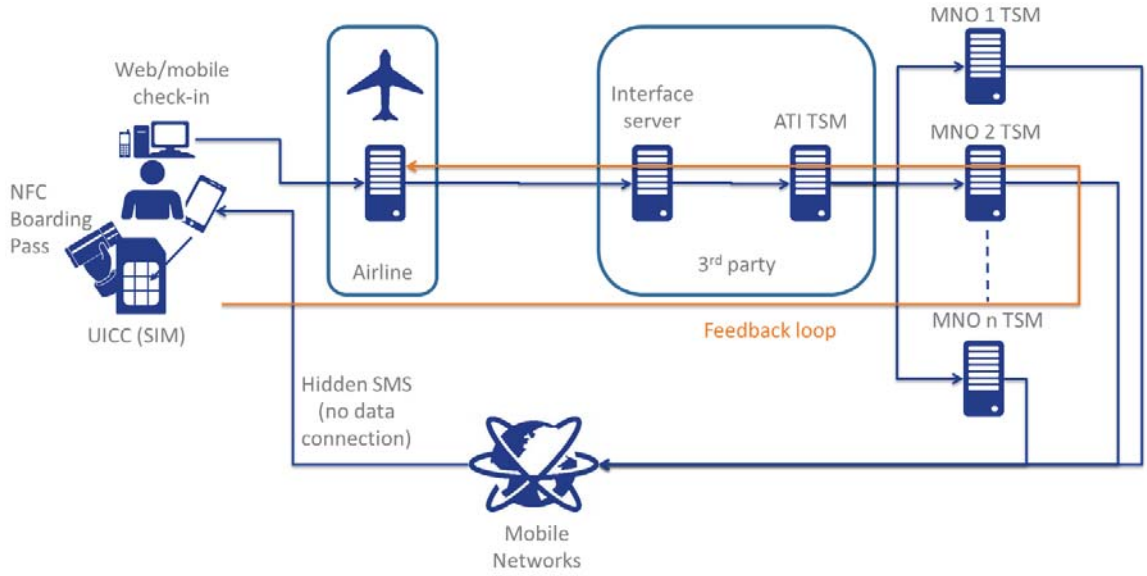
6.1.3.1 Implementation of SIM-based Mobile NFC Services in the Air Transport Industry

To provide NFC boarding passes to passengers' mobile devices, an interface with the SEI TSMs is required in order to be able to reach the passenger's SDs, with a communication channel dedicated to NFC services.

For a global solution working at the international level, a common approach is necessary in order to connect to as many MNOs as possible. It is possible to achieve this through a third-party aggregator, in a similar manner to an SMS aggregator today. This would allow IATA members to simply connect their web check-in service to a third-party interface server using simple web Application Programming Interfaces (APIs). The boarding pass information can be sent using a format based on IATA resolution 792, which is then translated into TSM commands to reach the passenger's SIM card using SMS as the transport bearer. This means that, in the case of the SIM-card SE type, there is no need for a cellular or WiFi data connection.

The memory storage space for boarding passes is limited by the memory space available on the UICC. This capacity is constantly expanding as technology improves. It is safe to assume today that a minimum of 10 boarding passes can be stored, following a round-robin scheme. Boarding pass updates are also supported and do not take any additional space. The old boarding pass would be replaced by the new one.

Thanks to the TSM technology, there is a feedback loop that allows a status message to get back to the airline server that can be used by Customer Care services to monitor the delivery of the boarding pass to the passenger. The diagram below is an example of such architecture.



6.1.3.2 Other Strong Points of the SIM SE

Further benefits arise from the established characteristics of the SIM card:

- **Maturity:** The SIM infrastructure and its supporting ecosystem are very mature, being the result of many years of development, usage and standardization. This leads to the SIM card providing the highest level of support across OS platforms, devices, and countries, and it is already supporting live secure services (for example, banking and ground transport).
- **Transferability:** The SIM card can easily be transferred to a different handset of any OS, brand, or model (as long as the handset meets the same NFC requirements as the original handset). This means that the customer can easily switch handsets and maintain the same services, user preferences, and customer support. (Apps would need to be re-installed, just like getting a new smartphone at any time, but the apps do not contain personalization details).
- **Personal:** Customers/passengers recognize the familiar SIM card and can readily relate it to other chip cards, so they should be comfortable with the concept of services on "their" SIMs (or can be easily educated so).
- **Serviceable:** No data connection is needed (only SMS) to receive, amend or cancel boarding passes – an important feature both for customer convenience and for security (in the event of handset loss).

6.1.4 Embedded Secure Element

6.1.4.1 Embedded Secure Element and Market Adoption

An embedded secure element (eSE) is a chip installed into all NFC-enabled devices. Its function of storing sensitive data in a secure manner has made it the choice of some key operators.

For example:

- Google Wallet is based on eSE.
- Visa announced a global partnership with Samsung at the Mobile World Congress 2013: it would preload its NFC application onto embedded chips in new Samsung NFC-enabled devices.

- JAL (Japan Airlines) and ANA (All Nippon Airways) airlines manage their boarding passes via NFC-enabled devices equipped with eSEs.

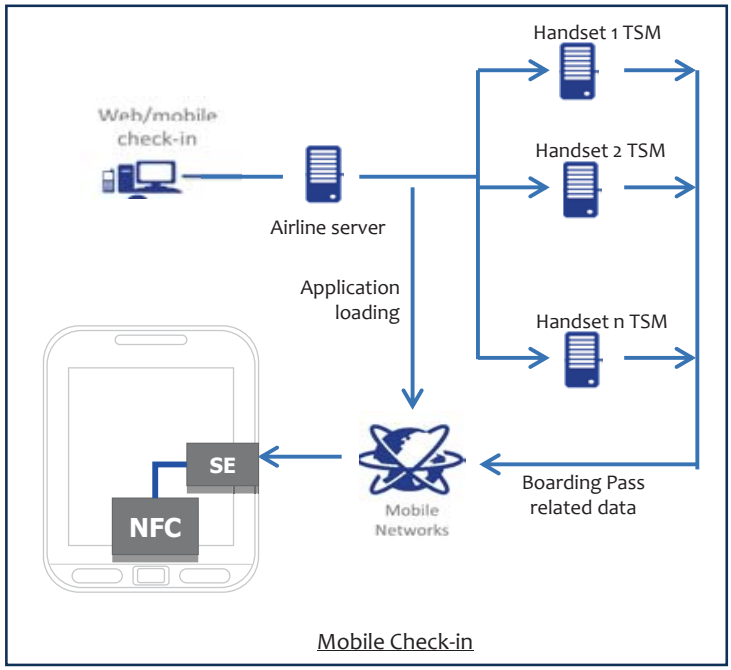
In today's implementations, the device is usually used like a card (i.e., operating in card emulation mode). In the future, the addition of flexible peer-to-peer mode is expected.

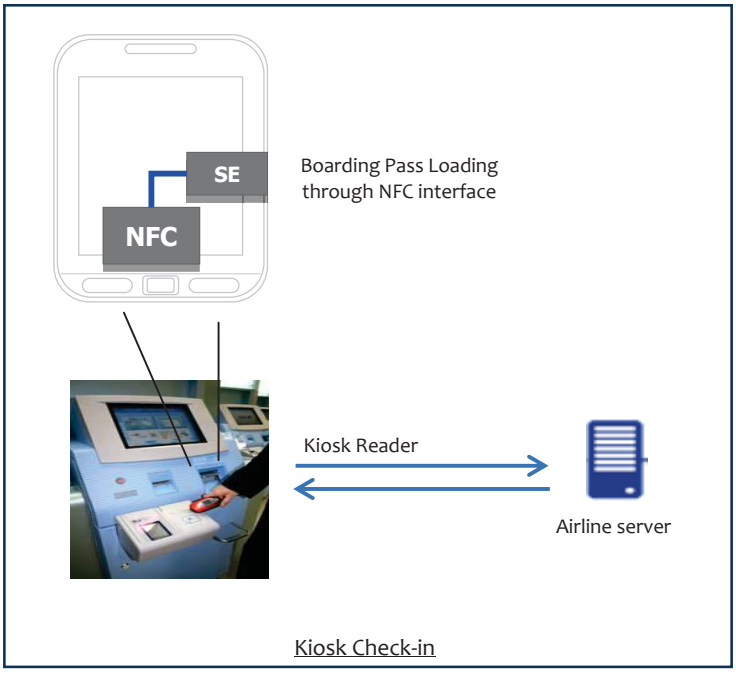
All the features listed in Sections 6.1.1 and 6.1.2 (security, BP management, BP format, and so on) are applicable to the embedded secure element.

6.1.4.2 eSE Airline Use Cases and Implementation

Boarding Pass provisioning:

The architecture for Boarding Pass provisioning and update is as follows:



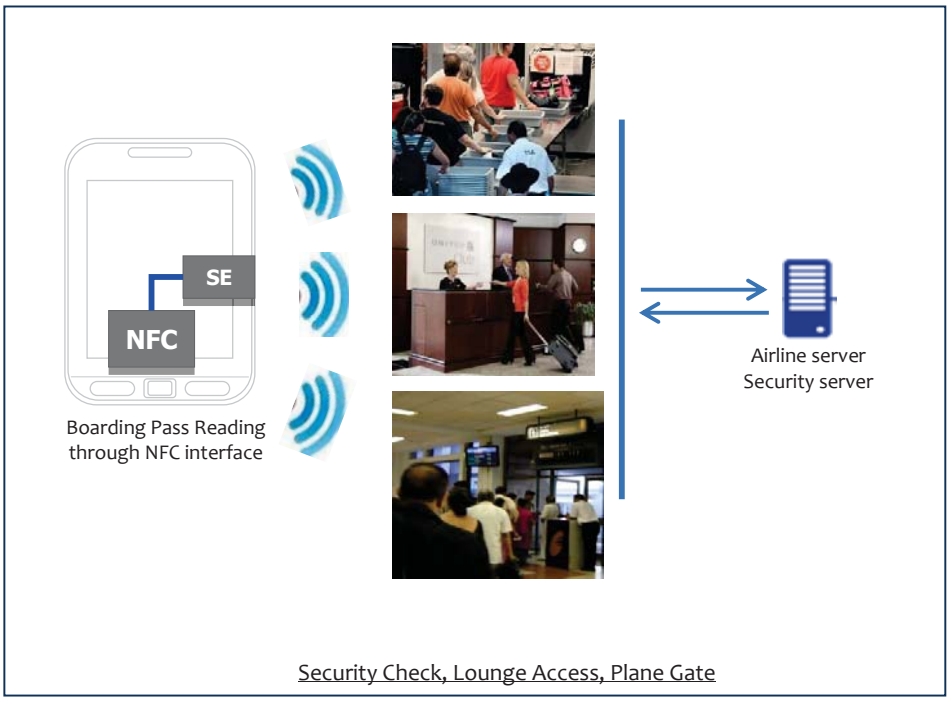


Such an architecture provides a global solution that works at the international level:

- The web and mobile check-in service is linked to an airline server sending the Boarding Pass to the end user's mobile device (Over The Air delivery).
- The check-in kiosk embeds a reader providing the Boarding Pass to the traveler's mobile device through the NFC interface when the traveler presents his or her device to the kiosk reader.
- Both check-in services allow for updates to the boarding pass, such as for flight change, seat allocation, etc.

Presenting the Boarding Pass at the Security Checkpoint, Lounge, at the Gate:

The user would be granted access (or denied access) to the airside, lounge or plane, depending on the data stored on the eSE. When presenting the NFC-enabled device to a reader to check the boarding pass, the system will determine the applicable access privileges. The various readers distributed throughout the airports may read the boarding pass from the eSE. See the illustration that follows.



6.1.4.3 *Benefits of the eSE*

There are various benefits provided by the eSE as regards customer control, user experience, and business scheme, in addition to the usual security features:

- By dealing with handset manufacturers (directly or through TSMs), airlines and service providers can control their security domains, their applications and their consumers. Airlines do not necessarily need a relationship with Mobile Network Operators.
- An airline can provide support to its customers if there are issues with the Boarding Pass.
- The hardware and software architecture of the device allows boarding pass reading with good speed, even if the device is off or in low power mode, as can be observed at current implementations such as in Japan.
- The eSE is capable of hosting payment services and credentials. The customer may use his or her device for payments as long as a payment application and one or more payment credentials are available in the eSE

6.1.5 microSD Card

6.1.5.1 *microSD Secure Element*

The microSD card has gained recognition as one of the standardized SE form factors, along with the UICC and the embedded chipset. This is a removable secure element based on the commonly used data storage memory card, which requires the mobile device to be equipped with an appropriate physical slot to accommodate the card.

The microSD card is a non-volatile memory card that was developed for use in portable devices, including mobile phones, digital cameras, etc. It requires that the portable device be equipped with a suitable slot for the card. According to the SD Association, approximately 78% of all mobile phones are now equipped

with a memory card slot. In addition, the SD Association has also identified the microSD card as the #1 memory card form factor for mobile devices.

To be clear, a current off-the-shelf memory card will not suffice as an SE, since the security requirements for a SE hosting sensitive applications would greatly exceed what is provided by a regular memory card. In addition, there are other requirements/standards that the memory card would need to comply with in order to be deemed a secure element comparable with the other secure element form factors described in this document.

The use of the Secure Memory Card as a Secure Element has been used in a number of NFC trials, primarily to support mobile NFC contactless payments at the retail point of sale.

There are two types of microSD for supporting NFC services: the full NFC card and the SE-only card. With the full NFC type, the microSD card comes with the SE and also the NFC RF and antenna built in. The full NFC version was also referred to as the active microSD SE.

Full-NFC microSD SE (Source: SD Association)

The advantage of this solution is that it allows a mobile device without NFC to be used to support NFC services. In other words, a non-NFC-enabled phone could in principle be immediately converted to an NFC-enabled device. As a result, the full NFC card was initially positioned as a bridging technology to support early mobile NFC implementation pending the wide availability of NFC-enabled handsets.

Several vendor-specific full NFC solutions have been developed and used to support technical and market trials and have been used to support commercial service in certain markets. To date, these have all focused on contactless payment at the point of sale.

With the SE-only card, also referred to as smart microSD by the SD Association, the SE is built in with an external (Single Wire Protocol based on the ETSI standard) connection to the NFC controller in the device. This allows the SE to work with the NFC antenna built into the device, removing some of the compatibility issues experienced with the full-NFC version.

SE-only microSD Card (Source: SD Association)

The introduction of the smart microSD expands the possible business models for NFC deployment. With the microSD card, it is now possible for any of several players to now potentially play the role of the SE Issuer. These would include Service Providers, Mobile Network Operators, microSD manufacturers, etc. Depending on which party issues the card, it is possible for the card to be utilized as a single or a multi-application platform.

In the instance where the Service Provider (SP) plays the role of the SE Issuer, the card is directly provided to the customer with the (SP) application pre-provisioned and personalized.

Another model that can be enabled by the smart microSD is the consumer-centric model. In this model, the card is purchased directly by the consumer and is provisioned with the required applications by a trusted third party authorized to provision the applications on behalf of the service providers.

A consumer controlled microSD card able to support multiple services simultaneously from different service providers is a potential business model. In addition to conforming to the SD Association requirements for smart microSD cards, such cards will have also have to conform to the security requirements of the services being supported on the card as well as the GlobalPlatform card specifications for managing multiple applications on a common card.

While such cards are not currently widely available, this is expected to change over the next few years and will need to be considered as a possible solution for all NFC services requiring the use of a secure element. The microSD SE is viewed as a form-factor that may accelerate the adoption of a more consumer-centric model for NFC services. In such a case, the microSD SE would be purchased directly by the consumer and selected services remotely provisioned through the assistance of a trusted third party.

The specifications needed to support a consumer-centric model are currently being developed within GlobalPlatform.

6.2 Storage in the Memory of the Device

6.2.1 Device OS

In this implementation option, the boarding pass is stored in memory that is accessible through the operating system on the device.

Two types of device storage are possible:

- Internal storage (typically: non-removable storage (flash) inside the device)
- External storage (typically: a removable SD card) if the device supports this option

Most platforms allow an application to have its own sandboxed storage. That means no other application on the system has access to the data.

6.2.1.1 Provisioning the Boarding Pass Over the Air

The boarding pass can be downloaded to the device and then stored in either internal or external storage. How this would typically work is that a user downloads an airline application from the platform's application store. This application identifies the user in some way, and it can then download boarding passes from a back end (provided by an airline or an organization representing multiple airlines) and store them in the device's storage. The boarding pass can be stored in the format defined in IATA resolution 792, with a small NFC-specific wrapper around it. Finally, the application can report back to the back end that it has successfully received the boarding pass.

Updating the boarding pass could be implemented with so-called "push notifications," which are supported on most platforms. Push notifications allow a back end to push a newly provisioned boarding pass to the device automatically. On receiving such a notification, the device wakes up, and it can then store the boarding pass in its storage, additionally with a notification to the user that this has happened. Status updates indicating whether the boarding pass was successfully updated can be sent back as well.

One of the IATA requirements is that provisioning the boarding pass must work even without downloading a separate airline application. This is only possible when the Operating System on the device already knows about NFC boarding passes; otherwise, the device wouldn't know where to get the boarding passes, or even who is the right customer. Currently, Operating Systems do not support NFC boarding passes because there is no defined standard for their format and location; however, once such a standard is defined, it could be a natural extension for platform applications like *Google Now*, which already scans e-mails to find boarding passes.

6.2.1.2 Provisioning the Boarding Pass Through a Kiosk

When the boarding pass is provisioned at a kiosk, this is done through the NFC interface of the kiosk. There needs to be an application on the device that interacts with the kiosk's NFC interface, and then stores the boarding pass received over NFC in the device's storage. This could be an airline application, or an application that is part of the Operating System in the device itself.

6.2.1.3 Retrieving the Boarding Pass

To retrieve the boarding pass from the device's storage, an app can use platform APIs to retrieve the boarding pass from the device's storage, and then present it over the NFC interface. Again, this app may be part of the Operating System.

6.2.1.4 Security Considerations

As mentioned above, most platforms allow each application to have its own sandboxed storage area. This means that the boarding pass would only be accessible to the application that has written it to the device storage. It cannot be read or exported by other applications.

Some potential vulnerabilities and ways to minimize the risk include:

- Exploiting a vulnerability in the Operating System of the device, allowing the boarding pass to be read by other applications, despite the sandboxing. This is difficult to do, however, and is only possible if the attacker roots or "jailbreaks" the device.
- Theft of the device. Password protection on the device helps to mitigate this vulnerability. Consumers may also contact their service providers to have their devices shut off or wiped clean (note that traditional paper boarding passes may be easily lost or stolen).
- Skimming the boarding pass, by holding a NFC reader close to the device. Skimming can be prevented by presenting the boarding pass over the NFC interface only when the device is in a certain state; for example, only when the device's screen is on, or when the device is unlocked.

6.2.1.5 Advantages of Storing Boarding Passes in Device Memory

- Device memory can easily be read/written by any application on every popular OS and platform.
- It is easy for any airline app on the device to find the current state of its provisioned boarding passes and visualize it.
- Device memory is a well-proven solution that is in use by millions of apps on every platform today; there are many deployed NFC apps that are already using the device memory for storage.
- There is enough device memory to store boarding passes, and it is free; no need to reserve and pay for space in an eSE/UICC.
- There is no dependency on mobile network operators and TSMs.
- There is no dependency on a mobile network to provision boarding passes; any kind of data connection will do. It will work on devices with NFC but without a SIM as well, e.g., tablets.

6.2.1.6 Disadvantages of Storing Boarding Passes in Device Memory

- Device memory is typically only powered when the device itself is powered; hence, if the device has run out of battery, it is impossible to provision or present the boarding pass.
- Some form of data connection (cellular, WiFi, cable) is needed to provision the boarding pass.
- There needs to be an application present that reads the data from device memory and presents it to the NFC interface; this may be an application that comes as part of the Operating System.

6.2.2 Trusted Execution Environment (TEE)

Trusted Execution Environment (TEE) is a standardized and secure technology used for storing and processing service provider assets in smart connected devices (e.g., tablets and smartphones). A TEE is built directly into the heart of a device (a system-on-chip application processor built by many of the leading chip suppliers to the industry). It enables trusted software to access device resources such as keypads, displays, mass data storage, biometric sensors, radio interfaces, and secure storage. TEEs provide a balanced level of protection and user convenience by securing interfaces such as the User Interface. The traveler's journey with a TEE-enabled device is simpler, since it facilitates faster ticket purchases as well as secured/trusted boarding pass data storage and presentation. In addition, the TEE may be used for loyalty, coupons, location-based offers, and other device and user identities.

TEE technology is standardized by GlobalPlatform – the same standards body that defines remote management of secure domains for secure elements and other devices requiring secure domains, such as the UICC. If a device has a built-in TEE, then the user can choose services that are designed to make use of the hardware isolation features of his or her device's application processor without being connected to any network via mobile RF network or WiFi. Such services would include simpler, faster, safer payments, viewing any content on any screen, or using his or her personal device of choice at

work. Currently, over 100M TEE-enabled devices have shipped to date, and adoption of using this environment is rising significantly.

6.2.2.1 Implementation of a TEE-based Mobile NFC Service in the Air Transport Industry

The traveler could opt to download an airline application similar to what occurs today or opt to have ticket credentials sent to an email address. Therefore, airlines can simply send boarding passes or other related travel information via email, perform trusted communications between the airline server and the device's trusted application, or directly through the NFC radio interface. Communication over the air would require network or WiFi connectivity.

The airline's trusted application can store boarding passes in three different ways/locations for NFC retrieval and/or presentation. The TEE can store a boarding pass into a known location in the device system memory, it can store a trusted (encrypted) boarding pass into the device's trusted storage, or it can securely store the boarding pass into an embedded or UICC-based secure element. The location and type of storage is determined by the level of security required for boarding pass protection.

6.3 Implementation Options – Comparison Chart

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
Solution Availability	Solution commercially available today	Yes	Yes	Yes	Yes	See Comments	TEE: Many devices come already equipped. However, current early implementations are very restricted in functionality and non-upgradeable.
	Solution stable and still available in 10/20 years	Yes	Yes	See Comments	Yes	See Comments	SMC: Depends on availability of microSD slots and specific accessories (casing) in mobile devices TEE: Emerging technology. Not mature yet. Should be available in the long run.
	Supported across multiple mobile OSs and devices	Yes	Yes	Yes	Yes	Yes	
	Supported in many countries	Yes	Yes	Yes	Yes	Yes	
Key Requirements	Supports IATA R-792 BCBP data format	Yes	Yes	Yes	Yes	Yes	
	No UI application on device required to provision/read BP	Yes	Yes		See Comments	See Comments	Support could be added
	No user interaction with the mobile device required to read/redeem BP (tap and go)	Yes	Yes	No	See Comments	No	DM: Depends on modes (card emulation, P2P, …) and security.

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
Additional Requirements	NFC BPs can be read/redeemed even when battery is completely depleted or removed	No	No	No	No	No	Even if it is possible on paper for the NFC chipset -- and through it a secure element -- to be powered through the field generated by a contactless reader, most devices available today do not support this scenario reliably or at all.
	NFC BPs can be read/redeemed even when device is in "low power" mode	Yes	See Comments	See Comments	No	See Comments	eSE,SMC: Depends on device design
	Operational benefit: Higher throughput than Barcoded BPs	Yes	Yes	Yes	Yes	Yes	
	Operational benefit: Higher security than Barcoded BPs on a mobile device	Yes	Yes	Yes	No	Yes	Higher security is inherent in the characteristics of Secure Elements and even of TEE, compared to storage in device memory.
	More reliable than Barcoded BPs	Yes	Yes	Yes	Yes	Yes	Reading over NFC is more reliable, as it is not subject to device alignment or environmental light.
	Enables building premium services based on BP	Yes	Yes	Yes	Yes	Yes	
	Enables building premium services based on other credentials	Yes	Yes	Yes	Yes	Yes	

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
Key Use Cases	Get new BP over the air	Yes	Yes	Yes	Yes	Yes	
	Get New BP at a Kiosk	Yes	Yes	Yes	Yes	Yes	
	Update BP over the air	Yes	Yes	Yes	Yes	Yes	
	Update BP at a kiosk	Yes	Yes	Yes	Yes	Yes	
	Redeem BP (through UI app)	Yes	Yes	Yes	Yes	Yes	
	Redeem BP (Tap & Go)	Yes	Yes	Yes	No	No	
	Card Present NFC Payment	Yes	Yes	Yes	No	No	As of today, schemes require credential stored in a secure element to consider transaction as card present.
Additional Use Cases	Third party or TSA is able to read all boarding passes on device, even if stored in multiple containers	See Comments	See Comments	See Comments	See Comments	See Comments	Possible. Depends on design
	Once used, BPs can be marked as read/redeemed	Yes	Yes	Yes	Yes	Yes	
	BPs can be marked as "cleared" by TSA	Yes	Yes	Yes	Yes	Yes	
	Once redeemed, BPs can be deleted or moved to a different container	Yes	Yes	Yes	Yes	Yes	
	User can read through device UI the human readable information of the BP	Yes	Yes	Yes	Yes	Yes	

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
Other Characteristics	Solution can use a common-use app for BP storage (BPs from different airlines stored in the same container)	Yes	Yes	Yes	Yes	Yes	
	BP storage app located in Secure Element	Yes	Yes	Yes	No	No	
	No TSM required for BP Provisioning	No	No	No	Yes	See Comments	Depends on solution design
	NFC radio can be remotely turned on without user intervention	No	No	No	No	No	
	NFC can work in Airplane mode	Yes	Yes	Yes	Yes	Yes	Device may turn NFC off when switched to airplane mode. But it may be possible to program mobile apps to automatically turn on NFC when launched.
	BP integrity assurance: BP can be signed according to NFC Forum specifications to ensure that it has not been modified since it was issued	Yes	Yes	Yes	Yes	Yes	
	NFC BPs can be issued by each individual airline	Yes	Yes	Yes	Yes	Yes	
	Can NFC BPs be issued by a single trusted third party on behalf of all airlines?	Yes	Yes	Yes	Yes	Yes	
	A very large number of BPs could be stored	See Comments	See Comments	See Comments	Yes	Yes	Secure memory is a finite resource. Number of BPs that can be stored will be optimized by parties involved. If a predefined maximum is reached, a procedure (to be defined by IATA) will be applied: it could be First In-First Out, or a prompt to user to delete used BPs, etc.
	NFC reader could read the NFC BP selected by user through device UI to be redeemed (and not any other one)	Yes	Yes	Yes	Yes	Yes	

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
Other Characteristics (cont.)	NFC Reader could read all BPs on device (even if stored in multiple containers) and select the appropriate one for redemption based on context (time & location)	Yes	Yes	Yes	Yes	Yes	
	Can one single NFC radio read BPs stored in multiple containers?	Yes	Yes	Yes	Yes	Yes	
	Could the same IATA standardized BP Container applet be used on Secure Elements (UICC, eSE, SMC) and in memory of the device?	Yes	Yes	Yes	Yes	Yes	
	With NFC disabled, can an application inside the device read stored BPs so as to display their info through the UI?	Yes	Yes	Yes	Yes	Yes	
	Without an application inside the device, is it possible to present the BP through the UI of the device for redemption in airports not equipped with NFC readers?	No	No	No	No	No	A UI application is needed to read the BPs. It could be a general-purpose application or an airline application. It could even be a native application coming with the device OS.
	No third-party agreement required to store credentials in the device	No	No	No	Yes	No	SIM: Agreement with Wireless Network required eSE: Agreement with Handset Vendor required SCM: Needs to be purchased TEE: Agreement with TEE issuer required

	Requirements & Questions	Credentials Stored in Secure Element			Credentials Stored in Device Memory		Comments
		SIM Card (SIM)	Device SE (eSE)	Secure Memory Card (SMC)	Device Memory (DM)	Secure Device Memory (TEE)	
NFC Modes	Card Emulation	Yes	Yes	Yes	Yes	Yes	
	Peer to Peer	See Comments	See Comments	See Comments	Yes	See Comments	Peer to Peer works for all solutions. But secure elements or TEE are not involved in current implementations.
	Reader mode	See Comments	See Comments	See Comments	Yes	Yes	ETSI specifications allow a SIM application to process/react to content read by device in reader mode.
Mobile OS	Android	Yes	Yes	Yes	Yes	Yes	At this point there is no standardized mode for managing multiple secure elements.
	Blackberry 10	Yes	Yes	Yes	Yes	Yes	
	Windows Phone 8 *	Yes	Yes	Yes	Yes		
	IOS 6, 7 *	See Comments	No	See Comments	No	No	This requires a special casing providing NFC radio and a secure element

* Based only on publicly available information

7 Economics of NFC Technology Adoption

Deploying NFC, as with all new technologies, requires changes and upgrades to existing infrastructure. NFC also adds new components to the infrastructure. And all of these changes involve a cost factor. The benefits of investing in NFC are reduction of existing expenses, introduction of new revenue streams, increase in customer satisfaction, and enhancement of internal communications.

This section sets out the infrastructure and service costs on one side, and some of the possible gains on the other. It is not meant to be a comprehensive cost-benefit analysis, but rather a guide for better understanding. The NFC Forum membership includes consultancies specializing in NFC, which can help build full revenue models and analysis.

7.1 Cost of NFC Adoption

The main cost factors common to all implementation options include:

1) The NFC card reader infrastructure
2) Credential (boarding pass, loyalty card) back-office processing systems
3) Any user-interfacing mobile application
4) Any common-use container application (for boarding passes, frequent flyer credentials, etc.)
5) When the container application is implemented in a SE or TEE, the cost of memory allocation and infrastructure to manage it must also be considered.

Concerning the NFC reader infrastructure, terminals will have to be upgraded to integrate an NFC reader. It should be noted that in some countries, equipment may be already upgraded to support EMV contactless payments, in which case the equipment would be totally reusable for boarding pass redemption, presentation of frequent flyer credential, or other usage. However, adding NFC to the existing contactless reader infrastructure adds two-way capabilities to enable use cases such as sending back updates and offers.

As for back-office processing systems, boarding passes can be transmitted and stored in the mobile device (in any of the proposed storage options) in the same format as they are now. In this case, no change to the back-office systems would be required. However, if airlines were to decide to introduce changes to the BCBP format to better take advantage of the new features of NFC, then these back-office systems would have to be updated accordingly.

Any mobile device user-interfacing application requires specialized development. These applications could either be brand-new developments or evolutions of existing airline, airport, or other third-party mobile applications already existing today. Depending on the implementation option, these applications will have to manage communication with the NFC chipset over NFC and/or with a common-use storage application where boarding passes or other credentials issued by different airlines may reside. Note that in the case of the SE implementation option, a mobile device user interfacing application is not absolutely required (an NFC reader could read boarding passes or other credentials directly from the SE container application), but it is highly recommended. The device application has to follow strict rules to communicate with the SE application.

The SE/TEE container application for common-use storage of credentials also requires specialized development. SE applications are subject to high security restrictions.

The SE space costs are related to leasing fees, transaction fees, or other fees associated with the use of memory. The SE memory is a limited resource, and the issuers of the SE (typically mobile network

operators for SIM and mobile device makers for eSE) have significant investment in managing it. This cost may change significantly between SE owners or regions and countries. The mechanism for updating the SE application with boarding passes, loyalty card information, or offers can be handled internally or externally.

Updating the content of the SE or TEE requires a Trusted Service Manager (TSM) platform to handle the required security. Service providers can deploy this infrastructure internally or contract it as a service from a third party provider.

7.2 Return on Investment

From past experience and similar deployments, there will be significant return on the investment in adopting NFC technology. One such example is mass transit systems' use of NFC and their cost savings in the areas of printed tickets, mechanical kiosks, and customer service agents, their increased revenues from return customers, and expansion into co-located and related businesses. More directed at the airline industry, NFC readers have reduced costs over barcode readers. These readers also lower customer service personnel costs, at the same time providing increased accuracy and reduced read time.

The use of NFC technology enhances the customer experience. NFC use is intentional, as opposed to passive, which consumers prefer. NFC can be used to deliver partnership offers, which can include profit sharing. With NFC, travelers can quickly access airport information (e.g., maps and services locations). NFC can enable parking garage payment and car location, one example of expanding the experience to co-located and related businesses.

In other ways, using NFC can increase customers' engagement and satisfaction with airlines – such as by providing easier payment, quick access to loyalty programs, one-touch entry to elite lounges, and timely delivery of updates to travelers.

Some other possible revenue and cost saving opportunities were presented in Section 3.2.

8 Platform/OS Support

This section provides details about how NFC is supported in the three leading mobile device operating systems that implement this technology today. Jointly these three operating systems cover more than 80% of the smartphone market, according to IDC's Worldwide Mobile Phone Tracker of September 4, 2013.

8.1 Android

The Android platform defines a set of public APIs that can be used by application developers writing third-party apps. Google makes sure that every manufacturer building an Android handset implements these APIs properly, by requiring them to meet the requirements of the Compatibility Definition Document (CDD) and pass the Compatibility Test Suite (CTS). More information can be found at http://source.android.com/compatibility/overview.html.

The Android platform has supported NFC since the Gingerbread release. As outlined in Section 2.1, NFC has three main modes of operation. The following sections describe each of the three modes and how they are supported in Android. The last sections describe the APIs available to store boarding passes on Android and options for over-the-air provisioning.

8.1.1 Reader/Writer Mode

Any Android device running Android Gingerbread (version 2.3.3 or later) is capable of reading/writing all NFC forum standard tag types. This capability is explicitly called out in the CDD document as well. Android additionally supports adding an Android Application Record to a tag, which if present will make sure that a specified Android application is launched whenever that tag is tapped.

Reader/writer mode could for example be used to read a boarding pass that is presented through a kiosk (the kiosk emulates an NFC tag with a boarding pass, the Android device reads it). If the kiosk additionally presents an Android Application Record in the tag, the user will not even have to launch an application to receive the boarding pass. The application can then store the boarding pass in the device memory.

This mode could also be used for presenting the boarding pass; the NFC terminal at the airport could emulate a standard NFC forum tag, and an Android application could write the boarding pass into the memory of that tag. The terminal would then read out the tag's memory to find the boarding pass. The advantage of this approach is that it is supported on every Android NFC-enabled device ever released.

8.1.2 Peer-to-peer (P2P) Mode

Android has proper support for P2P mode since the Ice Cream Sandwich release (version 4.0.0 or later). In Android this feature is called Android Beam. It basically allows any app to set a payload to be shared over the NFC interface. Whenever the device comes in range of another P2P-capable NFC-enabled device, the data is sent across. If the boarding pass is stored in the device storage, it is very easy to use Android Beam to present a boarding pass; the application just retrieves the boarding pass from device storage with standard Android APIs, and then uses the standard Android Beam APIs to pass the data to the NFC controller. On tap, the data will be passed from the NFC controller to the airport NFC terminal in P2P mode.

A downside of using Android Beam is that the application presenting the content must currently be running in the foreground – and so it requires users to launch the application that is presenting the

boarding pass before tapping. It's important to point out that this is not a limitation of the NFC P2P technology itself, but a design choice made by the Android team.

Supporting background P2P operations is on the Android roadmap for a future release.

8.1.3 Card Emulation Mode

Cards can be emulated in several ways:

- By a UICC
- By an embedded Secure Element
- On the device CPU itself

If a UICC or an embedded Secure Element does the card emulation, Android is typically not involved in the transaction at all. Android may still need to configure the UICC/eSE in various ways – for example, whether it should work when the device is switched off. This is typically done by private (and often device-specific) APIs that are not enforced through the CDD. As a result, there is no uniform way for users to manage the eSE/UICC state on their devices.

Emulating a card on the device CPU itself is an interesting option; in that case, the card emulation is done by a normal Android application (which could have been downloaded from the application store). This removes the dependency on an eSE or UICC to do the card emulation. Support for emulating cards on the host CPU is currently not present in Android, but is planned for a future release.

8.1.4 Storage APIs

Android does not contain any public platform APIs for storing data in a Secure Element, and such APIs are currently not planned to be added to Android. There are two well-known APIs that are not part of the public Android platform APIs, but which are added by mobile device manufacturers and wireless carriers on many handsets:

- The NFC-extras API from Google is an API for accessing embedded secure elements, publicly available in the Android Open Source Project (AOSP). This API is used by, for example, the Google Wallet application. The API contains a whitelist of signatures of applications that are allowed to talk to the eSE. On most devices running Google Wallet, that is only the Google Wallet application. To be able to use the NFC-extras API, an airline application would need to be added to this whitelist.
- The Seek for Android API is a publicly available reference API defined by the SIMalliance for communicating with all types of secure elements (SIM/eSE/SMC). Applications are granted access to the Secure Elements as specified in the GlobalPlatform Secure Element Access Control specification. Seek for Android is implemented by at least 13 different main Android device makers on at least 175 commercially available smartphones. Notable devices that do not ship the Seek for Android API are Google's own Nexus devices.

In summary, applications using Secure Elements will only work on Android devices that include the Seek or NFC-Extras API, and they will need to be allowed by the OEM and/or wireless carrier to use those APIs.

8.1.5 Back-end Connection and Push Notifications

The Android platform supports *Google Cloud Messaging* (GCM), which is a service that allows sending data from a server (back end) to a customer's Android-powered device. Response data can be sent back on the same connection.

GCM could be used to deliver boarding passes over-the-air, as well as sending back status messages to the back end. A useful feature of GCM is “user notifications,” which allows a back end to push a boarding pass to all devices a user owns. The boarding pass could then be stored in the device storage of each of the devices, and the traveler would have the option to present the boarding pass using any of his or her devices (for example, either phone or tablet).

8.2 Windows OS Support

This section has been prepared based solely on publicly available information. No direct input was provided by Microsoft.

While every attempt has been made to accurately reflect publicly available information, it is possible that this information is not entirely up to date on the Microsoft plans for the Windows Phone 8 operating system and its updates. If Microsoft provides additional information, this section will be updated accordingly in a future revision.

The Windows Phone 8 mobile operating system, which was released in October 2012, introduces support for all three NFC modes: peer-to-peer, reader/writer, and card emulation. In addition, Windows Phone 8 includes a Microsoft Wallet that can be used to store sensitive information about the device owner's payment cards and loyalty cards.

Windows Phone 8, in addition to supporting device to device data transfer, also supports data transfer between a Windows Phone 8 smartphone and a Windows 8 device such as a computer or tablet.

It should not be assumed that every Windows Phone 8 device is capable of supporting NFC applications. While Windows Phone 8 is a prerequisite for NFC support, enabling the technology will require the addition of the NFC chipset by the device manufacturer and support for the secure element (either embedded SE or SIM-based SE). Windows Phone 8 also provides support for the microSD card but there are no indications at this time that the passive microSD SE is supported.

A key consideration of note is that Windows Phone 8 devices will be upgradeable to the next version of Windows Phone. This is new (Windows Phone 7 phones cannot be upgraded to Windows Phone 8) and is significant from the viewpoint of continued support for any solution based on Windows devices. In any case, a new version of Windows Phone is not anticipated before late 2015 at the earliest.

For September 2013, the MasterCard website is showing 13 Windows Phone 8 devices that have already been approved to work with PayPass mobile contactless payment application. In addition, NFC World (www.nfcworld.com) also provides a list of available NFC-enabled phones, including a similar number based on the Windows Phone 8 OS.

8.3 BlackBerry 10 OS

The BlackBerry 10 OS platform is built upon the QNX Neutrino Real Time Operating System (RTOS), offering speed, stability, scalability, and new innovative features. NFC is one of those features supported by the platform for use cases identified in this document.

NFC and other features can be accessed via the related API offered by the BlackBerry 10 OS platform. For NFC the following functionalities are implemented: R/W, P2P, Virtual Target Emulation, and Card Emulation with UICC.

More information can be found on the BlackBerry 10 Developer Support Web page for NFC technology: http://developer.blackberry.com/native/documentation/bb10/com.qnx.doc.nfc/topic/manual/c_stub_nfcdevguide_general_introduction.html.

8.3.1 Reader/Writer Mode

The platform offers various APIs to read/write an NFC-Forum tag with NDEF/RTD contents. It allows an application to register for specific properties. When such properties are found on a tag, the application will be launched and then can take relevant actions. All NFC Forum NDEF/RTD formats are supported, such as Smart Poster, Text, and URI, but also static connection handover. The platform also allows the application to access at lower tag communication protocols for use cases not relying on NDEF/RTD contents. Thus, the BlackBerry 10 device can be easily implemented as a Boarding Pass scanner/reader/validator at the boarding gate, security checkpoint, control gate, or airline lounge.

8.3.2 Peer-to-peer Mode

The platform offers APIs to support Peer-To-Peer mode to exchange contents between devices. Small contents like business cards can be exchanged via NFC Forum Simple NDEF Exchange Protocol (SNEP). For more flexibility the platform also allows the application to access the lower Peer-To-Peer communication protocol, the NFC Forum LLCP. By supporting NFC Forum connection handover protocol, larger contents can be exchanged via Bluetooth or WiFi. An application that wants to send an NDEF message to the remote device only needs to register for the SNEP push service. The application will then be notified when the remote device is detected in order to send the content over SNEP. An application that wants to access at LLCP protocol level needs to be in the foreground and registered to the LLCP service. Once the LLCP connection is established, the application can exchange data accordingly. Thus, the BlackBerry 10 device is already able to support other IATA complementary use cases via Peer-to-peer mode.

8.3.3 Virtual Target Emulation Mode

The virtual target emulation is an advanced feature supported in the BlackBerry 10 OS platform, where card emulation is implemented by using phone memory instead of using UICC. The platform supports virtual target emulation at NDEF and ISO 14443-4 protocol levels. Both can run on NFC A or NFC B technology.

An application that wants to use NDEF virtual target emulation only needs to register the NDEF message and the technology to be emulated. As soon as it's in the foreground the emulation takes place, allowing a remote device to read the emulated NDEF message.

Virtual target emulation at ISO 14443-4 level is a flexible and powerful way to allow the application to emulate an ISO smart card. Here the BlackBerry 10 OS platform is fast enough to maintain all required timings from the ISO 14443 specification. The application needs to register via the related API and when a remote reader is detected, the application will be notified to exchange APDU with the remote reader. Thus, using ISO 14443-4 virtual target emulation mode the BlackBerry 10 OS platform is able to emulate a boarding pass, allowing a remote NFC reader to get the information as it would do with a plastic card. It's assumed that the application knows how to receive the BP, either OTA or from a kiosk. The

BlackBerry 10 OS platform has APIs to support phone memory storage, to access the crypto library, and to establish secure connection to the backend system.

8.3.4 UICC Card Emulation Mode

To support the NFC infrastructure for UICC card emulation mode, the BlackBerry 10 OS platform implements all relevant standardized functionalities such as SIMalliance Open Mobile API, ETSI TS 102 613 (SWP), ETSI TS 102 622 (HCI), ETSI TS 102 233 (BIP), GlobalPlatform SE Access Control and many more. Thus, the described OTA/provision mechanisms in Section 6.1.2 are supported, but also the standardized communication API between a wallet and the UICC is supported. The platform is also able to handle different battery power-modes: on/low/off. As a result the BlackBerry 10 OS platform supports the IATA SIM Card implementation option directly out of the box.

8.3.5 Summary

As described, the BlackBerry 10 OS platform is a flexible, scalable, and powerful platform enabling IATA members to implement the use cases in multiple ways. Several communication modes are supported, allowing the reader side to use reader/writer mode but also peer-to-peer mode to retrieve the needed information from the device or to push some information to the device. If IATA members select UICC card emulation mode, the platform supports completely what is required today in the NFC industry. The Virtual Target Emulation Mode is another inexpensive implementation option allowing similar flexibility and scalability.

Appendix

Air Travel NFC Projects Already Deployed

Ongoing NFC Deployment Initiatives in Air Travel

- Air France – Toulouse-Paris route (SITA-Air France-Orange) with a SIM-based NFC model
- JAL – Live implementation with a SIM & eSE-based implementation model (JAL-Sony-FeliCa-ARINC); see below
- SAS with NFC stickers
- Alaska Airlines with NFC stickers
- Air New Zealand with NFC stickers
- Toulouse airport for Lounge, Security, Parking access using SIM-based implementation model
- Malpensa (Milan) for building maintenance. 50,000 NFC tags installed. Further deployment planned (http://www.nfcworld.com/2013/05/22/324207/milan-airport-installs-50000-nfc-tags/)

Case Study: Japan Airlines "Tap & Go" Service

The "Tap & Go" service is a boarding pass service using NFC technology.

SERVICES
A mobile application is made available to Frequent Flyer Program members (26 million registered customers) and other travelers. Among other added-value services, this mobile application allows a customer to book a flight, pay for it, and get a boarding pass.

It can be used on all JAL domestic flights. Integrated into an overall mobile strategy, it enables more efficient operations at check-in, security, and boarding gates by allowing passengers to present their devices at the various "one-touch" points until they get onto the plane.

TECHNOLOGY
The service began with NFC-F (FeliCa) technology in 2005 and started NFC type A/B support in 2012: The boarding pass is stored in the FeliCa embedded secure element (eSE) or in the SIM, depending on the scheme. OTA issuance is performed thanks to the involved TSMs and MNOs.

LESSONS LEARNED
NFC is showing a high response and reliability rate, permitting fewer attendants for gate operations, and requiring only 20 minutes for boarding a typical Boeing 777.

Next steps include deploying NFC usage for other activities in airports, such as coupons, lounge access, and smart poster-based services, and also for international roaming, where again the user experience will have importance beyond just new technology for its own sake.

More About the NFC Forum

The NFC Forum was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. This mission drives efforts to provide programs that create a highly stable framework for extensive application development, seamless interoperable solutions, and security for NFC-enabled transactions. This foundation provides an ideal environment for experts in the Near Field Communication ecosystem to collaborate on solutions across the business and technical needs of their industries and to develop NFC programs to support them.

NFC technology opens up possibilities that are limited only by the imagination in payment and non-payment applications across every business sector. Non-payment NFC applications have the potential to revolutionize daily lives by creating new ways of carrying out tasks, accessing information, and interacting with people and organizations.

The NFC Forum's Sponsor members, which hold seats on the Board of Directors, include leading players in key industries around the world. These Sponsor members are: Broadcom Corporation, Google, Inc., Intel, MasterCard Worldwide, NEC, Nokia, NXP Semiconductors, Qualcomm, Renesas Electronics Corporation, Samsung, Sony Corporation, STMicroelectronics, and Visa Inc.

Interested companies are invited to become NFC Forum Members and to help accelerate the delivery of exciting new NFC solutions to consumers and businesses. Membership levels accommodate companies across a wide range of industries at different phases in NFC solution development. For more information on becoming an NFC Forum Member, visit the How to Join page on our website.

NFC Forum Specifications

An important part of the work of the NFC Forum is developing and distributing specifications, so as to enable development of NFC products and services and facilitate interoperability. At the time of this document's publication, 21 NFC Forum specifications have been approved, spanning these core functions:

- Data exchange formats
- Tag types
- Record type definition
- Device interface controller
- Protocols
- Reference applications
- Personal Health Device Communication

A list of all published specifications – with links to download them -- is available on the NFC Forum website at http://www.nfc-forum.org/specs/.

NFC Marks

NFC makes life easier and more convenient for consumers around the world by making it simpler to perform transactions, exchange digital content, and connect electronic devices with a touch. The NFC Forum has established two brand marks that support the NFC ecosystem: the N-Mark and the NFC Forum Certification Mark.

The N-Mark

The NFC Forum N-Mark, a stylized letter "N," is a universal symbol for NFC, helping consumers to easily identify NFC-enabled products, devices, and touch points, providing simple and nearly effortless access to the full power, ease, and convenience of NFC solutions.

Consistent use of the N-Mark where NFC touch points and services are available on mobile devices and other consumer electronics, as well as smart posters, signs, badges, labels, etc. indicates where to touch to enable NFC services. The N-Mark on a display screen, digital media, product packaging, or product or service promotional material indicates that the particular software, product, or service has NFC capabilities.

The N-Mark can be used by anyone at no cost after completing the N-Mark Trademark License Agreement and as long as asserting that the tag or device meets the applicable NFC Forum technical specifications. A device using the N-Mark is not required to be certified under the NFC Forum Certification program. Complete guidelines on how to use the N-Mark correctly are available on the NFC Forum website in the NFC Forum N-Mark Brand Guide.

NFC Forum Certification Mark

The NFC Forum Certification Mark is the industry-facing mark used to indicate that an NFC-enabled device implementation has met the standards of the NFC Forum Compliance Program (see more about this program in the NFC Compliance and Interoperability section of this document, below). It signifies global credibility and serves as an indicator across the NFC eco-system that NFC Forum Member products meet global interoperability standards and will perform consistently.

Use of the NFC Forum Certification Mark on collateral, supporting materials, packaging, & documentation is granted only to NFC Forum member companies that have successfully completed certification.

NFC Compliance and Interoperability

The NFC Compliance program was established because of the importance of certification and interoperability for the infrastructure and devices. The NFC Forum Compliance Program was established to encourage and facilitate development, and increase market availability of products that exemplify high-level compliance with NFC Forum specifications, thereby assuring interoperability between manufacturers. Only available to NFC Forum members, each aspect of the Compliance Program forms the foundation for a gold standard in NFC implementations and supports the goals of achieving interoperability.

The NFC Forum operates two programs to meet compliance and interoperability: the NFC Forum Certification program and Plugfest events. By fully embracing the NFC Forum Compliance Program, NFC Forum members establish confidence and credibility in the technology for everyone in the value chain, to ensure a flourishing NFC ecosystem.

NFC Forum Certification Program

The NFC Forum Certification program confirms an implementation's compliance to NFC Forum specifications. Conformance to the specifications provides consistency of behavior across NFC-enabled devices and sets the foundation for interoperability. NFC Forum Members facilitate the development and

market availability of products that comply with the NFC Forum specification(s) through participation in the NFC Forum Certification Program.

Only available to NFC Forum members, NFC Forum Certification provides differentiation by shortening the adoption process, lowering adoption costs, and making it easier for partners to work together. Certification is granted through a top-notch testing process for implementations that meet NFC Forum Device Requirements. An NFC Forum device is a device capable of operating in NFC Forum Peer-to-peer Mode and/or NFC Forum Reader-Writer Mode that may also support NFC Forum Card Emulation Mode. Because NFC Forum certified implementations are easier to integrate, they are always recommended. Companies cannot claim NFC Forum compliance without successfully completing the certification process.

The NFC Forum ensures the highest level of quality, reliability, and integrity at each step of the certification process. NFC Forum Approved Test Tools go through a formal validation process before approval for use in certification testing. Only an NFC Forum Accredited Test Laboratory (a laboratory that has satisfied and continues to satisfy all requirements defined by the NFC Forum) is authorized to provide certification-testing services to product manufacturers. An independent neutral third party administers the NFC Forum Certification Program and reviews each application to ensure that the implementation meets all the policy and technical requirements. Finally, an issue resolution panel is in place ensuring effective management of certification, technical, and procedural issues. By ensuring conformance, the Certification Program provides for consistency in the behavior of compliant devices, thereby setting the foundation for interoperability

NFC Forum Plugfest Events

The NFC Forum Plugfest events are designed to support early adoption of the NFC Forum Specifications by providing a real-world environment where device, tag, and test tool interoperability can be verified across manufacturer products. This program complements conformance testing under the Certification Program and fosters interoperability of NFC Forum implementations.

These unique events provide a safe, real-world environment for NFC Forum members to verify the level of interaction of their product-specific implementation and to demonstrate how a device will work with other NFC Forum members' implementations. NFC Forum Plugfest events are multi-day events that take place several times each year. Although optional, Plugfest events are part of a comprehensive integrated effort that reduces risk and the investment required in adopting new technology.

Terminology, Abbreviations, and Acronyms

This section provides a glossary of terms and abbreviations, and a reference list of acronyms used in this document. It is not intended as a comprehensive dictionary.

Glossary

Term	Definition
Authentication	The provision of assurance of the claimed entity or of data origin.
Authentication Method	The method used for the authentication of an entity or data origin
Authenticator	A security factor used in an authentication method. Typical examples are tokens, mobile codes and passcodes.
Bluetooth	Short-range (10-100m) wireless communication protocol
Card Emulation mode	Card emulation mode enables NFC devices to act like smart cards, allowing users to perform transactions such as retail purchases and transit access with just a touch. This mode is capable of functioning when the device is powered-off, although it is the service provider's decision whether to allow this. An example is where an NFC device acts as an NFC tag.
Command	An instruction from one device to another device in order to move the other device through a state machine
Content Provider	An entity that is the source of the content accessed via touchpoint on an NFC Smart Poster, such as a retailer that wants to sell its products illustrated on the poster, or a concert promoter that seeks to sell tickets to an event a poster advertises
Data Link Connection	A unique combination of source and destination service access point addresses used for numbered information transfer.
Digital Signage	Signage that uses digital media to display the information for the user. Most commonly these are LCD/Plasma screens (such as arrivals boards at airports), and they may have either NFC tags or card emulation devices providing NFC Smart Poster functionality
EMV	EMV® stands for Europay, MasterCard and Visa: a global standard for credit and debit payment cards based on chip card technology. EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.
EMVCo	EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa. For more information: EMVCo

FeliCa	FeliCa is a contactless technology based on NFC-F as defined in NFC Forum Digital Protocol and JIS X 6319-4. FeliCa is used in various commercial platforms, not only for cards but also for mobile, personal computers, and consumer electronics.
GlobalPlatform	GlobalPlatform (GP) is a cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology.
Groupe Speciale Mobile Association	The GSMA represents the interests of mobile telecommunications operators (Mobile Network Operators) worldwide. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organizations. Mobile Network Operators own and manage the SIM Card – the UICC on which the mobile subscription is managed – which is capable of acting as a Secure Element.
IEC	International Electrotechnical Commission is an international organization for the preparation and publication of International Standards for all electrical, electronic and related technologies.
ISO	International Organization for Standardization
ISO 14443	ISO standard governing proximity smartcards
Logical Data Link	A combination of source and destination service access point addresses used for unnumbered information transfer
Mobile Network Operator	A network operator providing voice and/or data services to handset users. The mobile network operator (MNO) may own its own physical network, or it may use other network facilities in which case it is a MVNO (Mobile Virtual Network Operator).
Mobile Virtual Network Operator	A Mobile Network Operator that uses the facilities of other networks to deliver services.
Mobile Wallet (mWallet, m-Wallet)	Mobile wallet refers to the functionality on a mobile device that can interact securely with digitized valuables. It includes the ability to use a mobile device to conduct commercial transactions in the physical world. A mobile wallet may reside on a mobile device or on a remote network/secure server. Alongside the ability to undertake payments, the Mobile Wallet may contain other content, such as identity, commerce and banking services, transport and other tickets, retail vouchers and loyalty programs. For more information: Mobey Forum and GSMA
Mobile Wallet Content Provider	The mobile wallet content providers are the organizations or the brands that issue content for use in the mobile wallet. Outside Financial Services, such a provider might be known as a Service Provider. Within Financial Services, an issuing bank could be an example of a content provider.
NDEF Application	The logical, higher-layer application on an NFC Forum Device that uses NDEF as a means to exchange information with other NFC Forum Devices or NFC Forum Tags.
NFC-A	One of the three base technologies of NFC. NFC-A is based on ISO/IEC 14443 A and ISO/IEC 18092.

NFC-B	One of the three base technologies of NFC. NFC-B is based on ISO/IEC 14443 B.
NFC-F	One of the three base technologies of NFC. NFC-F is based on ISO/IEC 18092 and JIS X 6319-4.
Near Field Communication	Near Field Communication (NFC) complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and enables a consumer to utilize one device across different systems.
NFC Controller	The NFC Controller handles the physical transmission of data over the RF interface and antenna
NFC Data Exchange Format (NDEF)	The NFC Data Exchange Format (NDEF) specification ensures a uniform format for data exchange in any NFC application. It defines the data structures for the exchange of information.
NFC-enabled Device	An NFC-enabled device is a device that is capable of performing near field communication
NFC Forum Certified Device	A device that implements at least the mandatory parts of the NFC Forum Protocol Stack and the mandatory NFC Forum Operating Modes and has received NFC Forum certification. For more information, refer to the High Level Conformance Requirement document (HLCR)
NFC Tag	A contactless tag that can store NDEF information on it and can be accessed by an NFC device
Operating Field	The radio Frequency field created by the NFC Forum Device in Poll Mode
Over-the-Air	Over-the-air (OTA) provisioning is the ability to download and manage content on a device over a cellular or wireless network. This applies to the over-the-air personalization and life cycle management in the secure element in a mobile device. This process is commonly executed through the mediation of a Trusted Service Manager (TSM), employing cellular and wireless networks to reach the mobile device. Further information: EPC, GSMA
Peer-to-peer mode	Peer-to-peer mode enables two NFC devices to communicate with each other to exchange information and share files. Users of NFC-enabled devices can quickly share contact information and other files with a touch. Two NFC-enabled devices create a connection to share information. Peer-to-peer mode is based on ISO NFC Forum Logical Link Control Protocol (LLCP).
Protocol Data Unit (PDU)	The sequence of contiguous octets delivered as a unit to the adjacent lower layer or received as a unit from the adjacent lower layer
Reader/Writer mode	Reader/writer mode enables NFC devices to read information stored on inexpensive NFC tags embedded in smart posters and displays. NFC-enabled devices can access information from embedded tags in smart posters. An example is when an NFC device reads an NFC tag or device acting in card emulation mode
Reader/Writers	Devices that can read from and write to NFC tags

Radio Frequency	Radio frequency (RF) is a rate of oscillation in the range of c. 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals.
Service Access Point	A Service Access Point (SAP) is an identifying label for network endpoints used in Open Systems Interconnection (OSI) networking.
Service	The capabilities and features provided to the adjacent upper layer
Service Provider	A service provider is the business entity providing the service in question either to end-user or to another business entity. In mobile financial services service provider normally refers to the company providing the technology that enables the service. Outside Financial Services the term Service Provider refers to an entity with which the end-user has a relationship, such a transport provider. A Service Provider can also be an entity such as an advertising agency that provides a communications, storage, or processing service, or any combination of the three, in a platform as an enabler to a content provider.
Signature RTD	A specification defining the record that contains a digital signature related to one or more records within an NDEF message. The signature can be used to verify the integrity and authenticity of the content
Smart Poster	Objects in or on which readable NFC tags have been placed
Trusted Execution Environment	Trusted Execution Environment (TEE) is an execution environment that runs alongside but isolated from an REE (run-time execution environment). A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly. Further information: Global Platform
Touchpoint	The place on an NFC Smart Poster or another NFC-enabled object that an NFC device should touch in order to obtain digital services, usually indicated by the N-Mark
Trusted Service Manager	A trusted service manager (TSM) is a role typical in a near field communication ecosystem, where hardware secure element is in use. The trusted service manager acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, mobile device manufacturers or other entities controlling the secure element (SE) on mobile devices. The trusted service manager enables service providers (SPs) to distribute and manage contactless applications remotely by allowing controlled access to the secure element in NFC-enabled handsets.
User Interface	A user interface (UI) is the system by which users interact with a machine. The user interface includes hardware and software components. On a mobile device the software component of a UI is realized though a mobile application (app).
Universal Integrated Circuit Card	The UICC (Universal Integrated Circuit Card) is the smart card used in mobile terminals in GSM and UMTS networks.
WiFi	Wireless Fidelity -- wireless networking technology based on IEEE 802.11 standards

Acronyms

Acronym	Description
APDU	Application Protocol Data Unit
API	Application Programming Interface
BCBP	Bar Coded Boarding Pass
CA	Certificate Authority
CDD	Compatibility Definition Document
CUPPS	Common Use Passenger Processing Systems
CUSS	Common Use Self-Service
EMV	Europay, MasterCard and Visa
EPC™	Electronic Product Code
ETSI	European Telecommunications Standards Institute
GP	Global Platform
GSM	Global System for Mobile Communications
GSMA	GSM Association
HCI	Host Controller Interface
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
JIS	Japanese Industrial Standard
LLCP	Logical Link Control Protocol
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	Near Field Communication Interface and Protocol
NFCIP-1	Near Field Communication Interface and Protocol-1
OS	Operating System
OTA	Over-the-Air
PIN	Personal Identification Number
POS	Point of Sale
RF	Radio Frequency
RTD	Record Type Definition
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SP	Service Provider
SWP	Single Wire Protocol
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
UI	User Interface
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
Wi-Fi	Wireless Fidelity

Contributors

The NFC Forum is grateful to all of its members who contributed to this paper. These companies included:

IATA is grateful to IATA's Fast Travel Working Group member airlines and strategic partners who contributed to this paper, particularly: