# TABLE OF CONTENTS

1. INTRODUCTION .................................................................................................................. 3  
   1.1. DOCUMENT OUTLINE ......................................................................................... 3  

2. WHAT IS NEAR FIELD COMMUNICATION ........................................................................ 4  
   2.1. INTRODUCTION ................................................................................................. 4  
   2.2. WHAT IS NEAR FIELD COMMUNICATION? ......................................................... 4  
   2.3. MORE DETAILS.................................................................................................... 7  

3. NFC USAGE ........................................................................................................................ 13  
   3.1. INTRODUCTION .................................................................................................. 13  
   3.2. MORE USAGE DETAILS ...................................................................................... 15  
      3.2.1 Banking .......................................................................................................... 15  
      3.2.2 Contactless Smartcards .................................................................................. 18  
      3.2.3 Smart Card Alliance ....................................................................................... 22  
      3.2.4 Other Applications ......................................................................................... 28  

4. SECURITY AND NFC .......................................................................................................... 30  
   4.1. THREATS ............................................................................................................. 30  
      4.1.1 Eavesdropping .............................................................................................. 30  
      4.1.2 Data Corruption ............................................................................................ 31  
      4.1.3 Data Modification .......................................................................................... 31  
      4.1.4 Data Insertion ............................................................................................... 32  
      4.1.5 Man-in-the-Middle-Attack ............................................................................. 33  
   4.2. SOLUTIONS AND RECOMMENDATIONS ............................................................ 34  
      4.2.1 Eavesdropping .............................................................................................. 34  
      4.2.2 Data Corruption ............................................................................................ 34  
      4.2.3 Data Modification .......................................................................................... 34  
      4.2.4 Data Insertion ............................................................................................... 35  
      4.2.5 Man-in-the-Middle-Attack ............................................................................. 35  
      4.2.6 Secure Channel for NFC ............................................................................... 35  
      4.2.7 Conclusion ..................................................................................................... 38  
   4.3. SMART CARD ALLIANCE INFORMATION ......................................................... 39  

5. NFC PHONES AND SDK AVAILABILITY .................................................................... 40  
   5.1. INTRODUCTION ................................................................................................. 40  
   5.2. NFC PHONES AND PERIPHERALS ..................................................................... 40  
      5.2.1 Android Phones .............................................................................................. 40  
      5.2.2 Samsung ........................................................................................................ 41  
      5.2.3 Apple iPhone ................................................................................................ 41  
   5.3. SDK PRODUCTS .................................................................................................. 43  
      5.3.1 NOKIA 6212 NFC Phone .............................................................................. 43  
      5.3.2 ALVIN Systems ............................................................................................. 43
1. INTRODUCTION

This white paper provides an overview of Near Field Communication (NFC)

1.1. Document Outline

Chapter 1 provides an introduction and outline of this document.
Chapter 2 provides an overview of “What is NFC in General”.
Chapter 3 provides an overview of the “usage” opportunities for NFC
Chapter 4 provides a more detailed overview of the security aspects of NFC
Chapter 5 provides an overview of available NFC enabled phones or peripherals for phones enabling NFC as well as SDK products for NFC
2. **What is Near Field Communication**

2.1. **Introduction**

This Section provides a high level overview of Near Field Communication (NFC)

2.2. **What is Near Field Communication?**

Near Field Communication or NFC is a short-range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimeter (around 4 inches) distance. The technology is a simple extension of the ISO/IEC 14443 proximity-card standard (proximity card, RFID) that combines the interface of a smartcard and a reader into a single device. An NFC device can communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices, and is thereby compatible with existing contactless infrastructure already in use for public transportation and payment. NFC is primarily aimed at usage in mobile phones.

NFC incorporates a variety of pre-existing standards including ISO/IEC 14443 both Type A (normal) and Type B (banking/short range), and FeliCa. NFC enabled phones thus show basic interoperability with the preexisting reader infrastructure. Especially in "card emulation mode" a NFC device should at least transmit a unique ID number to a pre-existing reader.

In addition, NFC Forum has defined a common data format called NDEF, which can be used to store and transport different kinds of items, ranging from any MIME-typed object to ultra-short RTD-documents, such as URLs.

NDEF is conceptually very similar to MIME. It is a dense binary format of so-called "records", in which each record can hold a different type of object. By convention, the type of the first record defines the context of the entire message.

NFC technology is currently mainly aimed at being used with mobile phones. There are three main use cases for NFC:

- card emulation: the NFC device behaves like an existing contactless card
- reader mode: the NFC device is active and read a passive RFID tag, for example for interactive advertising
- P2P mode: two NFC devices are communicating together and exchanging information.
NFC was designed and marketed by the NFC Forum. The NFC Forum is a non-profit industry association announced on March 18, 2004 by NXP Semiconductors, Sony and Nokia to advance the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. The NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. In September 2008, there were over 150 members of the NFC Forum.

Formed in 2004, the Forum now has 140 members. Manufacturers, applications developers, financial service institutions, and more all work together to promote the use of NFC technology in consumer electronics, mobile devices, and PCs.

The goals of the NFC Forum are to:

- Develop standards-based Near Field Communication specifications that define a modular architecture and interoperability parameters for NFC devices and protocols
- Encourage the development of products using NFC Forum specifications
- Work to ensure that products claiming NFC capabilities comply with NFC Forum specifications
- Educate consumers and enterprises globally about NFC

The NFC Forum provides a highly stable framework for extensive application development, seamless interoperable solutions, and security for NFC-enabled transactions. The NFC Forum has organized the efforts of dozens of member organizations by creating Committees and Working Groups.

In June 2006, only 18 months after its founding, the Forum formally outlined the architecture for NFC technology. As of September 2010, the Forum has released 13 specifications and 3 candidate specifications. The specifications provide a “road map” that enables all interested parties to create powerful new consumer-driven product
The NFC Forum has signed a series of agreements, with the GSM Association (GSMA), EMVCo and the Smart Card Alliance, designed to enable it to work more closely with each of the associations on the development of the NFC market and near field communication-based solutions.

The Memorandum of Understanding (MoU) between the NFC Forum and EMVCo will see the card payments standards body sharing technical information with the NFC Forum so that a certification program can be put into place for the use of NFC devices to make payments at the point-of-sale and also for them to act as POS terminals.

The partnership with the GSMA will see the two organizations sharing information and collaborating on joint marketing activities, such as seminar sessions, white papers and presentations.

The NFC Forum and the Smart Card Alliance, meanwhile, will team up on a number of joint marketing initiatives, including educational programs for vertical markets such as retail and transport. Other programs under discussion include presentations at each other’s events and meetings, a joint event targeting the retail market in the US and the provision for regular information sharing between the NFC Forum Marketing Committee and Smart Card Alliance Contactless and Mobile Payments Council.

The NFC Forum has already established liaisons with the European Telecommunications Standards Institute (ETSI) and the Mobey Forum. The GSMA and EMVCo, meanwhile, are also already working with GlobalPlatform on the development of a cross-industry NFC certification process.
2.3. More details

The protocol is based on a wireless interface. There are always two participating parties to the communication; hence the protocol is also known as peer-to-peer communication protocol. The protocol is designed to establish wireless network connections between computer peripherals and consumer electronic.

The interfaces operate in the unregulated RF band of 13.56 MHz. This means that no restrictions are applied and no licenses are required for the use of this RF band. Of course, each country imposes certain limitations on the electromagnetic emissions in this RF band. The limitations mean that in practice the distance at which the devices can connect to each other is restricted and this distance may vary from country to country. Generally speaking, we consider the operating distances of 0~20 cm.

As is often the case with the devices sharing a single RF band, the communication is half-duplex. The devices implement the “listen before talk” policy – any device must first listen on the carrier and start transmitting a signal only if no other device can be detected transmitting.

NFC protocol distinguishes between the Initiator and the Target of the communication. Any device may be either an Initiator or a Target. The Initiator, as follows from the name, is the device that initiates and controls the exchange of data. The Target is the device that answers the request from the Initiator.

NFC protocol also distinguishes between two modes of operation: Active mode and Passive mode. All devices support both communication modes. The distinction is as follows:

In the Active mode of communication both devices generate their own RF field to carry the data.

In the Passive mode of communication only one device generates the RF field while the other device uses load modulation to transfer the data. The protocol specifies that the Initiator is the device responsible to generate the RF field.

The application chooses the initial communication speed from the set of 106, 212 and 424 Kbit/s. Subsequently the application and/or the communication environment may require speed adaptation, which can be done during communication.

NFCIP-1 uses different modulation and bit encoding schemes depending on the speed. While establishing the communication, the Initiator starts the communication in a particular mode at a particular speed. The Target determines the current speed and the associated low-level protocol automatically and answers accordingly.

The communication is terminated either on the command from the application or when devices are out of range.
What makes the communication between the devices so easy is that the NFC protocol provides some features not found in other general-purpose protocols.

First of all, it is a very short-range protocol. It supports communication at distances measured in centimeters. The devices have to be literally almost touched to establish the link between them. This has two important consequences:

1. The devices can rely on the protocol to be inherently secured since the devices must be placed very close to each other. It is easy to control whether the two devices communicate by simply placing them next to each other or keeping them apart.

2. The procedure of establishing the protocol is inherently familiar to people: you want something to communicate – touch it. This allows for the establishment of the network connection between the devices be completely automated and happen in a transparent manner. The whole process feels then like if devices recognize each other by touch and connect to each other once touched.

Another important feature of this protocol is the support for the passive mode of communication. This is very important for the battery-powered devices since they have to place conservation of the energy as the first priority. The protocol allows such a device, like a mobile phone, to operate in a power-saving mode – the passive mode of NFC communication. This mode does not require both devices to generate the RF field and allows the complete communication to be powered from one side only. Of course, the device itself will still need to be powered internally but it does not have to “waste” the battery on powering the RF communication interface.

Also, the protocol can be used easily in conjunction with other protocols to select devices and automate connection set-up. As was demonstrated in the examples of use above, the parameters of other wireless protocols can be exchanged allowing for automated set-up of other, longer-range, connections. The difficulty in using long-range protocols like Bluetooth or Wireless Ethernet is in selecting the correct device out of the multitude of devices in the range and providing the right parameters to the connection. Using NFC the whole procedure is simplified to a mere touch of one device to another.
The following diagram shows on An Exploration of the NFC-related Elements on Mobile Handsets using Java for example:

Legend:
1. Radio Frequency unit and Baseband processor
2. NFC Proximity Antenna
3. NFC Processor with Security
4. SIM Card, connects to NFC Processor using Single Wire Protocol (a product by NXP)
5. Smart Card. Communication is performed over ISO XXX APDU
6. Handset Memory
7. The Application Processor includes the Runtime, APIs and NFC application, in this example, a Java runtime such as MIDP
8. External elements such as Smart Card, Readers, Tags

GSMA is pushing for the SIM Card, basically handing the NFC ecosystem over to the network providers.
An NFC device offers different operating modes which are the following:

Reader/Writer Mode: Operating in this mode, the NFC device can read and alter data stored in NFC compliant passive (without battery) transponders. Such tags can be found on SmartPoster e.g., allowing the user to retrieve additional information by reading the tag with the NFC device. Depending on the data stored on the tag, the NFC device takes an appropriate action without any user interaction. If a URI was found on the tag, the handset would open a web browser for example.

Card Emulation: An NFC device can also act as smart card (ISO 14443) after being switched into card emulation mode. In this case an external reader cannot distinguish between a smart card and an NFC device. This mode is useful for contactless payment and ticketing applications for example. Actually, an NFC enable handset is capable of storing different contactless smartcard applications in one device.

Peer-to-Peer: The NFC peer-to-peer mode (ISO 18092) allows two NFC enabled devices to establish a bidirectional connection to exchange contacts, Bluetooth pairing information or any other kind of data. Cumbersome pairing processes are a thing of the past thanks to NFC technology. To establish a connection a client (NFC peer-to-peer initiator) is searching for a host (NFC peer-to-peer target) to setup a connection. Then the NDEF (NFC Data Exchange Format) is used to transmit the data.
NFC technology integrated in a mobile device typically consists of two integrated circuits. The NFC controller is required for the analog digital conversion of the signals transferred over the proximity connection. An HCI (host controller interface) allows the host controller to set the operating modes of the NFC controller, process data sent and received and establish a connection between the NFC Modem and the secure element.

The second IC, a secure smartcard chip also referred to as the secure element, is used for the tag emulation mode. The secure element is connected to the NFC controller for proximity transactions (external mode e. g. for payment at point of sale) through the Single-Wire Protocol (SWP). The host-controller as well is able to exchange data with the secure element (internal mode e. g. for top up of money into the secure element over the air).
Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443 [7]), which only support communication between powered devices and passive tags, NFC also provides peer-to-peer communication. Thus, NFC combines the feature to read out and emulate RFID tags, and furthermore, to share data between electronic devices that both have active power.

Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct line of sight is required, which reacts sensitively to external influences such as light and reflecting objects. The significant advantage over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify the other’s phone, the connection between two NFC devices is established at once (<0.1s). Table 4.1 points out these different capabilities of NFC, Bluetooth and infrared. All these protocols are point-to-point protocols. Bluetooth also supports point-to-multipoint communications. With less than 10 cm, NFC has the shortest range. This provides a degree of security and makes NFC suitable for crowded areas. The data transfer rate of NFC (424 kbps) is slower than Bluetooth (721 kbps), but faster than infrared (115 kbps). In contrast to Bluetooth and infrared NFC is compatible with RFID.
3. NFC Usage

3.1. Introduction

NFC enables users to exchange information by holding their mobile phones within 20 centimeters of NFC logos. Due to the fact that the communication range is so small, the user – in principle, at least – initiates all forms of communication. NFC technology integrates three functions with which consumers are already familiar: smart cards (such as ID-, debit- or access cards); the accessing of digital content (such as clicking with a mouse); and the establishment of communication between two devices (Bluetooth, for example).

In card-emulation mode, an NFC device functions as a proximity card. In this mode, the NFC tag remains passive and awaits a signal from a reader/writer in the environment. When a user approaches a read/write terminal, the latter initiates a communication.
When using NFC to access digital content, a user will tap an NFC tag with his or her NFC handset. The typical use scenario for this function is known as ‘smart-postering’. The user's NFC phone initiates the communication, and the tag sends back its content. Typically, this content will be brief, such as a URL, a few sentences of text, or the initiation of a phone call. In this mode, the user’s NFC device works actively and initiates the communication.

NFC can be used to establish a connection between two devices, such as a mobile phone and a PC. The connection can either be used to transfer data using the NFC connection, or it can be used as a means of setting up another type of wireless connection, such as Bluetooth. The NFC Forum’s promotional presentations envisage this technology being used to transfer files such as photos or meeting agendas between NFC-equipped devices. Another potential use would be transferring funds from one electronic purse to another.
3.2. More Usage Details

3.2.1 Banking

The issue with device-to-device communications is security, especially over extended ranges. NFC has been designed for communications within a close range: ten or less centimeters. Holding the device (of whatever form factor) containing the payment details close to the reader addresses the security concern. The possibility of any person or device coming within range to eavesdrop on the messaging traffic is minimized.

Although many see NFC as a payments standard this is not the case. Payment is only one use of the technology. NFC can be used to configure and initiate other wireless network connections such as Bluetooth and Wi-Fi. In the payment context NFC is starting to be considered more than a communications protocol. It is being seen more as a proximity payment method, bundled with ISO14443, the proximity standard and EMV.

So what does this bundled NFC mean to the payments industry? What does it promise? In the passive mode it is always the NFC capable device, (with a power supply) to communicate, (two-way) with a contactless chip. The contactless chip may support the EMV security standard, or the chip may just hold a magnetic strip image.

This enables proximity payments where the card and device generates a standard purchase transaction under the request and response payment model.

The advantages of this technology are reflected in the MasterCard Paypass and Visa Wave solutions. These two payment methods are based on lower value proximity payments without the need for either signature or PIN.

The business justification is based on increasing the customer throughput per cashier, resulting in a higher retail sale volume at a lower cost for merchants while improving the consumer experience. Removing cash reduces handling costs and shrinkage.

The EMV application of Wave and Paypass does perform two-way card-to-device authentication. But obviously the cardholder is not authenticated. It will be interesting to see if the business case stacks up once a high market penetration rate of Wave and Paypass capable cards is reached and the merchant acceptance base expands.

From a payment perspective, unauthenticated transactions represent a payment risk. Keeping proximity fraud levels within budgeted limits is the key. The risk is intended to be carried by the issuer, although merchants will inevitably pay indirectly through the interchange rates.
More importantly NFC technology removes the need for a payment instrument to make contact with a payment device to initiate a payment request. Removing this physical contact means the chip can be supported from a variety of form factors. The plastic card becomes redundant.

The real potential of NFC is when the form factor is a mobile device. The card is limited by an inability to communicate neither back to the issuer or to the cardholder. It can only communicate with the merchant’s device. The mobile as a form factor is a three-way communications device, merchant, cardholder and issuer.

The ability to communicate back to the cardholder’s issuing bank introduces the ability for both cardholders and issuers to communicate unobtrusively with each other on an event-by-event basis, in real time. This completes the communications link in a way that is impossible for payment cards.

The transaction originates with the swipe of the card and passes to the issuer through the merchant and acquirer. It never passes back to the cardholder except as a paper receipt.
This closed communications loop will drive personalization.

The key advantage of using mobile to change the way transactions are processed is that time dependent network connections are removed from the typical on-us transaction flow, with authorization being routed over the mobile network to the issuers directly. For the customer they have a single device that will hold multiple payment instruments. Initiating a payment is easier and quicker. It is lower risk, as the handset can be protected with a password.

The cynic may say the problem has just been transferred to the mobile operator. If there are network capacity issues the operator is better equipped to resolve these than a financial institution. Financial institutions are only in real-time dealing with their traffic. The acquiring institutions should concentrate on settlement related payment tasks.
3.2.2 Contactless Smartcards

Sample provided by ST

The ST21 NFCA is designed for an optimized integration on a mobile phone with the communication links shown in Figure 1.

Figure 1. Mobile phone communication links

This product is based on an advanced Smartcard ST21 microcontroller with 36 Kbytes of EEPROM, 112 Kbytes of User ROM and 4 Kbytes of RAM and includes an integrated RF Analog Front End (AFE) supporting all the contactless proximity (ISO/IEC 14443, Calypso V1 Radio Protocol (B'), ECMA340 (NFCIP-1), and vicinity (ISO/IEC1 5693, ISO/IEC1 8000-3Mod1) standards.
The ST21 NFCA system-on-chip combines a complete hardware capability for 13.56 MHz contactless communication with an useful embedded firmware which handles:

- ISO/IEC 14443 A&B, Calypso V1 Radio Protocol (B’), ECMA340 (NFCIP-1), ISO/IEC 15693, ISO/IEC18000-3Mod1 in card emulation modes as well as reader modes
- Switch modes between operating modes and RF modes
- Host Controller Interface functions (HCI based on the ETSI specification)

In addition, the embedded firmware and associated macrocells support handling and protocol for the various interfaces:

- Single Wire Protocol (SWP) interface fully compliant with ETSI TS 102 613 Release 7
- C Slave interface fully compliant with NXP specification
- SPI Slave interface fully compliant with Free-Scale specification
- Asynchronous Receiver Transmitter in master configuration supporting ISO/IEC 781 6-3 T=0 and T=1 protocols

The ST21 NFCA is a serial access circuit based on an 8/16-bit CPU core. Operations will be synchronized with an internally generated clock issued by the Clock Generator module. The internal speed of the device is fully software programmable.

The CPU includes the Arithmetic Logic Unit (ALU), the control logic and registers controlled by the ST21 NFCA firmware. The CPU interfaces with the on-chip RAM, ROM and EEPROM memories via a 24-bit internal bus offering 16 MBytes of linear addressing space.

This device also includes a True Random Number Generator (TRNG), three 8-bit fully programmable timers, a Cyclic Redundancy Check (CRC3309) module, and a Data Encryption Standard (DES) accelerator.

Thanks to an enhanced power switch system, the ST21 NFCA is able to support several power supply sources ("Battery On", Battery Low and Battery Off” modes) which manage the power management of the device and its associated UICC.
Figure 2. ST21 NFCA block diagram
Figure 3. Firmware architecture overview

- Host Controller Interface
- OS and Switch Mode Module
  - SPI Slave Driver
  - PC Slave Driver
  - RF ISO/IEC 14443 A B
  - RF ISO/IEC 15693
  - RF ECMA 340
  - Card Emulation and Reader modes Driver
- SWP Master Driver
- ISO 7816 Master Driver

PC/SPI
RF Antenna

UICC SWP
Secure Element

SWP
Master
3.2.3 Smart Card Alliance

The Smart Card Alliance provides the following information regarding the use of NFC and Smart cards:

The ability to pay for transit fares, groceries, and other products by simply waving a mobile phone near a POS device represents a new payment frontier. Such payments, called proximity mobile payments, are defined as payments to a merchant that are initiated from a mobile phone that uses Near Field Communication (NFC) technology and that is held close to the merchant’s POS equipment.

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate smart chips that allow the phones to securely store the payment application and consumer account information and to use the information as a “virtual payment card.” NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocols currently used by contactless credit and debit cards.

NFC will soon be available as standard functionality in many mobile phones and will allow consumers to perform safe contactless transactions, access digital content, and connect electronic devices simply. An NFC chip in a mobile device can act as a card or a reader or both, enabling consumer devices to share information and to make secure payments quickly.

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

The convergence of payments and mobile communications is not just logical—it is inevitable.” In March 2007, John Philip Coghlan, then CEO of Visa USA, made this announcement at the CTIA Wireless Conference. Yet only a few years ago, people were still saying, “Some day, we will pay using mobile phones.” The Smart Card
Alliance and related industry groups representing financial institutions, merchants, and mobile operators have talked and written about “some day” for almost a decade. But now, virtually every industry group involved in the transaction chain is investigating the use of mobile payments. And mobile payment will soon be a standard transaction method for payment in many North American merchant locations.

What has happened to move mobile payments from “some day” to “inevitable?”

- **Contactless payment adoption by payment brands, issuers and consumers.** American Express, Discover Network, MasterCard, and Visa have issued contactless payment cards and devices based on a single standard. These contactless payment products (ExpressPay™ from American Express, Discover® Network ZipSM, MasterCard® PayPass™ and Visa payWave™) have shown both merchants and consumers the benefits of contactless payments. Consumers enjoy increased security, speed, and ease-of-use.

- **Contactless payment acceptance by merchants.** Merchants have seen the benefits of faster transaction time, increased spending and increased customer loyalty. Plus, transactions using contactless cards and devices are processed through a single, contactless-enabled point-of-sale (POS) system and through the existing financial networks, encouraging merchant adoption.

- **Mobile phone ubiquity.** Mobile phone subscribers don’t leave home without their phones. In addition, near field communication (NFC) technology has established communication standards that can facilitate a simplified and robust implementation of contactless payments using the mobile device. NFC, a short-range, standards-based wireless connectivity technology, will soon be available as standard functionality in most mobile phones. NFC will allow consumers to perform safe, contactless transactions, access digital content, and connect electronic devices simply. An NFC chip in a mobile device can act as a card and/or reader–enabling consumer devices to connect, receive and share information, content and data, in addition to making secure payments quickly.

- **Expanded mobile functionality.** The mobile device can deliver a variety of payment and payment-related services. The mobile device is a powerful new tool that can enable proximity mobile payments, remote payments through the mobile Internet or text messaging, and person-to-person money transfers. Value-added applications can enrich the purchase experience and include account management, banking, offers, and security applications.

What would drive a consumer to adopt and use mobile payments? The answer may be expanded payment functionality, increased convenience, enhanced security, and faster transactions.
The debate about who is going to build and deploy the infrastructure for mobile commerce has gone on for years. Some argued that the mobile operator would take on the payment process; others, that the financial institutions would deploy readers, software, and the necessary technologies. With the introduction of contactless financial payment cards and NFC-enabled phones, however, the debate is getting more interesting.

This white paper outlines the findings and conclusions of the Smart Card Alliance Payments Council. Specific to proximity mobile payment, it is the conclusion of this Council that proximity mobile payment, because it leverages the well-established financial payments infrastructure, and because it is based on NFC technology and the ISO/IEC 14443 standard, will become the mobile payment technology of choice for consumers using mobile phones for retail payment transactions in the United States.

This white paper describes what is necessary to implement and deploy proximity mobile payment systems, discusses the relevant technical and business issues from the perspective of the various stakeholders (e.g., mobile operators, the financial industry, end-users, providers and vendors), and outlines the potential opportunities and barriers that may impact its market adoption.

About the Smart Card Alliance Payments Council

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

The smart card industry and media alike continue to focus on mobile payments, regularly reporting on interest being shown in the new payment method. The purpose of this new research report is to look at the journey towards proximity mobile payments by examining the progress that is being made to define a sustainable business model. While the logic behind proximity mobile payments is generally
accepted, precisely when they will become widely available and how the industry will get there are still being debated. The convergence of mobile and payment is extremely complex, requiring the cooperation of many players and stakeholders.

As a result, the mobile payments landscape continues to evolve with various business models emerging worldwide. The Payments Council has considered four different business models for mobile payments deployment and surveyed key industry stakeholders on critical questions pertaining to the success of each model. The purpose of the survey was to develop a point of view on the emerging business models for the North American market.

**Expert opinion and even speculation were sought on the following topics:**

- Likely business models
- Global examples where these business models have been implemented
- Relative business model advantages
- Relationships among ecosystem stakeholders for each model
- Benefits and business case drivers for each stakeholder
- Emerging “killer app” capabilities

Alternative Business Models Considered The survey was conducted by members of the Smart Card Alliance Payments Council Mobile Payments Work Group, by either in-person or telephone interviews during December 2007 and January 2008.

The four potential mobile payments business model scenarios discussed with interviewees were as follows:

1. **Operator-Centric Model:** The mobile operator acts independently to deploy mobile payment applications to NFC-enabled mobile devices. The applications may support a prepaid stored value model or the charges may be integrated into the customer’s wireless bill.

2. **Bank-Centric Model:** A bank deploys mobile payment applications or devices to customers and ensures merchants have the required point-of-sale (POS) acceptance capability. Payments are processed over the existing financial networks with credits and debits to the appropriate accounts.

3. **Peer-to-Peer Model:** An independent peer-to-peer service provider provides secure mobile payments between customers or between customers and merchants.
4. Collaboration Model: This model involves collaboration among banks, mobile operators and other stakeholders in the mobile payments value chain, including a potential trusted third party that manages the deployment of mobile applications. Payments in this model are processed over the existing financial networks with credits and debits to the appropriate accounts.

For each business model, the industry experts that were interviewed were asked to comment on the following topics:

- What are the pros and cons of each model?
- What are the incremental benefits and business case drivers for each stakeholder?
- What is the reasonable split of the potential revenues to stakeholders?
- Are there other potential sources of revenue?
- Which stakeholder owns financial liability, risk, security and privacy?
- Are they aware of real-world commercial-scale implementations?

Interviewees were also asked to comment on the following topics:

- Which model holds the greatest potential for success?
- Are there other potential models or stakeholders that should be considered?
- What emerging capabilities will be “killer apps”?
- Which will reign supreme—remote mobile payments or proximity mobile payments?

Survey Participants

Stakeholder views were sought from financial institutions, mobile operators, merchants, potential trusted service managers, service providers and non-traditional players. Conclusions were drawn on points of agreement, points of disagreement and surprising findings, including any notable quotes.

The objective was to find 20 willing participants from key organizations in the mobile payments arena. The Work Group successfully conducted 21 interviews from the five stakeholder ‘camps.’

Survey Findings

The consensus of 86% of the industry stakeholders interviewed was that NFC-based proximity mobile payments will be adopted, and that the business model will require collaboration among banks, mobile operators, merchants, handset manufacturers and
other service providers. Although the Collaboration Model appears most feasible, rapid adoption is hindered by the number of players.

Although the industry appears poised to deploy mobile payments, it is a classic case of strategic deadlock in which stakeholders are waiting for someone else to make the first move. A bold move is needed by a player in the role of trusted service manager to orchestrate the activities of collaborators and competitors.

The activities that require orchestration include final selection of handset and chip standards, merchant enablement, standards for certifying and deploying secure payment applications, and, finally and most controversially, development of a model for revenue-sharing arrangements among stakeholders.

The report includes detailed results describing the survey respondents’ perspectives on the pros and cons of each model and on their opinions of potential new sources of revenue from advertising, loyalty and rewards, co-branding arrangements, and customer fees for new services.
3.2.4 Other Applications

It is impossible to give a complete picture of NFC applications as NFC is just an interface. The following sub sections introduce three example applications. These shall be viewed as typical use cases and where chosen to motivate the list of possible threats given in the next section.

Contactless Token

This covers all applications, which use NFC to retrieve some data from a passive token. The passive token could be a contactless Smart Card, an RFID label, or a key fob. Also, the token could be physically included in a device without any electric connections to that device.

What is important is that the only interface of the token is the contactless interface. This means it cannot act as a communication link to a device main CPU of a device because it cannot connect to the device main CPU via a contact interface. Let us also assume that the token has rather limited computing power, so it cannot run any complex protocols. The primary use would be to store some data, which can then conveniently be read by an active NFC device. Examples of such data would be a URL stored in a tag of a consumer product or the user guide of such a product. The user could then read the tag and get automatically linked to the support web page of that product. A different example would be to store the configuration data needed to access a WiFi network. New users could then easily configure their laptops to be connected to the network.

Ticketing / Micro Payment

In this example application, the NFC interface is used to transfer some valuable information. The ticket or the micro payment data is stored in a secure device. This could be a contactless Smart Card, but could as well be a mobile phone. When the user wants to perform a payment or use the stored ticket, the user presents the device to a reader, which checks the received information and processes the payment or accepts/rejects the ticket.

In this application example the user device must be able to perform a certain protocol with the reader. A simple read operation will not be sufficient in most cases. Also, the
The user device is likely to have a second interface which is used to load money or to buy tickets. This second interface can for example be linked to the mobile phone CPU. The ticket data could then be loaded into the mobile phone via the cellular network.

In this application sometimes the term 'Secure NFC' is used. However, this does not at all mean that the NFC link is somehow secured. The name just denotes a configuration using an NFC hardware chip in combination with a Smart Card chip. It should be called ‘Secure Smart Card and NFC’, but unfortunately the shorter name is used quite often.

**Device Pairing**

In this application the two devices communicating would belong to the same group of devices. An example could be a laptop and a digital camera. The user wants to establish a Bluetooth connection between the two devices to exchange image data. The Bluetooth link is established by bringing the two devices close together and running a given protocol over NFC between the two devices. This makes it obvious for the user which two devices get actually linked and takes away the burden of navigating through menus and selecting the right devices from lists of possible communication partners.

It should be noted that the NFC connection itself in this example is only used to establish the Bluetooth link. Image data is not transferred over NFC because NFC’s bandwidth is simply too small for transferring big amounts of data.
4. Security and NFC

4.1. Threats

4.1.1 Eavesdropping

Because NFC is a wireless communication interface it is obvious that eavesdropping is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can of course use an antenna to also receive the transmitted signals. Either by experimenting or by literature research the attacker can have the required knowledge on how to extract the transmitted data out of the received RF signal. Also the equipment required to receive the RF signal as well as the equipment to decode the RF signal must be assumed to be available to an attacker as there is no special equipment necessary.

The NFC communication is usually done between two devices in close proximity. This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more.

- RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)
- Characteristic of the attacker’s antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker’s receiver
- Quality of the attacker’s RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.
Additionally, it is of major importance in which mode the sender of the data is operating. This means whether the sender is generating its own RF field (active mode) or whether the sender is using the RF field generated by another device (passive mode). Both cases use a different way of transmitting the data and it is much harder to eavesdrop on devices sending data in passive mode.

In order to not leave the reader without any idea on how big the eavesdropping distances are, we give the following numbers, which as stated above are not valid in general at all, but can only serve to give a rough idea about these distances.

When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1 m.

### 4.1.2 Data Corruption

Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device.

Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.

### 4.1.3 Data Modification

In data modification the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption.

The feasibility of this attack highly depends on the applied strength of the amplitude modulation. This is because the decoding of the signal is different for 100% and 10% modulation.

In 100% modulation the decoder basically checks the two half bits for RF signal on (no pause) or RF signal off (pause). In order to make the decoder understand a one as a zero or vice versa, the attacker must do two things. First, a pause in the modulation must be filled up with the carrier frequency. This is feasible. But, secondly, the attacker must generate a pause of the RF signal, which is received by the legitimate receiver. This means the attacker must send out some RF signal such that this signal perfectly overlaps with the original signal at the receiver’s antenna to give a zero signal at the receiver. This is practically impossible. However, due to the modified Miller coding in the case of two subsequent ones, the attacker can change the second one into a zero, by filling the pause which encodes the second one. The decoder
would then see no pause in the second bit and would decode this as a correct zero, because it is preceded by a one. In 100% modulation an attacker can therefore never change a bit of value 0 to a bit of value 1, but an attacker can change a bit of value 1 to a bit of value 0, in case this bit is preceded by a bit of value 1 (i.e. with a probability of 0.5).

In 10% modulation the decoder measures both signal levels (82% and Full) and compares them. In case they are in the correct range the signal is valid and gets decoded. An attacker could try to add a signal to the 82% signal, such that the 82% signal appears as the Full signal and the actual Full signal becomes the 82% signal. This way the decode would decode a valid bit of the opposite value of the bit sent by the correct sender. Whether the attack is feasible depends a lot on the dynamic input range of the receiver. It is very likely that the much higher signal level of the modified signal would exceed the possible input range, but for certain situations this cannot be ruled out completely.

The conclusion is that for the modified Miller encoding with 100% ASK this attack is feasible for certain bits and impossible for other bits, but for Manchester coding with 10% ASK this attack is feasible on all bits.

4.1.4 Data Insertion

This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.
4.1.5 Man-in-the-Middle-Attack

In the classical Man-in-the-Middle Attack, two parties which want to talk to each other, called Alice and Bob, are tricked into a three party conversation by an attacker Eve. This is shown in Figure below

Alice and Bob must not be aware of the fact that they are not talking to each other, but that they are both sending and receiving data from Eve. Such a setup is the classical threat in unauthenticated key agreement protocols like Diffie-Hellmann protocol. Alice and Bob want to agree on a secret key, which they then use for a secure channel. However, as Eve is in the middle, it is possible for Eve to establish a key with Alice and another key with Bob. When Alice and Bob later use their key to secure data, Eve is able to eavesdrop on the communication and also to manipulate data being transferred.

How would that work when the link between Alice and Bob is an NFC link?

Assuming that Alice uses active mode and Bob would be in passive mode, we have the following situation. Alice generates the RF field and sends data to Bob. In case Eve is close enough, she can eavesdrop the data sent by Alice. Additionally she must actively disturb the transmission of Alice to make sure that Bob doesn’t receive the data. This is possible for Eve, but this can also be detected by Alice. In case Alice detects the disturbance, Alice can stop the key agreement protocol. Let’s assume Alice does not check for active disturbance and so the protocol can continue. In the next step Eve needs to send data to Bob. That’s already a problem, because the RF field generated by Alice is still there, so Eve has to generate a second RF field. This however, causes two RF fields to be active at the same time. It is practically impossible to perfectly align these two RF fields. Thus, it is practically impossible for Bob to understand data sent by Eve. Because of this and the possibility of Alice to detect the attack much earlier we conclude that in this setup a Man-in-the-Middle attack is practically impossible.

The only other possible setup is that Alice uses active mode and Bob uses active mode, too. In this case Alice sends some data to Bob. Eve can list and Eve again must disturb the transmission of Alice to make sure that Bob does not receive the
data. At this point Alice could already detect the disturbance done by Eve and stop the protocol. Again, let us assume that Alice does not do this check and the protocol continues. In the next step Eve would need to send data to Bob. At first sight this looks better now, because of the active-active communication Alice has turned off the RF field. Now Eve turns on the RF field and can send the data. The problem here now is that also Alice is listening as she is expecting an answer from Bob. Instead she will receive the data sent by Eve and can again detect a problem in the protocol and stop the protocol. It is impossible in this setup for Eve to send data either to Alice or Bob and making sure that this data is not received by Bob or Alice, respectively.

We claim that due to the above given reasons it is practically infeasible to mount a Man-in-the-Middle attack in a real-world scenario.

4.2. Solutions and Recommendations

4.2.1 Eavesdropping

As described in section 3.1, NFC by itself cannot protect against eavesdropping. It is important to note that data transmitted in passive mode is significantly harder to be eavesdropped on, but just using the passive mode is probably not sufficient for most applications which transmit sensitive data.

The only real solution to eavesdropping is to establish a secure channel.

4.2.2 Data Corruption

NFC devices can counter this attack because they can check the RF field, while they are transmitting data. If an NFC device does this, it will be able to detect the attack. The power which is needed to corrupt the data is significantly bigger, than the power which can be detected by the NFC device. Thus, every such attack should be detectable.

4.2.3 Data Modification

Protection against data modification can be achieved in various ways.

By using 106k Baud in active mode it gets impossible for an attacker to modify all the data transmitted via the RF link as described in section 3.3. This means that for both directions active mode would be needed to protect against data modification. While this is possible, this has the major drawback that this mode is most vulnerable to eavesdropping.
Also, the protection against modification is not perfect, as even at 106k Baud some bits can be modified. The two other options might therefore be preferred.

NFC devices can check the RF field while sending. This means the sending device could continuously check for such an attack and could stop the data transmission when an attack is detected.

The third and probably best solution would be a secure channel

### 4.2.4 Data Insertion

There are three possible countermeasures. One is that the answering device answers with no delay. In this case the attacker cannot be faster than the correct device. The attacker can be as fast as the correct device, but if two devices answer at the same time no correct data is received.

The second possible countermeasure is listening by the answering device to the channel during the time, it is open and the staring point of the transmission. The device could then detect an attacker, who wants to insert data.

The third option again is a secure channel between the two devices.

### 4.2.5 Man-in-the-Middle-Attack

As already outlined in section 3.5 it is practically impossible to do a Man-in-the-Middle-Attack on an NFC link. The recommendation is to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties. Additionally, the active party should listen to the RF filed while sending data to be able to detect any disturbances caused by a potential attacker.

### 4.2.6 Secure Channel for NFC

Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack.

Due to the inherent protection of NFC against Man-in-the-Middle-Attacks it is rather easy and straightforward to setup a secure channel.

A standard key agreement protocol like Diffie-Hellmann based on RSA [4] or Elliptic Curves could be applied to establish a shared secret between two devices. Because Man-in-the-Middle is no threat, the standard, unauthenticated version of Diffie-Hellman works perfectly.
The shared secret can then be used to derive a symmetric key like 3DES or AES, which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data.

**NFC Specific Key Agreement**

Besides the standard key agreement mechanism, it is also possible to implement an NFC specific key agreement. This one does not require any asymmetric cryptography and therefore reduces the computational requirements significantly. Theoretically, it also provides perfect security.

The scheme works with 100% ASK only and it is not part of the ISO standard on NFC. The idea is that both devices, say Device A and Device B, send random data at the same time. In a setup phase the two devices synchronize on the exact timing of the bits and also on the amplitudes and phases of the RF signal. This is possible as devices can send and receive at the same time. After that synchronization, A and B are able to send at exactly the same time with exactly the same amplitudes and phases.

While sending random bits of 0 or 1, each device also listens to the RF field. When both devices send a zero, the sum signal is zero and an attacker, who is listening, would know that both devices sent a zero. This does not help. The same thing happens when both, A and B, send a one. The sum is the double RF signal and an attacker knows that both devices sent a one.

It gets interesting once A sends a zero and B sends a one or vice versa. In this case both devices know what the other device has sent, because the devices know what they themselves have sent. However, an attacker only sees the sum RF signal and he cannot figure out which device sent the zero and which device sent the one.

This idea is illustrated below. The top graph shows the signals produced by A in red and by B in blue. A sends the four bits: 0, 0, 1, and 1. B sends the four bits: 0, 1, 0, and 1. the lower graph shows the sum signal as seen by an attacker. It shows that for the bit combinations (A sends 0, B sends 1) and (A sends 1, B sends 0) the result for the attacker is absolutely the same and the attacker cannot distinguish these two cases.
The two devices now discard all bits, where both devices sent the same value and collect all bits, where the two devices sent different values. They can either collect the bits sent by A or by B. This must be agreed on start-up, but it doesn’t matter. This way A and B can agree on an arbitrary long shared secret. A new bit is generated with a probability of 50%. Thus, the generation of a 128 bit shared secret would need approximately 256 bits to be transferred. At a baud rate of 106 kBaud this takes about 2.4 ms, and is therefore fast enough for all applications.

The security of this protocol in practice depends on the quality of the synchronization which is achieved between the two devices. Obviously, if an eavesdropper can distinguish data sent by A from data sent by B, the protocol is broken. The data must match in amplitude and in phase. Once the differences between A and B are significantly below the noise level received by the eavesdropper the protocol is secure. The level of security therefore also depends on the signal quality at the receiver. The signal quality however again depends on many parameters (e.g. distance) of the eavesdropper. In practice the two devices A and B must aim at perfect synchronization. This can only be achieved if at least one of A or B is an active device to perform this synchronization.

Note, that in a recently published paper [5], the same idea for key agreement between an RF reader and an RF tag is presented in a slightly different setup. The paper uses a special so-called noisy tag. This noisy tag is a standard RFID tag, which acts as a third party inserting random looking bits into the communication from the real tag to the real reader. The reader however can calculate the bits sent by the noisy tag and can then calculate the bits sent by the real tag. The problem we see with this
approach is that the noisy tag will not be able to do any synchronization with the real tag. This would be too complicated for a simple tag. Therefore, we think that this approach cannot work in practice. It would require a more sophisticated noisy device instead of the noisy tag to run that protocol in a secure way.

4.2.7 Conclusion

We presented typical use cases for NFC interfaces. A list of threats has been derived and addressed. NFC by itself cannot provide protection against eavesdropping or data modifications. The only solution to achieve this is the establishment of a secure channel over NFC. This can be done very easily, because the NFC link is not susceptible to the Man-in-the-Middle attack. Therefore, well known and easy to apply key agreement techniques without authentication can be used to provide a standard secure channel. This resistance against Man-in-the-Middle attacks makes NFC an ideal method for secure pairing of devices. Additionally, we introduced an NFC specific key agreement mechanism, which provides cheap and fast secure key agreement.

More on URL Spoofing cont.
4.3. Smart Card Alliance Information

The opportunities offered by the advent of proximity mobile payments are clear; differentiated payment services, increased transaction volumes, faster transactions, increased customer convenience, operational efficiencies and the ability to increase customer loyalty through targeted gift and loyalty programs. With implementations already in place in Europe and Japan, strong consumer interest and the ability to leverage the contactless POS infrastructure already in place, NFC-enabled proximity mobile payments show much promise. But how will security be managed in an ecosystem with so many stakeholders, each managing their own unique aspect of the process? The news is good.

Both the financial and mobile industries have made much progress in defining how NFC-enabled mobile payments will take place and how financial information will be secured. Security is bolstered by the use of industry standards and by the technology supporting proximity mobile payments. Industry organizations have defined standards based approaches to ensuring that payment account information is delivered securely to the mobile phone and stored securely in the phone’s secure element.

The NFC-enabled mobile phone leverages the existing ISO/IEC 14443 standard for communicating payment information from the phone to the merchant’s POS terminal. Appropriate risk analysis of an operational model for proximity mobile payments can identify where there is potential for fraud or misuse, develop mitigation measures and assign responsibility. From the consumer’s perspective, the proximity mobile phone payment looks just like a contactless credit or debit card transaction.

Mobile phones can also leverage two-factor authentication technology to secure the payment application and information. Requiring a passcode or a fingerprint to initiate or respond to the terminal’s attempt to initiate or validate a transaction can provide the consumer with additional comfort and a sense of control over a transaction.

While implementations may vary, industry players are moving in a consistent direction. Industry organizations are working to increase ease of access, global interoperability and security of mobile payment technology to consumers. Pilot studies in the United States and implementations worldwide have tested both the technology and the mobile payments process. Proximity mobile payments technology is solid, and will serve this exciting new payment frontier well. Industry stakeholders can leverage the proven technology and a merchant infrastructure that is ready to go to take advantage of consumers’ ever-growing love of mobile technology.
5. **NFC phones and SDK availability**

5.1. **Introduction**

This section provides a summary of available NFC phones as well as NFC peripherals for phones and NFC SDK kits.

5.2. **NFC Phones and peripherals**

5.2.1 **Android Phones**

NFC mobile phone chip suppliers Inside Contactless and NXP have both told NFC World this week that the first commercial NFC-enabled Android phones will arrive on the market later this year and that a wide range of NFC phones will be available from early 2011.

"First phones will be available this year and some more first half of 2011," Henri Ardevol, general manager of secure transactions at NXP Semiconductors, has told NFC World.

Loic Hamon, vice president of products and marketing for Inside Contactless' NFC business line, agrees. "We are very much in the real designing phase," he told NFC World, "working to win business from handset manufacturers for commercial handsets." While there is still nine to twelve months of development work to be undertaken by manufacturers before handsets will be ready to go on sale, he added, the first commercial NFC handsets will be available by the end of 2010 and there will be a "vast portfolio of phones next year for sure."

Both companies have announced moves to further support the development of open source Android NFC devices this week. Inside Contactless is making it easier for developers to begin work on creating NFC software for Android devices by placing its Open NFC protocol stack software on the Sourceforge.net website for anyone to download free of charge. And NXP, in conjunction with Trusted Logic, has released its own open source Android NFC API under an Apache license.

Both companies also claim that theirs is the superior solution, however. And both have announced plans to put their technology forward to the Open Handset Alliance (OHA), the group of 65 companies that developed Android, for adoption as the reference implementation — the de facto standard — for NFC in Android devices. This has raised concerns that competition between the two companies could delay the debut of NFC-enabled Android phones rather than hasten their arrival.

That is not likely to happen, though, Ardevol told NFC World. "We do not think that we will go head to head," he explained. "OEMs providing Android phones want
standard solutions, not proprietary ones. Not having a clear sign on the Android reference implementation will increase the risk of delay at OEMs... We will welcome Inside Contactless to the next steps as we think it is valuable to get more feedback and go with only one proposal to OHA."

Which solution will win the day? Inside Contactless' solution covers Linux, Windows Mobile and MeeGo as well as Android and, says Hamon, its solution is the most open — it has open-sourced all the code for its NFC protocol stack while NXP and Trusted Logic have only made available an API rather than the full source. However, "our solution is available now and everybody can get access to it without waiting further," says NXP's Ardevol.

Inside Contactless says it will release an Android NFC chip simulator and board to developers by the end of the third quarter of 2010.

5.2.2 Samsung

The model chosen by Samsung for its first new NFC phone is the bestselling S5230, known in different markets under a variety of brand names including Tocco Lite, Star, Player One and Avila.

Introduced in May 2009, the mid-range touchscreen phone sold over 10 million units within six months of launch and has topped the best seller lists in the United Kingdom, Italy and the Netherlands.

The phone has been chosen for a number of forthcoming near field communication trials including Telefonica's pilot in Sitges, Spain and Etisalat's test in Dubai. It is also being used this week in an NFC trial taking place at the Mobile World Congress and is also expected to be used in the French Nice NFC City trial due to begin during the second quarter of 2010.

The special NFC version of the S5230 is only available on a limited basis for use in trials, Samsung has told NFC World, and no commercial launch date has been set.

5.2.3 Apple iPhone

iPhone Case with MicroSD

DeviceFidelity has announced an iPhone 4 version of the NFC-enabling iPhone case it first released in May.

The new In2Pay iCaisse4 acts as a protective bumper for the iPhone 4 and incorporates a slot to accept DeviceFidelity's In2Pay microSD format NFC device. A new version of the In2Pay API has been released for iOS 4 and the company has also introduced a developer program for companies wishing to add support for In2Pay to their digital wallet, OTA and payments applications.
"With tremendous interest shown by financial institutions and wireless carriers for our In2Pay solution worldwide, we are glad to announce our latest offering and support for iPhone 4," says Amitaabh Malhotra, chief operating officer at DeviceFidelity. "We are confident that the latest figure-hugging design of the In2Pay iCaisse4 will aesthetically appeal to iPhone 4 users and make it their preferred way of making payments worldwide.

The NFC-on-MicroSD supplier has announced that a protective case designed to add near field communication functionality to the iPhone is now available.

**iCarte Slot**

The iCarte is a Near Field Communication (NFC) / Radio Frequency Identification (RFID) Reader, designed to provide NFC two-way communication, RFID read/write and contactless payment capability for iPhone. NFC and RFID tag information can be written and read by the iCarte and communicated to iPhone. The iCarte has an embedded smart-chip that can be configured as debit, credit, pre-paid and loyalty cards, for secure contactless transactions. iCarte can also read NFC Smart Posters, download or upload electronic coupons, tickets or receipts. The iCarte is ideal for iPhone users who want to use their iPhone for fast and secure contactless payments, transit payments, loyalty rewards, checking balances, top-up, discovering new services from smart posters or kiosks and exchanging information with other NFC phones. Business iPhone users can use the iCarte for commercial applications such as asset tracking, document tracking, healthcare, security and access control.
5.3. SDK Products

5.3.1 NOKIA 6212 NFC Phone

This developer set contains Nokia 6212 classic (NFC) mobile phone, ToP Encoder NFC tool for reading and writing NFC tags and Software Developer Kit (SDK) that allows own software development for CPR40.30-USD r/w device.

The phone is SIM unlocked. ToP Encoder NFC ver. 2 includes desktop r/w device (USB) and Windows software.

The product set contains:

Nokia 6212 classic (NFC)
Battery (BL-4u)
Battery charger (AC-3E European plug)
Three NFC tags with preconfigured content
Stereo headset (HS-40)
User documentation (*)
ToP Encoder NFC ver. 2 - Read/write tool
CPR40.30-USB reader/writer device with USB cable
ToP Encoder NFC ver. 2 Windows software on CD-ROM
Windows device drivers
User quide (in English, PDF)
Windows SDK
Compatible with CPR40.30-USB and other Feig Electronic devices
DLLs, C++ Class Library, Samples

5.3.2 ALVIN Systems

Alvin Systems announces NFC TAG MANAGER and NFC Software development kit (SDK)- unique solution platform on the NFC-Forum standardized technology architecture, with complete support for new NFC-forum standards;

- NFC Data Exchange Format (NDEF) 1.0
- NFC Record Type Definition (RTD 1.0)
- NFC Text Record Type Definition (RTD-Text 1.0)
- NFC URI Record Type Definition (RTD-URI 1.0)
- NFC Smart Poster Record Type Definition SPR 1.1

NFC Tag Manager is a software application that provides a platform for programming NFC tags with standards-based NFC data (such as smart poster) that
enable users to access content and information services with their NFC enabled devices in an easy and intuitive way, whereas the NFC SDK enables solution providers to offer new NFC enabled applications or add NFC functionality to existing solutions.

NFC Tag Manager provides complete support for NFC-forum Mandated Tags (ISO 14443 A, B) from NXP semiconductors and Innovision Group.

Offered with a plug-and-play USB NFC reader/writer and sample NFC Tags, NFC Tag Manager & NFC SDK provide a the complete and future-proof NFC toolkit for service providers, software developers, mobile operators, NFC label converters and research institutions.

How useful would you find the following features if they were available on your mobile phone?