Understanding Near Field Communication (NFC) Technology

Executive Summary

Payment systems and marketing loyalty programs are just the beginning for NFC technology. In addition to the mounting interest in NFC for mobile access control, NFC technology also promises to empower more efficient, effective industrial applications.

Specifically, combining NFC-enabled smart mobile devices with (rugged) RFID tags offers additional benefits when compared to traditional RFID solutions. When an application requires frequent interaction with tags at numerous process points by many different parties, the high expense of using traditional handheld readers is cost prohibitive. By replacing handheld readers with NFC smartphones at data collection points, the ROI for the application increases.

Additionally, while the NFC standards for tags enable a broad variety of use cases and security, the concept of “trust” is not generally specified. HID Trusted Tag™ Services are available to confer trust onto items that are the subject of transactions between individuals and organizations.

This white paper explores the capabilities and technological background of NFC and NFC tags, enabling organizations to evaluate the potential role NFC can have in their market.
What is Near Field Communication - NFC?

Two Views on NFC

Use Case View
Mobile devices with near field communication technology have a huge potential to make lives easier and more convenient for people. For example, with a touch, an NFC device can be used to pay for groceries or a bus fare. But NFC is not limited to payment and mass transportation. It can also be used to gain access to office buildings, hotel rooms and a home, further increasing convenience. In addition, an NFC device can be used to:

- Access a URL from a smart poster or business card and perform the function specified by the code;
- Authenticate whether goods, equipped with an RFID tag, are genuine, and display additional information about the items;
- Simply emulate a card or high-frequency (HF) RFID tag to perform access control or payment functions;
- Replace a traditional HF reader/writer to interact with RFID tags;
- Read data from a banking credential for the purpose of processing a payment at a Point of Sale (POS) terminal (POS emulation);
- Communicate with another NFC device for the purpose of file sharing, data transfer, gaming and data streaming (i.e., video, sound, and printing).

Technical View
NFC is a short-range wireless connectivity technology (also known as ISO 18092) that provides intuitive, simple and safe communications between electronic devices over a close distance using industry standards. Key features include:

- It is based on RFID technology operating at 13.56 MHz (HF)
- Its operating distance is typically up to 1.6 inches or 4 cm (often less – like touch)
- It is compatible with today’s field proven contactless RFID technology and includes a variety of existing standards including ISO/IEC 14443 both Type A and Type B and FeliCa
- Data exchange rates: 106, 212 or 424 kbit/s
  *The Keys to Truly Interoperable Communications,* NFC Forum white paper.

NFC Operation Modes
NFC devices are unique in that they can change their mode of operation to be in read/write mode, peer-to-peer mode or card emulation mode. The different operating modes are based on the ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 contactless smartcard standards. In order to obtain a NFC certification, devices must support at least two of the three modes.
Card Emulation
When an NFC-enabled device is used in card emulation mode, the smartphone is viewed more as a smartcard to the external reader rather than a mobile device. This enables NFC mobile phones to be used for contactless payments, ticketing and access control without the need to exchange existing infrastructure, such as door locks or payment terminals. Secure card emulation applications run in a “Secure Element”, see the following chapter.

Read/write mode
In read/write mode, the NFC device is capable of reading NFC Forum-specified tag types, such as an NFC smart poster. The tag can contain instructions for sending a short message or launching the browser with a specific URL. These capabilities make it possible to provide services, such as interactive and location-based advertisements or coupons. This mode is also useful for many industrial or logistics applications where interaction with an RFID tag is required — for example, monitoring maintenance logging. Another potential use case is enabling a guard to use a mobile device to read an access control card of a visitor or “check in” at wall mounted tags to prove his presence.

Peer-to-Peer mode
In peer-to-peer mode two NFC devices can actively exchange data by simply tapping together. For example, a tap can set up a Bluetooth or Wi-Fi connection, or exchange content such as virtual business cards and digital photos, or print a file from a mobile phone by just touching an NFC-enabled printer. Devices can act in two sub-modes:

- **Passive Communication**: The initiator device provides a carrier field and the target device emulates a transponder
- **Active Communication**: Both initiator and target device communicate by alternately generating their own field
NFC Devices

NFC-enabled devices typically come in the form of a smartphone with an integrated NFC chipset. There are dozens of NFC-enabled phones on the market today, including Android, Windows Phone and Blackberry devices. iPhone’s up to version 5 are not NFC-enabled, but add-on solutions are available to give the iPhone this communication capability.

Beyond smartphones, NFC can be included in PCs, laptops, vending machines, loudspeakers, etc. The range of potential uses is quite broad.

One of the key benefits of NFC is that, as NFC-enabled phones and tablets become the norm, virtually everyone will have an RFID reader/writer in their hand. Suddenly, technology that previously required costly and bulky devices operated by specialists is available to anyone. Companies who in the past had to equip workers with phones and specialized RFID readers now can save the cost of providing the extra RFID reader and benefit from the more advanced application programming environment and connectivity options of smartphones.

The core NFC functionality is inherently built into the operating system of NFC-enabled smartphones, so reading a tag and processing the URL, contact information or launch action stored on the tag requires no extra software to be installed.

Secure Element (SE)

NFC applications like payment and access control use data which must be stored in the smartphone in a secure way. This data is typically stored inside a secure element (SE) which is designed to be tamper proof and is certified according to at least Common Criteria certification (EAL 4+). Examples of SEs are a) the handset’s Subscriber Identity Module (SIM), also called a Universal Integrated Circuit Card (UICC), b) a chip embedded in the phone or c) an external device such as a MicroSD card, sleeve, sticker, or other add-on. There are pros and cons to each of these three SE options in such areas as migrating credentials when a user changes phone models, or determining who manages the access rights to the SE.

The ecosystem around the SE is very complex, as it involves parties like the Mobile Network Operator (MNO) or carrier, the handset manufacturer, various payment associations, the community of application vendors, and end users. Questions about who owns the SE remain unresolved, and key standards are still only just emerging. For instance, how will more than one NFC application share the same SE? Will it be possible for more than one SE to share the same NFC controller? These and other questions and issues are currently impacting the mass deployment of card-emulation applications.

Starting with Android 4.4 an alternative solution within the NFC standard called “Host Card Emulation (HCE)” is designed to overcome the restrictions of the Secure Element design, but since it is only supported in the newest generations of mobile operating systems and requires adjusted applications, it may take a while to become commonly adopted.

NFC Tags

What is an NFC Tag?

In General

Any standards-based HF RFID tag can be used with most NFC devices in read/write mode. Technically there is a distinction between NFC tags and NFC Forum tags, but in practice, both typically work equally well in today’s devices.
• An **NFC Tag** is a contactless tag which operates with ISO 14443 (or ISO 15693) infrastructure and NFC devices as defined by the NFC Forum, and is capable of storing NFC Data Exchange Format (NDEF) formatted data.

• An **NFC Forum Tag** is compatible to one of four NFC Forum Tag platforms capable of storing NDEF data. Only NFC Forum tags may carry the “NFC logo,” called N-Mark, which typically indicates where the phone/reader should be placed when the tag is tapped.

All NFC Forum tags are also NFC tags, but not vice versa; e.g.: Tags with MIFARE® Classic or ICODE® SLIx chips from NXP can be NFC tags but are not (yet) NFC Forum tags, whereas MIFARE DESFire® EV1- or MIFARE UL-based tags are also NFC Forum compliant. In practice, the user or application programmer will not notice any difference and all tags work well with most devices. Typically NFC Forum compliant tags are supported by all kinds of NFC handsets, whereas other NFC tags are supported by certain models only.

**NFC Forum Tag Types**

To date, the NFC Forum ([www.nfc-forum.org](http://www.nfc-forum.org)) has standardized four tag types (Type 1-4) based on ISO 14443. These tag types differ in technical details like memory size and protocol, and typically cover more than one chip model per type. MIFARE Classic- and ISO 15693-based tags are not yet officially recognized by the NFC Forum.

Examples of the most common NFC tag chip types are:

<table>
<thead>
<tr>
<th>Tag Type</th>
<th>Use Case</th>
<th>Chip</th>
<th>User Memory (bytes)*</th>
<th>UID Length (bytes)</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forum Type 1</strong></td>
<td>Specialized</td>
<td>Innovision Topaz</td>
<td>90 - 454</td>
<td>4</td>
<td>$</td>
</tr>
<tr>
<td><strong>Forum Type 2</strong></td>
<td>Most common, low cost, single application like smart poster, personal label etc.</td>
<td>NXP MIFARE UL, MIFARE UL-C, NTAG 203, 210, 212 etc.</td>
<td>46 – 142</td>
<td>7</td>
<td>$</td>
</tr>
<tr>
<td><strong>Forum Type 3</strong></td>
<td>Specialized, Asian markets</td>
<td>Sony FeliCa (Lite)</td>
<td>224 – 3984</td>
<td>8</td>
<td>$$$</td>
</tr>
<tr>
<td><strong>Forum Type 4</strong></td>
<td>High memory applications, high security (in non NFC mode)</td>
<td>NXP MIFARE DESFire EV1 -2K, 4K, 8K, Inside Secure VaultIC 151/161, HID Trusted Tag™</td>
<td>1536 - 7678</td>
<td>7</td>
<td>$$$</td>
</tr>
<tr>
<td>MIFARE Classic</td>
<td>Very common, high memory</td>
<td>NXP Mifare Classic 1K, 4K</td>
<td>716 - 3356</td>
<td>4 or 7</td>
<td>$$</td>
</tr>
<tr>
<td>ISO15693</td>
<td>If long read range is required, industrial rugged tags</td>
<td>NXP ICODE SLIx family, EM4233, Fujitsu FRAM MB89R118C, MB89R112, HID Vigo™</td>
<td>32 – 2048 (112 for ICODE SLIx)</td>
<td>8</td>
<td>$ - $$$</td>
</tr>
</tbody>
</table>

* Note that the actual usable maximum size of NDEF text (e.g. a URL or plain text) is typically at least 7 bytes less than the available user memory specified by the chip vendor.
Trusted NFC Tags

HID Global provides a unique trusted tag that has the capability to generate a cryptographic authentication code every time the tag is tapped and append that code to the URL that is read from the tag. HID Trusted Tags are NFC Forum Tag Type 4 compliant.

To the tapping device, the URL displayed appears like any standard URL and directs access the desired web server without requiring any special app being installed. This web server then subtracts the authentication code and sends it to the HID Trusted Tag Service for verification.

This unique functionality allows the server to distinguish true taps of a particular tag from someone accessing the server via URL refresh or URL sharing. It’s up to the platform provider to decide whether a shared URL should lead to denial of the service or just logged for statistical purposes.

See the [HID Trusted Tag overview](#) and [How it Works](#) videos.

NDEF Data Format

The NDEF specification defines a message encapsulation format to exchange information; e.g., information between an NFC Forum device and another NFC Forum device, or an NFC Forum Tag. The logical structure is very simple and consists of a sequence of identifiers as well as length and payload records.

An extensive set of identifiers is already defined in the standard, including URLs, contact information, plain text, phone numbers, images, SMS, e-mail, geo location, among others. When an NFC-enabled phone’s operating system reads such an identifier, it inherently knows how to process it without needing any additional application software to be installed. For example, reading a URL type of NDEF message causes a browser to open to the specified URL, while reading a contact causes the contact application to open and import the contact.
Multiple NDEF records can exist within one message on a single tag, but it is the message type that determines which action the smartphone’s operating system performs when a tag is tapped. NFC and non-NFC data may coexist on one physical tag to support legacy applications.

Today, however, many NFC applications working with tags are not using the NDEF data format. They simply read the unique ID of the chip to identify the tag and access an external database record on the phone or on-line, where the rest of the data for this tag is stored. To the end-user this still appears like an NFC application, although no NDEF specific data is stored on the tag.

**Physical Form Factors of NFC Tags**

NFC tags can come in any form that is typically available for traditional RFID tags. Essentially, the entire HF tag portfolio of HID Global can be used as NFC tags. This includes tiny embeddable discs like Piccolino or ClearDisc, and ruggedized or even flame-resistant tags for industrial use like the IN Tag™, Poly Tag®, LogiTag™ or Jewelry Tag families, as well as ISO cards, key fobs and printable on-metal stickers or clear labels.

**NFC Use Cases with HID Global**

HID Global’s NFC-enabled systems are used for many different applications by customers around the world today, and this is just the beginning of the emerging NFC market. Get inspired by some of the examples below:

**Industrial Application: Harvest Logistics**

HID Global, in partnership with system integrator Fundación Ada Byron (FAB), worked with Bodega Norton Winery in Argentina to develop a solution to replace a cumbersome, outdated tracking system that was used for compensating employees.

The old system was based on the manual distribution and collection of thousands of aluminum and plastic chips that tracked the amount of grapes picked by harvesters. The chip system presented inherent administrative and logistical difficulties. The paper-based system required that one day a week was allocated for collecting, counting and processing the chips, therefore halting production in the fields.

With the new solution, each harvester was issued an armband equipped with a unique contactless MIFARE®-based ISO card. Grape collection bins were tagged with HID Global Epoxy Disc tags and vineyard supervisors were outfitted with NFC-enabled smartphones. The new system now enables vineyard supervisors to simply place their smartphone next to the harvester’s armband, which triggers an audible beep assuring both the harvester and supervisor that the collection bin has been counted and credited appropriately.

See the video and case study for more details.
**Industrial Application – Time and Attendance Monitoring**

Combining all the technologies (NFC, GPS, GSM) in one device is very beneficial for attendance workflow.

- Proof that staff have visited checkpoint locations (Patient rooms, devices to monitor, etc.)
- Alerts in the event a location is not visited
- Versatile recording of other dates; e.g., start/end shift, time of visit, incidents, etc.
- Instructions can be displayed on screen, detailing routes and tasks to be performed
- Worker may use multimedia; e.g., take pictures
- Central real-time and historic view of data
- Easy messaging to staff, etc.
- Only one device to carry and charge

**Commercial Applications - Loyalty Marketing Programs**

NFC tags have been used in commercial retail applications for many years. Generally these tags are pre-encoded with NFC data formats (NDEF) to launch URLs, play multimedia messages, etc. on NFC-enabled smart mobile devices.

HID Trusted Tag offers unique functionality that allows a server to distinguish true taps of a particular tag from someone accessing the server via URL refresh or URL sharing. The platform provider can decide whether a shared URL should lead to denial of a service or just log the information for statistical purposes.

HID Trusted Tags add value for Digital out of Home (DOOH) marketing campaigns because the URL cannot be copied, cloned or shared. Programs such as,

- Loyalty programs or sweepstake campaigns can make sure the customer was physically present to receive a service, where a certain number would grant the discount.
- Free downloads of sponsored songs when touching an NFC enabled poster can ensure only people actually interacting with the poster receive the intended reward, avoiding the URL being shared and used via a blog or social site without the desired NFC experience.
- Brand protection of valuable goods that can be authenticated with any standard NFC phone and provide enriched product specific customer information via the web. The dynamic code generation of HID Trusted Tags avoids the need for a dedicated APP to be installed on the phone while still providing strong cryptographic authentication of the tapped good.

See the [Trusted Tag DOOH video](#) for more details.

**Mobile Keys™ Access Control**

While the above examples use the NFC read/write mode to interact with physical tags, the NFC card emulation mode can also be used so the NFC device can act like a card or tag towards other readers or door locks, for example. Several cards or other logon credentials can be converged into a single NFC-enabled mobile phone and provisioned or revoked over the air. From the perspective of a NFC reader (e.g., a door lock or Windows PC), the phone appears no different than a card because it is simply using its secure element or HCE to emulate this card.
Especially for Access Control also Bluetooth Low Energy (BLE) may be used as alternative technology to NFC. As an advantage it works with all modern phones incl. iPhone, but requires BLE enabled door locks whereas NFC can interact with existing infrastructure.

**Readers and Reader Boards**

Finally, HID Global offers a set of NFC-enabled readers or reader boards. Reader boards are embedded into custom housings like vending machines or time attendance systems to add general RFID or NFC functionality.

**Summary**

The worldwide availability of NFC-enabled devices enables the large population of smartphone users to take advantage of low-/no-cost RFID capabilities, opening new use case possibilities and reducing costs at the same time. The proven HID Global HF tag portfolio stands ready to support these new applications. Additional services such as HID Trusted Tag™ Services or HID Secure Identity Services™ for mobile access applications add security and convenience where needed.

**About HID Global**

HID Global is the trusted source for innovative products, services, solutions, and know-how related to the creation, use, and management of secure identities for millions of customers around the world. The company’s served markets include physical and logical access control, including strong authentication and credential management; card printing and personalization; visitor management systems; highly secure government and citizen ID; and identification RFID technologies used in animal ID and industry and logistics applications. Primary brands are ActivId®, EasyLobby®, FARGO® and HID®. Headquartered in Austin, Texas, HID Global has over 2,200 employees worldwide and operates international offices that support more than 100 countries. HID Global® is an ASSA ABLOY Group brand. For more information, visit [http://www.hidglobal.com/](http://www.hidglobal.com/)

hidglobal.com