# Near Field Communication

## Table of Contents

- Near Field Communication (NFC) ................................................................. 2
- NFC Basics ................................................................................................. 3
- NFC Technology ......................................................................................... 5
- NFC Operation .......................................................................................... 7
- NFC Operation Modes ............................................................................... 9
- NFC Data Exchange Format ................................................................. 11
- NFC Tags .................................................................................................. 13
- NFC Tags Types ....................................................................................... 14
- NFC Usage .............................................................................................. 16
- Notices ..................................................................................................... 17
063 Mark Williams: Near field communication.
**NFC Basics**

Short-range wireless technology

Allows two-way communication between devices

A descendant of RFID

Developed by the NFC Forum

Standardize

- ISO 18092
- ECMA 340

Compatible with smartcard technologies

- Phillips MIFARE®
- Sony FeliCa

**Near field communication is a short-range wireless technology that allows two devices, when they come in close contact with each other, to communicate. When I say close contact, I mean very close contact. We're talking about millimeters and centimeters.**

It's a descendant of the Radio Frequency Identification Technology, and it was developed by the NFC--Near Field Communication Forum.

There are a couple of semi-competing standards that are out there that define near field communication and how it functions.
and works. One of those is an international standard—it is the ISO 118092—and the second one is ECMA 340, and ECMA 340 defines the near field communication interface and protocol for communications.

Not only are there standards that define how near field communication works, but there's also a couple of technologies that are out there that are allowing us to take our near field communication capabilities and embed them, if you will, or make them emulate this concept of smartcard technologies. So Phillips has the MIFARE capability, and Sony what is known as FeliCa, and they are—again, the idea is to use near field communication to emulate smartcard technologies.
NFC Technology

Frequency: 13.56Mhz (HF band)
- Globally available & unregulated
- No licenses required

Distance: 4 - 5 cm

Data Rate: up to 424kbps

Inductive coupling: Uses magnetic field to transmit power

Half-duplex: Single channel used for transmit and receive

Security is provided by the close proximity.

**065 The way near field communication works is that it uses the high-frequency communication band. It operates in the frequency range of 13.56 megahertz. One of the nice benefits of using 13.56 megahertz is that HF is a globally available and unregulated communication spectrum, so we don’t have to have any licenses in order to create and operate NFC systems.

As mentioned, the distance for near field communications is really small. I have to actually be in contact. The two devices have to be touching, or within just 4 to 5 centimeters of each other. And not only is the distance
very small, but actually the data rates are-- by today's standards, they are small as well. We can have up to 424 kilobits per second communication. When we think about that, we're going to back to modem days for communications.

The way near field communication works is that it is using this concept of inductive coupling, so basically magnets. Anytime I have a magnet, there's a magnetic field, and when I have two magnets put within close proximity to each other, we're able to use that magnetic field to transmit this data. Right?

There's a couple different ways that we can operate the near field communication device. I can use it in what's known as half-duplex mode, which is basically where we are taking turns with our communication. I can use it even in full-duplex mode, although half-duplex mode is what's happening today. Full-duplex mode is something that is hopefully on the horizons.

The only security that we really have associated with near field communication is the fact that we're small, we're very close together, and that's what provides security. This concept of doing eavesdropping in near field communication-- it is possible, but it is difficult to achieve because of the close proximity one has to come.
**NFC Operation**

**Devices**
- **Initiator**
  - Begins the conversation and controls data exchange
- **Target**
  - Responds to initiator

---

**Touch mobile phone to tag**

**Phone reads tag and performs actions**

**Possible actions**
- Initiate call
- Configure settings
- Launch browser and load website
- Store contact information
- Launch application

---

**066 How does it operate?**

Well, I have two devices. One device might be my phone, another device might be your phone, and what's going to happen is maybe I have a photo that I would like to share with you, so I bring my phone close to your phone and the near field communication is going to say, "Oh, I see that there is a target." One of the devices will be the initiator, the other device will be the target, and we see that there is an initiator and a target and the initiator will then start a transfer of data. All right? So two mobile phones touching each other.
Or I could have a tag. Think of a tag as just a sticker with a small electronic chip in it. So I could take my phone and bring it close to this tag and information will be read from that tag and it will be stored on my phone.

So what can I use near field communications for? All kinds of possibilities exist, such as let’s say I wanted to use NFC to unlock my doors. So when I come up to my house, my phone reads the NFC tag that is on my lock, my door lock, and says, “Oh, this is an authorized phone. You can come into the house.” So I can unlock my doors. When I come into my home pass, I can have an NFC tag that says, “Oh, you’re now in your home, so we’re going to operate the phone in this type of mode.” Or, “You’re now at work, so we’re going to operate the phone in a different type of mode.”

I can use NFC to launch applications. I can use NFC to initiate phone calls, change the way my device behaves. All right? So NFC can be used--basically the imagination is the only limiting factor to what I could possibly do with NFC.
NFC Operation Modes

Operational Modes

- **Active**
  - Both devices create an RF signal for data transmission
- **Passive**
  - One device creates the RF signal
  - Passive device uses “load modulation” to respond to initiator

Communication Modes

- **Read / Write**
  - Data transmission using NFC Forum message format
    - Insecure
- **NFC card emulation**
  - Allows communication as a standard Smartcard
    - Secure
- **Peer to peer**
  - Device to device link-level communication

**067 So, how does it operate?**

Well, we have two modes. We have an active mode and a passive mode. When we’re using it in active mode, both the devices, like the phones--two phones side by side--are going to create this radio frequency signal. In passive mode, usually with the tags, one device creates the signal while the other device is basically, I’ll say, riding along on that signal to carry information. So the term that we use for there is load modulation, to respond to the initiator. All right?

Those are the operational modes, active and passive. What about the communication modes? I have read-
write function, which allows me to, as the name implies, read information off of a device or write information to a device. So, for example, my phone is next to your phone and I'm transmitting a file to you or receiving a file from you. When we think about the typical read-write communication, one of the issues we have with it is the inherent insecurities of it, and what makes it insecure is the write function. If I can get next to an NFC device and it has the ability to write something onto my device, well, if I don't have trust in that NFC device-- say that tag, for example-- that can be a little bit scary for me.

I could use my near field communication device to emulate a smartcard. I mentioned the Sony FeliCa, for example, as a technology that allows me to use to my near field communication-- my phone, for example-- to emulate a smartcard for secure authentication to gain access to a device. And, again, in the peer-to-peer mode, I can communicate between two devices, basically transmit and receive any kind of data that we want. Near field operations.
NFC Data Exchange Format

One or more records

Type
- Defines the kind of data being carried
- Specified by the application

Payload examples
- URL
- MIME media
- NFC specific info.
  - Defined in NFC Record Type Definition (RTD) file

**068** Now, what is the data that is being transmitted? When two devices come into close proximity with each other, there has to be a way for-- a common format for me to put the data into, just like with any type of network communication.

So we have our NFC Data Exchange Format, which is nothing more than a collection of records. You can have numerous records. Each record has a header and a payload. The header tells us information about the source of the information, the destination-- so it’s an identifier of the record itself-- how big that payload is that
we're carrying, and what type of data that we have.

When we think about what that data could be in these payloads of our records, it could be in the form of a URL. So, I go up to a device-- maybe there's some poster on the wall somewhere for a particular vendor, and I bring my phone up close to it, and near field communication reads the tag and automatically that tag is going to launch a web browser on my phone and it's going to take me to that vendor's website. There might be some type of multimedia type of information that's available to us, or just communication information that's needed between the two NFC devices-- the handshaking information could be in the payload as well. All right?

So, again, what could I do with these data exchanges? Pretty much anything that I like-- launch an application, browse to a URL, transmit data from Point A to Point B. The options are many. All right?
NFC Tags

Enables endless flexibility of uses

Allows NFC devices to be “touched” to passive NFC tags

Tags Based on

- ISO 14443 (contactless Smartcard standard) or
- Sony FeliCa (conforms to ISO 18092 passive communication standard)

4 Tag types

- Type 1
- Type 2
- Type 3
- Type 4

**069 Now, when we talked about active mode NFC, we said, "My device and your device are both supplying power," and that is a traditional way of transmitting data, but I also mentioned this concept of tags, NFC tags, and I said it might be in the form of a sticker that has an electronic circuit in it. Well, when we think about these tags, there has to be some standard for how these tags are created and how they're written, and so the tags are based upon the smartcard standard of ISO 14403 or, again, I mentioned Sony's FeliCa standard, which conforms to ISO 18092, which is another international standard for how we do passive
communications. Different types of tags are available to us. When we think about the types of tags that we have available--

**NFC Tags Types**

<table>
<thead>
<tr>
<th>Tag Type</th>
<th>Standard</th>
<th>Capability</th>
<th>Memory</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ISO 14443</td>
<td>Read and re-write</td>
<td>96 bytes expandable to 2 kbytes</td>
<td>106 kbps</td>
</tr>
<tr>
<td>2</td>
<td>ISO 14443</td>
<td>Read and re-write</td>
<td>48 bytes expandable to 2 kbytes</td>
<td>106 kbps</td>
</tr>
<tr>
<td>3</td>
<td>Sony FeliCa</td>
<td>Pre-configured by manufacturer as read only</td>
<td>2 kbytes</td>
<td>212 kbps</td>
</tr>
<tr>
<td>4</td>
<td>ISO 14443</td>
<td>Pre-configured by manufacturer as read / re-write or read only</td>
<td>32 kbytes</td>
<td>106 kbps – 424 kbps</td>
</tr>
</tbody>
</table>

**070** Here is a list of what the tag types are, what the standard is that defines the tag types, and what we can do with them, and basically how much storage space that they have available and how much speed.

So notice that many of the tags are based upon the international standard for smartcards, ISO 14443. Only one tag type, Tag 3, is based
upon the Sony FeliCa technology that's out there. All right?

So types 1 and 2 are probably the most common tag types that we have available to us. They give us a bandwidth capacity of 106 kilobits per second, so they're relatively small in bandwidth, and they're also fairly small in how much memory, how much information can be stored on them. Type 2 tags can only store about 48 bytes. That could be expanded up to 2 kilobytes per second, but typically 48 bytes, which is plenty for some simple URLs, whereas if I needed, say, a longer URL to transmit, then maybe I would use a type 1 tag, which gives me up to 96 bytes of information.

If I needed even more storage of information, that's when I go to the tag type 3, the Sony FeliCa, or the type 4, which allows me to have up to 32 kilobytes of information.

One of the issues with type 3 and type 4 is that they are what they are. They come preconfigured from the manufacturer to store information. You and I as the average, everyday users, we don't have the ability to write our own information to the tags, whereas with the typical type 1 and type 2 tags I can write anything that I want for them. All right?
NFC Usage

Device to device data transfer

Point-of-sale

Vending machines

Access Control
  • Turnstiles
  • Locks

Contactless ticketing

Auto-configure smartphone

**071 What do I use near field communications for? Again, the options are many. My imagination is the only limiting factor here. I have seen near field communications used for vending machines. So instead of having to put money into the vending machine or having to put a credit card into the vending machine, I have a pay type of service on my phone and I can just go up to the vending machine, put my phone up to it, get the product that I’m looking for, and it’s automatically going to charge my phone or my pay service.

Contactless ticketing. I could use it to automatically configure my
smartphone to do certain types of actions, transfer data— you name it, I can use a near field communications for it.

**Notices**

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.