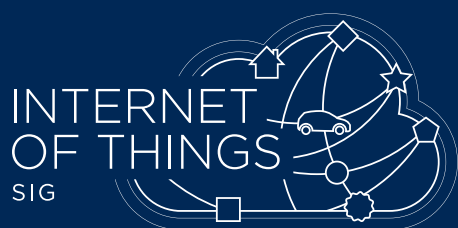




Improve the IoT User Experience with NFC Simple Secure Pairing

Best Practices, Recommendations & In-Market Examples

White Paper
September 2019

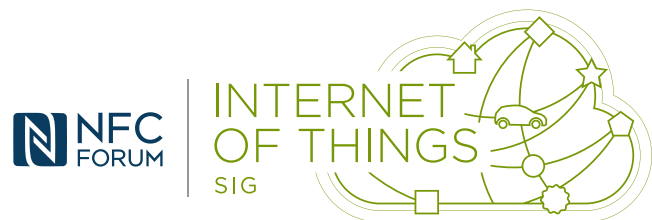


Contents

Introduction.....	4	Simple Secure Pairing Recommendations.....	10
Objectives	4	1: Touching to connect and disconnect.....	10
Simple Secure Pairing and the Connection Handover Specification.....	4	2: Connection by a new device	11
Security in Connection Handover.....	5	3: Connecting to a new accessory device.....	11
Scope of This Document.....	6	4: Connecting via a third device.....	12
General Recommendations.....	7	Bluetooth-specific Recommendations	12
NFC accessory device.....	7	1: Use of all supported profiles.....	12
1: NFC antenna location	7	Simple Secure Pairing with NFC - In-Market Examples.....	13
2: NFC touchpoint indication.....	7	Conclusion	14
3: Use of the N-Mark.....	7	Appendix.....	15
4: Other options helping the user to find the touchpoint	7	More about the NFC Forum.....	15
5: Operating volume.....	8	NFC Forum Specifications	15
6: Short touch duration.....	8	NFC Compliance and Interoperability.....	15
7: NFC contact surface	8	NFC Forum Certification Program.....	15
8: NFC antenna dimension	9	NFC Forum Plugfest Events	16
9: Conformance and performance testing.....	9	NFC Modes.....	16
10: Automatic actions.....	9	Terminology, Abbreviations, and Acronyms.....	17
11: Feedback upon completion.....	10	Glossary.....	17
		Acronyms.....	17

Contributors

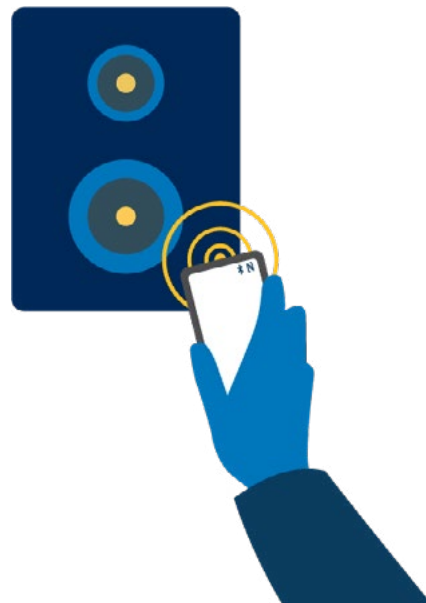
- Vincent Chauvin, Apple
- Erich Reisenhofer, NXP Semiconductors
- Matthew Bright, Thinfilm
- Michał Grochala, Nordic Semiconductor
- Rachel Furst, Blue Bite



Simple Secure Pairing with NFC

Benefits for Consumer:

- **Faster, simpler connections** – no need for Bluetooth/Wi-Fi submenus or searching through lists to find surrounding devices
- **No conflicts** – pair only the devices you intend to pair
- **Secure exchanges** – share credentials securely with just a tap
- **Easier disconnects** – tap again to unpair
- **Save power** – use NFC field to enable/disable sleep mode from a battery-driven Bluetooth/Wi-Fi device



The Many Possibilities for Simple Secure Pairing with NFC



Introduction

With Near Field Communication (NFC) technology now included as standard equipment on millions of Android and iOS smartphones worldwide, NFC has emerged as a powerful tool to complement and enhance the value and performance of consumer electronics devices that form an increasingly important part of the Internet of Things (IoT), from headphones and speakers to smart home systems, appliances, and game consoles. NFC's growing global deployment allows for wide interoperability, and its ease of use makes NFC a natural choice when IoT device manufacturers want to streamline and improve the User Experience (UX) throughout the lifecycle of an IoT device.

NFC technology is unique in its near-touch or “tap”-based user experience. Users simply hold their NFC phone near the item with which they want to interact. Because NFC operates at a distance of only a few centimeters, users can quickly and easily interact directly with a specific desired item, with no menus to navigate or multi-step procedures to follow. This unique expression of user intent improves not only the user experience but also the security of the system.

Consumers demand simplicity, and product managers compete to make their products the easiest to set up and maintain. In Smart Home and other IoT use cases, NFC is becoming a popular way to improve the user experience for unboxing and onboarding devices designed to communicate with wireless networks using Bluetooth, Wi-Fi or other wireless technologies. This application of NFC – referred to as Simple Secure Pairing – is based upon the NFC Forum's [Connection Handover Technical Specification](#).

This specification can be used to facilitate a wide range of use cases, including audio or video streaming, remote control of devices, communication with wearable sensors, or NFC initiation of file transfers to be completed using a non-NFC wireless technology, such as Bluetooth or Wi-Fi. To learn more about the technical implementation of this technology, read the “[Simplifying IoT: Connecting, Commissioning and Controlling with Near Field Communication \(NFC\)](#)” white paper.

These various use cases share a common element: they are initiated with a tap of an NFC-enabled device. However, the user experience following that tap can vary widely between implementations, even for identical use cases. For example, users may find that, when tapped with an NFC smartphone, one pair of NFC headphones acts differently from another pair of headphones. Inconsistent implementations can lead to user confusion, which is why this white paper is designed to promote a consistent user experience that can ultimately improve user satisfaction.

Objectives

NFC is inherently intuitive and easy to use. Therefore, it is important for NFC solution providers to ensure that users have a consistent and pleasant user experience. Consistency also reduces the failure rate for initial consumer use of an NFC-enabled item – which is a very important consideration. The simplicity of the “touch paradigm” is one of the major advantages of NFC.

This document provides a set of recommendations to help product managers, engineers, and software developers to better align user experiences across Simple Secure Pairing implementations.

Simple Secure Pairing and the Connection Handover Specification

The NFC Forum was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC. Since then, the NFC Forum has created a set of specifications to support and enable various use cases. The NFC Forum specification that standardizes the implementation of Simple Secure Pairing is the [Connection Handover specification](#).

Connection Handover focuses on use cases in which the total amount of data to be transferred is too large to be transmitted over NFC during the time of a touch, for situations in which data is to be streamed for a longer time or when additional authentication is required to establish a connection.

It is easy and fast to establish a communication link between two devices with NFC, but the connection is then limited to a short communication distance and low data speed compared to other wireless communication technologies. However, those other carriers often require a more complicated network configuration or connection setup process.

Using the Connection Handover specification, solution developers can deploy applications that offer the best of both worlds by combining the simple, one-touch and secure setup of NFC with the high-speed, longer distance communication of Bluetooth or Wi-Fi. The specification enables developers to choose the carrier for the information to be exchanged. If matching wireless capabilities are revealed during the negotiation process between two NFC-enabled devices, the connection can switch to the selected carrier.

The specification distinguishes between **static** and **dynamic** NFC connection handover.

- In **static connection handover**, an NFC-enabled device in reader/writer mode detects an NDEF (NFC Data Exchange Format) tag that contains a static handover message. The NFC device analyzes the handover message, and if it contains valid data for a carrier the device supports, the device initiates a corresponding connection. Usually, static handover is used to establish a connection between an NFC device and **an accessory or peripheral device**, such as a Bluetooth speaker or Wi-Fi network. Note that there are commercially-available NFC tags that can change the NDEF message dynamically, enabling them to encode additional information in the connection handover message, such as for device authentication.
- **Dynamic, or negotiated, connection handover** utilizes NFC in peer-to-peer mode and occurs **between two NFC devices** – for example, two smartphones. A touch initiates a negotiation between the two devices, in which one device proposes a set of carriers and the other may select one of those.

*Note: This document covers user experience recommendations for **static** connection handover. Dynamic/negotiated handover is outside the scope of this document.*

Note: Connection Handover specifies a framework only. The data definitions for specific carriers are outside the scope of the NFC Forum. Other communication standards bodies, such as the Bluetooth SIG and the Wi-Fi Alliance, have specified corresponding data structures.

Security in Connection Handover

The Connection Handover protocol greatly simplifies the establishment of connections for various wireless technologies. While most of these technologies have their own, well-defined security procedures, not all devices have required I/O capabilities to support full authentication and protect from “man-in-the-middle” attacks. Considering this – and the fact that authentication is crucial at the moment of connection establishment – NFC offers significant advantages. Due to the physical proximity requirement of the tap-based communications model, NFC provides additional (and for some devices the only possible) device authentication. By limiting pairing or handover to devices within very close (i.e., a few centimeters) physical proximity, NFC facilitates communication between the intended devices. As a result, NFC ensures that only these devices can take advantage of wireless security procedures that protect against passive eavesdropping and other attack types, thereby providing the highest levels of security during connection handover.

Scope of This Document

This paper focuses on Simple Secure Pairing between NFC and carriers such as Bluetooth and Wi-Fi for the following use cases:

- Connection to an established network
- Audio or video streaming (including services such as [Miracast](#))
- Image or file transfer
- Connection to wearables and medical sensors (confidential data transfer)
- Connection of an IoT device to a network

This document assumes that the type of device that is touched determines the action the user wants to perform. This is usually the case when:

- One of the devices is a (potentially mobile) multi-purpose NFC-enabled device (e.g., a smartphone). Such a device is referred to as an **NFC device** in this document. An NFC device supports NFC in at least Reader/Writer mode.
- The other device is an accessory or a single-purpose device such as a speaker, printer, or a low-powered sensor referred to as an **NFC accessory device** in this document. NFC accessory devices usually offer either Bluetooth or Wi-Fi as carriers; both may be offered in rare cases.

These use cases can often be enabled using static handover. In this situation an NFC accessory device is the Handover Selector and an NFC device is the Handover Requestor (see the [Connection Handover specification](#) for details). NFC does not work when two NFC accessory devices are touched to each other, as both incorporate only an NFC tag, and two tags cannot communicate.

Concrete examples of targeted use cases are:

- Bluetooth audio streaming between a smartphone and a speaker or headset
- A Miracast session between a smartphone and a TV
- Transfer of an image between a digital camera and a smartphone over Wi-Fi
- Connection to a new Wi-Fi network (hotel, conference, or friend's home)

In addition to a set of Simple Secure Pairing recommendations that apply to all carriers, this white paper also includes recommendations that apply specifically to Bluetooth pairing.

Note: User experience recommendations for use cases that are based on touching two NFC devices are not within the scope of this document.

General Recommendations

General recommendations apply regardless of the application, and are related to the NFC touchpoint, the operating volume, and overall transaction time.

NFC accessory device

1: NFC antenna location

Recommendation

The position of the NFC antenna should enable the end user to hold the NFC device in a familiar way. It should be easy for the user to position the NFC device near the touchpoint (NFC antenna) of the NFC accessory device.

Rationale

For NFC to work, the user must touch the devices together at the point where the antennas are located, in order to establish a connection. Making this touch easy by considering daily life usage of the device improves the end user experience.

2: NFC touchpoint indication

Recommendation

Indicate the position of the touchpoint on a device so that the user clearly and unambiguously understands where to touch.

Rationale

It is very difficult for the user to determine the antenna position, as NFC-enabled electronic devices have a variety of antenna positions. Being able to locate the touchpoint quickly and accurately significantly improves the user experience and increases the success rate of using NFC.

3: Use of the N-Mark

Recommendation

Use the NFC Forum N-Mark to clearly indicate the touchpoint for both the NFC device and the NFC accessory device.



Rationale

Different marks are confusing for the user. For more information about the N-Mark, please refer to the Appendix of this document or to <http://nfc-forum.org/our-work/nfc-branding/n-mark/>.

4: Other options helping the user to find the touchpoint

Recommendation

In addition to the N-Mark, other media should be used to show the interaction.

Rationale

A mobile device offers plenty of options to train users in using NFC. For instance, when enabling NFC for the first time, a pop-up window can demonstrate how to tap the NFC accessory device. The NFC accessory device should include information, such as a short “Getting Started” instruction, to show the touchpoint.

5: Operating volume

Recommendation

Sufficient Operating Volume is a prerequisite for a seamless and enjoyable NFC user experience. Therefore, the NFC device should pass the Operating Volume tests with reasonable margin, and the NFC accessory device should extend the minimum required operating volume of 5 mm to the need of each specific use case (e.g. payment requires 4 cm).

Rationale

Extending the Operating Volume far beyond the required 5 mm helps the user to find the touchpoint and reduces the overall transaction time, as the transaction can start earlier. In general, this recommendation is very use case-dependent and there is always a trade-off between power consumption/costs and operating volume extension.

6: Short touch duration

Recommendation

The duration required for the NFC touch should be as short as possible to optimize the user experience. To ensure a satisfying touch-and-go experience, a touch should not need to last longer than 500 milliseconds (measured from the time the devices are brought close enough together to enable RF communication until the time the NFC transaction has finished). If more time is needed, a progress indicator should be implemented.

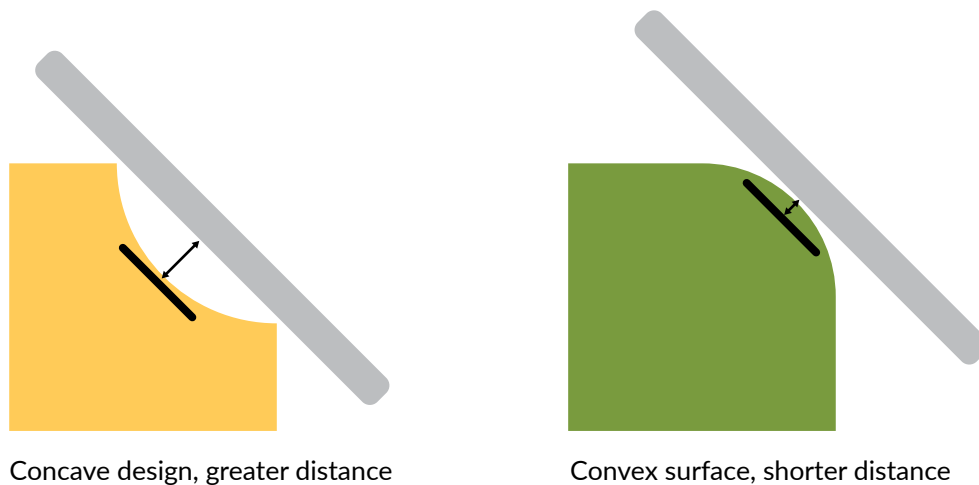
Rationale

Even though some use cases or specific implementations may require touching the devices for a longer time period, the targeted user experience with NFC is a short touch of the two devices. A time of 500 milliseconds is long enough for exchanging the amount of data via NFC that is necessary for the targeted use cases. A progress indicator, such as a progress bar, helps the user to be patient.

7: NFC contact surface

Recommendation

Due to the variety of positions of NFC antennas on NFC devices, the surface of the NFC antenna should be preferably flat or convex to minimize the distance between the NFC antenna and the NFC device and to accommodate several NFC device designs.



This graphic shows how an NFC antenna with flat or convex surface (right) enables a shorter distance between the NFC antenna and the NFC device. The concave design (left) requires greater distance, which can negatively affect the user experience.

Rationale

The NFC Forum requires a minimum Operating Volume of 5 mm. Minimizing the physical distance between the NFC antenna and the NFC device provides more useful Operating Volume for the user and should improve the user experience with the NFC accessory device.

8: NFC antenna dimension

Recommendation

The NFC antenna dimension could benefit by having dimensions similar to reference antennas used during [NFC Forum Certification](#) and should, preferably, not exceed the maximum and minimum dimensions of Listeners 1 and 6. The NFC Forum Listener 3 represents the median antenna dimensions and could be a suitable target.

Rationale

Every NFC device certified by the NFC Forum is tested with three reference listeners, listed below. Therefore, it is likely that an NFC tag with a similar antenna would perform consistently in the NFC Forum operating volume.

- Listener 1: 71.6mm x 41.5mm
- Listener 3: 46mm x 32mm
- Listener 6: 24.7mm x 19.7mm

9: Conformance and performance testing

Recommendation

The NFC Forum highly recommends performing the established conformance and tag performance testing. [NFC Forum Plugfests](#) are one-week events that offer a safe, real-world environment where developers with NFC Forum-specified devices can verify device interaction across product implementations. They offer NFC Forum members and non-members device-to-device interoperability testing, end-to-end data sharing, and access to a library of various NFC Forum tags, smart posters and NFC Forum devices.

Rationale

Interoperability is the key to the optimal user experience. NFC devices and NFC tags ensure smooth and reliable transactions. Tag performance testing shows the complete achievable operating volume and makes it easy for the implementer to choose the tag best suited for each application.

10: Automatic actions

Recommendation

Devices should be able to perform a required action with as few additional user actions as possible.

Rationale

The entire rationale for using NFC in the Internet of Things to connect the unconnected is to reduce the number of user interactions. Requiring the user to enable or disable a carrier or annoying the user with additional confirmation messages such as “Do you want to pair your device?” would diminish the user experience.

11: Feedback upon completion

Recommendation

Give feedback to the user indicating when the user can detach the two devices.

Rationale

To make a connection, users need to touch one device to another device, targeting the touchpoint. However, a user cannot know how long to touch the two devices together. Therefore, when the devices have completed their operation over NFC, the user should be notified that the devices can be moved apart.

Providing such feedback significantly increases the success rate of connections using NFC handover, as the users can wait for feedback from the device; they do not need to determine on their own when to move the devices apart.

Usually the NFC device is equipped with a richer user interface than the accessory device; therefore, the user feedback should be provided on this device and only optionally on the accessory device.

Flow example:

1. The user touches an NFC device to an NFC accessory device.
2. The NFC accessory device powers up.
3. The NFC device discovers the NFC tag of the NFC accessory device and reads the stored NDEF message.
4. The NFC device provides feedback to the user, such as a visual indication or by vibrating.
5. The user moves the NFC device away from the NFC accessory device.

Simple Secure Pairing Recommendations

1: Touching to connect and disconnect

Recommendation

Touching two devices that are not connected should connect the devices. Touching them again should disconnect them.

Rationale

There are many cases where repeating the same operation results in canceling the previous operation (e.g., the switch or on/off button on devices). This paradigm is therefore well understood by most users. To make connection and disconnection operations consistent, this rule should be applied to NFC simple secure pairing.

Disconnecting a device in this case is also the most natural behavior, as the other possible options -- either to do nothing or to try to connect again -- do not bring any benefit to the user.

Flow example:

1. The user touches an NFC device to an NFC accessory device.
2. The NFC device discovers the NFC tag of the NFC accessory device, reads the stored NDEF message, and establishes a connection, such as for audio streaming. If Bluetooth is not already active, the device activates it in order to facilitate the ongoing connection.
3. The user moves the NFC device away from the NFC accessory device and continues to use the devices, now paired via Bluetooth.

4. To initiate the disconnection process, the user touches the NFC device to the NFC accessory device a second time.
5. The devices disconnect (and may turn off Bluetooth immediately or after some idle time).

2: Connection by a new device

Recommendation

When an NFC accessory device that currently has an active connection with an NFC device is touched by another NFC device targeting the same type of service, it should disconnect from the currently connected NFC device and establish a new connection with the more recently touched NFC device.

Rationale

By touching the devices at specific, designated touchpoints, the user has clearly expressed the intention to connect the devices and continue using the same type of service with the newly touched device. The most recent touch should always have a higher priority than previous touches, as it represents the latest intention of the user.

A consequence of this rule is that an NFC accessory device can only be actively connected with a single NFC device at a time.

Note: This recommendation applies only if the connection is established via NFC and the newly touched NFC device requests the same type of service as previously connected NFC device. Parallel connections to multiple devices should still be possible using other means of establishing connection or when different types of services are used by the different NFC devices.

Flow example:

1. The user touches NFC device A to an NFC accessory device.
2. NFC device A discovers the NFC tag of the NFC accessory device and reads the stored NDEF message.
3. NFC device A is connected to the NFC accessory device, such as for audio streaming.
4. The user detaches NFC device A from the NFC accessory device.
5. The user touches NFC device B to the NFC accessory device.
6. NFC device B discovers the NFC tag of the NFC accessory device and reads the stored NDEF message.
7. The user detaches NFC device B from the NFC accessory device.
8. If NFC device B requests the same service as NFC device A from the NFC accessory device (e.g. audio streaming), NFC device A is disconnected from the NFC accessory device.
9. NFC device B is connected to the NFC accessory device, such as for audio streaming.

3: Connecting to a new accessory device

Recommendation

When an NFC device that currently has an active connection with an NFC accessory device is touched to another NFC accessory device of the same type, it should disconnect from the currently connected NFC accessory device and establish a new connection with the more recently touched NFC accessory device.

The type of an NFC accessory device refers to the combination of the function offered by the device and the carrier used; for example, a Bluetooth speaker and a Bluetooth headset are of the same type.

Rationale

By touching the devices, the user has expressed the intention to connect the devices. The most recent touch should always have a higher priority than previous touches, as it represents the latest intention of the user.

A consequence of this rule is that an NFC device can only have an active connection with a single NFC accessory device of a given type at any one time.

Flow example:

1. The user touches an NFC device to NFC accessory device A.
2. The NFC device discovers the NFC tag of NFC accessory device A and reads the stored NDEF message.
3. The NFC device is connected to NFC accessory device A, such as for audio streaming.
4. The user detaches the NFC device from NFC accessory device A.
5. The user touches the NFC device to NFC accessory device B.
6. The NFC device discovers the NFC tag of NFC accessory device B and reads the stored NDEF message.
7. The user detaches the NFC device from NFC accessory device B.
8. The NFC device is disconnected from NFC accessory device A.
9. The NFC device is connected to NFC accessory device B, such as for audio streaming.

4: Connecting via a third device**Recommendation**

By touching a third NFC device, such as an NFC tag acting as a proxy to a NFC accessory device by providing network information and credentials, the NFC device should connect to or disconnect from the NFC accessory device.

In the case of Wi-Fi, the NFC device should request the authorization or inform the user in order to prevent an undesired connection to the network.

Rationale

By touching the third device, the user has expressed the intention to connect to or disconnect from the target network.

Bluetooth-specific Recommendations

1: Use of all supported profiles**Recommendation**

When an NFC device is touched to an NFC accessory device to establish a Bluetooth audio connection, all audio-related Bluetooth profiles supported by both devices should be used for the connection.

Rationale

If only a subset of the possible functionality is used, the user would be confused about which features are available over the connection.

Example

If a NFC-enabled mobile phone is touched to a Bluetooth headset, [A2DP, AVRCP, HFP, and HSP profiles](#) should all be connected.

Simple Secure Pairing with NFC – In-Market Examples

A growing number of consumer electronics manufacturers are taking advantage of the ease and convenience of Simple Secure Pairing with NFC to enhance their customers' use and enjoyment of their products. Below are some representative examples:



Users of the Logitech P710e speakerphone can participate in conference calls quickly and easily by touching their NFC-enabled mobile devices to the speakerphone to make a Bluetooth connection.



Printing from a mobile device becomes as easy as a tap with NFC Simple Secure Pairing and a growing number of Epson and other brand printers.



Drivers get instant access to the music libraries on their mobile devices when they use NFC-enabled Simple Secure Pairing to establish a Bluetooth connection with Sony in-car media receivers and CD players.



Smartphone users can begin enjoying the 360-degree 4K video capabilities of Samsung's GEAR 360 digital camera with just a tap of the two devices.



Business users on the go can set up and deliver presentations in seconds using NFC to pair their devices with Epson ultra-mobile business projectors.



The Touch & Print feature on Canon PIXMA printer enables users to print a photo or document by simply opening the Canon PRINT App and tapping their NFC compatible Android device to the printer.

Conclusion

Simple Secure Pairing with NFC is one of the best ways to improve the experience for people using wireless devices. For IoT device manufacturers, it can help ensure that users of your products can enjoy using them immediately and often. By following the guidelines in this document, developers can build user-friendly solutions that take maximum advantage of NFC technology to help ensure fast, easy connections for users, reduce support costs, improve security, and save power.

To learn more about Simple Secure Pairing and view additional use cases, please visit the [NFC Forum](#) website.

Appendix

More about the NFC Forum

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

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

The NFC Forum's Sponsor members, which hold seats on the Board of Directors, include leading players in key industries around the world. Interested companies are invited to become NFC Forum members and to help accelerate the delivery of exciting new NFC solutions to consumers and businesses. Membership levels accommodate companies across a wide range of industries at different phases in NFC solution development. Learn more about becoming an NFC Forum member at our [website](#).

NFC Forum Specifications

An important part of the work of the NFC Forum is developing and distributing specifications, so as to enable development of NFC products and services and facilitate interoperability. At the time of this document's publication, 23 NFC Forum specifications have been approved, spanning these core functions:

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

A list of all published specifications – with links to download them -- is available on the NFC Forum [website](#).

NFC Compliance and Interoperability

The NFC Forum Compliance Program establishes a strong foundation for NFC implementations and fosters a gold standard of confidence and credibility to advance Near Field Communication technology. By fully embracing the NFC Forum Compliance Program, NFC Forum Members ensure a flourishing NFC and IoT ecosystem.

Participation in the NFC Forum Compliance program is available only to NFC Forum member organizations. Companies interested in becoming NFC Forum members should visit the [Join the Forum](#) page.

The NFC Forum operates two programs to meet compliance and interoperability: the NFC Forum Certification Program and Plugfest events.

NFC Forum Certification Program

The NFC Forum Certification program confirms an implementation's compliance to NFC Forum specifications. Conformance to the specifications provides consistency of behavior across NFC-enabled devices and sets the foundation for interoperability. NFC Forum members facilitate the development and market availability of products that comply with NFC Forum specifications through participation in the NFC Forum Certification Program.

Available exclusively to NFC Forum members, [NFC Forum Certification](#) affords differentiation by shortening the adoption process, lowering adoption costs, and making it easier for partners to work together. Certification is granted through a top-notch testing process for implementations that meet [NFC Forum Device Requirements](#). NFC Forum defines different device classes. An NFC Forum Universal Device is a device capable of operating in NFC Forum Peer-to-Peer Mode and/or NFC Forum Reader/Writer Mode that may also support NFC Forum Card Emulation Mode. An NFC Forum Reader/Writer Device is capable of operating as Initiator and Reader/Writer. An NFC Forum Tag Device, implements at least one tag communication protocol. Because NFC Forum-certified implementations are easier to integrate, they are always recommended. Companies cannot claim NFC Forum compliance without successfully completing the certification process.

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

NFC Forum Plugfest Events

NFC Forum Plugfest events, open to both Forum members and non-members, are designed to support early adoption of the NFC Forum specifications by providing a safe, real-world environment where device, tag, and test tool interoperability can be verified across manufacturers' products. This program complements conformance testing under the Certification Program and fosters interoperability of NFC implementations.

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

NFC Modes

NFC Forum Universal Devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer. The NFC Forum technical specifications unlock the full capabilities of NFC for the different operating modes and are based on the ISO/IEC 18092 NFC IP-1, JIS X 6319-4, ISO/IEC 14443 and ISO/IEC 15693 contactless smart card standards (referred to as NFC-A, NFC-B, NFC-V and NFC-F in NFC Forum specifications).

- **Card emulation mode** enables NFC devices to act like smart cards, allowing users to perform transactions such as purchases, ticketing, and transit access control with just a touch.
- **Peer-to-peer mode** enables two NFC devices to communicate with each other to exchange information and share files. Peer-to-peer mode is standardized on the ISO/IEC 18092 standard and based on NFC Forum's [Logical Link Control Protocol Specification](#).
- **Reader/writer mode** enables NFC devices to read information stored on inexpensive NFC tags.

A NFC Reader/Writer Device is a sub-set of a NFC Forum Universal Device, as it acts only in Reader/Writer mode or as Initiator.

A NFC Tag Device implements at least one tag communication protocol as defined in the Tag Type specifications.

Terminology, Abbreviations, and Acronyms

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

Glossary

Term	Definition
Bluetooth	Short-range (10-100m) wireless communication protocol
Card Emulation Mode	Card emulation mode enables NFC Universal Device to act like a smart card, allowing users to perform transactions such as retail purchases and transit access with just a touch. This mode is capable of functioning when the device is powered-off, although it is the service provider's decision whether to allow this. An example is where a NFC Universal device acts as an NFC tag.
NDEF Application	The logical, higher-layer application on an NFC device that uses NDEF as a means to exchange information with other NFC devices or NFC Tags.
Near Field Communication	Near Field Communication (NFC) complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B, ISO/IEC 15693 and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and enables a consumer to utilize one device across different systems.
NFC Accessory Device	An accessory or a single-purpose device e.g. a speaker or printer that has NFC capability implemented.
NFC Data Exchange Format (NDEF)	The NFC Data Exchange Format (NDEF) specification ensures a uniform format for data exchange in any NFC application. It defines the data structures for the exchange of information.
NFC-Enabled Device	An NFC-enabled device, also called an NFC device, is a device that is capable of performing near field communication.
NFC Tag	A contactless tag that can store NDEF information and can be accessed by an NFC device
Peer-to-Peer mode	Peer-to-peer mode enables two NFC devices to communicate with each other to exchange information and share files. Users of NFC-enabled devices can quickly share contact information and other files with a touch. Two NFC-enabled devices create a connection to share information. Peer-to-Peer mode is based on NFC Forum Logical Link Control Protocol (LLCP).
Reader/Writer mode	Reader/writer mode enables NFC devices to read information stored on inexpensive NFC tags embedded in smart posters and displays. NFC-enabled devices can access information from embedded tags in smart posters. An example is when an NFC device reads an NFC tag or device acting in card emulation mode
User Interface	A user interface is the system by which users interact with a machine. The user interface includes hardware and software components. On a mobile device the software component of a user interface is realized through a mobile application (app).
Wi-Fi	Wireless Fidelity -- wireless networking technology based on IEEE 802.11 standards

Acronyms

Acronym	Description	Acronym	Description
BT	Bluetooth	NFC	Near Field Communication
LLCP	Logical Link Control Protocol	RF	Radio Frequency
NDEF	NFC Data Exchange Format	Wi-Fi	Wireless Fidelity