NFC FORUM

Technology Roadmap Series

2026

NFC-FORUM.ORG

NFC Forum Publishes Its Latest Technology Roadmap

Six key initiatives are highlighted, offering an insight into the future of NFC tech

NFC Forum, the global standards body for Near Field Communication (NFC) technology, has today announced its latest roadmap for the development of NFC Forum Standards and its corresponding technical capabilities. New topics to be progressed over the forthcoming years include faster data rates, end-to-end application testing, and security advancements. Additionally, ongoing work will continue to evolve the NFC Wireless Charging offer, advance multipurpose tap and explore new digital key requirements.

The roadmap was collaboratively developed by the NFC Forum Board members - including representatives from Apple, Google, Huawei, Identiv, Infineon, NuCurrent, NXP Semiconductors, Sony, and ST Microelectronics - in consultation with the NFC Forum membership and industry partners to ensure anticipated market requirements are addressed.

The six key roadmap priorities include

Faster Data Rates

Exploring the potential to increase the standardized current rate at which data can be transferred between two devices by up to eight times, delivering a smoother and more responsive NFC user experience.

Improving Reader Mode Interoperability

Providing end-to-end interoperability testing to confirm that new and updated applications successfully and consistently operate on NFC Forum Certified Devices, improving NFC Reader Mode reliability across all use cases.

Security Advancements

Publishing NFC Forum's first-ever NFC Controllers Security Profile, as well as looking to future proof NFC security protocols against Post Quantum Computing threats and strengthening NFC against relay-based attacks.

Wireless Power Evolution

Commencing work on the next generation of NFC Forum Wireless Charging Specifications to define device category specific profiles, support devices with multiple wireless charging receivers, and deliver higher charging power levels.

Multi Purpose Tap

Defining the technical proposals required to bring the concept of supporting several actions with a single 'tap' to market. This includes the ability of the NFC Reader to specify and request the specific credentials needed to perform a user action.

Digital Keys

Exploring innovative new digital key experiences to ensure NFC Forum Standards support a range of industry requirements.

Faster Data Rates

Q&A with **Frank Dawidowsky**, Secretary at NFC Forum, and **Andreas Woerle**, Co-Chair of the Analog and Digital Working Group at NFC Forum

NFC Forum is exploring the possibility of increasing the rate at which data can be transferred between two devices. This would see the current rate of 106 kilobits per second (kbps) available for NFC-A/B, increase up to a rate of 848kbps. This increase of up to eight times the current rate would allow data packets to be transferred faster, delivering a smoother and more responsive user experience.

Frank Dawidowsky (FD) and **Andreas Woerle** (AW) share insights into NFC Forum's objectives for this advancement and what this means for the wider marketplace.

Faster data rates have been possible for some time, with many chips already capable of operating at 848kbps. Why is the NFC Forum looking to standardize faster data rates now?

FD: The use cases for NFC have flourished in recent years, thanks to a proliferation of connected devices across ecosystems including access control, digital keys, digital identity, smart mobility and IoT. But as these ecosystems mature to provide a more comprehensive offer to customers, they require richer, larger data packets. Faster data rates will therefore allow these heavier payloads to be delivered with the same 'tap-and-go' transaction flow that NFC users expect.

This work is further motivated by the need to be able to deliver quantum-ready solutions, as and when these are required. The cryptographic algorithms necessary to mitigate the quantum threat dictate the exchange of more data. Faster data rates may, therefore, also be desirable to avoid a slower user experience.

What work does NFC Forum need to undertake to make faster data rates a reality?

AW: The Digital Protocol Specification would only require a relatively minor update, while the Analog Specification would need to undergo a significant update to reflect the modulation requirements that come with faster data rates. Creating appropriate testing, however, is even more complex. At elevated data transfer speeds, a higher bitrate can lead to different antenna designs, and so new testing equipment and protocols are needed to ensure that devices maintain performance, consistency and reliability.

As faster data rates would also impact the shape of the analog signal encoding the binary information, it is also important to ensure that devices can interoperate with those of other liaison partners. Conducting comprehensive mapping against ISO/IEC 14443 to ensure the analog waveform stays within the defined boundaries, is also vital.

What use cases will benefit most from the change in the NFC Forum Standard?

FD: NFC Forum's move for faster data rates has been driven by a number of its members and liaison partners who are looking to evolve their NFC-based solutions to meet future use case requirements.

Identity solutions such as NFC-enabled passports and digital IDs would be able to reduce their dependence on connection handovers. For example, when reading a mobile driver's license (mDL) that includes a large data package with imagery, NFC may be used to initiate the transaction, but WiFi or Bluetooth often finalizes the communication. Faster data rates would allow NFC to complete the full data exchange.

AW: Similarly, industry leaders in access control, like those providing door locks, are echoing calls for faster data rates to optimize their solutions. Stronger cryptography and dynamic authentication protocols require larger key sizes, meanwhile new access control features such as temporary access permissions further expand the packet size. As these solutions are often deployed outside, in high throughput areas, or in noisy RF environments, making sure that verified users can keep moving at speed is important.

What is its impact on the wider NFC user community?

FD: Any changes undertaken by NFC Forum are carefully considered and communicated to our partners. Ensuring industry harmonization is crucial to avoid interoperability issues. The role of NFC Forum, however, is broad. NFC technology is embedded across a range of markets and use cases, and the long-term requirements of each must be supported.

AW: This is another reason why testing is key; we recognise that more options also mean comprehensive testing to avoid interoperability issues in the field.

What is the timeline to deliver this work item?

AW: While the technical elements and specification adjustments are likely to materialize quickly over the coming year, defining the certification requirements and creating the testing protocols will take longer. There is, however, a strong commitment from the Forum to deliver this update in a timely manner to support the identity and access control communities.

Reader Mode Interoperability

By **Michael Stark**, *Board Vice Chair at NFC Forum,*
and **Frank Dawidowsky**, *Secretary at NFC Forum*

NFC Forum plans to deliver end-to-end interoperability testing to confirm that new and updated applications successfully and consistently operate on NFC Forum Certified Devices. The outcome of this activity is to improve NFC Reader Mode reliability across all use cases.

NFC Forum Board Members **Michael Stark** (MS) and **Frank Dawidowsky** (FD) share with us the importance of this work item, how it might be delivered and potential timeframes.

What are the different elements on NFC Reader Mode that need to be tested?

MS: NFC technology communicates in three ways: Card Emulation Mode, which allows a device to act as a smartcard for access control or to make a payment; Peer-to-Peer Mode, enabling two devices to exchange data directly; and Reader Mode, where a device can read and write data on a passive NFC tag or perform a transaction with another device in Card Emulation Mode.

In Reader Mode, the device generates an electromagnetic (EM) field, which a passive NFC tag can then use to power up its electronics when it is brought within range. The reader device provided field is employed to exchange authorized data between the two devices.

The reader device provided EM field defines the operating volume available for successful data exchange. The aim of the end-to-end testing program is to specify a testing methodology and environment to check consistent performance when reading from, or writing to, tags of any Tag Type within any position of the operating volume.

How is NFC Reader Mode being used, and what are the use cases that will benefit from the proposed testing?

FD: There are already many valuable use cases using Reader Mode today. For example, allowing individuals to check the value on a transit card by tapping it on their smartphone or enabling electronic passport holders to view their data in a similar way. An increasingly important use case is accessing the digital product passport (DPP) information of how to re-cycle and re-use a product.

Reader mode payments, otherwise known as Tap-on-Mobile payments or SoftPOS, are another popular example, allowing merchants to use their own NFC-enabled reader device such as a smartphone or wearable to accept contactless payments. This helps lower the barriers of adoption for digital payment acceptance, encouraging financial inclusion across a range of payment platforms.

While the opportunities are endless, for users to accept and adopt reader mode payments, it is essential that the technology can interoperate consistently to achieve familiarity, trust, ease and convenience amongst users.

Is testing not already undertaken?

FD: There are application specific tests that can be performed to support individual use cases, such as certain types of payment and proprietary vendor tests. NFC Forum's offering, however, would be the first overarching standardized NFC Reader Mode interoperability testing that would be delivered end-to-end across all use cases. This would make it an essential foundational testing tool, and has huge potential in achieving a globally standardized and expected technical baseline.

How does NFC Forum plan to deliver the testing?

MS: We are still in the planning stage around the mechanics of deploying the tests. Initial work is focused in developing a testing app that will support OS application developers in ensuring new and updated apps successfully operate on NFC Forum Certified Devices.

FD: Additionally, the vision is to share reference test cards and devices to support developers. A decision on whether the final tests are performed by an individual company or qualified laboratory will be made over the coming months as we investigate the commercial practicalities of using the tests.

When is this testing offer scheduled to launch?

FD: There is still much work to do, but we are hopeful that this will be delivered in 2026, with a clear action plan for new iterations and testing cycle management.

Security Advancements

By **Andreas Woerle**, *Analog and Digital Working Group Co-Chair,*
Marc Lajon, *Security Working Group Chair, and* **Jean-Rémi Ruiz**, *Board Vice Chair*

Technology has transformed our lives for decades. With every new advancement, however, comes new, malicious threats. Ensuring technology is robust, trusted and secure is paramount. Within the NFC Forum Technical Committee, the Security Working Group with Analog & Digital Working Group at different layers, define security specifications, and also provide methodology for evaluating Product NFC Controller Security.

Security features strongly in the latest NFC Forum Technology Roadmap covering three key areas:

Future proofing NFC security protocol against Post Quantum Computing threats

Quantum computing will redefine cryptographic security. NFC Forum is planning to assess the impact of Post-Quantum Cryptography (PQC) on NFC systems, considering complexity algorithms, memory, and processing power constraints.

The Technical Committee and its Working Groups are sensitive to the commercial and operational impact PQC may have on the wider NFC community, and the requirement to define suitable and realistic standards in a timely manner that is workable to the community.

The Forum aims to evolve standards, such as NFC Authentication Protocol (NAP), to ensure resilience against PQC threats and maintain secure NFC communications for the long term. As part of this initiative, integration of NAP within protocols like Tag NDEF Exchange Protocol (TNEP) is in progress to strengthen authenticated data exchange between smartphones and IoT devices.

Establishing a global NFC security framework

To create a consistent security foundation, NFC Forum has approved the draft specification and will be publishing its first-ever NFC Controllers Security Profile Specification in 2026. This profile outlines security requirements and guidance for chipset implementing NFC technology to counter recognized and potential threats.

Following on from the launch of this work, NFC Forum is developing an evaluation outline to be used by independent third-party laboratories to confirm that products are compliant against the NFC Controller Security Profile. Additionally, the Forum intends to collaborate with liaison partners to further promote this work across industries.

By creating a globally recognized security baseline, developers and vendors will have a clear reference on NFC security expectations. NFC user communities can confidently define their security needs and select products that conform to a specified, well understood standardized NFC Controller Security Profile.

Strengthening NFC against relay-based threats

Relay attack, where an attacker intercepts and transfers over a long distance a legitimate communication between an NFC card and reader, is a threat and poses a risk to NFC-enabled systems. NFC Forum is investigating applying the mechanism being specified by ISO/IEC 14443 to all NFC technologies to strengthen defenses against such attacks.

These improvements aim to safeguard against criminal activities such as unauthorized vehicle or building access and fraudulent transactions, including illegal payments.

While the role of NFC Forum is to develop interface specifications at the physical and data link layers rather than define application-specific security requirements, it is acknowledged that addressing relay attacks cannot be prevented by application cryptography alone.

Therefore, the Analog & Digital Working Group is researching additional protective measures at the data link layer to ensure robust security. This involves analysis and research by the industry experts within the NFC Forum member companies, as well as monitoring ISO developments.

Updates will incorporate relay attack protection mechanisms into NFC technical specifications to make relay attack protection a global standard.

Wireless Power Evolution

By **Michael Stark**, *Board Vice Chair at NFC Forum,*
and **Jacob Babcock**, *Board Member at NFC Forum*

The NFC Wireless Charging Standard was developed to address the ever-growing requirement to charge small IoT devices. With the current ability to provide negotiated power up to 1 Watt, this standard delivers a range of unique benefits to the market with a flexible antenna design and enables sealed product housings to avoid corrosion issues with pin connectors.

Central to the wireless charging drive, however, is sustainability and the necessity to remove contact charging waste, including countless charging cables and disposable batteries; something that the EU Common Wireless Charging efforts aim to address. While basic physics dictate that 'a one-size-fits-all' approach is not feasible, defining single charger standards per device type would offer industry clarity.

NFC Forum is committed to supporting the EU in this endeavor. The NFC Wireless Charging 2.0 Specification recently passed the final draft international standard (FDIS) in ISO and will soon be adopted by the International Electrotechnical Commission (IEC) / Technical Committee 100 to become globally recognized as part of the IEC Standard 63652. Something the Forum looks forward to communicating in more detail.

But this is not the end of our work on wireless charging and power; in fact, it is the beginning. As technology advances, so must the standard. After five years within the marketplace, NFC Forum is looking to begin its next iteration and update the specification to address new market requirements to achieve higher charging power levels and device category specific requirements.

Define device type specific profiles

The NFC Wireless Charging 2.0 Specification currently supports an open ecosystem, compliant to Class 6 antennas, meaning that it covers a wide range of devices with variations in their physical layout and electrical properties for specific applications. There is a need to reduce this scope with wireless charging profiles to help manufacturers in their design.

Creating unique profiles for individual products / device classes would enable NFC Forum to detail specific wireless charging requirements per use case. An example of this is the past success with the Universal Stylus Initiative (USI), which promotes a unique technical standard for interoperable active pen styluses. The Forum's digital pen cooperation introduced the Reference Equipment with Class 7 antennas.

This experience showed that activity could ease design requirements for the manufacturer and improve efficiency, allowing charging to be completed in a manner suitable for that specific product. The introduction of an ecosystem specific wireless charging profile is also expected to accelerate the adoption of NFC Wireless Charging solutions, as it will make it easier for product managers to implement the technology.

Devices with multiple wireless charging receivers

The NFC Forum is exploring how NFC Wireless Charging Standards might be extended to support devices with multiple charging receivers. While technical challenges exist, the aim is for this innovation to allow wireless power from a single poller to be received at the same time by more than one listener in a device's operating volume. Compared to hardware connectors, this innovation would offer new design opportunities for product designers.

A potential use case of this innovation is Smart Glasses. When folded for storage, product designers could use this new standard to charge batteries in each temple at the same time, since they would be aligned and in close proximity in a case. For a variety of reasons, this could drastically simplify charging for these new devices.

Optimized charging up to 3 Watts from 1 Watt

Extending the charging capabilities of NFC Wireless Charging was introduced as a concept in NFC Forum's last Technology Roadmap. The value of the work is significant, as it would reduce charging times for existing use cases and potentially support new ones.

While the premise is simple, the ambition is high. All parts of the NFC chip and overall system design must be able to support the extended charging function. Another consideration is that all the test equipment, which is currently only qualified to assess products up to 1 Watt, needs to be updated to validate that products will perform at the extended power safely.

Over the last few years, time has been taken to assess the work and resources required to achieve this considerable work item, which is predicted to take 3 to 4 years to accomplish once member resources are allocated. With NFC Release 15 launched, NFC Wireless Charging extension is expected to be one of the next technical focuses of the NFC Forum experts.

Multi-Purpose Tap: Improving Contactless Experiences

Multi-Purpose Tap is a concept that has been emerging over the last few years, whereby users would be able to leverage the capability of NFC devices to allow both reading and writing of data across a connection to complete multiple actions at the same time. This would mean that transactions that would typically require multiple stages can be completed quickly and easily with 'just one tap'. For example, when making a purchase in store, the payment could be made, and simultaneously any loyalty points would be awarded and a receipt sent all at once.

Seamless Service Discovery

One of the building blocks of a Multi-Purpose Tap solution will be the ability of NFC Reader Devices to specify and request specific credentials needed to perform a user action. Today, payment reading devices are able to request the preferred payment card from a mobile wallet to complete that transaction. The NFC Forum is exploring how new industry standards might enable a broader ecosystem of use cases so that NFC Readers of all types could request relevant credentials to complete a desired action.

The benefit to users is an improved user experience, whereby all credentials can be stored and accessed directly through a digital wallet. In the future, this could allow all forms of ID cards, digital keys, travel and event tickets, along with countless other credentials, to be accessible with a simple tap – and require no additional input from the user.

Strong User Interest

Time and again, when the NFC Forum and our research partners survey end consumers and product designers alike, the promise of Multi-Purpose Tap has strong appeal. The challenge with this concept is that unlike most NFC compliant product connections, many of the expected use cases require integration with back-office systems and service providers.

The NFC Forum continues to host meaningful conversations to progress the broader vision of Multi-Purpose Tap, and tangible steps like Service Discovery demonstrate meaningful progress and strong market interest for the concept.

The Value of Standards

Due to the extensive global adoption of NFC Forum Standards on smartphones, NFC Forum is well-positioned to advance the Multi-Purpose Tap initiative. While still in the ideation phase, subject matter experts from a number of verticals have come together within the Forum to collaborate on the next phase of the project. Their current work aims to determine a clear technical proposal for this feature and define how it will operate.

Our remit is to define baseline functionality to ensure technical interoperability across NFC Forum-certified devices. With multiple different markets and functionalities needing to align, defined and trusted standards play a critical role in specifying the guidelines of interaction between devices. This ensures that different applications do not disrupt or impact another service or component, ensuring that products perform as expected on a consistent basis, and deliver a seamless user experience regardless of the hardware used on either side of the transaction.

Enhancing NFC Digital Keys

Popularity of digital key solutions based on NFC Forum technologies is growing thanks to the seamless, convenient key management solutions they offer.

Following the success of its collaboration with the Car Connectivity Consortium (CCC) and Intelligent Car Connectivity Ecosystem Alliance (ICCE), the NFC Forum is opening its door to explore innovative new digital key experiences, ensuring NFC Forum Standards support a range of industry requirements both in and outside of the automotive sector. As part of its Technology Roadmap, it is seeking market engagement on how its standards can evolve.

There are at least three potential areas that will be explored further.

Key Form Factor Flexibly and Simplified Management

While the smartphone has been the primary host for digital keys so far, we're seeing an increasing number of new personal devices that are equally capable of securely hosting and presenting the required credentials.

For example, as NFC has power harvesting capabilities, it can support battery-less devices such as fobs, plastic cards, or even passive wearables, enabling them to use the power from a smart lock to open a door. In reverse, small devices such as battery-less padlocks can draw power from an NFC smartphone to unlock. Removing the need for both sides of the exchange to have a battery enables simpler, more durable, cost-efficient designs.

The ease with which digital keys can be self-provisioned using NFC is also driving interest. Digital keys can be issued or revoked quickly and easily using a smartphone, giving full control to who can access a vehicle, room or building instantly. This creates effective key management potential for car sharing and rental, hospitality and building access.

Hybrid Solutions

Arguably one of the most high-profile digital key initiatives to date has been that of the CCC. Its Digital Key Specification uses NFC to provide secure tap-to-lock / tap-to-unlock functionality across both smartphone and smartcard keys. It successfully uses NFC in concert with other wireless technologies like Bluetooth Low Energy (BLE) and Ultra-Wideband (UWB).

By layering these technologies together, it creates a complementary system that allows the door to be opened as a vehicle owner approaches the car using BLE and UWB, offering completely hands-free entry. While NFC delivers an highly secure user-intent proximity solution that most importantly works even if the user's smartphone is in power reserve mode – something not possible with any other wireless technology

This hybrid model is the perfect blend of convenience, security and reliability, providing other sectors with a best-practice model to replicate and build upon.

More Than Just A Key

An NFC digital key can contain far more than just the credentials required to lock and unlock a door. It can also save individual user profiles that can be automatically applied whenever the user taps their key.

For example, if a vehicle has multiple drivers, then each digital key can also store a personalization profile for settings such as climate controls, seat positioning, and in-car payment accounts which are automatically applied when the vehicle is unlocked.

Furthermore, NFC Forum Standard compliant tags are ideally suited to store Digital Product Passport (DPP) data. The same tag used to provide digital key functionality can store the necessary traceability data that supports enhanced circularity, through effective re-using, re-manufacturing, or re-cycling a product in line with incoming regulation by the European Union.