Near Field Communication (NFC)

Begriff und Funktionsprinzip

Near Field Communication (NFC) ist ein international standardisierter Funkübertragungsstandard für sehr kurze Distanzen im Bereich weniger Zentimeter. Technisch basiert NFC auf induktiver Kopplung im Hochfrequenzbereich bei 13,56 MHz und baut auf bestehenden RFID-Standards (z. B. ISO/IEC 14443) auf. Ein aktives Feld eines Lesegeräts kann dabei einen passiven Transponder (Tag) mit Energie versorgen und Daten austauschen. Durch die geringe Reichweite wird eine räumlich stark begrenzte, bewusst initiierte Interaktion ermöglicht, etwa durch gezieltes Annähern oder Auflegen eines Geräts.

Komponenten und Betriebsarten

Bei NFC wird häufig zwischen dem sogenannten **Initiator** (z. B. Smartphone oder Lesegerät) und dem **Target** (z. B. Karte oder Tag) unterschieden. Initiatoren erzeugen aktiv das elektromagnetische Feld, während viele Targets passiv sind und ihre Energie aus diesem Feld beziehen. Technisch werden drei Betriebsarten unterschieden: Im *Reader/Writer-Modus* liest oder beschreibt ein Gerät NFC-Tags, im *Card-Emulation-Modus* verhält sich etwa ein Smartphone wie eine kontaktlose Chipkarte und im *Peer-to-Peer-Modus* tauschen zwei aktive Geräte direkt Daten aus. Diese Betriebsarten bilden die Grundlage für die typischen Anwendungen von NFC im Alltag.

Typische Anwendungen

NFC wird in vielen kontaktlosen Bezahlverfahren eingesetzt, etwa bei Bankkarten, Smartphones oder Smartwatches im Handel oder im öffentlichen Nahverkehr. Darüber hinaus dienen NFC-Karten und -Transponder der Zugangskontrolle, zum Beispiel in Gebäuden, Hotels oder Car-Sharing-Systemen. NFC-Tags können in Plakate, Produkte oder Objekte integriert werden, um beim Berühren mit dem Smartphone automatisch Webseiten, Apps, WLAN-Zugänge oder Automatisierungen aufzurufen. Im Smart-Home- und Automatisierungsbereich werden NFC-Tags genutzt, um wiederkehrende Abläufe anzustoßen, etwa das Aktivieren bestimmter Szenen, Profile oder Kurzbefehle.

NFC-Tags und Datenspeicherung

NFC-Tags sind kleine, oft auf Folie gedruckte oder in Karten integrierte Chips mit einer Spule als Antenne. Sie unterscheiden sich in Speicherkapazität, Herstellertechnologie und Kompatibilität (z. B. MIFARE, NTAG, verschiedene NFC Forum Tag Types). Die Daten auf einem Tag sind in der Regel sehr kompakt, da häufig nur URIs, kleine Datensätze oder Konfigurationsinformationen gespeichert werden. Für viele Anwendungen werden Inhalte im NDEF-Format (NFC Data Exchange Format) abgelegt, wodurch unterschiedliche Geräte standardisierte Datentypen (z. B. Webseiten-Links, Texte, vCards, WLAN-Konfigurationen) erkennen können. Je nach Tag-Typ lassen sich Daten dauerhaft (read-only) oder mehrfach beschreibbar abspeichern.

Sicherheit, Reichweite und Grenzen

Die geringe Reichweite von NFC reduziert das Risiko ungewollter Ausleseversuche, stellt aber keinen vollständigen Schutz vor Angriffen dar. In sicherheitskritischen Anwendungen wie Bezahlsystemen kommen

zusätzliche kryptografische Verfahren, Signaturen und Protokolle zum Einsatz, die über den eigentlichen Funkstandard hinausgehen. Mögliche Angriffe sind etwa das unbefugte Auslesen eines Tags, Relay-Angriffe mit zwischengeschalteten Geräten oder Manipulationen an schlecht gesicherten Implementierungen. In der Praxis werden Risiken häufig durch Kombination von kurzer Distanz, Benutzerinteraktion (explizites Hinhalten) und höheren Sicherheitsschichten (z. B. Tokenisierung, Secure Elements im Smartphone) verringert. Die Datenrate von NFC ist im Vergleich zu WLAN oder Bluetooth relativ gering, reicht aber für kurze Datensätze und Authentisierungsvorgänge aus.

From:
https://wiki.ct-lab.info/ - **Creative Technologies Lab | dokuWiki**

Permanent link:
https://wiki.ct-lab.info/doku.php/extras:codikon:hardware:nfc?rev=1764914300

Last update: **2025/12/05 05:58**