Transmission of IPv6 Packets over Near Field Communication

draft-ietf-6lo-nfc-18

Younghwan Choi (ETRI),

Y-G. Hong (Daejon Univ.), J-S. Youn (DONG-EUI Univ.), D-K. Kim (KNU)

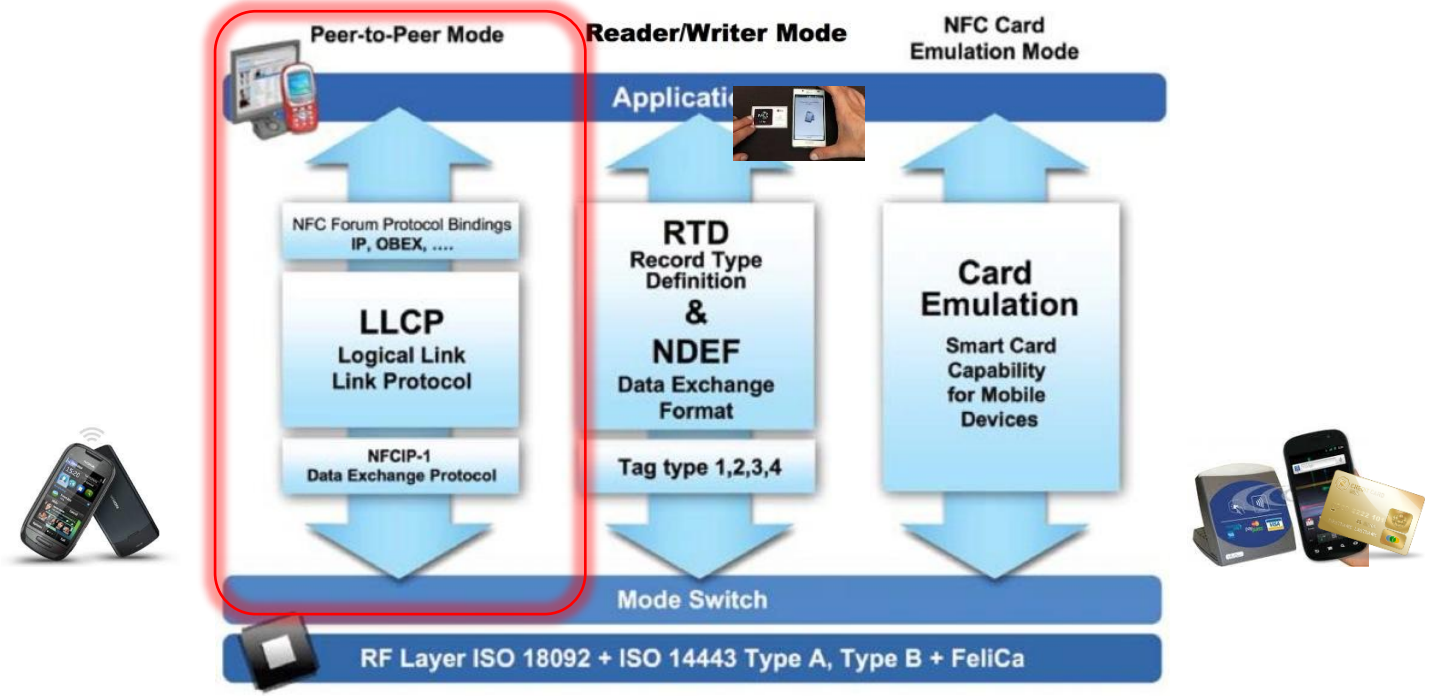
6lo WG Meeting@IETF115 – London, UK

2022. 11. 09.

What is Near Field Communication (NFC) ?

- NFC technology enables (Source: NFC Forum)
  - simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch.
- NFC Functions

  (Source: NFC forum)



History and status of IPv6-over-NFC

Such a long history ☺☺

- **WG Adoption: draft-ietf-6lo-nfc-00** (Mar 03, 2015)
  - Update Stateless address autoconfiguration
- **1st ~ 5th Revision**
  - **ver-01** (July, 2015)
    - MAC PDU size and MTU
    - SLAAC and IPv6 link local address
    - Fragmentation and Reassembly
  - **ver-02** (Oct, 2015) @Buenos Aires
    - Dispatch Header (added)
    - Header Compression (modified for GHC)
  - **ver-03** (Apr. 2016) @Berlin, DE
    - Some typos fixed
    - Section 7. Security Considerations
  - **Ver-04** (Jul. 2016)
    - NFC FAR-related sentence updated
    - Related to "multi-hop topologies"
  - **ver-05** (Oct. 2016) @Seoul, KR
    - Feedback from NFC forum
    - IID generation (feedback from Dave)
- **Revisions for WGLC**
  - **ver-06** (by Dave Thaler, Sep. 2016)
    - IID generation (2nd rev.)
  - **ver-07** (by James Woodyett Jun. 2017)
    - IID generation (4th rev.) ->RFC7217
    - Neighbor Discovery -> Reworded
  - **ver-08,-09** (by Pascal Thubert, Nov. 2017)
    - Neighbor Discovery -> Reworded
  - **ver-10, -11** (by Shepherd, Jul. 2018)
    - Revised texts for clarification about NFC MTU & FAR, ND, Security
- **No more feedback from NFC forum** (since Jan. 2017)
- **WGLC** (Mar. 2018~Jul. 2018) **New Shepherd**: Samita Chakrabarti
  - **ver-11, -12** (by IoTdir & INTdir, Nov. 2018)
  - **ver-13** (1st IESG reviews, Mar. 2019)
  - **ver-14, -15** (2nd IESG reviews, Jul. 2019)
- **1st Telechat**
  - **Ver-16, -17** (1st Telechat reviews, Aug. 2020)
- **2nd Telechat (scheduled on 15/12/2022)**
  - **Ver-18 (15th IETF, London)**

Transmission of IPv6 Packets over Near Field Communication

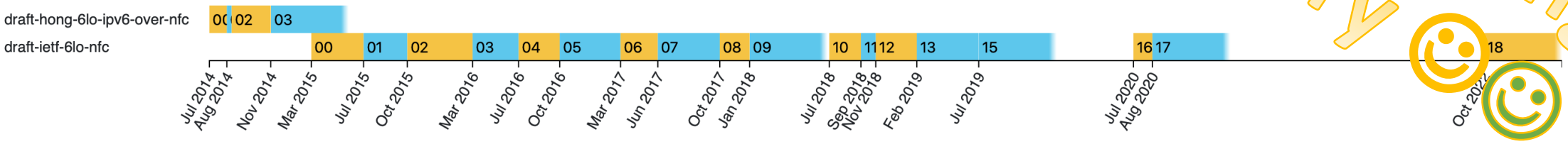
draft-ietf-6lo-nfc-18

Such a long history

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18



Document	**Type**	Active Internet-Draft (6lo WG)
	Authors	Younghwan Choi ✉, Yong-Geun Hong ✉, Joo-Sang Youn ✉, Dongkyun Kim ✉
	Last updated	2022-11-04 (Latest revision 2022-10-22)
	Replaces	draft-hong-6lo-ipv6-over-nfc
	Stream	Internet Engineering Task Force (IETF)
	Intended RFC status	Proposed Standard
	Formats	txt html xml htmlized pdf bibtex
	Reviews	SECDIR Last Call review (of -13) Has Issues GENART Last Call review (of -12) On the Right Track OPSDIR Last Call review (of -12) Has Nits TSVART Last Call review (of -12) Ready with Issues IOTDIR Early review (of -10) On the Right Track INTDIR Early review (of -10) Ready with Nits SECDIR Telechat Review Incomplete, due 2022-12-13
Stream	**WG state**	Submitted to IESG for Publication

Since the previous meeting (114th IETF, US)

- **Comments from Erik,**
  - Revision of § 7. Security Considerations (Jul. 2022)
    -> Revised to Ver. -18 (published on Oct. 2022, *details on the next slide*)
  - Add a new reference, RFC3756 about "sub-IP layer security considerations for IPv6" (Nov. 2022)
    -> Ver.-19 will be published as soon as 6lo session finished in 115th IETF)

Revised to Ver. -18 (published on Oct. 2022)

7. Security Considerations

NFC is often considered to offer intrinsic security properties due to its short link range. When interface identifiers (IIDs) are generated, devices and users are required to consider mitigating various threats, such as correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning.

IPv6-over-NFC uses an IPv6 interface identifier formed from a "short address" and a set of well-known constant bits for the modified EUI-64 format. However, NFC applications use short-lived connections, and a different address is used for each connection, where the latter is of extremely short duration.

7. Security Considerations

LLCP [LLCP-1.4] of NFC provides protection of user data to ensure confidentiality of communications. The confidentiality mechanism involves the encryption of user service data with a secret key that has been established during link activation. LLCP of NFC have two mode (i.e., ad-hoc mode and authenticated mode for secure data transfer. Ad-hoc secure data transfer can be established between two communication parties without any prior knowledge of the communication partner. Ad-hoc secure data transfer can be vulnerable to Man-In-The-Middle (MITM) attacks. Authenticated secure data transfer provides protection against Man-In-The-Middle (MITM) attacks. In the initial bonding step, the two communicating parties store a shared secret along with a Bonding Identifier. For all subsequent interactions, the communicating parties re-use the shared secret and compute only the unique encryption key for that session. Secure data transfer is based on the cryptographic algorithms defined in the NFC Authentication Protocol (NAP).

Furthermore, NFC can be considered to offer intrinsic security properties due to its short link range. When interface identifiers (IIDs) are generated, devices and users are required to consider mitigating various threats, such as correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning. However, IPv6-over-NFC uses a random (but stable) identifier (RID) [RFC7217] as an IPv6 interface identifier, and NFC applications use short-lived connections, and a different address is used for each connection, where the latter is of extremely short duration.

Next Steps

- Revision for Ver.-19 (on Nov. 2022)
- 2nd Round of Telechat on 15/12/2022

Any Questions & Comments?