Ecma/TC47/2008/089
(Rev. 1 – 18 December 2008)

SECURITY

NFC-SEC

NFCIP-1 Security Services and Protocol

Cryptography Standard using ECDH and AES

White paper

Dec 9, 2008

Table of contents

1 Introduction

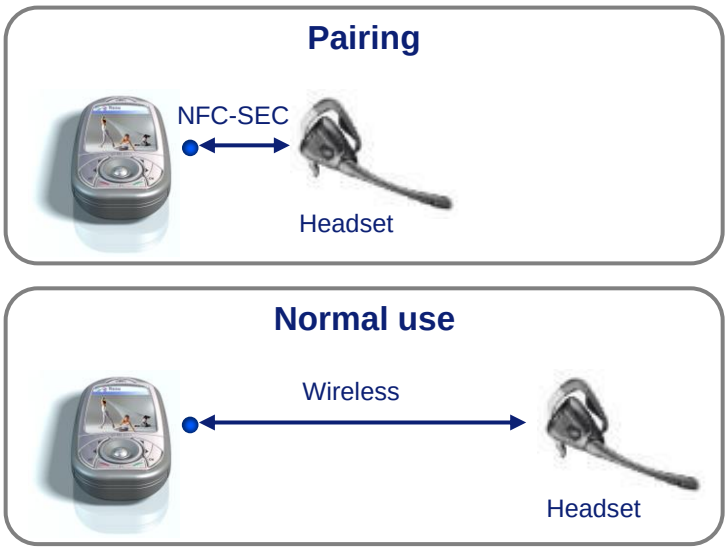
NFCIP-1 is standardised in ECMA-340. It specifies the signalling interface and protocols for Near Field Communication (NFC) which is a wireless communication technology for closely coupled Consumer Electronic devices.

The complementary series of NFC security standards (NFC-SEC) defines a protocol stack that enables application independent and state of the art encryption functions on the data link layer, on top of NFCIP-1.

2 Use Cases

NFC security standards will be deployed for all those NFC connections which require protection against eavesdropping and data manipulation and which do not necessarily require application specific encryption mechanisms.

A typical example is the initial association ("pairing") of devices for longer range wireless communications. Bluetooth or WiFi pairing protocols will use NFC security standards to exchange security-sensitive connection contexts on a protected NFC connection before switching to their respective longer range wireless technologies.



Secure pairing of wireless devices with NFC

3 Standards Series Structure

The modular concept for NFC security standards simplifies the specification and allows for easy future extensibility, as illustrated in Figure 1.

A common framework standard, which defines the services, the PDUs and the protocol is specified in ECMA-385 NFC-SEC: NFCIP-1 Security Services and Protocol standard.

The common framework is complemented with ECMA-386 NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES. It specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the Advanced Encryption Standard (AES) algorithm for data encryption and integrity.

More cryptography standards may follow in the future, each of them identified by a Protocol IDdentifier (PID).

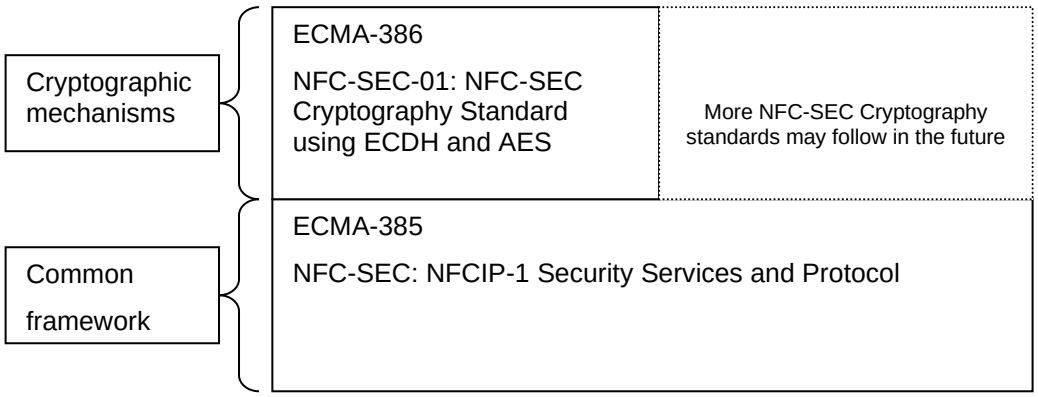


Figure 1 - Structure of the NFC-SEC standards series

4 The Services

NFC-SEC defines two services, as illustrated in Figure 2.

The Shared Secret Service (SSE) establishes a shared secret between two peer NFC-SEC Users, which they can use at their discretion for proprietary encryption mechanisms.

One step further the Secure Channel Service (SCH) uses the shared secret established beforehand for a standardised secure channel service to protect all subsequent communication in either direction according to the mechanisms specified by the cryptography standard.

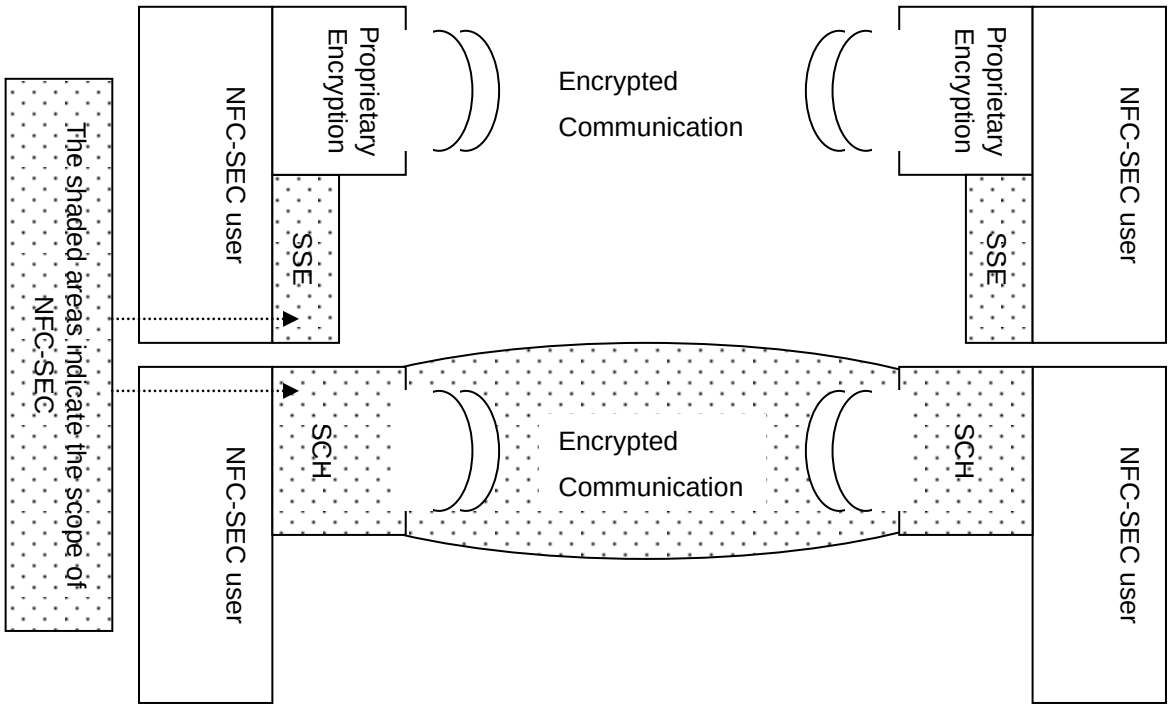


Figure 2 - The NFC-SEC services SSE and SCH

5 The Protocol

Four basic protocol steps are defined, as illustrated in Figure 3.

The steps "key agreement", followed by "key confirmation" are required for both SSE and SCH. "PDU security" provides the actual data encryption and protection, required only by SCH. Finally both SSE and SCH end with a "Termination" protocol step.

NFC-SEC-PDUs are conveyed in NFCIP-1 DEP "Protected PDU"s. For SCH, the protocol provides sequence integrity based on protected sequence numbers.

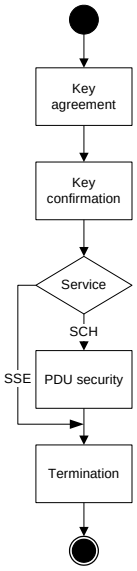


Figure 3 - Basic protocol steps

6 NFC-SEC-01 Mechanisms

NFC-SEC-01 provides the message contents and the cryptographic methods to enable secure communication between NFC devices that do not share any common secret data ("keys") before they start communicating with each other.

Public key cryptography, more specifically the Elliptic Curve Diffie-Hellman key exchange scheme, is used to establish a shared secret between these devices. This shared secret is used to establish the SSE and the SCH. The security parameter of the mechanism is 192 bit.

The mechanism does not protect against Man-in-the-middle (MITM) attacks because no entity authentication can be provided when the peer NFC devices do not share any secret beforehand. The practical risk of MITM attacks is regarded as low in the targeted use cases due to the short operating distance and the specific RF characteristics of NFC [see *Security in NFC (Strengths and Weaknesses)*]. Users should be aware and carefully evaluate the potential vulnerability of planned implementations.

The specified Key derivation function, key confirmation, data integrity checks and data encryption functions are based on AES. Data confidentiality is ensured by AES with 128 bit key length in CTR mode, which is secure and suitable for restricted communication bandwidth because no padding is required.

7 FAQ

Q: why is NFC-SEC limited to NFCIP-1?

A: the reason is that NFC-SEC has dependencies and uses requirements of NFCIP-1 in clauses 9 and 11;

Q: why does NFC-SEC-01 provide no entity authentication?

A: for the addressed use cases the peer NFC devices do not share any common secret. That is why it is not possible to perform entity authentication; future NFC-SEC cryptography standards may address other use cases and then also provide entity authentication;

Q: what is the response to ENC and TMN messages?

A: ENC is acknowledged by another ENC. Upon reception of TMN the protocol goes to IDLE state and does not need to be acknowledged;

Q: why is the content of error messages not specified?

A: the reason is good cryptographic practice to prevent related attacks;

Q: how will the registration of future NFC-SEC cryptography standards work?

A: a publicly available register, maintained by Ecma International will lists those schemes that requesters claim to be fit for use with the NFC-SEC services and protocol and for which the requester provides an URL that points to the publicly available scheme using the request form at the register;

Q: why are Q_A and Q_B used as permanent public keys in NFC-SEC-01?

A: the way when and how to refresh Q_A and Q_B is out of the scope of NFC-SEC since refreshing may depend on application and implementation of the standard;

Q: how does NFC-SEC react when it detects an attack on the SCH?

A: it simply aborts the SCH and sends an indication to the NFC-SEC user and the peer NFC-SEC entity. The NFC-SEC user can then decide either to abort the transaction or to re-establish the SCH with new keys.

8 Related Standards and References

NFC security standards are based on well established international standards and most were developed by ISO/IEC JTC1/SC27.

The framework reference ISO/IEC 11770-1 and the basic model is based on ISO/IEC 7498-1, the security architecture of ISO 7498-2 is deployed and the conventions for the definition of OSI services from ISO/IEC 10731 is adopted.

The NFC-SEC cryptography standard uses the general specifications of ISO/IEC 15946-1 and the key management mechanisms using asymmetric techniques of ISO/IEC 11770-3. Block ciphers of ISO/IEC 18033-3 are referenced and the modes of operation for an n-bit block cipher of ISO/IEC 10116 are deployed. IEEE standard 1363 specifications for Public-Key Cryptography and FIPS 186-2 Digital Signature Standard are referenced. ISO/IEC 18031 is used for Random bit generation.

Further NFC standards published as of October 2008:

1) ECMA-340 “Near Field Communication – Interface and Protocol (NFCIP-1)”
2) ECMA-352 “Near Field Communication Interface and Protocol – 2 (NFCIP-2)”
3) ECMA-356 “NFCIP-1 - RF Interface Test Methods”
4) ECMA-362 “NFCIP-1 - Protocol Test Methods”
5) ECMA-373 “Near Field Communication Wired Interface (NFC-WI)”

8.1 Other references

Security in NFC (Strengths and Weaknesses) by Ernst Haselsteiner and Klemens Breitfuß:

http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

Ecma International:

http://www.ecma-international.org