Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14140
Date:	2009-11-25
Replaces:	
Document Type:	National Body Contribution
Document Title:	NB of Switzerland's contribution on the security models
Document Source:	National Body of Switzerland
Project Number:	
Document Status:	For consideration at the SC6 Study Group meeting in Berlin.
Action ID:	FYI
Due Date:	
No. of Pages:	4

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

NFC-SEC vs. 7816 security model

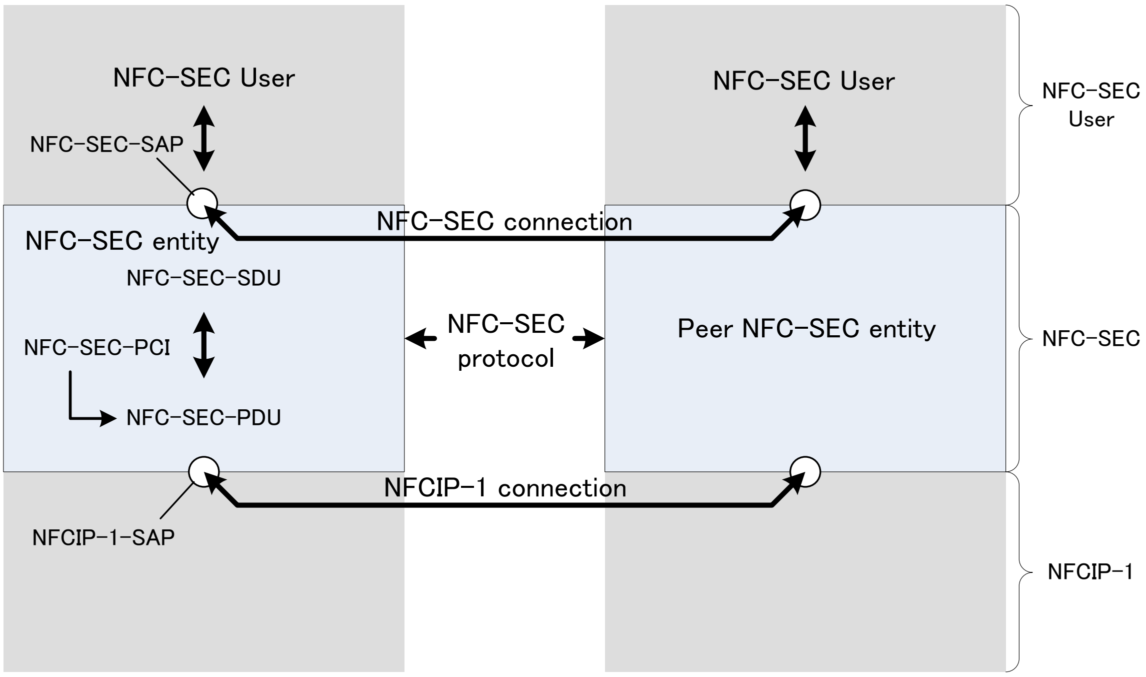
The Swiss NB submits this contribution to Sc6, for consideration under agenda item 2 "Security Models" at the forthcoming Berlin meeting of the Special Group on Harmonization, providing some technical explanation for the Swiss NB position expressed in 6N14063:

Begin of citation from 6N14063:

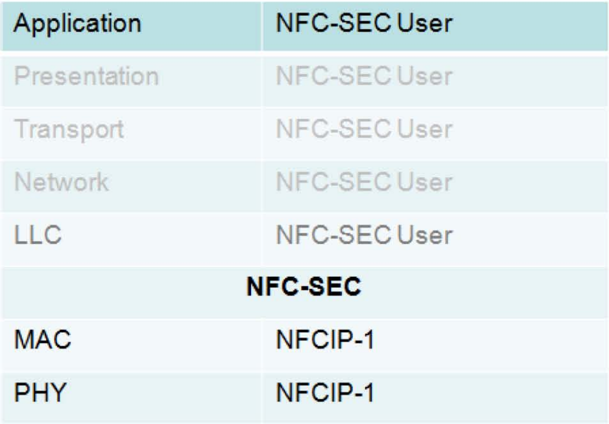
> *NFC-SEC is not an obstacle for interworking of IS 14443 and IS 18092 devices:*
>
> 1. *While IS 13157 defines the use of NFC-SEC in conjunction with IS 18092, the use of NFC-SEC in conjunction with IS 14443, can be easily specified without change of IS 13157, as NFC-SEC is well architected according to IS 7498-1 (the OSI layering model) and IS 7498-2 (the OSI security architecture). Work on such a specification can be launched by a NWIP.*
> 2. *While NFC-SEC is a sub-layer of the Data Link layer, IS 7816 security resides in the application layer. They complement each other (in conformance with IS 7498-2), and there is no conflict between them*.

End of citation.

The following drawing from 13157 shows the relationship of the NFC-SEC layer to the layer below (NFCIP-1) and the layer above (named NFC-SEC User).



18092 defines the PHY and MAC layer of NFCIP-1. Therefore, in the OSI model (see 7498-1), NFC-SEC is a sub-layer of the Data Link Layer. The NFC-SEC User comprises all layers on top of NFC-SEC, i.e. the whole stack from the Logical Link Control (LLC) up to the Application layer, and typically represents the application.

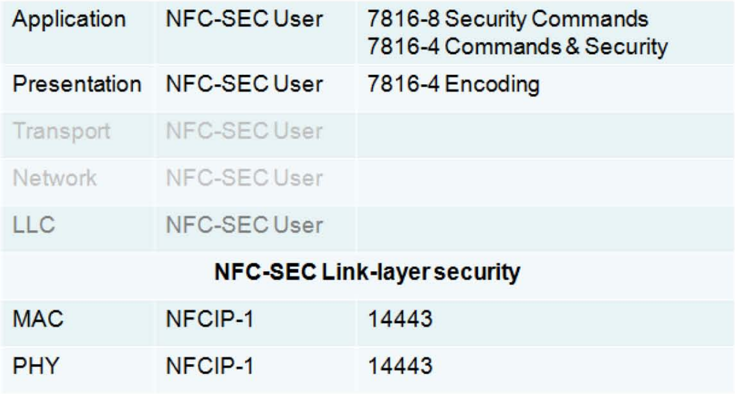


Application	NFC-SEC User
Presentation	NFC-SEC User
Transport	NFC-SEC User
Network	NFC-SEC User
LLC	NFC-SEC User
NFC-SEC	
MAC	NFCIP-1
PHY	NFCIP-1

The NFC-SEC Secure Channel Service provides a secure channel, which, once activated, operates independent from and transparent to the application.

The Shared Secret Channel can be invoked by the NFC-SEC User to establish and deliver a secret shared with the peer entity.

In contrast, 7816-4 and 7816-8 (security commands) reside in the application layer. Therefore the 7816 and 13157 security services are completely independent and complementary, and both can be present and perfectly coexist in one and the same implementation.



Application	NFC-SEC User	7816-8 Security Commands 7816-4 Commands & Security
Presentation	NFC-SEC User	7816-4 Encoding
Transport	NFC-SEC User	
Network	NFC-SEC User	
LLC	NFC-SEC User	
NFC-SEC Link-layer security		
MAC	NFCIP-1	14443
PHY	NFCIP-1	14443

7816 security

- Resides in the application layer (part of the application commands and operation),
- Defines application-to-application security
- Is applied on per-command basis

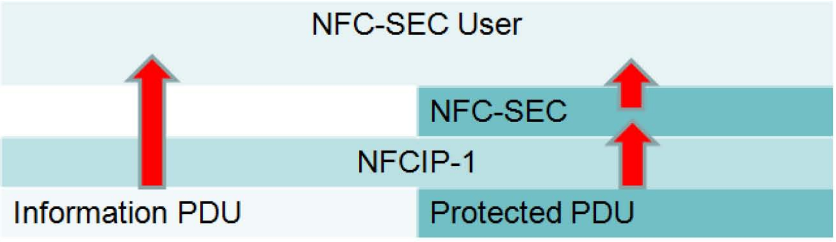
13157 security

- Resides in the link layer (part of link layer operation)
- Defines device-to-device security

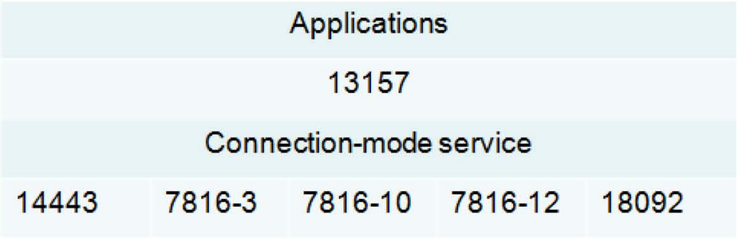
- Provides a transparent Secure Channel (application-independent)
- Establishes shared secrets on behalf of the NFC-SEC User

Implementation of security services in the link layer is foreseen by ISO 7498-2 (the OSI Security Architecture) and common practice in networks, e.g. WLAN security of ISO/IEC 8802-11.

To enable exchange of enciphered and plaintext information, in the next revision of 18092 the Data Exchange Protocol will provide two types of, messages, enciphered and clear. NFC-SEC will apply its processing only to the former type messages, while the latter ones will bypass NFC-SEC. The API enabling applications to select the secure or the plaintext channel, is out of scope of 18092. This feature is a pure 18092 feature. It is independent of 13157 and not required for NFC-SEC operation.



NFC-SEC assumes an underlying Connection-mode service, which peer-NFC-SEC entities use for data exchange. Such a connection-mode service is common to point-to-point protocols such as 14443, 15693, 7816-3, 7816-10, 7816-12 and 18092, and thus also 21481. Therefore NFC-SEC is easily implemented on top of these protocols. Extension to arbitrary connection-oriented protocols is achievable with a suitable adaptation of the sequence integrity service to the (possibly variable) sliding window size of these protocols.



Applications				
13157				
Connection-mode service				
14443	7816-3	7816-10	7816-12	18092