Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14199
Date:	2010-01-28
Replaces:	
Document Type:	Disposition of Comments
Document Title:	Disposition of Comments on the ISO/IEC DIS 13157
Document Source:	Barcelona BRM
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	23

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

Template for comments and secretariat observations	Date: 2009-11-12	Document: **DoC ISO/IEC DIS 13157**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
GB1	Annex B	Table B.1 and B.2	TE	Changes to ISO/IEC 18092 should not be specified in this standard.	Any changes to ISO/IEC 18092 should be carried out in accordance with the ISO/IEC Directives and not specified in this NFC-SEC Fast Track.	Accepted by: Changing the annex B title and introduction of annex B
SG1				All references to ECMA 340 shall be changed to ISO 18092 or ISO 18092:2004 appropriately		Accepted, Already fixed in the ISO/IEC formatted version
SG2				This document shall be named as ISO 13157-1		Accepted
SG3				All reference to ECMA 386 shall be changed to ISO 13157-2 (i.e. the second ballot document)		Accepted
SG4	11.2, page 19	PID		". "PID values are registers at <ECMA url>" shall be changed to "PID values are registered with a suitable subcommittee in JTC1". In general, the subcommittee shall be tasked to resolve details such as (a) terms and conditions for registering a PID - can an organization register for a PID without publication of implementation details (to what level of detail); (b) allocation of PID for proprietary implementation if there is a demand.		Resolved by Each part of the multipart standard define their own PIDs and Thus the registration authority is avoided
KR1			GE	It is highly recommended that the work seek comments from the 10892/14443 Harmonization Study Group in JTC 1/SC 6/WG 1 and a note on future harmonization be added if needed		Resolved by Inserting the following note at the end of the scope: This standard does not address application specific security mechanisms (as typically needed for smart card related use cases and standardized in the ISO/IEC 7816 series). NFC-SEC may complement application specific security mechanisms of ISO/IEC 7816.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
JP 1	1 Scope and 2 Conformance		ge	The security mechanism for the IC Cards is specified in the ISO/IEC 7816 series. And the ISO/IEC 14443 is the contact-less interface specification for the ISO/IEC 7616 (IC Cards) objects. Therefore, it is impossible to use DIS 13157 (ECMA-385) for the interface to the ISO/IEC 7816 (IC Cards) objects. The SCOPE of DIS 13157 states "This standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services." This text implicitly and undesirably indicates a possibility to apply DIS 13157 on the interface for the IC Cards. It should be avoided.	The SCOPE of DIS 13157 should be changed as follows: This standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services. The NFC-SEC is applied for the Data Exchange Protocol of the NFC.	Resolved by inserting a note at the end of the scope: NFC-SEC is exclusively designed for the data exchange protocol of ISO/IEC 18092
JP 2	9.4	2nd sentence	te	When a NFCIP-1 device was set on a cradle and multiple transaction is ongoing, in this use-case is not covered. In this use-case, the SSE and SCH instances are still active even after the deactivation of NFC-SEC, if the NFCIP-1 level of connection is still alive. This use-case is usually happen when NFCIP-1 is used with cradle.	The sentence should be changed as follows: After Release or Deselect of NFCIP-1, after finish of NFCIP-1 transaction or when the NFCIP-1 device is powered off, SSE and SCH instances shall be terminated and the associated shared secret and the link key shall be destroyed.	Rejected The term NFCIP-1 transaction is not well defined and might lead to ambiguities. Also it is rather the application layer and not the transport layer that can decide if a transaction is completed.
JP 3	Annex B		ge	The annex B of this DIS is a technical changing request to the ISO/IEC 18092.	The annex B of this DIS should be removed from this DIS, and it should be proposed to the SC6 as the technical changes to ISO/IEC 18092 instead of the annex of this DIS 13157 (NFC-SEC).	Resolved by GB1
JP 4	B.4	Figure B.1	te	The byte PPi of bit 7 is newly specified as SECi. This is technical change of ISO/IEC 18092.	The annex B of this DIS should be removed from this DIS, and it should be proposed to the SC6 as the technical changes to ISO/IEC 18092 instead of the annex of this DIS 13157 (NFC-SEC).	Resolved by GB1

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
JP 5	B.4	Table B.1	te	The specification of length reduction value (LRi) is different from the ISO/IEC 18092. It is technical changing request. The implementation, indicates the payload length by LEN and its valid length by LRi, is conform to the ISO/IEC 18092 as of today. If this specification was changed by this DIS 13157, then this implementation becomes nonconformity.	The annex B of this DIS should be removed from this DIS, and it should be proposed to the SC6 as the technical changes to ISO/IEC 18092 instead of the annex of this DIS 13157 (NFC-SEC).	Resolved by Defining only bit 7 of PPi in 13157-1 and for bits 6 to 0 referencing to NFCIP-1
JP 6	B.4	Figure B.2	te	The specification of length reduction value (LRt) is different from the ISO/IEC 18092. It is technical changing request. The implementation, indicates the payload length by LEN and its valid length by LRt, is conform to the ISO/IEC 18092 as of today. If this specification was changed by this DIS 13157, then this implementation becomes nonconformity.	The annex B of this DIS should be removed from this DIS, and it should be proposed to the SC6 as the technical changes to ISO/IEC 18092 instead of the annex of this DIS 13157 (NFC-SEC).	Resolved by Defining only bit 7 of PPt in 13157-1 and for bits 6 to 0 referencing to NFCIP-1
JP 7	B.4	Figure B.2	ed	Typo. bit 6: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.	Typo correction: bit 6: RFU. The Target shall set it to ZERO. The Initiator shall ignore it.	Accepted
JP 8	B.4	Table B.3	te	A new type of PFB is introduced for the ISO/IEC 18092. This is a technical change request to ISO/IEC 18092.	The annex B of this DIS should be removed from this DIS, and it should be proposed to the SC6 as the technical changes to ISO/IEC 18092 instead of the annex of this DIS 13157 (NFC-SEC).	Resolved by See GB1
DE 1	Whole document		GE, TE	Germany disapproves the DIS 13157 (ECMA-385) and DIS 13158 (ECMA 386) for the reasons below. Germany will change its vote to approval, if at least DE 2 below will be satisfactorily resolved.		Noted DE2 is resolved

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
DE 2	Whole document		GE, TE	The usage of ECMA-385 is closely bound to ECMA-340 (ISO/IEC 18092). So does ECMA-386 when applying it with ECMA-385. The passive mode communication of ECMA-340 is also used between NFC devices and contactless chipcards. Security features of chipcards, however, being in accordance with ISO/IEC 7816, are implemented according to one or more parts of ISO/IEC 7816, regardless they are contact or contactless chipcards. Therefore ECMA-385 may be undesirably interpreted to be used also for the interface between NFC devices and chipcards. This should be avoided.	Germany requests an additional and clarifying sentence, e.g. in the scope text of the two DIS texts, that ECMA-385 should not be applicable for the interface to chipcards, because the security features for the interface to chipcards are specified in the series of ISO/IEC 7816.	Resolved by KR1
DE 3			GE, TE	It is highly recommended for SC6 to hold both the DIS after the ballot end, as it can be foreseen that changes will be done for ECMA-340 in due time because of the harmonization process of NFC and ISO/IEC 14443. As both the DIS are related to ECMA-340, modifications to those are much probable as a consequence of the harminzation process.		Resolved by GB1
FR1	Introduction	Whole	Te	"The Standard specifies common NFC-SEC services and a protocol. This standard is a part of the NFC-SEC series of standards. The NFC-SEC cryptography standards of the series complement and use the services and protocol specified in this standard" The wording is unclear: What's such a thing as a " common NFC-SEC services"? Common to what ? Which type of protocol is it referred to ? Protocol to do what ? What's that "NFC-SEC series of standards"?	Rewrite completely the introduction. It looks like every time that a new PID is allocated the corresponding " cryptography standard" will be standardized as a new ISO standard.	Resolved by following clarification and SG1 The interpretation of France is correct. The PID is a normative requirement s specified in 13157. If a new PID is standardized , then obviously it must be linked with normative requirements in a new standard.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR2	1 Scope	First sentence	Te	The Scope defines this standard as the secure channel for NFCIP-1. However section 2 “Conformance” points out that “ Conformant Implementations that use the NFCIP-1 protocol shall also conform to the requirements in Annex B” Which seems to mean that: 1. other protocols than NFCIP-1 might also support ISO/IEC 13157. 2. when ISO/IEC 13157 is implemented over NFCIP-1 then the NFCIP-1 compliant devices require additional requirements (Annex B) And therefore that this ISO/IEC 13157 layer is not independent from the underlying layers , failing to comply with OSI model	“This standard specifies a mechanism to establish a secure channel between two devices that communicate using a contactless interface. To establish this secure channel this standard specifies access points to invoke security services, called NFC-SEC services, and a protocol to be executed. When the contactless interface complies with ISO/IEC 18092, these devices shall in addition comply with the requirements set forth in Annex B”	Resolved by GB1
FR3	2	First paragraph	Te	PID is not the most suitable mechanism to provide a flexible framework to specify security	Delete ‘identified by the selected PIDs”	Resolved by SG4
FR4	3	First Reference but applicable to the whole document	Ed	The document must refer to ISO standards when available	Replace ECMA-340 by ISO/IEC 18092 Idem for NFICP-1	Accepted Already fixed in the ISO/IEC formatted version
FR5	7 General	First sentence	Ed	The expression “follows concepts” is not acceptable in an ISO standard	Replaces “follows concepts” by “shall comply with”	Resolved by changing text to "NFC-SEC as illustrated in Figure 1 uses the OSI reference model specified in ISO/IEC 7498-1."

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR6	8	First sentence	Te	The expression "shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards" may rise some ambiguity for interpretation. What happens if the SSE service is invoked a second time, prior to any SCH? Is the former shared secret replaced by the last calculated one? Are there now two independent shared secrets? Does this requirement refer only to those shared secrets calculated as a result of the SSE or apply also to any shared secret obtained by other means ?	Clarify the point or complete the paragraph as follows: " …. before of afterwards, using the SSE or another methodology out of the scope of the standard" In section 8.2 replace "… establish a link key" by "… establish a session key"	Resolved by clarification: If the SSE is invoked a second time, a new shared secret is generated. The requirement is that this shared secret shall be cryptographically uncorrelated to the previous one, within and even across subsequent NFCIP-1 connections. Rejected: 8.2 Replace "link key" by "session key": See terminology used by this standard in section 4: "4.3 Link key: Secret key securing communications across a secure channel".
FR7	8	First sentence	Ed	The services provided by SSE and SCH are not properly described. The current sentence refer to the SSE and should be included in § 8.1.	Replace " Shared secrets established with the services bellow shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards" by: "This chapter describes two services , SSE and SCH, that the NFC-SEC layer provides to the NFC-SEC User. When invoked, these services enables the cryptographic protected transmission of NFC-SEC User messages between the peer entities by means of a protocol described in chapter 9"	Resolved by adding the explanation proposed by France

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR8	8.1	Whole section	Te	It's not evident the interest of the SSE service " establish a shared secret between two peer NFC-SEC users, **which they can use at their discretion**" The generation of a shared secret makes sense as a first stage needed for the subsequent creation of a secure channel using a set of session keys derived from this shared secret. When reading the DIS ISO/IEC 13158 the SSE is just the first step for SCH so SSE is not as such an independent service but the mere execution of NFC-SEC protocol 9.1 and 9.2 steps. When looking at section , the only difference is that ,meaning that the shared secret for the SCH is kept by the NFC-SEC layer, whereas the shared secret for the SSE is moved up to the NFC-SEC User Layer (but that's not explicitly described in Annex B)	The interest for the SSE service is questionable. A sound Use Case shoud be provided.	Resolved Use cases are described in the NFC-SEC white paper and should not appear in the standards text
FR9	8.1	End of the paragraph	Ed	Refer to FR6	Add as a third paragraph: " Shared secrets established with the services bellow shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards" Or an alternative sentence as a result of FR5 resoiution	Resolved by Following resolution FR8 this text is appropriate in 8.1

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR10	8.1	End of the second paragraph	Te	The NFC SEC cryptography scheme should be not necessarily a standard. Any security scheme may be indexed in using a URI different as the current PID definition.	Replace ".. . according to the NFC-SEC cryptography standard identified by the PID" by ".. . according to the cryptographic mechanisms agreed between the peer entities"	Resolved by SG4
FR11	8.2	First sentence	Ed	The service provided by the SCH is to be better described. It's not just about the creation of a secure channel, but rather on the protected transmission of NFC-SEC User PDUs	Replace " The SCH provides a secure channel" by " The SCH provides a service of transmission of cryptographically protected NFC-SEC User PDUs, by the creation of a secure channel "	Rejected This substantial editorial change could be misunderstood by other NBs which accepted the current wording and regard secure channel as the appropriate term
FR12	8.2	Second Paragraph	Te	A more precise wording is needed and the reference to PID removed , see FR8	Replace the current text by: " Invocation of the SCH shall establish a *session* key"	Resolved by FR6

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR13	9	Whole	General	Sections 9 to 12 mix concepts and the text should be more precise A protocol is not made up of mechanisms but consists of an exchange of Protocol Data Units (PDUs) that makes possible the instances of the communicating entities executing the protocol to go through a predefined machine state. Each protocol stage is then finished when as a result of the transmission /reception of one or more PDUs each entity comes to an unambiguous state. That's more rigorous description has been done in Annex A and should be referred to here. Otherwise there is no link between Annex A SDL schemes and the protocol stages defined in this chapter.	Replace the initial sentence of chapter 9 by the following: "Upon invocation of a NFC-SEC service, the peer NFC-SEC entities shall create instances to start the execution of the NFC-SEC protocol. The execution of the NFC-SEC protocol consists of four stages as described in the next section. Associated to each of these stages the NFC-SEC entities transit between the machine states according to chapter 10. To start the execution of the protocol both NFC-SEC entities, the Sender and the Receiver shall be in the Idle state" Examples add the following sentences at the end of each section. 9.1 "At the end of the Key Agreement stage , the NFC-SEC Sender entity is in the SELECT state and the NFC-SEC Receiver entity is in the Established Recipient state" 9.2 "At the end of the Key Verification stage , the NFC-SEC Sender entity and the NFC-SEC Receiver are both in the Confirmed state"	Rejected This substantial editorial change could be misunderstood by other NBs which accepted the current wording
FR14	9.1	First sentence	Te	The NFC SEC cryptographic schemes to be used to provide the NFC-SEC schemes should not necessarily be identified with a PID. Any security scheme may be referred to by using a URI different as the current PID definition. Refer to FR comment on section 11.2	Replace the current text by: " During this initial stage, a shared secret is established by the exchange of the ACT_REQ and ACT_RES PDUs resulting in the execution of a Key Agreement protocol"	Resolved by SG4

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR15	9.2	Title	Ed	The Term Key “Confirmation” is misleading. In the OSI model confirmation is the SDU send by layer N-1 to layer N when a Service Request SDU was received on the SAP offered by layer N-1. But in the text “Confirmation” is a NFC-SEC protocol stage, not a SDU.	Replace the Title “Key Confirmation” by “Key Verification”	Rejected Key confirmation is the standardised technical term (see ISO/IEC 11770-1).
FR16	9.2	Only sentence	Te	Avoid the reference to the PID. According to Table 2, the VFY_REQ and VFY-RES PDUs don’t convey any PID information. This protocol stage should be linked with the corresponding instances machine states (refer to FR14)	Replace the current text by “ The peer NFC-SEC entities shall verify their agreed shared secret using the VFY_REQ and VFY_RES PDUs. At the end of the Key Verification stage , the NFC-SEC Sender entity and the NFC-SEC Receiver shall be both in the Confirmed state, as per chapter 10”	Resolved by SG4 and Clarification: The reference to the state machine is mentioned in clause 10 States and sub-states
FR17	9.3	Title	Editorial	The Title of the section PDU security is not very informative. There is no such a thing as PDU security , the PDU ENC conveys a cryptographically protected message passed by the NFC-USER layer using the SDU Send Data .	Replace the current title by: “Encrypted PDU Exchange (EPE)”	Rejected PDU security is more than encryption therefore the term is appropriate

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR18	9.3	Second Sentence	Te	The wording lacks of precision. ENC doesn't protect anything. It is a special PDU that conveys in the Payload Data protected by cryptography The NFC SEC cryptography scheme should be not necessarily a standard. Any security scheme may be indexed in using a URI different as the current PID definition.	Replace the second sentence by "The peer NFC-SEC entities shall protect data exchange using ENC, according to a mutually agreed cryptographic scheme.	Resolved by SG4
FR29	9.	Figure 2	Te	The Invocation of SSE and SCH services give rise to the execution of different processes with different flow diagrams.	Redesign Figure 2 with two different General flows: One for the SSE service and other for the SCH services The SEE is made of 9.1, 9.2 and 9.4 The SCH is made of 9.1 9.2 9.3 and 9.4	Resolved by Replacing the caption of figure 2 with "General flow of the NFC-SEC services"
FR20	9.4	Whole	Te	The current paragraph is mixing events from different protocol layers. Termination PDU (TMN PDU) only applies to NFC-SEC layer and is different from the Release or Deselect of NFCIP-1. TMN PDU means that both NFC-SEC instances are in the Idle State, according to A.4.4 , ready for another Service Invocation, not necessary that the associated shared keys are destroyed. This means that if the NFCIP-1 layer is selected or the NFC device is powered off the NFC-SEC instances, if any, are not "Terminated"	Add to the end of the first sentence, the following: "Both instances shall then enter the Idle state, ready for the invocation of a new NFC-SEC service" Replace the sentence " After Release or Deselect of NFCIP-1, or when the NFCIP-1 device is powered off, SSE and SCH instances shall be terminated and the associated shared secret and the link key shall be destroyed" by a NOTE: " After Release or Deselect of NFCIP-1, or when the NFCIP-1 device is powered off, any key generated as a result of the execution of a NFC-SEC service shall be destroyed"	Resolved . by adding "upon transition to the IDLE state"

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR21	11	Whole	Te	The NFC SEC is defined to run only over the NFCIP-1 layer. This restriction prevents the use of the NFC SEC over any logical layer exposing equivalent features.	Replace NFCIP-1 by “adjacent lower layer” Define the “adjacent lower layer” as the NFCIP-1 layer or any logical layer exposing equivalent features	Resolved by JP1
FR22	11	Table 2	Te	The table appears inconsistent with regards the purposes of the different PDUs. For instance by its own nature the PDUs VFY_REQ and VFY_RES should convey a field (“payload”) with the data to be confirmed. The same applies to ENC whose purpose is to transmit a cryptographically protected message. The payload conveys this message. The term “prohibited” is unusual in standards. The term “absent” (A) is preferable for not required field.	Replace Table 2 by the following: NFC SEC PDU / SEP / PID (SCID) / NFC SEC Payload ACT_REQ / M / M / C ACT_RES / M / A / C VFY_REQ / M / A / M VFY_RES / M / A / M ENC / M / A / M TMN / M / A / A ERROR / M / A / A	Resolved by adding " is further specified in 11.3"

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR23	11.2	Whole	Te	The notion of Protocol Identifier is disputable. Actually according to section 9 there is only one protocol in this standard, the NFC-SEC, whose execution is required to render both the SSE and the SCH services. What actually changes during the instantiation of the NFC-SEC entities is the set of crypto-algorithms to render SSE and SCH services. However the possibility to execute the same protocol with different algorithms is not new. When more than one algorithm is involved terms such as " Security Context " or "Security Environment" are usual. Because Security Environment is standardized by ISO/IEC 7816 for this purpose and to avoid any ambiguity, we suggest the use of Security Context Identifier (SCID) as more appropriate that the somehow misleading PID. For SCID encoding refer to next comment	Replace Protocol Identifier (PID) by Security Context Identifier (SCID)	Resolved by SG4

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR24	11.2		Technical	As currently defined the PID is a URI (Unique Resource Identifier) indexing a NFC SEC cryptography scheme. This PID asks for a registration where a principle without registration will be more convenient, flexible and faster. In removing the registration, we remove dependencies between the ECMA and other (private or public) organizations willing to reuse this standard. As an alternative the following encoding for the Security Context Identifier (SCID) is suggested. This approach makes unnecessary the mess to launch a new part of the standard every time a new PID is recognized.	SCIDs are 128-bit values that identify NFC-SEC cryptography specification. SCID value is computed as follow: • The NFC-SEC cryptography specification is identified by a URI according to the RFC3936 specification. The URI shall contain the URL of the organization maintening the specification. • A MD5 is applied on the URI according to the RFC1321 specification. • The SCID is the result of the MD5 operation. The SCID field is present in the ACT_REQ, but absent in all the other PDUs according to Table	Resolved by SG4

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR25	11.3	Whole	Te	There is not much content on this paragraph. "The TMN PDU shall contain no NFC-SEC payload" (already specified in Table 2 and in 11.4) "The NFC-SEC payload field shall contain an integer number of octets" (is padding required ? if yes how to identify it ?) "Its use is the ERROR PDU is specified in the Error sub-clause" (redundant) "Its use in all other PDUs depends on the PID" For the purpose of the interoperability of NFC-SEC implementations it's useless. It could be argued that the exact structure of the PDU Payload depends on the PID (SCID). However when looking at DIS ISO/IEC 13158, even if the structure of , eg the ENC field, is provided, the encoding for the portioning of the different data elements (eg, making up the PDU ENC Payload) is missing.	Either to rewrite it completely or to remove it. A formal description of the structure and the encoding of the 7 PDUs (using eg ASN.1 and DER-TLV ISO standards 8824 and 8825) is necessary for interoperability of NFC-SEC implementations.	Resolved by new text "Its use, structure and encoding in all other PDUs is specified in NFC-SEC cryptography standard identified by PID"
FR26	11.4	Whole	Ed	The information there is redundant with the content of Table 2. In addition ,by removing it the content of the section becomes more consistent. Indeed the current text mixes the description of the data fields of NFC-SEC PDUs with the structure and encoding of two of these PDUs (11.4 for TMN and 11.5 for ERROR)	Remove section 11.4	Resolved by new text " The TMN PDU consists of the SEP field only as specified in table 2. "

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR27	11.5	Whole	Te	The content of this section is inconsistent with Table 2. Indeed Table 2 states that the ERROR PDU only conditionally contains a payload whereas section 5 indicates that the payload for ERROR "…shall contain a zero-terminated byte string …" . On the other hand, the generation and reception of the PDU ERROR automatically puts the state of both NFC-SEC entities in "IDLE". This means that the NFC-SEC protocol doesn't support any ERROR Recovery procedure. Therefore the interest for a Payload in the PDU ERROR is questionable. Finally, apart from the zero-terminated byte string requirement, the very limited amount of information here is redundant with Table 2	Remove 11.5	Resolved by new text The ERROR PDU starts with the SEP field and, if it contains a payload, this payload shall contain a zero-terminated octet string in the NFC-SEC Payload field.
FR28	12	Whole	General Te	The information provided in this section that should constitute the technical core of this standard is poor and for sure prevents the implementation of interoperable solutions. The sentence "This clauses specifies rules for the NFC-SEC protocol" is to be avoided	Replace sentence "This clauses specifies rules for the NFC-SEC protocol" by " This clause specifies the rules for processing the NFC-SEC protocol that an implementation of this standard shall comply with. An SDL representation of the protocol machine specification is provided in Annex A"	Rejected Because annex A is properly referenced in 10 and it is inappropriate to repeat the conformance statement
FR29	12.1	Fifth Bullet	Te	"When a NFC-SEC entity receives an SDU in a state where it is not allowed or with invalid contents, it shall respond with an ERROR SDU and leave the state unchanged" That's a consistent requirement. Notice however that SDUs are not part of the NFC-SEC protocol which only deals with the exchange of PDUs.	(1) Remove this bullet or (2) put this text as a NOTA warning of the difference between ERROR SDU and ERROR PDU.	Resolved by Changing the title of 12.4 to "Protocol and Service errors"

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR30	12.2	First Bullet	Te	If this is the case a mechanism to indicate the upper bounds acceptable for a PDU length should be included in the protocol and prior to the transmission of any PDU (indeed the Payload of the ACT-REQ/ACT_RES might already exceed the Recipient/Sender buffering capability). If such a discovery mechanism is not provided the bullet is useless.	Complete the protocol specifying a discovery mechanism for the maximum length acceptable for a PDU or remove this bullet	Resolved Because the mechanism to signal whether a SDU cannot be accepted is an Error SDU

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

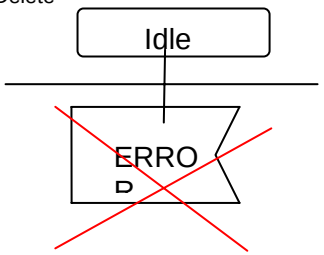
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR31	12.4	Whole	Te	Unclear and incomplete paragraph. Basic issues addressing security concerns aren't addressed What happens if during the SCH services after sending an ENC PDU a PDU ERROR is received? Are the shared secret key and the derived session keys still available? On the other hand the standard fails to precise how the different fields that make up a cryptographically protected Payload in the ENC PDU are identified. That's essential for the parsing and correct processing by the peer NFC-SEC entity. (as an example refer to ISO/IEC 7816-4 mechanism for Secure Messaging)	Replace the first sentence by the following: "Prior to the transmission of the ENC PDU the sender process cryptographically the Data passed on using the SDU "Send Data". This process uses a cryptographic agreed scheme. The outcome of this process is then mapped into the NFC-SEC Payload of the ENC PDU". "Upon reception of the ENC PDU , the Recipient proceeds to the cryptographic process of the NFC-SEC payload, according to the cryptographic agreed scheme. If no error is detected an SDU Data Available shall be moved on to the NFC-SEC Layer" Add then the following " During the process of the ENC PDUs the reception of any ERROR PDU will result in the abort of the cryptographic processing. Both entities shall moved on to the Idle State according to A.4.4. The previous Security Status is cancelled, meaning that any agreed shared secret or derived session keys are definitively lost" Finally a common mechanism to enable the recognition by the recipient of the different fields making up the NFC-SEC Payload is to be included in the standard. Otherwise interoperability of the implementations cannot be guaranteed.	Resolved by FR20

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

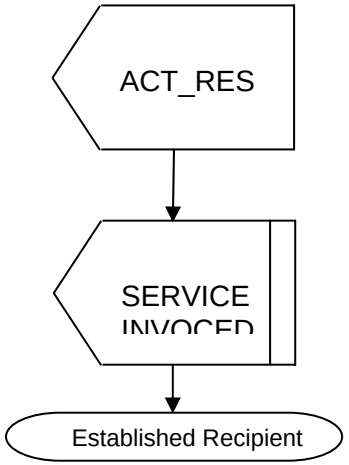
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR32	Annex A	First sentence	Te	The first sentence " The NFC-SEC protocol machine in this Annex specifies the sequence of PDUs to establish the SSE and to establish, use and Terminate the SCH" First there is no reason why one of the services is completely described whereas the other isn't. Meaning that Informative Annex A is incomplete. Second , that 's not accurate. In section A.4.4 " Confirmed State" the Terminate SDU and the TMN PDU apply to both SSE and SCH.	1. Complete the Annex A (refer to FR comment hereafter) and then 2. Replace The first sentence " The NFC-SEC protocol machine in this Annex specifies the sequence of PDUs to establish the SSE and to establish, use and Terminate the SCH" by simply saying " This Annex consists of an SDL description of the NFC-SEC protocol exchange when rendering NFC-SEC services"	Resolved by phrasing "establish and terminate the SSE".
FR33	Annex A.3	List of SDUs	Te	When the Recipient receives the PDU ACT_REQ and answers with a PDU ACT_RES , an SDU should be sent to the NFC-SEC USER to report that a NFC-SEC Service has been requested. This information informs the USER layer that the NFC-SEC entity has moved to the "Established Recipient" State and is no longer able to receive the SDU of the Idle State (refer to FR comment This SDU should include the type of the service and the Security Context Identifier	Add the following Confirm SDU to the list "Service Invoked Indicates the receipt of a Service Request (type of service, SCID)"	Rejected Because NFC-SEC was designed to keep the list of SDUs to a minimum and there is another way to indicate this information: The NFC-USER is informed by the ESTABLISHED SDU.
FR34	Annex A.4	A.4.1	Te	In the IDLE state no PDU conveying a ERROR is expected to be received. The IDLE state is either the initial state or the state acquired after a PDU ERROR is sent or received	Delete 	Rejected. Due to asynchrony in timing, an ERROR PDU may be received immediately after transit to the IDLE state. See also 12.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

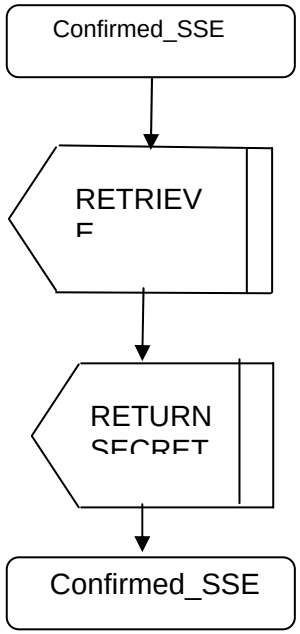
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR35	Annex A.4	A.4.1	Te	Upon transmission of ACT_RES by the recipient, the NFC-USER Layer should be aware that an Invocation of Service has been received by the NFC entity, so that the NFC-SEC Layer state has been moved from "Idle" to "Established Recipient" . This SDU should indicate the type of Requested Service, SSE or SCH. This SDU is to be included in Annex A.3	Modify the SDL diagram follows by inserting the "Service Invoked" SDU: 	Rejected. See FR33

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR36	Annex A	A.4.4	Te	During the execution of the SSE services, once the NFC-SEC entities are in the state "Confirmed" (after the SDU "Established" is sent in A.4.3) the Shared Secret is available and the NFC-USER is invited to retrieve the shared secret. That means that in diagram A.4.4 a case has been missed. That case makes use of the SDU's "Retrieve Secret" and " Return Secret" defined in A.2 and A.3 The machine state of the NFC-SEC peers remain anyway at the "Confirmed" State.	Add the following to the flowchart: 	Resolved The diagram is updated accordingly

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
FR 37	Annex B	Clause B.4	Te	It is not reasonable to have a normative chapter in one Draft for publication as an ISO standard explaining the amendments to be brought in another ISO standard (ISO/IEC 18092) for compliance. That's even more chocking as the declared purposed of this DIS is to provide a secure channel for devices compliant with ISO/IEC 18092 (refer to scope) . Meaning that actually isn't unless first ISO/IEC 18092 is amended!	Remove Annex B which has nothing to do in this standard Make things properly: proceed to amend what is to be amended first and only then try to have this DIS approved.	Resolved See GB1

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.