

Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14103
Date:	2009-10-06
Replaces:	
Document Type:	Summary of Voting/Table of Replies
Document Title:	Summary of Voting on ISO/IEC DIS 13157, Information technology -- Telecommunications and information exchange between systems -- NFC-SEC: NFCIP-1 Security Services and Protocol
Document Source:	ITTF
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	34
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	

Ballot Information			
Reference	ISO/IEC DIS 13157	Committee	ISO/IEC JTC 1/SC 6
Edition number	1		
English title	Information technology -- Telecommunications and information exchange between systems -- NFC-SEC: NFCIP-1 Security Services and Protocol		
French title	Technologies de l'information-- Téléinformatique -- Services de sécurité et protocole NFC-SEC: NFCIP-1		
Start date	2009-03-27	End date	2009-08-27
Opened by ISO/CS on	2009-03-27 00:07:26	Closed by ISO/CS on	2009-08-29 00:16:33
Status	Closed		
Voting stage	Enquiry	Version number	1
Note			

Result of voting
<p>P-Members voting: 18 in favour out of 23 = 78 % (requirement \geq 66.66%)</p> <p><i>(P-Members having abstained are not counted in this vote.)</i></p> <p>Member bodies voting: 5 negative votes out of 25 = 20 % (requirement \leq 25%)</p> <p><i>Approved</i></p>

Votes by members					
Country	Member	Status	Approval	Disapproval	Abstention
Algeria	IANOR	P-Member			X
Armenia	SARM	P-Member			
Australia	SA	P-Member			X
Austria	ASI	O-Member	X		
Azerbaijan	AZSTAND	P-Member			
Belgium	NBN	P-Member	X		
Canada	SCC	P-Member	X		
China	SAC	P-Member	X		
Côte d'Ivoire	CODINORM	P-Member			X
Czech Republic	UNMZ	P-Member	X		
Denmark	DS	P-Member			X
Ecuador	INEN	P-Member			X
Finland	SFS	P-Member			X
France	AFNOR	P-Member		X *	
Germany	DIN	P-Member		X *	
India	BIS	P-Member	X		
Ireland	NSAI	P-Member	X		
Italy	UNI	P-Member	X		
Jamaica	BSJ	P-Member	X		
Japan	JISC	P-Member		X *	
Kazakhstan	KAZMEMST	P-Member	X		
Kenya	KEBS	P-Member	X		
Korea, Republic of	KATS	P-Member	X *		
Libyan Arab Jamahiriya	LNCSM	P-Member			
Luxembourg	ILNAS	P-Member	X		
Malaysia	DSM	P-Member			X
Malta	MSA	P-Member			X
Netherlands	NEN	P-Member	X		
New Zealand	SNZ	P-Member			X
Nigeria	SON	P-Member	X		
Norway	SN	P-Member			X
Pakistan	PSQCA	P-Member			
Philippines	BPS	P-Member			X
Portugal	IPQ	O-Member			X
Russian Federation	GOST R	O-Member	X		
Singapore	SPRING SG	P-Member		X *	

Slovenia	SIST	P-Member	X		
South Africa	SABS	P-Member			X
Spain	AENOR	P-Member	X		
Sweden	SIS	P-Member			X
Switzerland	SNV	P-Member	X		
United Arab Emirates	ESMA	P-Member			
United Kingdom	BSI	P-Member		X *	
Uruguay	UNIT	P-Member			X
USA	ANSI	Secretariat	X		
Venezuela	FONDONORMA	P-Member			
P-Member TOTALS Total of P-Members voting: 23			18	5	14
TOTALS			20	5	15
(*) A comment file was submitted with this vote					

Comments from Voters			
France	AFNOR	P-Member	France(AFNOR).doc
Germany	DIN	P-Member	Germany(DIN).doc
Japan	JISC	P-Member	Japan(JISC).doc
Korea, Republic of	KATS	P-Member	Korea,Republicof(KATS).doc
Singapore	SPRING SG	P-Member	Singapore(SPRINGSG).doc
United Kingdom	BSI	P-Member	UnitedKingdom(BSI).doc

French comments on ISO/IEC DIS 13157

1. General Considerations on this Fast Track

1.1. The Context

AFNOR regrets the decision of ISO JTC1 to launch the Fast-Track ballot for the two DIS ISO/IEC 13957 and 13958 that we consider premature with regards the on-going effort of harmonization between NFC-Specifications and ISO/IEC 14443 undertaken by ISO JTC1 SC6 and SC17 experts. Indeed, at the kick-off meeting held in Fukuoka, the Terms of reference for this harmonization effort were agreed and one of the issues to be discussed was precisely the security of the contactless channel, which constitutes a serious concern for those industries intended to use RF channels for delivery of new services (eg, mobile payment). These concerns would be far better addressed through a collaborative open effort than by the submission of a Fast Track procedure.

AFNOR is supportive of any harmonization effort intended to increase the interoperability of RF devices that by their own nature will be heterogeneous. That's exactly the reason why to push unilaterally for the publication of new standards in the very sensitive issue of the security is not good for harmonization. Notice that AFNOR stressed the need to have the NFC-SEC issue discussed at the SC6-SC17 Study Group as one key technical point to address accordingly to resolution 42 quoted above by ECMA and before any decision on launching this Fast Track is made.

1.2 ISO/IEC 7816 security model

Still due to the diversity of applications requiring a secure channel that can be deployed, the only way to strike the balance security vs flexibility is by a standard feature enabling the terminal to discover and then select one of the security mechanisms required by the card to perform a protected operation (eg, reading ,writing, updating data). In ISO/IEC 7816 model this mechanism intervenes upon the successful selection of a card application. This selection enables the discovery by the terminal of the access conditions required by the card in this particular applicative context. Because these access conditions are defined as a Boolean function, all the possible combinations for authentication and secure channel requirement are possible. In addition, individual atomic access conditions may refer to different cryptographic algorithms and keys that fit for a particular application. Finally when accessing a card, these access conditions may refer to either the contact or the contactless interfaces separately or both . The principle of layer independency of the OSI model is then respected. In particular the model applies exactly the same for ISO/IEC 14443 cards type A and type B.

That means that ISO/IEC 7816 security architecture is robust, well-proved and most of all flexible. The point is that this flexibility enables to optimize the security for a particular application with regards the real risks enabling a rationale cost approach (scalability). In addition the security contexts are set and executed independently of each other (security environment concept) , meaning that less security is not the price to pay for this flexibility. Finally, the model doesn't bind to a particular algorithm or protocol. All may be referred to within this model by using for instance a unique Object Identifier (OID). This flexible model enables the interoperability between communicating devices.

1.3 NFC- SEC Model

The above presentation matters in order to better understand some of the comments hereafter. Compared with the ISO/IEC 7816 model, the security model proposed by DIS ISO/IEC 13157 (ECMA 385) appears restrictive with respect the following:

1. The model only considers at present two cryptographic algorithms: AES for encryption and ECDH for key agreement purposes
2. Subsequent algorithms require the allocation of a PID by ECMA ... and a new Fast-Track for any pair of new algorithms (shared key + encryption)
3. The model doesn't apply to ISO/IEC 14443 Type B cards, because NFC-SEC is built only on NFCIP-1 (ISO/IEC 18092), at least in theory (refer to comments)
4. The model doesn't explain how to protect the exchanged messages. There is no such a thing as the ISO/IEC 7816 Secure Messaging mechanism here, where the structure and encoding of the cryptographically protected messages is specified. It is just said that the message is to be encrypted then authenticated. That's correct, but it's just the way secure channels work and doesn't guarantee interoperability
5. The secure channel is established at the transport layer level. How does this secure channel would interact with a second end-to-end secure channel?

Whilst it has been argued that the model only applies to peer-to-peer mode between NFC devices, the end-to-end security is the key issue, specially considering use cases (proximity payments). That means that when an end-to-end security channel is created, the NFC-SEC layer is a redundant and again the interest of the approach deserves discussion. How in that case the end-to-end secure protocol interacts with the NFC-SEC layer? .A good case, is how to implement NFC-SEC with a secure layer over for instance, ISO/IEC 28361. When the use cases are unclear, too specific or not corresponding to an urgent demand by different sectors potentially users of the NFC Technology, the interest for such an ISO standard may be disputed.

No original approach is brought in by this Fast-Track submission, the proposed framework is a direct application of the Canetti and Krawczyk model for secure channels. A communication between two devices is protected through a session, established by two consecutive stages: one session key negotiation followed by encryption and/or message authentication using standard protocols. No specific protocol is submitted. The point is: Does this submission actually justify for a new pair of ISO standards?

Notice also that DIS ISO/IEC 13157 includes the requirements for a *NFCIP-1 compliant device* to support NFC-SEC, which constitutes an extension of the NFCIP-1 published standard (ISO/IEC 18192). That's not the usual way to proceed: It means that during the creation of NFC-SEC, as a secure layer on top of NFCIP-1, the promoters realized that somehow was lacking in the underlying layer. The logical process would have been to amend ISO/IEC 18192 first, then proceed to the definition of the NFC-SEC protocol properly. Instead, the extra requirements were added as an Informative Annex in ECMA 385. It's clear that Annex B is to be moved in a future revision/amendment to ISO/IEC 18192. That should have been done first: If now DIS ISO/IEC 13157 is published as an ISO standard, an amendment and the corresponding NWIP is to be approved to remove Annex B. Time and energy wasted. Refer to Annex B comments below.

Date 30/6/2009	Document Comments on Fast Track NFC-SEC 385
-------------------	---

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR1	Introduction	Whole	Te	<p>“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”</p> <p>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”?</p>	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.	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR2	1 Scope	First sentence	Te	<p>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"</p> <p>Which seems to mean that:</p> <ol style="list-style-type: none"> 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) <p>And therefore that this ISO/IEC 13157 layer is not independent from the underlying layers , failing to comply with OSI model</p>	<p>"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.</p> <p>When the contactless interface complies with ISO/IEC 18092, these devices shall in addition comply with the requirements set forth in Annex B"</p>	
FR3	2	First paragraph	Te	<p>PID is not the most suitable mechanism to provide a flexible framework to specify security</p>	Delete 'identified by the selected PIDs"	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
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	
FR5	7 General	First sentence	Ed	The expression “follows concepts” is not acceptable in an ISO standard	Replaces “follows concepts” by “shall comply with”	
FR6	8	First sentence	Te	<p>The expression “shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards” may rise some ambiguity for interpretation.</p> <p>What happens if the SSE service is invoked a second time, prior to any SCH?</p> <p>Is the former shared secret replaced by the last calculated one? Are there now two independent shared secrets?</p> <p>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 ?</p>	<p>Clarify the point or complete the paragraph as follows:</p> <p>“ before of afterwards, using the SSE or another methodology out of the scope of the standard”</p> <p>In section 8.2 replace “... establish a link key” by “... establish a session key”</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
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.	<p>Replace “ Shared secrets established with the services bellow shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards” by:</p> <p>“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”</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR8	8.1	Whole section	Te	<p>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”</p> <p>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.</p> <p>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.</p> <p>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)</p>	The interest for the SSE service is questionable. A sound Use Case should be provided.	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR9	8.1	End of the paragraph	Ed	Refer to FR6	<p>Add as a third paragraph:</p> <p>“ Shared secrets established with the services bellow shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards”</p> <p>Or an alternative sentence as a result of FR5 resoition</p>	
FR10	8.1	End of the second paragraph	Te	<p>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.</p>	<p>Replace “.. . according to the NFC-SEC cryptography standard identified by the PID”</p> <p>by</p> <p>“.. . according to the cryptographic mechanisms agreed between the peer entities”</p>	
FR11	8.2	First sentence	Ed	<p>The service provided by the SCH is to be better described.</p> <p>It's not just about the creation of a secure channel, but rather on the protected transmission of NFC-SEC User PDUs</p>	<p>Replace “ The SCH provides a secure channel”</p> <p>by</p> <p>“ The SCH provides a service of transmission of cryptographically protected NFC-SEC User PDUs, by the creation of a secure channel “</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
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 <i>session key</i> ”	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR13	9	Whole	General	<p>Sections 9 to 12 mix concepts and the text should be more precise</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>Replace the initial sentence of chapter 9 by the following:</p> <p>"Upon invocation of a NFC-SEC service, the peer NFC-SEC entities shall create instances to start the execution of the NFC-SEC protocol.</p> <p>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"</p> <p>Examples add the following sentences at the end of each section.</p> <p>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"</p> <p>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"</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR14	9.1	First sentence	Te	<p>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.</p> <p>Refer to FR comment on section 11.2</p>	<p>Replace the current text by:</p> <p>“ 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”</p>	
FR15	9.2	Title	Ed	<p>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.</p> <p>But in the text “Confirmation” is a NFC-SEC protocol stage, not a SDU.</p>	<p>Replace the Title “Key Confirmation” by “Key Verification”</p>	
FR16	9.2	Only sentence	Te	<p>Avoid the reference to the PID. According to Table 2, the VFY_REQ and VFY-RES PDUs don't convey any PID information.</p> <p>This protocol stage should be linked with the corresponding instances machine states (refer to FR14)</p>	<p>Replace the current text by</p> <p>“ The peer NFC-SEC entities shall verify their agreed shared secret using the VFY_REQ and VFY_RES PDUs.</p> <p>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”</p>	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
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)"	
FR18	9.3	Second Sentence	Te	<p>The wording lacks of precision. ENC doesn't protect anything. It is a special PDU that conveys in the Payload Data protected by cryptography</p> <p>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.</p>	<p>Replace the second sentence by</p> <p>"The peer NFC-SEC entities shall protect data exchange using ENC, according to a mutually agreed cryptographic scheme.</p>	
FR29	9.	Figure 2	Te	The Invocation of SSE and SCH services give rise to the execution of different processes with different flow diagrams.	<p>Redesign Figure 2 with two different General flows: One for the SSE service and other for the SCH services</p> <p>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</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR20	9.4	Whole	Te	<p>The current paragraph is mixing events from different protocol layers.</p> <p>Termination PDU (TMN PDU) only applies to NFC-SEC layer and is different from the Release or Deselect of NFCIP-1.</p> <p>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.</p> <p>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"</p>	<p>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"</p> <p>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"</p> <p>by a</p> <p>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"</p>	
FR21	11	Whole	Te	<p>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.</p>	<p>Replace NFCIP-1 by "adjacent lower layer"</p> <p>Define the "adjacent lower layer" as the NFCIP-1 layer or any logical layer exposing equivalent features</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments																																
FR22	11	Table 2	Te	<p>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.</p> <p>The same applies to ENC whose purpose is to transmit a cryptographically protected message. The payload conveys this message.</p> <p>The term “prohibited” is unusual in standards. The term “absent” (A) is preferable for not required field.</p>	<div>Replace Table 2 by the following:</div> <table><tr><th>NFC SEC PDU</th><th>SE P</th><th>PID (SCID)</th><th>NFC SEC Payload</th></tr><tr><td>ACT_REQ</td><td>M</td><td>M</td><td>C</td></tr><tr><td>ACT_RES</td><td>M</td><td>A</td><td>C</td></tr><tr><td>VFY_REQ</td><td>M</td><td>A</td><td>M</td></tr><tr><td>VFY_RES</td><td>M</td><td>A</td><td>M</td></tr><tr><td>ENC</td><td>M</td><td>A</td><td>M</td></tr><tr><td>TMN</td><td>M</td><td>A</td><td>A</td></tr><tr><td>ERROR</td><td>M</td><td>A</td><td>A</td></tr></table>	NFC SEC PDU	SE P	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	
NFC SEC PDU	SE P	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																																			

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR23	11.2	Whole	Te	<p>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.</p> <p>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.</p> <p>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.</p> <p>For SCID encoding refer to next comment</p>	Replace Protocol Identifier (PID) by Security Context Identifier (SCID)	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR24	11.2		Technical	<p>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.</p> <p>As an alternative the following encoding for the Security Context Identifier (SCID) is suggested.</p> <p>This approach makes unnecessary the mess to launch a new part of the standard every time a new PID is recognized.</p>	<p>SCIDs are 128-bit values that identify NFC-SEC cryptography specification. SCID value is computed as follow:</p> <ul style="list-style-type: none"> The NFC-SEC cryptography specification is identified by a URI according to the RFC3936 specification. The URI shall contain the URL of the organization maintaining the specification. A MD5 is applied on the URI according to the RFC1321 specification. The SCID is the result of the MD5 operation. <p>The SCID field is present in the ACT_REQ, but absent in all the other PDUs according to Table</p>	

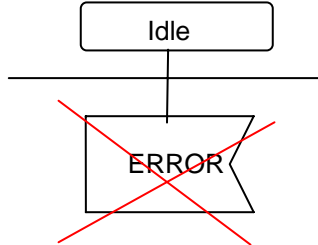
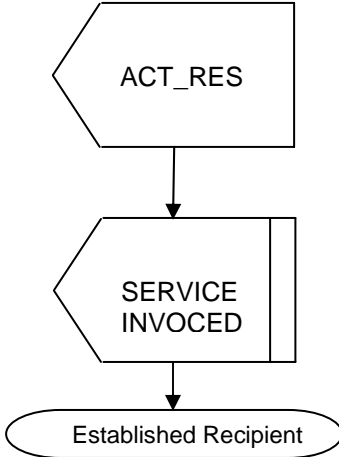
National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR25	11.3	Whole	Te	<p>There is not much content on this paragraph.</p> <p>“The TMN PDU shall contain no NFC-SEC payload” (already specified in Table 2 and in 11.4)</p> <p>“The NFC-SEC payload field shall contain an integer number of octets” (is padding required ? if yes how to identify it ?)</p> <p>“Its use is the ERROR PDU is specified in the Error sub-clause” (redundant)</p> <p>“Its use in all other PDUs depends on the PID”</p> <p>For the purpose of the interoperability of NFC-SEC implementations it's useless.</p> <p>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.</p>	<p>Either to rewrite it completely or to remove it.</p> <p>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.</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR26	11.4	Whole	Ed	<p>The information there is redundant with the content of Table 2.</p> <p>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)</p>	Remove section 11.4	
FR27	11.5	Whole	Te	<p>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 ..." .</p> <p>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.</p> <p>Finally, apart from the zero-terminated byte string requirement, the very limited amount of information here is redundant with Table 2</p>	Remove 11.5	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR28	12	Whole	General Te	<p>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.</p> <p>The sentence "This clauses specifies rules for the NFC-SEC protocol" is to be avoided</p>	<p>Replace sentence "This clauses specifies rules for the NFC-SEC protocol" by</p> <p>" 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"</p>	
FR29	12.1	Fifth Bullet	Te	<p>"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"</p> <p>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.</p>	<p>(1) Remove this bullet or (2) put this text as a NOTA warning of the difference between ERROR SDU and ERROR PDU.</p>	
FR30	12.2	First Bullet	Te	<p>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).</p> <p>If such a discovery mechanism is not provided the bullet is useless.</p>	<p>Complete the protocol specifying a discovery mechanism for the maximum length acceptable for a PDU or remove this bullet</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR31	12.4	Whole	Te	<p>Unclear and incomplete paragraph. Basic issues addressing security concerns aren't addressed</p> <p>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?</p> <p>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.</p> <p>(as an example refer to ISO/IEC 7816-4 mechanism for Secure Messaging)</p>	<p>Replace the first sentence by the following:</p> <p>"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".</p> <p>"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"</p> <p>Add then the following</p> <p>" 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"</p> <p>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.</p>	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR32	Annex A	First sentence	Te	<p>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”</p> <p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> 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” 	
FR33	Annex A.3	List of SDUs	Te	<p>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</p> <p>This SDU should include the type of the service and the Security Context Identifier</p>	<p>Add the following Confirm SDU to the list</p> <p>“Service Invoked</p> <p>Indicates the receipt of a Service Request (type of service, SCID)”</p>	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR34	Annex A.4	A.4.1	Te	<p>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</p>	<p>Delete</p> 	
FR35	Annex A.4	A.4.1	Te	<p>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.</p> <p>This SDU is to be included in Annex A.3</p>	<p>Modify the SDL diagram follows by inserting the "Service Invoked" SDU:</p> 	

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR36	Annex A	A.4.4	Te	<p>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.</p> <p>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</p> <p>The machine state of the NFC-SEC peers remain anyway at the “Confirmed” State.</p>	<p>Add the following to the flowchart:</p> <pre> graph TD A[Confirmed_SSE] --> B[/RETRIEVE SECRET/] B --> C[/RETURN SECRET/] C --> D[Confirmed_SSE] </pre>	

National Committee	Clause/Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	Comments
FR 37	Annex B	Clause B.4	Te	<p>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.</p> <p>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!</p>	<p>Remove Annex B which has nothing to do in this standard</p> <p>Make things properly: proceed to amend what is to be amended first and only then try to have this DIS approved.</p>	

Template for comments and secretariat observations

Date: 2009-08-25	Document: 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
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.		
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.	
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.		

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	<p>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.</p> <p>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."</p> <p>This text implicitly and undesirably indicates a possibility to apply DIS 13157 on the interface for the IC Cards. It should be avoided.</p>	<p>The SCOPE of DIS 13157 should be changed as follows:</p> <p>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.</p>	
JP 2	9.4	2 nd sentence	te	<p>When a NFCIP-1 device was set on a cradle and multiple transaction is ongoing, in this use-case is not covered.</p> <p>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.</p> <p>This use-case is usually happen when NFCIP-1 is used with cradle.</p>	<p>The sentence should be changed as follows:</p> <p>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.</p>	
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).	
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).	

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	<p>The specification of length reduction value (LRi) is different from the ISO/IEC 18092. It is technical changing request.</p> <p>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.</p>	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).	
JP 6	B.4	Figure B.2	te	<p>The specification of length reduction value (LRt) is different from the ISO/IEC 18092. It is technical changing request.</p> <p>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.</p>	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).	
JP 7	B.4	Figure B.2	ed	<p>Typo.</p> <p>bit 6: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.</p>	<p>Typo correction:</p> <p>bit 6: RFU. The Target shall set it to ZERO. The Initiator shall ignore it.</p>	
JP 8	B.4	Table B.3	te	<p>A new type of PFB is introduced for the ISO/IEC 18092. This is a technical change request to ISO/IEC 18092.</p>	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).	

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.

Template for comments and secretariat observations	Date: 2009-08-25	Document: ISO/IEC DIS 13157
---	------------------	------------------------------------

1	2	(3)	4	5	(6)	(7)
MB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment²	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
KR			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		

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.

Singapore's vote for SO/IEC DIS 13157 Information technology -- Telecommunications and information exchange between systems -- NFC-SEC: NFCIP-1 Security Services and Protocol

DISAPPROVE with comments:

SG1) All references to ECMA 340 shall be changed to ISO 18092 or ISO 18092:2004 appropriately.

SG2) This document shall be named as ISO 13157-1.

SG3) All reference to ECMA 386 shall be changed to ISO 13157-2 (i.e. the second ballot document).

SG4) Page 19 of 30, clause 11.2 "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.

Template for comments and secretariat observations

Date: 15.07.2009	Document: ISO/IEC 13157
------------------	-------------------------

1	2	(3)	4	5	(6)	(7)
MB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment²	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
GB	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.	

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.