Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14104
Date:	2009-10-06
Replaces:	
Document Type:	Summary of Voting/Table of Replies
Document Title:	Summary of Voting on ISO/IEC DIS 13158, Information technology -- Telecommunications and information exchange between systems -- NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES
Document Source:	ITTF
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	10

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 13158	**Committee**	ISO/IEC JTC 1/SC 6
Edition number	1		
English title	Information technology -- Telecommunications and information exchange between systems -- NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES		
French title	Technologies de l'information -- Télécommunications et échange d'information entre systèmes -- Norme de cryptographie NFC-SEC-01: NFC-SEC utilisant ECDH et AES		
Start date	2009-03-27	**End date**	2009-08-27
Opened by ISO/CS on	2009-03-27 00:07:30	**Closed by ISO/CS on**	2009-08-29 00:17:37
Status	Closed		
Voting stage	Enquiry	**Version number**	1
Note			

Result of voting

P-Members voting: 20 in favour out of 23 = 87 % (requirement >= 66.66%)

(P-Members having abstained are not counted in this vote.)

Member bodies voting: 3 negative votes out of 25 = 12 % (requirement <= 25%)

Approved

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			20	3	14
TOTALS			22	3	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
Korea, Republic of	**KATS**	**P-Member**	Korea,Republicof(KATS).doc
Singapore	**SPRING SG**	**P-Member**	Singapore(SPRINGSG).doc

French comments on ISO/IEC DIS 13158

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 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 mechanism 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 bellow.

Date	Document
30/6/2009	Comments on Fast Track DIS ISO/IEC 13158

National Committee	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	TC47 dispositions
FR1	Whole Document		General	The choice made for the pair of cryptographic protocols proposed is a good one, and ensures the creation of a robust secure channel. However, both crypto-algorithms (ECDH and AES) are already been standardized and therefore the real question is the added value of such Fast Track proposal. DIS ISO/IEC 13158 actually is a mapping of these algorithms into the PDUs of the NFC-SEC protocol, to show how the NFC-SEC services may be provided. Therefore the problems and limitations noted above for DIS ISO/IEC 13157 are not completely solved. More precisely DIS contains material typical for an Informative Annex to be added to DIS ISO/IEC 13157 instead of an independent standard.		

Template for comments and secretariat observations

Date: 2009-08-25	Document: **ISO/IEC DIS 13158**

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.

Template for comments and secretariat observations	Date: 2009-08-25	Document: **ISO/IEC DIS 13158**

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
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 on ISO/IEC DIS 13158 Information technology -- Telecommunications and information exchange between systems -- NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES

DISAPPROVE with comments:
SG1) This document shall be named as ISO 13157-2.

SG2) All reference to ECMA 385 shall be changed to ISO 13157-1 (i.e. the first ballot document).