Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14201
Date:	2010-01-28
Replaces:	
Document Type:	Disposition of Comments
Document Title:	Disposition of Comments on the ISO/IEC DIS 13158
Document Source:	Barcelona BRM
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	3

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 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
SG1				This document shall be named as ISO 13157-2		Accepted
SG2				All reference to ECMA 385 shall be changed to ISO 13157-1 (i.e. the first ballot document)		Accepted
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 NOTE 2 in 13157-1
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.		Duplication of DE 1 on 13157 See DoC for 13157-1
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.	Duplication of DE 2 on 13157 See DoC for 13157-1
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.		Duplication of DE 3 on 13157 See DoC for 13157-1

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
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.		Noted This standard has normative requirements

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.