Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14108
Date:	2009-10-13
Replaces:	
Document Type:	Other document (Defined)
Document Title:	The BRM convenor's remark for the BRM of NFC-SEC DIS 13157 and DIS 13158
Document Source:	BRM Convenor
Project Number:	
Document Status:	For the BRM of Fast Track DIS 13157 and DIS 13158.
Action ID:	FYI
Due Date:	
No. of Pages:	11

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

Welcome to the BRM of NFC-SEC DIS 13157 and DIS 13158

San Jose, Nov 12, 2009

Convener: Mr. O. Elzinga, Ecma Intl.

Project Editor: Mr. R. Meindl, Austria

Secretary: Ms. Jooran Lee, Korea

Draft standards to be addressed

- DIS 13157 based on ECMA-385
  - NFC-SEC: NFCIP-1 Security Services and Protocol
- DIS 13158 based on ECMA-386
  - NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES

Draft agenda

1. Opening (09:00)
2. Roll Call of Participants
3. Review of purpose, process and procedure of Ballot Resolution Meeting
4. Review of scope and purpose of DIS 13157 by project editor
5. Review of Ballot Result for ISO/IEC DIS 13157
6. Comment Resolution from the proposed Dispositions ISO/IEC DIS 13157
The Project Editor will draft *the proposed Disposition of Comments report*
7. Review of scope and purpose of DIS 13158 by project editor
8. Review of Ballot Result for ISO/IEC DIS 13158
9. Comment Resolution from the proposed Dispositions ISO/IEC DIS 13158
The Project Editor will draft *the proposed Disposition of Comments report*
10. Any Other Business
11. Close of Meeting

JTC 1 Fast-Track Procedure Ballot resolution meeting

•Ballot resolution meeting:

- SC shall call a ballot resolution meeting in case of negative votes or contentious technical comments;
- NO-voters *must* attend;
- To turn NO-votes into YES-votes.
  - By approving disposition of comments; Preferably by consensus, otherwise by majority vote.
  - NB or NC shall confirm their vote change to "approve" to ITTF in writing.

•Within one month following the meeting, the International Editor drafts:

- the final DIS text; and Disposition of Comments report from proposal versions amended and approved in the meeting.
- per 13 in ISO/IEC JTC 1 directives 5th edition, 3rd version.

DIS 13157

- Title: Information technology -- Telecommunications and information exchange between systems -- NFC-SEC: NFCIP-1 Security Services and Protocol
- Scope: This standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.
- Purpose: excerpt of *Ecma/TC47/2009/003* …targeted use cases focus on supplementing the active and passive peer-to-peer modes of ISO/IEC 18092 which are not related to card technologies in ISO/IEC 14443 or their standardized Security layer (ISO/IEC 7816-4).

NFC-SEC White Paper

Ecma/TC47/2008/089 *..excerpt*

- NFC security standards will be deployed for all those NFC connections which require protection against eavesdropping and data manipulation and which do not necessarily require application specific encryption mechanisms.
- A typical example is the initial association ("pairing") of devices for longer range wireless communications. Bluetooth or WiFi pairing protocols will use NFC security standards to exchange security-sensitive connection contexts on a protected NFC connection before switching to their respective longer range wireless technologies.
- NFC-SEC-01 provides the message contents and the cryptographic methods to enable secure communication between NFC devices that do not share any common secret data ("keys") before they start communicating with each other.

DIS 13157 Ballot Result

- Ballot was Approved with end date: 2009-08-27
- P-Members voting: 18 in favour out of 23 = 78 % (requirement >= 66.66%)
- Member bodies voting: 5 negative votes out of 25 = 20 % (requirement <= 25%)
- Ballot response by members (see *tc47-2009-045.zip)*
  - Approve: 18
  - Disapprove: 5
  - Abstain: 15
  - No response: 6
- Draft DoC
- Draft DIS13157 Rev

DIS 13158

- Title: Information technology -- Telecommunications and information exchange between systems -- NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES
- Scope: This International Standard, NFC-SEC-01 specifies the message contents and the cryptographic methods for PID 01. This International Standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity.
- Purpose: excerpt of *Ecma/TC47/2009/003* …provides the message contents and the cryptographic methods to enable secure communication between NFC devices that do not share any common secret data ("keys") before they start communicating with each other

DIS 13158 Ballot Result

- Ballot was Approved with end date: 2009-08-27
- P-Members voting: 20 in favour out of 23 = 87 % (requirement >= 66.66%)
- Member bodies voting: 3 negative votes out of 25 = 12 % (requirement <= 25%)
- Ballot response by members (see *tc47-2009-046.zip)*
  - Approve: 20
  - Disapprove: 3
  - Abstain: 14
  - No response: 6
- Draft DoC
- Draft DIS13158 Rev

Any Other Business