

INCITS B10.1 N03-010  
Apr 30, 2003

## MEETING MINUTES

INCITS B10.1 - IC Cards with Contacts

April 30, 2003  
Marriott Courtyard – San Diego Central  
San Diego, CA

1. Call to order – joint session with B10.5 for initial topics
  - Introductions and welcome to new members
  - Review of agenda B10.1 N03-005  
Approved with no changes
2. Approval of minutes N03-002  
Approved with no changes
3. Reviewed activity during joint session
  - N-03-004 WG4 meeting notes and presentations
  - Ballots for today (single vote for all) on the restructure of 7816
    - ◆ SC17 N 2268 – FCD Part 4
    - ◆ SC17 N 2266 – FCD Part 5.2
    - ◆ SC17 N 2270 – FCD Part 6
    - ◆ SC17 N 2272 – FCD Part 8
    - ◆ SC17 N 2274 – FCD Part 9
  - Five Year Systematic Review Request ([in030344](#))
    - ◆ ISO/IEC 7816-1
  - SC17 N 2299 – CD Part 3
    - ◆ Need to review the document and prepare comments by email
4. WG4 Report by Jim Russell
  - Ref: N03-004 WG4 meeting notes and materials - Rennes March 2003.zip
    - ◆ Japanese proposal – national ID card
    - ◆ Use of ASN.1 proposal
    - ◆ IBM proposal for hierarchical name space
    - ◆ Preliminary WD of 7816-3 reviewed and released for CD ballot
    - ◆ FCD 7816-11 comment resolution – final FCD with comments expected shortly for review before release as FDIS
    - ◆ Interconnection Task Force was cancelled

- ◆ 7816-12 USB Task Force preparing CD
    - \* The scope of the WD was changed dramatically after meeting with the USB technical body. The card will not be a separate device type.
  - ◆ ISO/IEC 7816-15 is at FDIS level. US comments for including tags from ASN.1 module were not accepted. We may propose a new work item to include them in the text in a different manner. The text is not reader-friendly.
  - ◆ The schedule of future meetings and activities was reviewed.
    - \* June 23-27, Colorado Springs, CO hosted by Atmel
    - \* September 22-26, Helsinki, Finland, Nokia hosting
    - \* Optional December 1-5 in Paris or London
5. Call to order – separate session
6. WG4 work activity – ballots – recommendations to B10
- ISO/IEC 7816 FCDs for parts 4, 5.2, 6, 8 and 9
    - ◆ Developed comments and positions on all five parts as a single vote
    - ◆ SC17 N 2268 – FCD Part 4
      - \* Editorial comments attached (
    - ◆ SC17 N 2266 – FCD Part 5.2
      - \* Editorial comments attached
    - ◆ SC17 N 2270 – FCD Part 6 (no comments)
    - ◆ SC17 N 2272 – FCD Part 8 (no comments)
    - ◆ SC17 N 2274 – FCD Part 9 (no comments)
  - Five year systematic Review
    - ◆ ISO/IEC FDAM 7816-1 - vote to reaffirm the standard
      - \* Moot Point. Amendment prepared and out for imminent ballot
      - \* Apparently the ISO server had a severe outage and this was lost and not noticed.
  - ISO/IEC CD 7816-3 released Apr 1, 2003 with 4 month ballot
    - ◆ Closing August 1, 2003
    - ◆ Will have to handle as a letter ballot
      - \* Comments together by June 15
      - \* B10 letter ballot
    - ◆ All members were asked to review the CD and send comments to the chairman who will send collect them and send them to all members.
  - ISO/IEC FCD 7816-11
    - ◆ Waiting to review comment resolution and final FCD draft for release as FDIS
7. Future work efforts
- FDIS 7816-15 Cryptographic Application (Imminent request)
    - ◆ US comments rejected
    - ◆ Need to determine next course of action
      - \* New work item to embed object tags in part 8

- \* Need to coordinate our request with the use of ASN.1 in other standards
- \* See WG4 report for presentation on ASN.1

8. Liaison activity

- WG3 Travel Documents
  - ◆ Major change in direction
  - ◆ More biometric data with need for digital certificate
  - ◆ More use of CBEFF header in the structure
- WG11 Interoperability and Biometrics on cards
  - ◆ No activity on biometrics. LDS withdrawn by WG3
  - ◆ Group could address interoperability issues with GSC-IS
- M1 Biomertics
  - ◆ Has formed subgroup on biometric formats; preparing for SC37 work groups
  - ◆ Adopted BIOAPI, CBEFF and 7816-11

9. Next B10.1 meetings

- Aug 27, 2003                      Datacard,/3M, Minneapolis, MN
- January TBD, 2004              Intellicheck, Florida

10. Next WG4 meetings and expected agendas

- June 23-27, Colorado Springs, CO; Atmel hosting for USA (with remaining B10 \$)
  - ◆ 7816-4, 5, 6, 8, and 9, comment resolution
  - ◆ 7816-15 FDIS handling
  - ◆ 7816-12, review for release as CD
- List of delegates
  - ◆ James Russell (HOD)
  - ◆ Brian Beech
  - ◆ Philippe Hiolle
  - ◆ Philip McCauley (may attend)
  - ◆ Dale Anderson, ATMEL (host)
- September 22-26, Helsinki, Finland, Nokia hosting
  - ◆ 7816-3 CD1, comment resolution
- Optional December 1-5 in Paris or London
  - ◆ 7816-11, FDIS handling
  - ◆ 7816-2, revision (if approved)
  - ◆ 7816-4, 5, 6, 8, and 9 FDIS handling?
  - ◆ 7816-12 CD1, comment resolution

11. Other Old Business

- No old business

12. New Business

- No new business
13. Adjournment
- Meeting adjourned at 4:25 PM.
14. Joint meeting at 4:30 to discuss status and next steps with NIST GSC-IS
- The goal was to explore a way to take the GSC-IS to an Global Standard.
  - Is there an existing B10 group that can handle this work?
  - Where should the work be targeted for an ISO standard
  - The results of this meeting will be presented to B10 on May 1, 2003
    - ◆ NIST will continue to work on the document for July release
    - ◆ NIST will send this to B10 members for review
    - ◆ Call for volunteers to work on the standard

US Comments on ISO/IEC SC17 N2268 FCD 7816-4

All comments are Editorial. There are no technical comments.

No.	Page	Location	Modification	Reason
1.	vi	Paragraph 2	Replace the sentence with: This part of ISO/IEC 7816 is an application level standard and is technology independent. The application level standards apply equally to IC cards with contacts and contactless IC cards.	Accuracy. Clarify intent of SC17.
2.	1	Normative references	Make consistent with references used in the FCDs for parts 5.2, 6, 8 and 9. Remove dates from the references.	Grouping of revision of standards
3.	3.	3.19 a	Insert the definition of the word “file” <b>file</b> an organized collection of data that is addressed by an identifier Vocabulary?	Referenced extensively but not defined.
4.	7	Last paragraph	Move before the previous paragraph.	Clarity. Finish discussion of command parameters.
5.	8	5.1.1 First paragraph third sentence	Change to read: “Bit 8 of CLA distinguishes between ...”	English.
6.		5.1.1 Second paragraph second sentence	Change "CLA set to 00x xxx and CLA set to 01xx xxxx" to "CLA set to 00x xxx (type four) and CLA set to 01xx xxxx (type sixteen)"	Clarity
7.	9	5.1.2 first paragraph, second and third sentence	Delete the second sentence entirely and delete the word “consequently” in the third sentence.	No reason to reference Part 3. Does not apply to contactless.
8.	11	Third paragraph.	Make the second sentence the first sentence	Reference the table before the values in the table.
9.	11	Third paragraph	Change the phrase “are not interindustry” to “are not used in interindustry interchange”	Clarity, specificity
10.	11	Penultimate paragraph	Delete the parenthetical reference to Part 3. Revise sentence to read: “Two values of SW1 are specified below and are independent of any transmission protocol.”	Superfluous English
11.	12	Table 7	Add initial column the same as in Table 6	Clarity
12.	15	Last paragraph	Delete the paragraph.	Unnecessary restriction on tags. 7816 reserves all application tags and defines relationships

				with other tag authorities.
13.	16	5.2.4.3 Last line	Change “whilst” to “while”	Consistency
14.	16	Penultimate dash	Add: These other files are said to be immediately under the DF.	Clarity for use on page 17 under selection by file identifier.
15.	17	5.3.1, 3rd paragraph, last sentence	Replace "In order to select unambiguously..." with "In order to unambiguously select..."	English
16.	22	First paragraph	Replace semicolon with a period after (see Table 13). Capitalize the next word “Each”.	Clarity, English
17.	22	Second dash	Replace semicolon with a period after “ISO standard.” Delete the word “either and insert the following as the beginning of the next sentence: “The identified object(s) is Replace the first “or” with a comma.	Clarity, English
18.	22	First Example	The length of the DO should be ‘0B’ not ‘09’	Accuracy
19.	22	5.4.3 first paragraph	Insert the phrase “to be able” between the words “security status” and “to process” and before “to access”	Clarity, English
20.	22	5.4.3 second paragraph	Delete the text “; it” and replace with the word “and”	Clarity, English
21.	22	5.4.3 fourth paragraph	Replace semicolon with a period after “data objects”. Capitalize the next word “Each”.	Clarity, English
22.	26	First paragraph	Replace the first sentence Secure messaging protects all or part of a command-response pair by ensuring two basic security functions: data confidentiality and data authentication. Delete the fourth and fifth sentences.	Clarity, English
23.	26	Table 27	Delete the last entry. Context specific tags should not be completely reserved!	Application level tags have already been reserved!
24.	27	Fourth dash	Replace the word “integrated” with “included” in both uses.	English, accuracy
25.	30	6.2.3.1 Second paragraph	Replace the word “integrate” with “include” in both uses.	English, accuracy
26.		6.2.3.1 First dash	Delete the last two words, “to integrate.”	Clarity
27.	30	6.2.3.1 Second dash, first sentence	Change to read: The padding shall apply after the last data object included in the data block.	Clarity

28.		6.2.3.1 Second dash, last sentence	Replace the sentence with: “Padding for authentication has no influence on transmission.”	Clarity
29.		6.2.3.1 Add new third bullet	Padding bytes shall not be transmitted.	Specificity, clarity
30.	30	6.3.1 First paragraph	Replace the word “integrate” with “include”	English, accuracy
31.	47	7.4.2 NOTE	Delete – background is not necessary	This is application level not technology level.
32.	56	8.1 second dash	Include retrieval of the EF.ATR (tag ‘5F51’).	ATR file available as well as historical bytes.
33.	68	Annex B title	Change to: Examples of Object Identifiers	Clarity
.				

US Comments on ISO/IEC SC17 N2266 FCD 7816-5.2

The comment is Editorial.

No.	Page	Location	Modification	Reason
1.	1	Normative references	Make consistent with references used in the FCDs for parts 4, 6, 8 and 9. Remove dates from the references.	Grouping of revision of standards