

Minutes

INCITS B10.1 - IC Cards with Contacts

January 23, 2002
San Marcos Hotel
Chandler, AZ

1. Call to order by the Chairman, J. Russell at 9:00
 - Printed agenda distributed to all present

2. Introductions and welcome to new members. The chairman introduced Phil McCauley as the Vice Chairman and then reviewed the status of all members. He will contact AT&T and Mobile-Mind for names of principals. Attendees were:

John K. Ho	3M	P
Gerry W. Smith	American Express Technologies	P
Peter Saunders	American Express Technologies	A
Francis Christian	ATMEL	P, L-B10.5
Brian Beech	DataCard	P
Lucille Chrispen	Defense Information Systems Agency / DOD	P
Gilles Lisimaque	Gemplus	P
Philip McCauley	MAG-TEK	P, Vice Chairman
Philippe Hiolle	MasterCard International	P
James F. Russell	MasterCard International	A, Chairman
Robert Warnar	Vissers'	O

3. Review of agenda
 - Phil McCauley handed out CD-ROMs with all documents.
 - Discussion of joint activity with B10.5 moved from item 8 to item 6 on the agenda
 - Added two voting recommendations to prepare
 - ◆ SC17N2061 CD7816-6 - Interindustry data elements for interchange
 - ◆ SC17N2064 CD7816-16 - Registration of integrated circuit manufacturers
 - The discussion regarding the review of the restructuring of 7816 was added under new business

4. WG4 Report by Phil McCauley (distributed by email, included below)

5. Next WG4 meeting and work activity

- Discuss comments made on CD 7816-11
 - The US comments were made in cooperation with CBEFF, the recognized leader in the area of biometrics in the US. This position may promote significant changes in the direction of the standard. Clearly, WG4 has limited expertise and there is no other ISO committee. See item 9 below.
- Restructuring of 7816 parts 3, 4, 8, 9
 - The draft CDs and ballots were released on Monday Jan. 21, 2002 with a closing date of April 21, 2002.

Due to the nature of the changes, the committee will request an extension. This may be a delicate matter since WG4 wants to consider the ballot results at the May meeting.

6. Discussion of joint activity with B10.5 (future joint meetings)

- J. Russell reviewed the history of the IC card committees. WG4 and the US TAG, B10.1, were formed develop standards for IC cards which then had only cards with contacts. This resulted in ISO/IEC 7816. When the contactless card technology work began, WG8 and the US TAG, B10.5, were formed to develop the technology standards. The application level parts of ISO/IEC 7816 (parts 4 and on) were adopted for use on contactless cards.
- The work on ISO/IEC 7816 has continued with application level development. The technology parts 1, 2 and 3 have been enhanced to include the latest technological developments with low voltage cards. The application portion of the standard is being reorganized (parts 4, 8, and 9) and some application level material in part 3 is being moved to part 4 and some technology material is being moved from part 4 to part 3. The result will be that the normal operational application information will be in part 4. Part 8 will contain some special cryptographic material and part 9 will deal with card life cycle. Parts 5 and 6 remain intact.
- The work on the contactless technology evolved to three standards: closely coupled, vicinity and proximity. This work is in its final stages of development and is entering a maintenance mode. The subcommittee now can address other standards.
- It has been difficult to get US attendance at B10.1 and WG4 meetings recently. Additional members of the US delegation are needed.

- The group discussed the option of either convening joint meetings or combining the two subcommittees. Some concerns were expressed that this might lead to meetings requiring more than one day. B10.1 meetings have historically been only one day or less and recent meetings have been half days. The group is willing to try a joint meeting provided it lasts only one day. The technology aspects can be handled in breakout sessions if required.
 - The chairmen, Jim Russell and Francis Christian, will develop a joint agenda for the next meeting. If this is not practical, then separate technology sessions will be scheduled.
7. Votes to provide to B10 plenary. See below for recommendations sent to B10.
- FDAM 7816-3 (anticipated)
 - ◆ This has not been received, but the recommendation will be to approve.
 - SC17 N 2037 PDAM 7816-2 (SC17 N 2037)
 - ◆ Approval. No comments.
 - SC17 N 2047 NWI - Interconnection system for components on a card
 - ◆ The recommendation is to disapprove with comments. (see below for comments)
 - SC17N 2061 – CD 7816-6 Interindustry data elements for interchange
 - ◆ The recommendation is to disapprove with comments. The US will change its vote to approval if the comments are accepted. (see below for comments)
 - SC17 N2064 ISO/IEC 7816-13 Registration of integrated circuit manufacturers
 - ◆ The recommendation is to disapprove with comments. (see below for comments)
8. Comments on FCD 7816-15 - Cryptographic token on a card
(This hasn't been issued yet, but we plan to prepare a submission)
- The main theme is to make the document usable by non-technical people
 - The key issue: the actual data structures and tags should be documented as such!
 - The subcommittee will prepare a new section 9 for the FCD that specifies the data structures and tags based on the ASN.1 specification.
9. Liaison activity
- B10.8 - Driver's license Meeting Thursday AM
 - ◆ WG10 has a new convener.
 - Proposed B10.11 - Biometrics
 - ◆ Status of new work group: JTC1 vs. SC17. J Russell presented a description of the current situation.. JTC1 had an initial meeting of a new working group, M1. This group will probably be an oversight group that relies on B10's subcommittee on Biometrics for technical work. M1 is voting to endorse the BIOAPI and the CBEFF as standards. We are using these standards for ISO/IEC CD7816-11.

10. Next B10.1 meetings
 - May 8, 2002 - DuPont – Richmond, VA
 - August 14, 2002 - MasterCard – St. Louis, MO

11. Next meetings
 - May 13-17, 2002 - Munich, Germany
 - September 30 – October 4, 2002 - (US or Denmark)

12. Old Business – none

13. New Business

The restructure of ISO/IEC 7816 was discussed. The following people will address the various parts.

 - Part 3 – Gemplus, MagTek and MasterCard
 - Parts 4, 8 and 9 – American Express, Gemplus and MasterCard

14. Adjournment at 3:30 PM

Recommendations to B10 on SC17 Ballots from B10.1
Prepared January 23, 2002

1. FDAM 7816-3
This FDIS-level ballot has not been received, but the vote will be to approve.
2. SC17 N2037 PDAM 7816-2/DAM1 Dimensions and location of the contacts –
Amendment 1: Assignment of contacts C4 and C8

The US votes to approve with no comments.
3. SC17 N2046 NWI – Sizes and locations of a finger print sensor and display device

B10.1 concurs with disapproval of the NWI due to the lack of a working draft.
4. SC17N2047 NWI – Interconnection system for components on a card

The US votes to disapprove the new work item.

Reasons:

1. The US does see the justification or benefit of standardizing the components contained in a sealed package at this time. Each card manufacturer will require the latitude to develop a cost-effective solution.
 2. The application requirements are not well known at this time.
 3. The proposal should be submitted with an initial working draft.
 4. The proposal is missing the annex regarding patent information.
5. SC17N 2061 – CD 7816-6 Interindustry data elements for interchange

The US votes to approve with comments. The US will change its vote to approval if the comments are accepted.
 1. Clause 7, table entry '5F4B'
Change name of data element to 'reserved for historical use (see note 2)'
Reason: editorial, clarity for reader
 2. See comments in response to SC17 N2064 below. The result will be to retain the specification of the registration authority for IC manufacturers in part 6 but to delete the table of IC manufacturers.
 6. SC17 N2064 ISO/IEC 7816-13 Registration of integrated circuit manufacturers

The US votes to disapprove with comments.

The US agrees that there is a need to identify IC manufacturers and to have a list registered identifiers. However, the industry changes are so frequent that maintaining the list of company names and addresses in an ISO/IEC standard is not responsive to the needs of the industry. We recommend that such a list be freely available from one of

the standards committee's web sites with the URL of that web site specified in an ISO/IEC standard.

The process of assigning identifiers is defined in ISO/IEC 7816-6 AM1. We recommend that this standard be retained with the definition of the registration authority but with the deletion of the list of registered manufacturers. We recommend that this list of registered manufacturers be implemented as a standing document on the SC17 web site and that it be readily available for download to any interested party. The registration authority should update the standing document as new identifiers are assigned.

In addition, the US requests that the registration authority implement a procedure to validate the company names and addresses on a frequent basis, preferably at least once each year. The following conditions are noted as the rationale for this request:

- Motorola was purchased by Atmel and no longer is a manufacturer
- Emosyn –EM Marin – this joint venture has disappeared and each company is separate
- Hyundai is now Hynix . It is in bankruptcy and Micron may purchase it.
- Some known companies are not registered:
 - ◆ Goldkey (Taiwan)
 - ◆ Datang (China)
- The addresses and persons to contact need to be affirmed if the list is to be a reliable source of information.
- The addition of email addresses and web site URLs to the information will facilitate communication with the company representatives and the dissemination of information about the manufacturer's products.

The US recognizes the additional effort that will be required and suggests that the registration authority may have to charge a modest fee to recover the cost of the extra efforts.

7. Four SC17 ballots to be voted in unison for the restructure of ISO/IEC 7816:
- SC17 N 2059 ISO/IEC PDAM 7816-3/Amd 2 Structures and transmission of APDU messages
 - SC17 N 2060 ISO/IEC CD 7816-4 Interindustry commands for interchange
 - SC17 N 2062 ISO/IEC CD 7816-8 Interindustry Commands for a cryptographic toolbox
 - SC17 N 2063 ISO/IEC CD 7816-9 Interindustry commands for cards and file management

The revisions are quite extensive and will require a great deal of work. Although they are supposed to be editorial, some technical changes were made. While this is a first CD on the revised text, we will require more than a normal period of time to prepare our comments and obtain approval with a 30 day letter ballot. We will ask B10 to request an extension. If this is not granted, we may have to present our comments at the next WG4 meeting which is scheduled for May 13-17, 2002.

Report of WG4 meeting
December, 2001
Philip McCauley, MagTek, HOD

1 Attendance

Delegates were present from Canada, France, Germany, Japan, Netherlands, and the US.

2 Identification cards - Integrated circuit(s) cards with contacts - Part 15 : Cryptographic token information in IC Cards

Reviewed comments and resolved most. Had some problems with U.S. comments because strong language was used is asking for non-specific changes. I must agree with the committee that the normal method of presenting comments is with specific (read that "precise text") changes requested and the reasoning behind the request. The committee considers such comments in a much more favorable light and works to resolve them well. This is a sensitive issue for both the committee and myself. As things stand at this point in time, the smart card industry in the US gives minimal support to B10.1 and ISO standardization processes. If they think that there is more work to be done, they should participate! If they are content to let European companies to do the work, they should at least not complain about the result.

Specifically, the US comment titled "Title and Scope" was well received. Changes were made to the scope to more clearly reflect the title. The comment about the specificity of tags was mostly ignored as WG4 considers the tags to be unambiguously defined using the ASN.1 syntax. If there is confusion about this, we can easily get clarification. I will distribute to B10.1 members a document authored by RSA Labs that serves as a good tutorial about ASN.1. I do not profess to be an ASN.1 expert, but it has been demonstrated to my satisfaction that tags are unambiguous. WG4 respectfully invites the US to submit a proposal for showing the tags in a more "7816" format.

The US comment titled "Files and Objects" was well received. The group felt that such an option might be useful. That said, the US is invited to submit a proposal!

In the US comment titled "Sharing the Cryptographic Information with other Applications" it is evident that there is a misunderstanding of what was meant by "sharing". The scope has been modified to indicate that sharing is with applications in the outside world, not with other applications in the card. The commands used to access the information are as indicated in other parts of 7816, e.g. Select File, Read Binary, Read Record etc. An examination of the ASN.1 structure will show how these are indicated.

The editorial comments were well received and solved appropriately.

3 Resolution of comments on ISO/IEC FCD 7816-5, Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers

All comments resolved. Clause 7.5.5 (Registration Category 'E') was changed to read:

“Values in the registration category 'E' are to be used by standard applications not linked to a provider. The standard application identified is 'E8' followed by the value of the Object Identifier pointing to the standard that defines the application. The coding of the identifier extension is application specific. Other codings in category 'E' are reserved by SC17.”

This was done to allow more flexibility in the use of category 'E'.

4 Reorganization of 7816-4

We reviewed working drafts for 7816-3 Amendment 2 (APDU mapping), 7816-4, 7816-8, and 7816-9 making some minor changes. The drafts, with the agreed changes, will be balloted as first CD together. In my opinion, the effort has been a good one, though there will be some problems that need correction. The reorganization is substantial and we (B10.1) should anticipate spending significant time reviewing these drafts, submitting comments as appropriate.

5 Proposed WD ISO/IEC 7816-12, USB electrical interface and operating procedures

The proposal was discussed. It was decided that a task force is needed to complete and improve the Working Draft prior to release as a CD. Steffen Drews, the editor and representative of Philips Semiconductors, told the group that the semiconductor manufacturers think that in about two years time they will have solved the problem of internal oscillator precision necessary for running full speed USB without an external clock. In light of this the group decided, for the time being, not to pursue standardization of an external clock mechanism. There was some talk of what is needed on the “host” end to deal with a USB Smart Card. The possibility of specifying an “API” was discussed and there was some interest expressed. I think that this topic will result at most in something low level (a device class specification) at most. Work on this standard will continue with a document released for CD ballot possibly as early as June of 2002.

6 Biometrics

Though 7816-11 was not on the agenda for this meeting, I discussed the US comments informally with Bruno Struif, the editor of 7816-11. He has some concerns about some of the proposed changes that may be valid. I intend to pursue convening an informal meeting with the CBEFF drafting group (F. Podio, C. Tilton, L. Reinert), Bruno, and members of B10.1. Such a meeting may help us to find common ground allowing us to improve the standard.

7 Next meeting

The next meeting will be held the week of May 13-17, 2002 in Munich.