

Minutes of the August 27, 2003, B10.5 meeting

The B10.5 meeting in Minneapolis MN was called to order with the B10.1 group. The two groups held a joint meeting to listen to each other's reports so that the two groups can share general information. Then the two groups went to separate rooms for their separate meeting.

The Joint Group discussed the Gemplus document on security testing B10.5 N03-143. The consensus of the reviewers of the document was that it was a good tutorial and description of the problem and the need. It could be the subject of a technical report. The question was raised as to what can be done to provide adequate tests to assure implementers that chips meet the security requirements.

There is a Common Criteria Protection Profile that can be referenced and used to satisfy this need. The problem is not just the chip but entire system in which the card is used. The Trusted Computing Group has a subcommittee that is working on this issue. Jim Russell noted that we have no expertise in our committees but that it is very important to us. We will try to have a presentation on this subject at the next meeting regarding the information developed by the Trusted Computing Group.

The attendees were asked to introduce themselves and the roll was taken for the B10.5 group
B10.5 Voting members for this meeting are:

1. Francis Christian – FC Consulting, Rep: Atmel, Chair
David Dressen – Atmel
2. Norman Kort - Cubic
3. Barry Kefauver – Fall Hill Associates
4. Shrinath Eswarahally – Infineon Tech
5. Jim Ferguson– Innovision
6. Ray Freeman – Assa Abloy ITG
7. Jean-Marc Delbecq - VeriFone
8. Jim Dray – NIST/U.S. Government
9. Henk Dannenberg – Philips
10. Ed Barrett – Sony
11. Bob Gilson - US Dept Of Defense Manp
12. Christophe Goyet – Obertur Card System
13. Curtis Watson - TI
14. Peter Saunders – American Express
15. Won Jun – G & D

Guest and Observers for this meeting are:

1. Walt Bonneau – Three Point Consulting
2. Eric Le Saint - ActivCard
3. Mike Neumann – Schlumberger
4. Rob Dixon - OTI

New members are guests/observers for the first meeting and then a full voting member the second meeting after registering with INCITS and paying fees. There are no members in jeopardy of their voting rights at this time.

2. The Draft Agenda for, B10.5, N03-136r1r was approved with the addition of the AMEX topic.
3. The revised minutes of the April 30, 2003 meeting, B10.5 N03-134r1, were approved.
4. Report of ISO/IEC meetings and other areas of interest -
 - 4.1. David Dressen & Ed Barret gave a review of the WG8 meeting that included discussions on: Higher Baud Rates. Three proposals were submitted: Proposal 1 (data rate to 847KB/S), Proposal 2 (data rate to 13.56MB/S), Proposal 3 (data rate to 27.12MB/S). The TF2 have a discussion on the use of RFU bits within ISO14443 Parts 3 & 4 that there are concerns because of the varying use of these bits by different card suppliers. For more detail see the TF2 minutes N03-142.

- 4.2. WG3 – ICAO London July 22-23 -
Barry Kefauver gave an update on the New Orleans resolution for Travel Documents (Passports & Visas) usage for implementing biometric security. It was stated that the following biometrics and the order of usage would be applied: First, Facial Recognition is the primary biometric, optionally as a second method fingerprint, and third eye-retina. There were concerns of IP/IPR on eye retina. If IP/IPR issues were not resolved, the eye-retina biometric would be removed. In addition, it was decided that contactless chips would be used for Passports. This decision created complains by a few countries as to the implementation of only contactless devices. There were presentations also given by various teams that had previously developed successful contactless device systems. Three new taskforce were created: First: E-Passport (Devices/Chips), Second: PKI/Security, Third: LDS/Interoperability.
- 4.3. Walt Bonneau presented a brief review, of the APTA-UTFS committee structure and the primary working task groups; the Financial Management Sub-Committee and its associated Three Work Package groups addressing PICC, PCD, Security and Backend Communications, and Settlement issues to establish guidelines and standards for the transit industry.
- 4.4. Report on NIST Ad Hoc meeting -
Teresa Schwarzhoff gave a review of the August 26th “Ad-Hoc” meeting. It was stated that the Ad-Hoc attendees gave a unanimous vote of approval to submit to the B10 plenary the request to create a new work group to achieve ISO status on the NIST GSC documents. Until the JTC1/SC17 vote to approve this NP, it was stated that the AD-Hoc group would stay active to keep the work effort moving forward.
5. FCC Rule change status N03-138

Francis Christian gave a brief review on the FCC Petition. There have not any new input on the final approval by the FCC. Texas Instruments will continue to monitor and give an update report at the next B10.5 meeting.
6. SC17 Ballot recommendations for Contactless Cards:
 - 6.1. Ballot SC17N2341 - ISO/IEC 10373-6/FPDAM1 – Identification cards – Test methods – Part 6: Proximity Cards – Draft Amendment 1: Protocol test methods for proximity card
---The group recommends is - Approved with editorial comments, Attachment 1
 - 6.2. BALLOT SC17N2342 – ISO/IEC 14443-3:2001/PDAM1 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision – Amendment 1: Bit rates for *fc/64*, *fc/32* and *fc/16*
---The group recommends is - Disapproved with reasons, Attachment 1
 - 6.3. Ballot SC17N2343 - ISO/IEC - 14443-2:2001/PDAM2 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal amplitude – Amendment 2: Bit rates for *fc/64*, *fc/32* and *fc/16*
---The group recommends is - Approve
 - 6.4. Ballot SC17N2344 - ISO/IEC 10373-6/P-DAM3 – Identification cards - Test methods – Proximity cards – Amendment 3: Protocol test methods for proximity coupling devices
---The group recommends is - Approved with editorial comments, Attachment 1
7. Old Business –
 - 7.1. Peter Saunders of AMEX asked if there would be an addition to 14443 to standardize application selection for financial interoperability (A Common infrastructure and approval). A poll was taken to determine interest in such a task. The poll showed that there was a lot of interest. Peter stated that this would be a small step in achieving interoperability with 14443 and 7816 to gain co-operation with the banking industry. It was suggested that AMEX should submit a document at the next B10.5 meeting for a New Work Proposal and they agreed to do so.

- 7.2. Determine direction for the Limited Use Card:
After a group discussion it was concluded that the editor should make the suggested changes (Including Groups inputs until Sept 8, by email). Then the document will be re-submitted to SC17 for the approval of a NEW Work Item. If the New Work Item does not get approved then the B10.5 group will take the document through the INCITS process for a USA standard. The decision is to be made so that a new standard can be started at the next B10.5 meeting. See attachment 2 for more details.
8. New Business –
 - 8.1. Joe Naujokas informed B10.5 that WG1 submitted a formal request to WG8 on July 21, 2003 to review three of the tests in ISO/IEC 10373-1. The three tests are ultraviolet light, X-Ray and electromagnetic fields. After discussing these subjects, the group recommend that the test be left unchanged at this time.
9. Future INCITS Meeting Schedule
 - 9.1. January 21, 2004 Intelli-check, Palm Harbor FL
 - 9.2. April/May 2004 – TBD
10. Future ISO meetings and delegates
 - 10.1. WG8 November 24-27 - Francis Christian (HOD), David Dressen, Jim Dray
 - 10.2. SC17 October 6-7, 2003, in Singapore
11. Adjourn at 4:00 PM

Attachment 1 - Ballot Recommendations:

Ballot SC17N2341 - ISO/IEC 10373-6/FPDAM1 – Identification cards – Test methods – Part 6:
Proximity Cards – Draft Amendment 1: Protocol test methods for proximity card

Approved with editorial comments,

Comments:

- 1) Table G.2 (Test Methods) has a German language stated error that needs correction
- 2) G.4.2.2, G.4.3.2, G.4.4.2 & G.4.8.2 error noted to remove in the RF/I/O table the word Sub-carrier.
- 3) G.4.6.2 Scenario B4 Last command should also reference Note-1
- 4) G.4.7.2 Scenario B6 has same error as above.
- 5) G.4.8.2 Scenario B9 First command should reference Note-2 as well.
- 6) G.4.16.2 Scenario B18 Needs ISO14443 Note-1 as per Scenario B4 for the two I(O)'s.
- 7) G.4.15.2 Scenario B17 both commands require the ISO 14443 note.

BALLOT SC17N2342 – ISO/IEC 14443-3:2001/PDAM1 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision – Amendment 1: Bit rates for fc/64, fc/32 and fc/16

Disapproved with reasons,

Reasons:

In Section 5.4 the 100msec Minimum delay time stated to ensure that a PICC was in a Power-OFF state, is simply too long a period.

It was recommended that we provide input/edits to help clarify the document as part of the balloting. These words are stated below:

“Time to Power Off a PICC

When the field (see ISO/IEC 14443 Part-2) powering a PICC is removed for at least XX.X* msec, the PICC shall be in a Power Off State.”

Additional comments were made on the value of 100 msec by the group based on concerns over Security and Unnecessary Long Transaction times several members wanted more time to evaluate a good delay time.

The timing and process to select a good delay is was established as follows:

Input must be sent to the B10.5 Chair and other members on XX.X value by September 05, 2003.

This will allow the Chair the time to issue an email ballot for a group approval on a number for the delay by September 11, 2003.

Additional proposed changes:

Page 5 Clause 5: Change words from: Alternation of ... to: Alternating between ...

In Section 7.1.6 the US requests adding a note:

“The value of TR0 is changed from the original ISO/IEC 14443-3 standard. This is a technical change.”

Ballot SC17N2343 - ISO/IEC - 14443-2:2001/PDAM2 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal amplitude –

Amendment 2: Bit rates for fc/64, fc/32 and fc/16

Approve

Ballot SC17N2344 - ISO/IEC 10373-6/P-DAM3 – Identification cards - Test methods – Proximity cards – Amendment 3: Protocol test methods for proximity coupling devices

Approved with editorial comments.

Comment:

Error in the Contents Annex-H a German Language error bookmark not defined.

Attachment 2

Determine direction for the Limited Use Card

Presentation was given by Walt Bonneau on the latest version of the submitted July 30, 2003 "Limited Use" (LU) specification for approval by the B10.5 committee to provide a submission for either ANSI-INCITS or ISO for a new work order. It was mentioned that the LU proposal had already received varying input from the transit industry, vendors from the US, UK and Japan.

The document was reviewed by each section for general comments and input by the Group. It was concluded that there was interest in supporting this proposal but only after additional changes were to be made. These included:

- 1) Die area to card surface thickness tolerance for stacking purposes be added
- 2) Die restricted printing area be added
- 3) Removal of specific antenna types
- 4) Life cycle Table should state Minimum not Maximum
- 5) Suggested that an ISO 15497 like Type 1,2,3 card type table be added in replacement of the Life Cycle table. In addition as an informative a usage mode is given.
- 6) Move references to materials to the informative notes
- 7) Specify the Coefficient of Friction in a single "X" direction also review the stated values.
- 8) On the Electrical specification need to better define the distance read/write activation distance. Also explore using 3.0cm versus 2.54 cm.
- 9) Possible addition or modification to the 10373-6 testing document in support of LU changes/differences.

The Chair proposed after group discussion concluded that the editor make the suggested changes (Including Groups inputs by Sept 8) so that the document/proposal would be re-submitted to SC17 to proceed with the NWI. If they do not accept the document than B10.5 will take the document through the INCITS standard process. The B10.5 agreed unanimously to re-submit the "Cleaned-up document" to SC17 in time for their next meeting approval.

NCITS B10.5 Document List for 2003

NCITS B10.5	N03-100r3	Document List for 2003	F. Christian
	N03-101	Members List	F. Christian
	N03-102	Meeting Roster 1-22-2003 Clearwater	F. Christian
	N03-103	Agenda January 22, 2003 Clearwater	F. Christian
	N03-104	AMEX NP Contactless Protocol	G. Smith
	N03-105	AMEX Support document for NP	G. Smith
	N03-106	AMEX input document for NP	G. Smith
	N03-107	CTS NP on LU CSC	W. Bonneau
	N03-108	CTS Support document for NP	W. Bonneau
	N03-109	SC17N2225 Ballot	SC17 Web
	N03-110	SC17N2258 Ballot	SC17 Web
	N03-111	WG8 Calling Notice for Japan 3-2003	WG8 Web
	N03-112	B10.5 position on ballot SC17N2225	F.Christian
	N03-113	B10.5 position on ballot SC17N2258	F.Christian
	N03-114	Minutes of January 22, B10.5 meeting	R.Roebuck/F.Christian
	N03-115	B10.5 Recommendation to B10 on LUC	F.Christian
	N03-116	WG8/TF2 MINUTES TOKYO 03-03-03	F.Christian
	N03-117	WG8 March 5-7, 2003 report	F.Christian
	N03-118	Issue from SC17/WG3 &WG10	WG8 Web
	N03-119	Pres on ECMA-340	WG8 Web
	N03-120	ECMA-340 information	WG8 Web
	N03-121r1	Draft Agenda April 30, 2003, San Diego	F.Christian
	N03-122	Spectral Simulation of Type A & B	F.Christian
	N03-123	ISO Card standards relationship	P. Hiolle
	N03-124	B10.5 WG8 and TF participation	E.Barrett
	N03-125	Sony response to SC17n2301	E. Barrett
	N03-126	SC17N2301 document	SC17 Web
	N03-127	WG8n844 Austria LUC comments	WG8 Web
	N03-128	WG8n843 ISO/IEC10373-6 FDAM2	WG8 Web
	N03-129	WG8n835 ISO/IEC10373-6 PDAM1	WG8 Web
	N03-130	WG8n846 more ECMA-340 information	WG8 Web
	N03-131	WG8n849 France input on LUC	WG8 Web
	N03-132	WG8n847 June 2003 TF2 mtg information	WG8 Web
	N03-133	WG8n851 German response to LUC	WG8 Web
	N03-134	B10.5 Minutes April 30, San Diego Meeting	F.Christian
	N03-135	Hotel reg for WG8/TF2 in Colorado Springs	F.Christian
	N03-136	Agenda, B10.5, Meeting August 27, 2003	F.christian
	N03-137	Limited Use Specification Proposal Ver2.0	Walt Bonneau
	N03-138	FCC update document July 17, 2003	F.Christian
	N03-139	B10.5 N03-139 Ballots 8-27-03	F.christian
	N03-140	WG8 work projects 7/29/2003	F.Christian
	N03-141	WG8 N836 Agenda of Mtg 31 in Paris	F.Christian
	N03-142	WG8/TF2 Min Col Spgs 6/2003	F. Christian
	N03-143	Security STD Test Proposal v.01	F.Christian
	N03-144	B10.5 minutes of August 27, 2003, MTG	F.Christian