ISO/IEC JTC 1/SC 17/WG 8
Integrated circuit cards without contacts
E-mail of Secretary: andreas.lamm@din.de
Secretariat: DIN

TF3 N171 TF3 Freising minutesv5

Date of document	2013-09-13
Expected action	Info
Source	Reinhard Meindl (acting TF 3 convener)

WG8/TF3 15th meeting 12th September 2013

To prepare standards for: ISO/IEC 15693 series

Identification cards - Contactless Integrated Circuit(s) cards - Vicinity cards

Venue: ***TI Germany Gmbh, Haggertystrasse 1, D-85356 Freising, Germany***

Date: ***12th September 2013 - 9:00 to 17:00***

Attendance: ***K. Aslanidis (DE), J. Perez(CH), D. Orsatti (FR), F. Amtmann (AT), C. Schwar (AT)***
By telephone: Jean Marie Gaultier (FR), K. Finkenzeller (DE)

Acting convener: Reinhard Meindl (AT)

Agenda:

1. **Roll call**

   Membership:
   JP NB informed us that kaneko.yoshiaki@jp.fujitsu.com replaces yamamoto.hideaki@lab.ntt.co.jp for TF3 membership of JP NB.

2. **Introduction and approval of proposed agenda**

   TF3 approved draft agenda as laid out herein.

3. **Approval of minutes of last meeting**

   wg8n2093 TF3 N163 Minutes 14th TF3 meeting London July2013
   Minutes were approved as laid out.

4. **ISO/IEC 15693-3/Amd.2 Clarif of DataEl**

   wg8n2099 Proposed NP ISO IEC 15693-3 Amd2 Clarification of use of Data
   wg8n2104 TF3 N164 ISO-IEC 15693-3 A2 v2 Clarification of data elements
   TF3 reviewed n2099 and n2104 and after minor modification of the draft CD (exchanged the term "isolated EOF" with "EOF") it approved unanimously both actual documents to be submitted to wg8 for approval and submission for ballot to wg8 and sc17

5. **ISO/IEC 15693-3/Amd.3 Memory Extension**

   wg8n2100 Proposed NP ISO IEC 15693-3 Amd3 Extended VICC memory organization
   TF3 revised the scope and purpose of amd.3 as follows:

   NEW Scope of the proposed deliverable for AMD4:

   This amendment specifies mechanisms to address memory organisation beyond 256 blocks.

   Backward compatibility with infrastructure compliant to the current standard revision shall not be compromised.

   New Purpose and justification of the proposal *(attach a separate page as annex, if necessary)*

   TF3 anticipates a market demand for increased memory to enable new applications.

Proposed development track should be 24 months with 1st CD in Q4/2013 (to be confirmed during TF3 Singapore).

wg8n2105 TF3 N165 15693 opening for more memory capacity

Interrogators may process or not-process or ignore when a RFU bit of the legacy standard is set to an unexpected value according to new proposal. There is no definition what happens if a RFU bit is received.

Instead of RFU bit usage this contribution proposes an optional new command. (similar to the TT2 specification of NFC Forum with a sector organization of the larger memory).

Sector select has a risk that the sector may be lost when power is lost at the field border; can be compensated by operating in SELECTED state which would also be reset by power-on-reset. Discussion whether SELECTED state shall be recommended or mandated. The presented concept requires 3 commands to make the first READ or WRITE unless CARD SELECT is combined with SECTOR SELECT which would again make 2 commands sufficient.

New card in front a legacy reader behaves like a legacy card. Larger memory is not visible in such a case. If legacy reader is formatting an extended memory card then only sector 0 is available for extended readers in case format information is stored in sector 0. Legacy reader will not understand the content in case of format information – compensate that format information shall not be stored in sector 0.

Most members like to have old readers be able to use extended memory cards in the same way as legacy cards.

Discussion as an alternative solution between the 2 existing proposals we could specify one optional command to address higher memory only. Means duplication 3 commands.

wg8n2109 TF3 N169 NWI EMVICC ResponsestoTF3issues 11092013

When signing DSFID with current RFU protocol_extension_bit the legacy uses of sc31 RFID tags would no longer be possible with extended memory cards.

Other bits instead of protocol_extension_bit would also be acceptable but still bear the same risk of undefined RFU reception in the current standard but it can be handled on protocol side.

Legacy reader may misunderstand a DSFID of an extended memory card because it expects legacy meaning of DSFID but again no side effects possible.

Limited interoperability but advantage that there are no side effects and no wrong operation possible because legacy readers would not be able to read, write or lock the extended memory cards.

In the commands the address field then could be 8, 16, 24 or 32 bits long (reduction would be acceptable).

wg8n2110 TF3 N170 ISO-IEC 15693-3 A3 (E) EMVICC Amendment

Reflects exactly the concept of wg8n2109.

EMVICC may not be the perfect naming. VICC include both EM and SMVICC.

Conclusion on Amd.3:

There are 2 incompatible proposals from FR and AT available.

A third idea was born and would have to be texted before processed further.

No immediate possible compromises visible.

More contributions necessary

Next steps:

Clarify and discuss in next meeting whether the memory access for legacy readers of lower part of extended memory cards is required or not.

Decision whether to start NP only will be taken in Tf3 Singapore.

Minutes TF3 Freising	ISO(IEC JTC 1/SC 17/WG 8 N 2114 ISO/IEC JTC1/SC17/WG8/TF3 N 171

6. ISO/IEC 15693-3/Amd.4 Security Framework

wg8n2092 TF3 N162 Technical contribution proposal to revise ISOIEC 15693-3

TF3 reviewed and agreed that this contribution should be a starting point for amd 4. It addresses 2 of 6 commands and should be complemented with timing and error codes. Opcodes need to be allocated.

The project editor kindly offered to provide a 1st draft of amendment for review and probably improvement in next TF3 Singapore. The AT NB will provide an input for timing requirements. TF3 proposes to submit the revised NP (without CD) at WG8/SC17 in Singapore and work in parallel to complete a CD document for submission after the NP is approved.

wg8n2101 Proposed NP ISO IEC 15693-3 Amd4 Adding security framework

The project will not address crypto algorithms or security protocols and we will have to be interoperable with existing standards. The security has to be seen as external block that can be activated or not. Our work will act as an interface to the crypto modules. Lets define commands as a framing for crypto suites particularly in 29167. Focus on transport layer.

We should define only a set of optional commands, e.g. authentication; has to be sufficient to cover cryptographic and an optional new SECURE state.

There is a generic document of sc31 with generic requirements on 29167 (WG7 standing document SD2) with a specific part for 18000-3M1 gives us a hint which commands are needed.

Our commands will be a generic interface and select specific algorithm of 29167 via the Crypto suite identifier.

4 optional functionalities (probably 4 separate Commands) are needed for our amendment including timings and including error codes that are related to security.

* Authenticate - card/reader and mutual authentication

* AuthComm – light version of SecureComm

* SecureComm – establish a secure channel

* KeyUpdate – update the Crypto Key

Proposal to add a * Challenge and * ReadBuffer (as response) commands which is an abbreviation to all tags instead of individual authentication. Good for complex crypto computations.

The state machine of 15693 needs to be amended with an additional optional SECURE state.

TF3 also looked into sc31n4104 which is the same contents as wg8n2092 for today agenda. It is agreed to be a good starting point but things like timing and other functionalities might also be necessary. Frame sizes ? (may be part of crypto suite – so our interface must be transparent).

For UHF standard the situation seems similar.

Untraceability: can be part of some of the crypto suites in 29167 (e.g. in part 19). Would not be compatible to GS1 requirements. Untraceable command will be part of GS1 epc UHF Gen 2 version 2.0. Our amendment would need to specify this untraceability command.
We would need switch mechanism in our amendment (on/off).
Conclusion: Untraceability is **excluded** from current amendment because not directly related to security and can be handled separately from security.

short discussion whether to go for a new part 4 instead of amendment for part 3.

Conclusion: unanimous decision to stick to an amendment of part 3

TF3 revised the scope of the NP as follows:

NEW Scope of the proposed deliverable for AMD3:

This amendment of the existing ISO/IEC 15693-3 international standard will implement the architecture including an optional new SECURE state and commands for optional

security features for the ISO/IEC 15693 air interface standard for radio frequency identification (RFID) devices using the crypto suites defined in ISO/IEC 29167.

A card and the interrogator may support none, a subset, or all of the specified security features. It should also include a mechanism for an interrogator to get information about the security features that are actually implemented and supported by a card.

wg8n2106 TF3 N166 NXP Security framework for ISOv2

TF3 reviewed this contribution.

Open question: Should this amd also address file management? – unanimous decision not to address file mgmt. with this amd.

No further comments or objections were raised.

7. Liaison post entrance/outlet

wg8n2084 TF3_N161_SC31 Liaison Request to SC17

wg8n2107 TF3 N167 Security in 15693 e-mailing with SC31 liaison officer

This agenda topic was not addressed due to a lack of time.

8. Confirm dates, venues, focus topics for further meetings

Next TF3: 23.-24.10.2013 in Singapore, each day 18.00 – 21.00.

9. Close meeting

The acting convener closed the meeting at 5pm.