ISO/IEC JTC1/SC17 N 3522   **WG8 N 1449**

DOCUMENT TYPE: Request for Comments

TITLE: Request for Comments – on the SC 31 Proposal for a New Work Item, Information technology – Automatic identification and data capture techniques - Air Interface for file management and security services for RFID.

BACKWARD POINTER:

SOURCE: SECRETARIAT ISO/IEC JTC1/SC17

STATUS: The SC27 secretariat requests comments on the NWIP by SC31 above.   There appears to be some overlap with SC17 in this work item particularly relevant to WG4 and WG8. Could comments to be returned by 2008-09-26. This will allow for discussion at the SC17 plenary if so required.

ACTION ID: ACT

WORK ITEM:

DUE DATE: 2008-09-26

DISTRIBUTION: P and L-Members of ISO/IEC JTC1/SC17
                      JTC1 Secretariat
                      ISO/IEC ITTF

MEDIUM: SERVER

NO. OF PAGES: 12

Secretariat ISO/IEC JTC1/SC17, APACS, Mercury House, Triton Court, 14 Finsbury Square, London EC2A 1LQ, England;
Telephone +44 (0)20 7711 6255; Fax: +44 (0)20 7711 6299; e-mail: chris.starr@apacs.org.uk

Document Type:	**Proposed NP**
Document Title:	**SC 31 Proposal for a New Work Item, Information technology -- Automatic identification and data capture techniques -- Air Interface for file management and security services for RFID**
Document Source:	**SC 31 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 31 Secretariat.**
Action ID:	**ACT**
Due Date:	**2008-10-18**
No. of Pages:	**12**

ISO/IEC JTC 1/SC 31

Automatic Identification and Data Capture Techniques

Secretariat: ANSI (USA)

DOC TYPE:	**New Work Item Proposal**
TITLE:	**Information technology -- Automatic identification and data capture techniques -- Air Interface for file management and security services for RFID**
SOURCE:	**National Body of Austria**
PROJECT:	
STATUS:	**The National Body Austria is submitting this NP for consideration of work within SC 31. Also included is the illustrative attachment, which describes how this new standard should be included in the RFID environment. The general concept is a new ISO standard applicable for ISO 18000-6, and other parts of ISO 18000 that describes new Security and File Management Commands based on reserved and in future assigned opcodes in the ISO 18000 series.**
	Per Resolution 5 of the Seoul Plenary Meeting, P-Members are requested to use the attached form (SC031-N-2578 - Form 13B Comment Document.doc) for submission of comments on any project ballot.
	P-Members have an obligation to vote and are requested to cast votes on the SC 31 website (LiveLink balloting system) by the date indicated on the cover page.
ACTION ID:	**COM**
DUE DATE:	**2008-10-08**
DISTRIBUTION:	**ISO/IEC JTC 1/SC 31 members**
MEDIUM:	**ISO TC Portal (LiveLink)**
NO. OF PAGES:	**10 (including this cover)**

New Work Item Proposal

July 2008

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-07-11	Proposer: ONORM, Austria
Secretariat: ANSI	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 31 N 2578 (SC031-N-2578)

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.) Specification of Data Value Domain

`Information technology  - Automatic identification and data capture techniques – Air Interface for file management and security services for RFID`

Scope (and field of application)

So far, RFID tags have been mainly passive backscatter tags with limited computing capabilities and modest storage capacity used for the purpose of identification and tracking. The amount of data to be stored on such tags could easily be handled by using given data structures being stored at fixed memory addresses within fixed memory ranges while data manipulation remained very basic. As there was no immediate need to handle a significant number of different data structures, the logical memory layout was basically predefined, and user memory or the absence thereof was not a major issue. No real file system had to be introduced, as all required operations could be carried out on word or even bit level. Security features had to be aligned with the limitations of passive RFID and therefore remained rudimentary.

However, as technology matures, new features such as battery support and integration of sensors are added, and complexity increases. In particular, the addition of batteries to tags and the allowance of higher cost levels in the applications supported by battery assisted tags tend to lead to very large increases in tag memory. Historically, almost all mobile media with similar memory capability has been supported by file systems on-board the media.

Battery assisted tags, as currently being specified in the ISO/IEC FCD 18000-6REV1 standard, equipped with one or more simple- or full-function sensors are expected to utilize an addressable memory range from hundreds of words to tens (or even hundreds) of kilowords for static sensor data such as a sensor identifier, semi-static data such as sensor scheduling configurations, and a high amount of dynamic data as for instance measurement record sets and alarm bits. Similar amounts of memory space may be required for interrogator written files. Battery tags may also have semi-static tag control data such as the tag settings words described in the current draft of ISO 18000-6. In contrast to prevailing applications, tag data will become more and more complex and highly dynamic in the near future. As a consequence, effective and deliberate file management is required in order to maintain data integrity and memory efficiency.

Therefore, this work item covers file management for RFID tags that is intended to be used as a supportive, complementary but optional concept together with existing air interface specifications and tag data standards for passive and semi-passive RFID tags.

As a file system without access control is vulnerable and due to the fact that existing security features for RFID such as link cover coding and memory access via password protection at granularity of the whole memory do not support a file- or directory level security policy and moreover may not be considered very reliable, a set of contemporary security services needs to be defined. Those security services should cover single sided- and mutual-authentication as well as establishment of a secure communication channel (exchange of a session key and encryption of the data transmitted over the air interface) and encrypted memory, all in alignment with the file system.

The security services covered by this work item are intended as optional tag features indicated to the interrogator by proper means during tag inventory and being enforced as a conditional requirement for file access, if required. This work item is intended to pay special attention to the enhanced capabilities of battery assisted sensor tags and upcoming new applications and the related growing demand on security and privacy, as well as to the enhanced processing capabilities of such tags enabling the support of state-of-the-art crypto algorithms.

Both file management and security are intended to be defined in alignment with existing air interfaces. The primary focus of the work item will be on HF and UHF RFID and the according existing air interfaces, i.e. ISO/IEC 18000-3 and ISO/IEC 18000-6, will be taken as a starting point for all further development. The new International Standard will cover only extensions on file management and security beyond the scope of the mentioned air interfaces and will not replace any existing International Standard.

Purpose and justification - attach a separate page as annex, if necessary

Due to growing demand from the market, several tag manufacturers have already developed fairly complex battery assisted sensor tags providing a growing amount of user memory that has to be managed by a basic file systems providing easy access to and protection of the stored data.

There is a high demand on effective file management due to several basic requirements:

- Integrity of data has to be observed (this is the first duty of a file system)

- Memory has to be efficiently utilized for maximum utility and cost control, which requires efficient packing of data and linking of pages or blocks of data for files that grow over time (this is the second most important function of a file system)

- Demand to store data in hierarchical structures, e.g. directories, for convenient access (this is the next most important function of a file system)

- File-level access control, as opposed to less convenient low level addressing

- Maintaining low error rate transfer of significant amounts of data across the hostile RFID wireless link is most efficiently performed with the data packaged in files, and particular using a journaling file system

- Application of security and data compression techniques are also most efficiently performed upon data managed in file form.

- The assumption of interrogator and infrastructure based memory management breaks down for interrogators that are not always network enabled (such as portable interrogators)

- Sensor files are updated by the tag itself, and thus accurate directory information cannot be maintained by the infrastructure.

These requirements are so far not sufficiently covered by the existing International Standards for RFID.

Furthermore, sensor tags are being used in supply chain tracking and the emerging crucial sensor data (e.g. sensor alarm status) needs to be protected from manipulation. As a consequence, different sections of data need to have different levels of security assigned and access control needs to go beyond a single access password to provide higher flexibility and avoid exposure of protected content.

Additionally, duplication of UII data (cloning), abuse via replay of commands, eavesdropping and unauthorized tracking of objects and persons needs to be prevented. There is a growing concern on privacy issues, i.e. among European users, that reflects this requirement. As RFID technology matures, new applications requiring more enhanced security features will emerge. In the near future, there might be for instance a growing demand on "after sell services" such as RFID tags being used for maintenance or warranty support, which prevents RFID tags from being permanently disabled (killed) after purchase, and hence effective privacy protection is required.

Hardware manufacturers already pay credit to those security requirements with a number of released products implementing different types of security protocols. The variability among those products reflects the need for standardization. An International Standard on security services for RFID is needed to increase the trust of users in RFID technology and to contribute to the spread of RFID in public and domestic applications.

As the topics of file management and security are closely interlinked, this work item covers them as a joined topic.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

__X__ a single International Standard

_____ more than one International Standard (expected number: ....)
_____ a multi-part International Standard consisting of .... parts
_____ an amendment or amendments to the following International Standard(s) ....
_____ a technical report , type 1...........

And which standard development track is recommended for the approved new work item?

_X__a. Default Timeframe

_____b. Accelerated Timeframe

_____c. Extended Timeframe

Relevant documents to be considered

ISO/IEC 18000-6

ISO/IEC 18000-3

ISO/IEC 15961-1

ISO/IEC 15961-2

ISO/IEC 15961-3

ISO/IEC 15961-4

ISO/IEC 15962

ISO/IEC 24753

IEEE 1451.7

ISO/IEC 18000-1

ISO/IEC 18000-2

ISO/IEC 18000-4

ISO/IEC 18000-7

ISO/IEC 24791-1

ISO/IEC 24791-2

ISO/IEC 24791-3

ISO/IEC 24791-5

ISO/IEC 24791-6

Co-operation and liaison

ISO/IEC JTC 1/SC 31/WG 4

ISO/IEC JTC 1/SC 31/WG 4/SG 3

ISO/IEC JTC 1/SC 31/WG 4/SG 6

ISO/IEC JTC 1/SC 31/WG 4/SG 1

ISO/IEC JTC1 SC27

ISO/IEC JTC1 SC27/WG2

Preparatory work offered with target date(s) :

Austrian NB is pleased to be the sponsoring member for this work item, and the first CD ballot will be within 12 months of approval of the work item.

Signature: Raymond Delnicki, ISO/IEC JTC 1/SC 31 Secretariat

Will the service of a maintenance agency or registration authority be required? ..No...............
- If yes, have you identified a potential candidate? ....
- If yes, indicate name ....

Are there any known requirements for coding? ..No...............
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? ..Not known at this stage................
- If yes, please provide full information in an annex

Are there any known requirements for cultural and linguistic adaptability? No

-If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC 31 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 31 and JTC1/SC31/WG4 respectively

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation: 2008-07-11	**Closing date for voting:** 2008-10-08	**Signature of Secretary:** Lisa Rajchel

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _X__ Desirable ___ Supportive ___	Products with features similar to those covered by this work item are already on the market. The mentioned features are essential for some applications.
A.2 Regulatory Context	Essential _X __ Desirable ___ Supportive ___ Not Relevant ___	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_X __	
B.2 Commitment to other organisation	Yes ___ No_X__	

B.3 Other Source of standards	Yes _X__ No___	
C. Technical Status		
C.1 Mature Technology	Yes _X__ No___	Products are already on the market. The work areas of file management and security are both historical areas of research in computer science, wireless communications, and RFID.
C.2 Prospective Technology	Yes _X __ No___	The work item is expected to contribute on the spread of RFID technology, will consolidate the current status of the technology in respects to competitors, and is expected to make RFID technology even more versatile for future applications.
C.3 Models/Tools	Yes _ __ No_ X __	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes _X__ No___	Criteria will be determined, but this standard will not provide conformance tests
D.2 Interoperability	Yes _X__ No___	This NP will be developed in alignment with existing air interface specifications and application interfaces.
E. Adaptability to Culture, Language, Human Functioning and Context of Use		
E.1 Cultural and Linguistic Adaptability	Yes_____ No___N/A____	
E.2 Adaptability to Human Functioning and Context of Use	Yes_____ No___N/A____	

| F. Other Justification | | |

THE FOLLOWING CRITERIA MUST BE FOLLOWED FOR THIS BALLOT.

As per JTC 1 Paris Resolution 8.2, JTC 1 approves document JTC 1-N-4477 as the new JTC 1 NP Acceptance Criteria. In order to allow National Bodies and Subcommittees time to transition to this new procedure, all NPs submitted as of 1 March 1997 **must comply** with this new procedure. Document JTC 1-N-4477 states its Principle for NP Acceptance as:

The existing JTC 1 Directives (cl. 6.2.1.3) require the commitment of five National Bodies; in addition the criteria (proforma) defined in this paper shall also be satisfied.
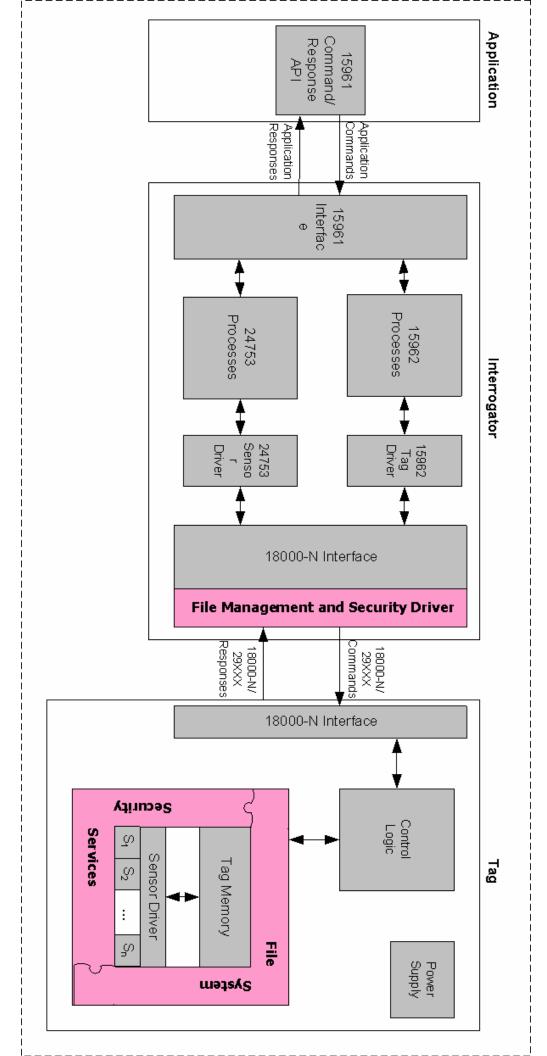
Assumptions :

- That the proposed NP acceptance criteria be applied at the initialization and the approval stages.
- That in accordance with existing procedures NP's may be initiated by SC's and or NB's.
- That SC's shall have a business plan which defines and justifies their work program.
- That NP's shall fall within the scope of the JTC 1 Business Plan and where applicable the SC Business Plan.
- That when a NP is initiated the proposer shall, in addition to existing requirements, complete the new proforma and submit it along with the NP. This proforma shall be circulated along with the NP ballot.
- That NB's during the balloting stage understand that in case of serious doubt, giving a firm negative vote would be helpful to ensure relevance and utilization of critical resources within JTC1.
- That JTC 1 provide input and direction to emphasize these criteria as a new approach for NP planning and NB balloting.
- That the JTC 1 secretariat engage in modification to the JTC 1 procedures related to NP's and their balloting.

6.2.1.3

It is the responsibility of NBs to review each NP to ensure proper coordination among standards development activities and avoidance of duplication of efforts. In this regard, NBs should take particular note of related standardisation activities identified in the proposal and are encouraged to seek input from the national counterparts to these organisations when developing a position since direct input from the international organisations identified may or may not be possible within the time frame of the ballot. Each proposal shall be voted on by letter ballot (see Form G4), even if it has appeared on the agenda of a meeting. In order to be approved, the proposal shall be supported by a majority of all P-members of JTC 1 with at least five P-members of the SC to which the project will be assigned committed to active participation. If the NP is submitted by an SC, the SC should first determine that at least five of its P-members will participate. This does not prevent initiation of discussion of technical documents pertaining to a proposed new item, pending approval of the item by NP letter ballot of the JTC 1 P-members or the SC approval of a study period. If the result of the JTC 1 NP letter ballot is negative, discussion of the proposal shall be abandoned.

The above criteria **must be** taken into account when voting on each of the 6 Questions of this NP ballot.

MB[1]	Clause/ subclause (e. g. 3.1)	Para- graph/ Figure/ Table (e. g. Table 1)	Type of com- ment[2] (e. g. ed)	Comments: Justification for change	Proposed change	*DRAFT – For Comment* **Observations of the secretariat** on each comment submitted

[1] **MB = Member body (Enter two-letter country code, e. g. CN for China)**
[2] **Type of comment:**   **ge** = general   **te** = technical   **ed** = editorial   **NB Columns 1, 2, 4, 5 are compulsory**

FORM 13B (ISO) 2001-07-01