



we simulate your future

NWIP Air Interface for File Management and Security Services for RFID

Josef Preishuber-Pflügl, David Tschische
j.preishuber-pfluegl@cisc.at, d.tschische@cisc.at

ISSUE: 18.07.2008

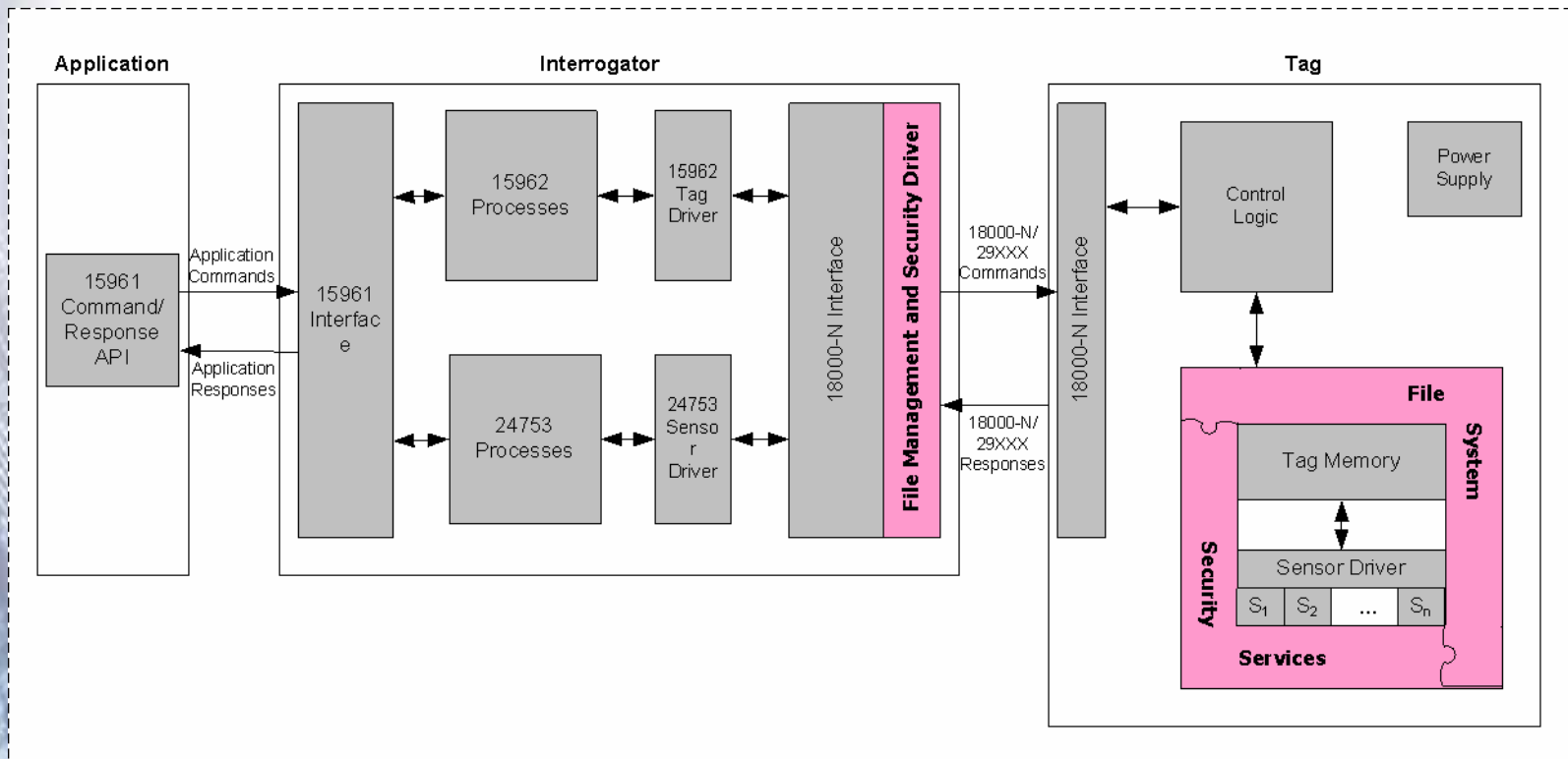
New Work Item Proposal

Proposer: ONORM, Austria

Title: Information technology - Automatic identification and data capture techniques – Air interface for file management and security services for RFID

Logical Overview

Usage of a future ISO/IEC 29XXX Standard on File Management and Security Services for RFID



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

Cooperation and Liason

- 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

Reasons for the NWIP

- RFID technology has matured
 - Existing mechanisms for data manipulation and security are out-dated
 - Products supporting file management and enhanced security are already on the market
- Impact of new features such as battery support and integration of sensors
 - Increased complexity
 - New applications
 - Higher cost levels
 - Increased memory size
 - Complex data structures
 - Increased processing capabilities
- Growing concern on privacy issues
 - State-of-the-art security is demanded by the market
 - Absence of enhanced security features may harm the position of RFID technology on the market
- NWIP is expected to contribute on the spread of RFID
- NWIP is expected to consolidate the current status of the technology in respect to competitors

File Management – Purpose and Justification I

Basic Requirements:

- Integrity of data has to be observed
- 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
- Demand to store data in hierarchical structures, e.g. directories, for convenient access
- 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

File Management – Purpose and Justification II

Basic Requirements: (cont'd)

- 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

File Management – Goals for Standardization

- File management as an **optional** feature beside existing memory structures specified in existing International Standards for RFID such as ISO 18000-6 or ISO 18000-3
- Applicable to passive tags but focus on battery-assisted tags
- File management to be used standalone or in combination with the optional security services

Security – Purpose and Justification

Current Situation: Primitive Security Features

- Kill password/Access password
- Link cover coding
- Locking of memory banks and memory blocks
- Security features aligned with the limited processing power of passive RFID tags

Many possible threats

- Duplication of UII data (Cloning)
 - Eavesdropping
 - Replay attacks
 - Illegal tracking of objects and persons (Privacy issues)
 - ...
- More advanced **optional** security features required

Security: Service Oriented Approach

Services:

1. Secure Authentication
 - Reader to Tag
 - Tag to Reader
 - Mutually
2. Establishment of a Secure Communication Channel
 - Exchange of a session key
 - Encryption of transmitted data
3. Encrypted Memory

Security Services – Goals for Standardization

- Provide a set of **optional** security services
- Security to be used as a complementary concept for file management
- Enable usage of security services without being forced to support file management
- Allow to choose from a set of supported cryptographic algorithms
- Modular concept: security services decoupled from each other (as far as applicable)

Why it makes sense to address File Management and Security Services in a single International Standard

- both are required
- a file system without security features is vulnerable
- existing security features above file level, e.g. on memory bank level, don't address all needs
- no extra-effort for alignment required

Summary

New work item proposal on **optional File Management** and **optional Security Services** for RFID

- In alignment with existing standards
- No restrictions on frequency band (UHF and HF planned)
- Provide hooks for the upcoming standard in all relevant documents
 - Normative references
 - Reserved command codes
 - Reserved memory locations
 - Reserved XPC bits
 - ...