

**ISO/IEC PDTR 24729:
RFID guidelines on tag data security
- (EU related) surrounding and
consequences**

Comments made by
Ulrich.friedrich@atmel.com

ISO/IEC PDTR 24729

- Part1: RFID enabled labels and packaging supporting ISO/IEC 18000-6C
- Part2: Recycling and RFID tags
- Part3: Implementation and operation of UHF RFID interrogator systems in logistic applications
- Part4: **RFID guidelines on tag data security**

ISO/IEC PDTR 24729-4 (2)

- It is intend to provide guidance to users and system designers on potential threats to data security and countermeasures available to provide RFID data security
- Three section
 - Possible threats to data access
 - Methodology for assessing the various possible threats in order to determine the relative risk level of the specific application
 - Countermeasures to effectively address specific possible threats

ISO/IEC PDTR 24729-4 (security)

- Prevention of unauthorized reading and changing of RFID data
 - Confidentiality
 - Including protection of personal privacy and property information
 - Integrity
 - Availability

ISO/IEC PDTR 24729-4 (threats)

- Gather
 - Skimming (unauthorized read) / Eavesdropping (man in the middle)
 - Data tampering
- Mimic
 - Spoofing (tag emulation)
 - Cloning a tag
- Denial Of Service
 - Blocker functions
 - Unauthorized kill of tag
 - Jamming / shielding

ISO/IEC PDTR 24729-4 (RFID data access security risk management)

- Risk analysis considering for example
 - Damage potential
 - How easy it is
 - What is needed to do the attack
- Probability

ISO/IEC PDTR 24729-4 (countermeasures)

- Some examples are listed
 - WORM technology
 - TagID
 - Memory lock
 - Password protection
 - Authentication
 - Encryption
 - Cloaking information (transmitted UUI \neq stored UUI)
 - Use the right frequency to reduce the risks
 - Physical activation of a tag (mechanical switches)

Consequences

- The user has to do a risk analysis. Then they have to check marketing slides or the air interface descriptions before doing a decision on the right RFID system.
- Should we, for example provide in an informative annex information about countermeasures implemented in this air interface?
 - Because there is also a discussion about privacy and security, especially in Europe

Current Status

- Some regulations currently in use
 - EG directive related to data protection 95/46/EG
 - EG directive for RF equipment 1999/5/EG
 - EG directive related to data confidentiality linked to communication equipment
- CEN/TC225 (European Committee for Standardization)
 - April 2007 they have published a draft proposal for standard developments linked to work, which should be done in the field of RFID – Privacy and security (privacy by design)
 - November 2007 they have given RFID terms to the EU expert group
- 2007 the EU commission has established an expert group dealing with data protection and privacy linked to RFID.
 - A first output was published some weeks ago
 - They are asking for feedback until 25th of April 2008
- January 2008: ISO/IEC PDTR 24729-4 : RFID guidelines on tag data security

CEN proposal for European standardization in the field of RFID

- Based on the identification of important business cases for European industries they have proposed five areas for work items
 - RFID Privacy and Security
 - RFID implementation guidelines
 - The application of RFID in European Automotive sector
 - Automotive Product authentication & tracking using RFID
 - Electronic custom forms
- It was announced that their work will be based on an gap analysis of current RFID standards linked to “privacy by design” aspects
 - For example: Erase of serialization (ItemID and/or TagID??; consider our discussion yesterday!!!)
- Goal is also to identify pre-existing security/privacy solutions as well as to propose candidates which should be considered in future standards

First central outputs of the European expert group

- The consumer should be able to decide at POS which kind of de-activation they want to use
 - Temporary deactivation and getting personal control over (pieces of data)
 - Perma kill
- The consumer should be informed about the use of RFID, his possibilities how to deal with, as well as the use cases of the data within the store/company
- To generate a profile by tracking is not allowed for companies
- Each company dealing with RFID and/or its data should present a contact person responsible for RFID issues

Some open issues

- Assumption: class1 tag
 - How many levels of access/security we have to support covering multi tier supply chain as well as after sales market/privacy protection?
- Who is the owner of the data on tag?
 - Is re-use of data possible also after POS and who is then the authorized “person” to de-lock
- Is waste management of items possible without the help of the consumer
 - Means if the consumer has blocked communication to avoid tracking, is it possible to get such data out of the tag?
- Our responsibility
 - Reaction only or