

Encoding of Security Functionality in ISO18000-6C [1]

WG4/SG3 Meeting
07. - 08.04.2008, Vienna

Institute for Applied Information Processing
and Communications

IAIK – Graz University of Technology
www.iaik.tugraz.at

Overview

- Who we are
- Motivation
- Misleading assumptions about security in context of RFID
- Potential security services
- Current Situation in ISO18000-6C
- Important Considerations
- Our approach
- Conclusion

Who we are

- “VLSI & Security” research group
- One out of six research groups @ IAIK
 - e-Government, Cryptography, Network Security,
- Focus on secure application specific hardware implementations of cryptographic algorithms
 - Area efficient, low power, high speed, ...
- Integrating cryptographic security to RFID technology = challenging research topic

Motivation

- Collaboration in the BRIDGE project
 - 3-year EU project
 - > 20 partners (universities, solution providers, users)
 - Standardization is a crucial topic
- Developing technically reliable solutions
- Academic interest
 - Standardization is a new topic for us

Misleading Assumptions about Security in Context of RFID

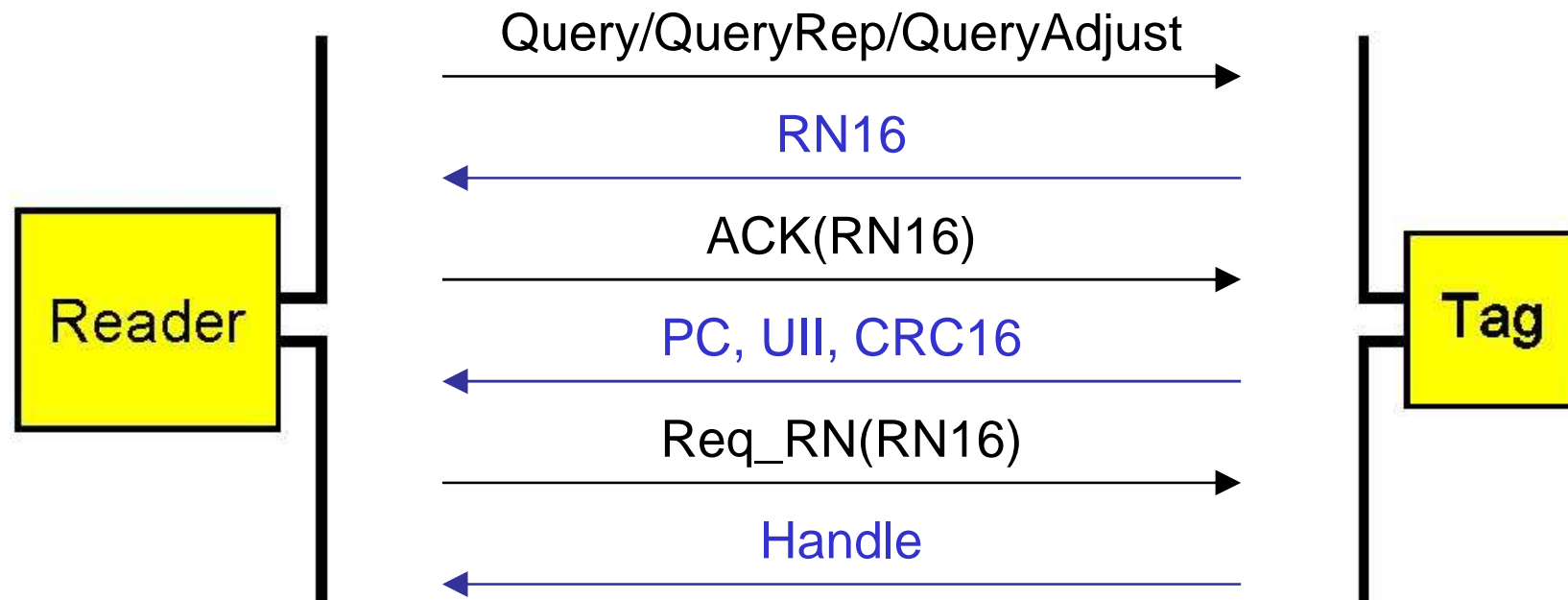
- Security = encrypted channel (privacy)
- Cryptographic security is technically not feasible
- “Some security” is enough since tags are low-cost

Potential Security Services

- Authentication
 - Tag authentication (e.g. anti cloning)
 - Reader authentication (e.g. restrict access to tag memory)
 - Mutual authentication (e.g. secure channel)
- Anonymity (fake-ID, pseudonym)
- Encrypted channel (e.g. anti-eavesdropping)
- Integrity of data
- Secure key update (transfer of ownership)
- Secure key exchange
- ...

Current Situation in ISO18000-6C[1]

- Usage of strong cryptographic security is not considered
 - UII transmitted in plain
 - No tag/reader authentication
 - Some data 'blinded' with random number (previously replied by tag in plain!)



Important Considerations (1)

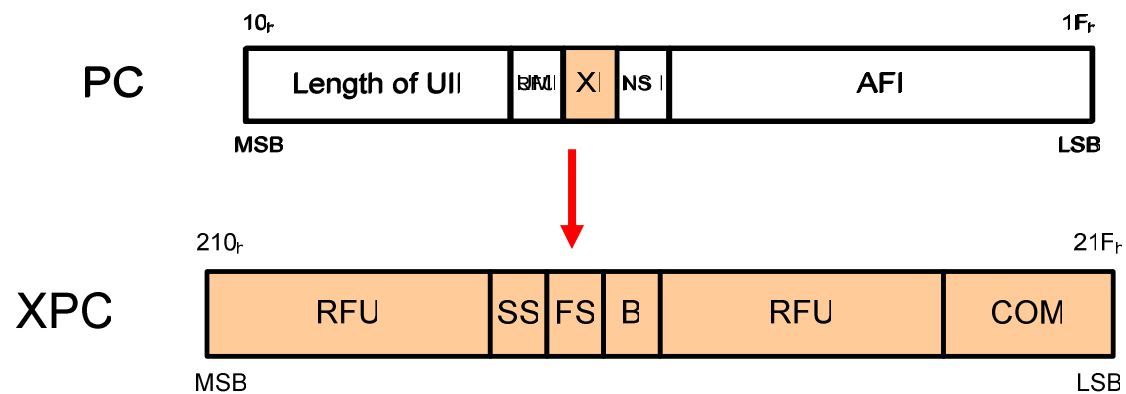
- Compatibility of secure and insecure infrastructure
 - Secure reader should be able to communicate with insecure tags
 - Secure tags should be visible for insecure reader
 - → introduction of additional security layer
- Must not prevent “state-of-the-art” IT-security methods
- Should use open solutions (not exclusively proprietary)
- Should be designed for a long lifetime
- ...

Important Considerations (2)

- How to signal the presence of security functionality?
 - Are there any security features available on the tag?
 - Is replied UID of tag *real* or a *pseudonym*?
- How many bits are necessary for encoding of security functionality?
- How to provide detailed information about the implemented security functionality?
- Extensibility/flexibility
 - Various crypto types (symmetric, asymmetric, hash, ...)
 - Various crypto primitives (AES [2], TEA [3], ...)?
 - Various key lengths?
 - More than one crypto primitive present at once?
 - Space for adding security services afterwards?
- ...

Our Approach (1)

- Based on suggestion from sensor community in ISO/IEC 18000-6
- Using the XPC (Extended Protocol Control)
 - Located in UII memory bank at address 210_h
 - XPC comprises information about additional tag functions
 - Recommissioning (COM 0:2)
 - Sensor functionality (SS, FS)
 - Battery functionality (B)
 - XI flag in PC indicates the presence of the XPC



Our Approach (2)

- Introducing SE (security enhanced) bit in the XPC
 - Signaling presence of security functionality
 - Reader immediately knows whether security functionality is present or not
- Only 10 bits available in XPC
 - Beside SE bit 2-3 additional bits for indicating important security services (e.g. anonymity, tag authentication, reader authentication)
- Probably appending security data to sensor data in tag reply
 - Sensor data (up to 496 bits) can be added to the tag reply after ACK
 - May be a problem if sensor data and security data present at once → long tag reply



- Alternatively using TID memory to provide detailed information about security functionality
 - Indicating supported crypto types/security services
 - Directly in TID memory or via pointer in TID memory to dedicated memory location that contains the information

Conclusion

- General acceptance of crypto functionality in UHF RFID tags requires standardization
- Our approach is based on suggestion from sensor community
 - Using a combination of XPC and TID
- Potential problems
 - Tag reply gets long if sensor data is present as well
 - Additional costs (communication overhead, protection of memory,)

References

- [1] International Organization for Standardization: ISO/IEC 18000-6C: Air Interface for Radio-Frequency Identification (RFID) Devices Operating in the 860MHz to 960MHz Industrial, Scientific, and Medical (ISM) Band used in Item Management Applications
- [2] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard
- [3] D.J. Wheeler and R.M. Needham. TEA, a Tiny Encryption Algorithm