Symmetric Authentication for RFID Systems in Practice

A Solution for Security Enhanced RFID Systems

Sandra Dominikus, Elisabeth Oswald, Martin Feldhofer

Sandra.Dominikus@iaik.tugraz.at

Institute for Applied Information Processing and Communications (IAIK) — VLSI Group

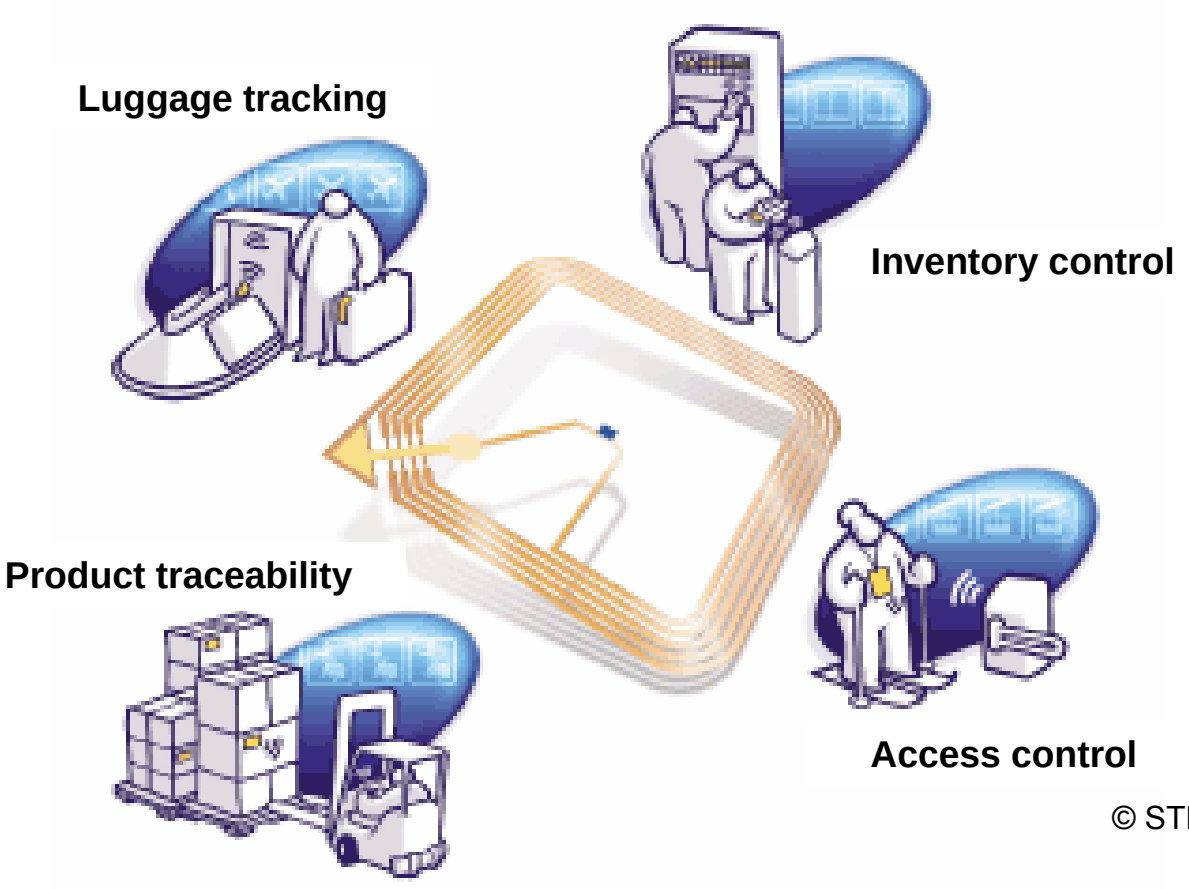
Faculty of Computer Science
Graz University of Technology

VLSI

Presentation outline

- Motivation
- Security Threats
- Symmetric Authentication
- ISO/IEC 18000 Protocol
- Sample Authentication Protocol
- Performance
- Conclusion

Examples for successful Applications of RFID Technology



© STMelectronics

Enhanced security applications

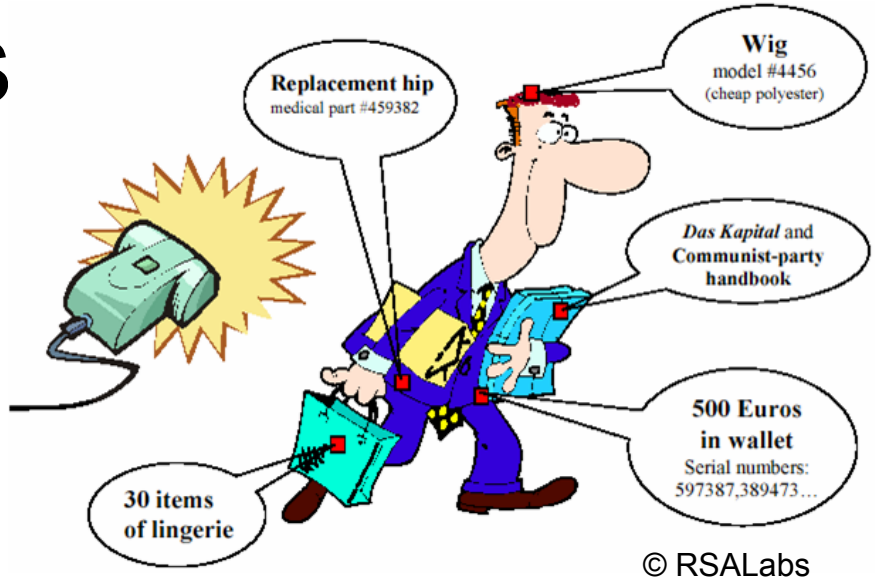
- Airport Luggage Transportation
- Car immobilizer
- Securing of high value banknotes
- Protection of branded goods
- RFID containing sensible data
- Consumer tracking

Reasons for vulnerabilities

- Working principles of RFID Technology
  - Contact-less
  - No clear line-of-sight
  - Broadcast of signal

Perfect working conditions for attacker!

Security threats

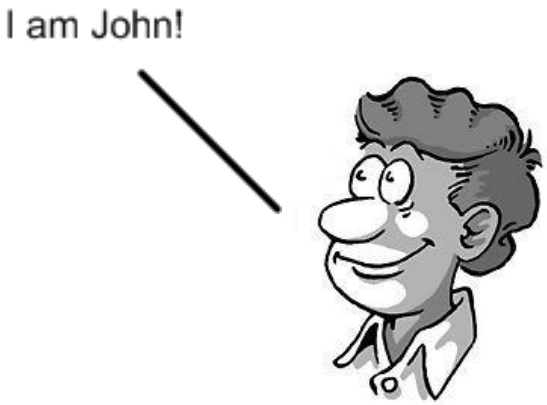


© RSALabs

- Violation of privacy
  - Consumer tracking
  - Data protection
- Unauthorized access to the tag's memory
- Forgery of tags

Cryptographic approach

- Identification
  - Claim to be have a certain identity (e.g. username)



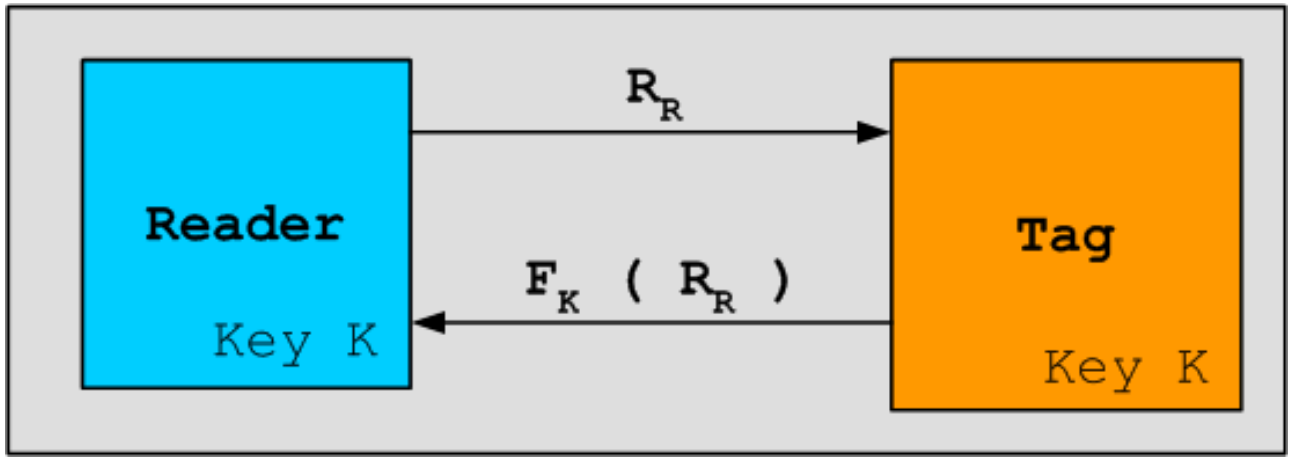
- Authentication
  - Proof of identity
  - Showing knowledge, possession, inherent feature

Symmetric Authentication (1/2)

- Fast and efficient
- One shared Key
- Key distribution
- Key management
- Closed systems

Symmetric Authentication (2/2)

- Challenge response (strong authentication)
  - Knowledge of a secret (Key K)
  - Time-variant challenge (R_R)
  - Response depends on challenge and secret

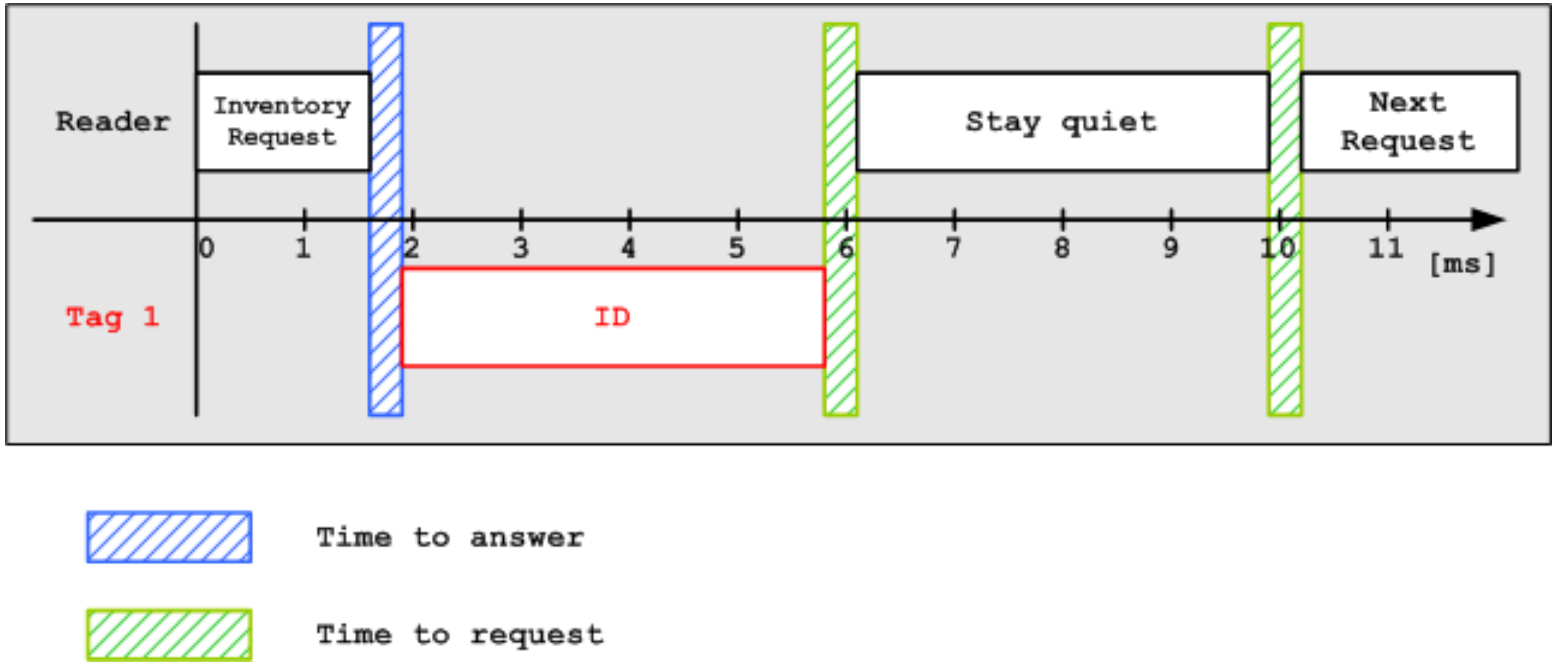


Requirements for security-enhanced tag

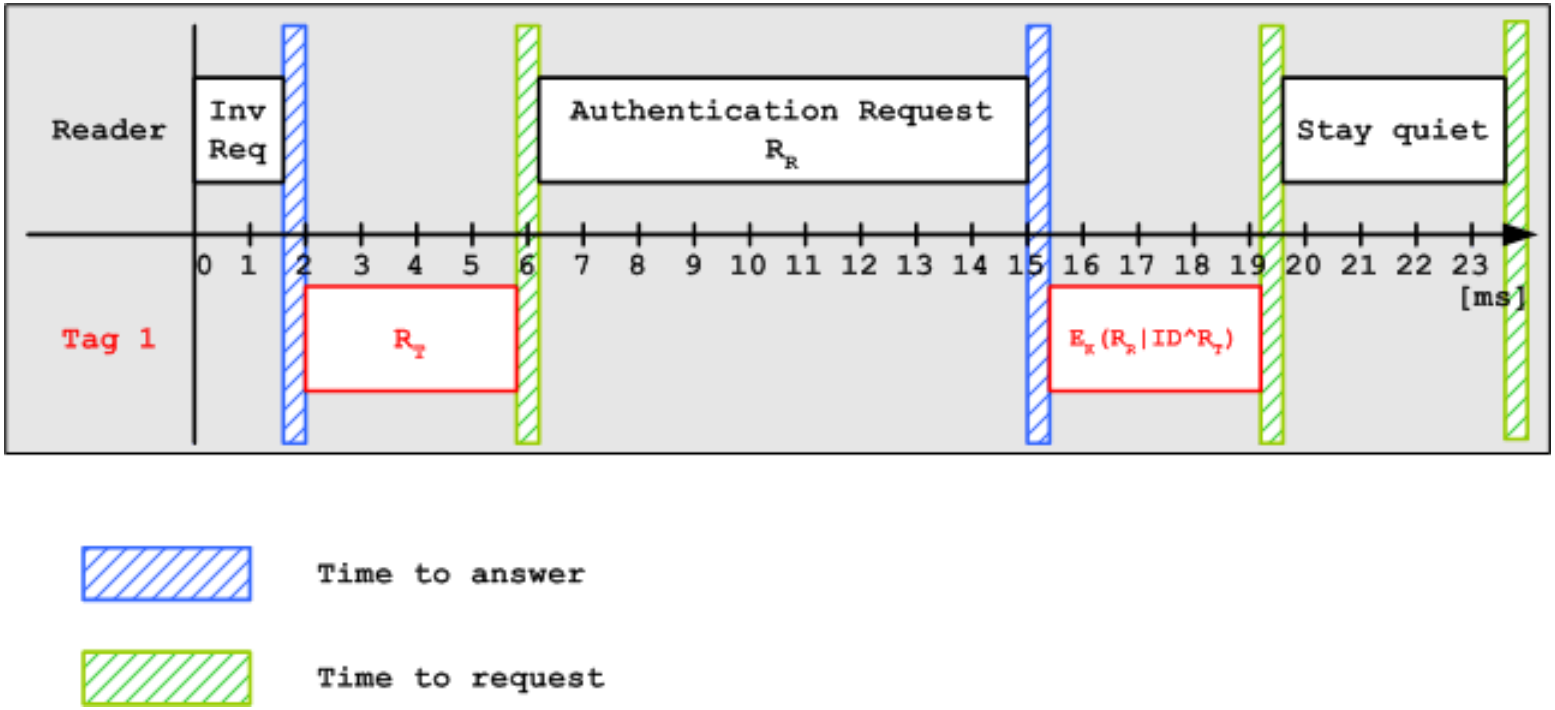
- Goals:
  - Prevent forgery (Tag authentication)
  - Prevent unwanted access (Reader auth.)
  - Supply of privacy (Reader authentication)

- Requirements:
  - Provision of non-predictable nonces
  - Strong cryptographic primitives
  - Standardized symmetric algorithm (AES)
  - Standardized crypto protocol
  - Useable with existing infrastructure → compatibility to existing standards (ISO/IEC 18000)

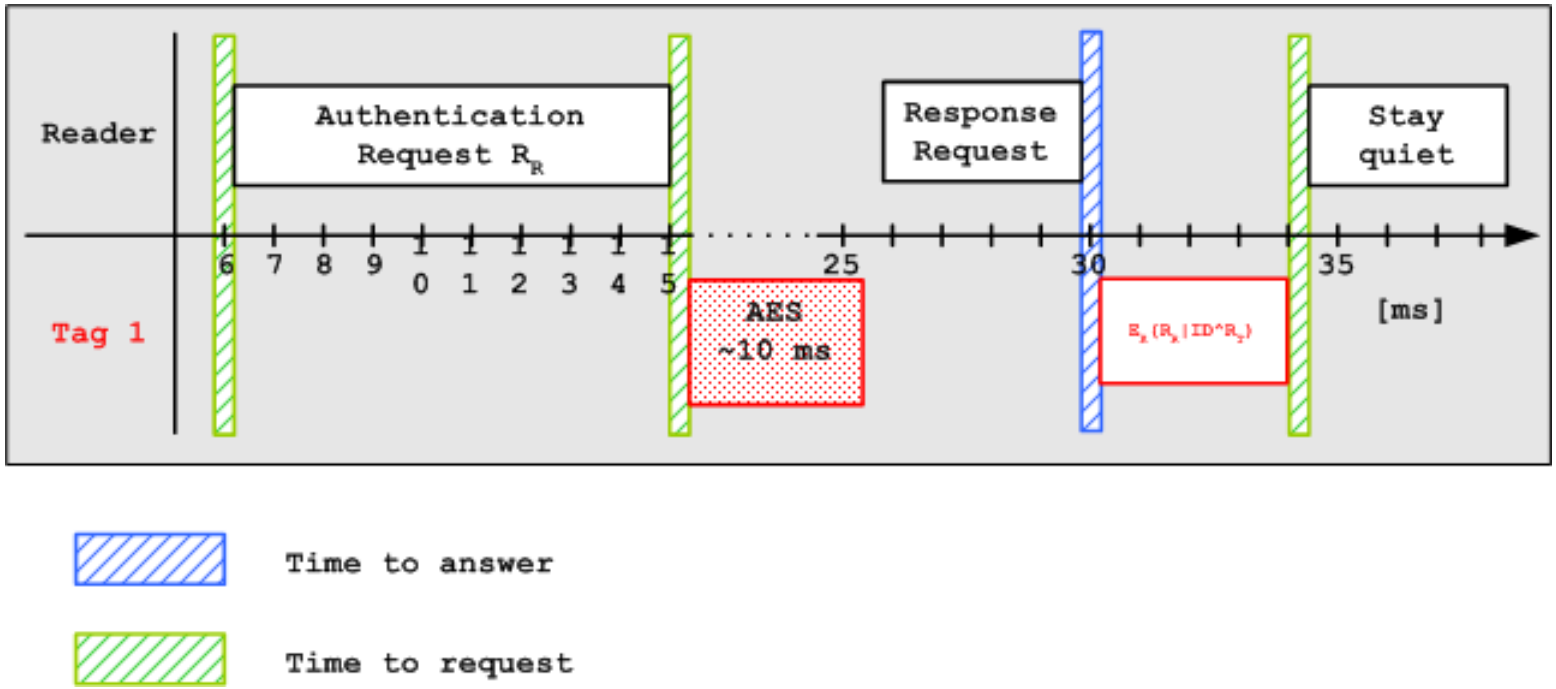
ISO/IEC 18000 Protocol



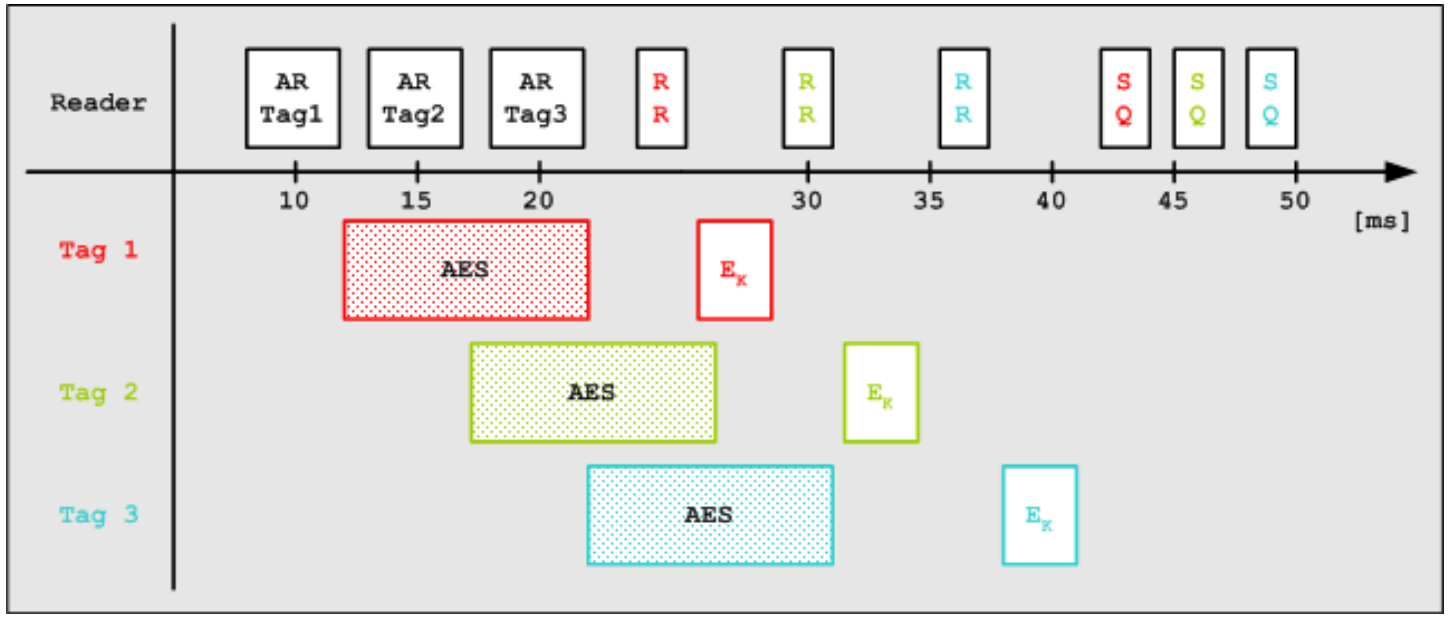
Tag Authentication (with Tracking Prevention)



Interleaved Protocol (1/2)



Interleaved Protocol (2/2)



- Authentication of approx. 50 tags per second possible

Performance (1/3)

- Performance: simple for one Tag, complex for more Tags
- PETRA: Protocol Evaluation Tool for RFID Application
- Emulates behavior of RFID systems in a cycle accurate manner
- Parameters set by user (e.g. #Tags, Protocol)
- Allows to simulate protocols and get “typical values”

Performance (2/3)

	1 Tag		20 Tags	
	[ms]	Factor	[ms]	Factor
Reference Protocol	10.23	1	359	1
Tag Auth. With ID	20.94	2.0	583	1.6
Tag Auth. With Tracking Prev.	23.36	2.3	622	1.7
Reader Auth.	20.94	2.0	580	1.6
Mutual Auth.	25.77	2.5	680	1.9
Mutual Auth. With Key Exchange	25.77	2.5	676	1.9

Performance (3/3)

- Interleaved Protocols
  - Worst case:
    - one Tag
  - Best case:
    - optimum number of Tags
    - Timing ratio keeps constant

	Interleaved	
	Best	Worst
Tag Auth. With ID	1.4	2.3
Tag Auth. With Tracking Prev.	1.3	2.1
Reader Auth.	1.4	2.3
Mutual Auth.	1.3	2.6
Mutual Auth. With Key Exchange	1.3	2.6

Conclusion

- Appropriate AES core for RFID
- Standard authentication protocol
- Integrated into RFID communication standard
- The overall performance is acceptable for enhanced security
- Solution for Authentication in RFID Systems in Practice