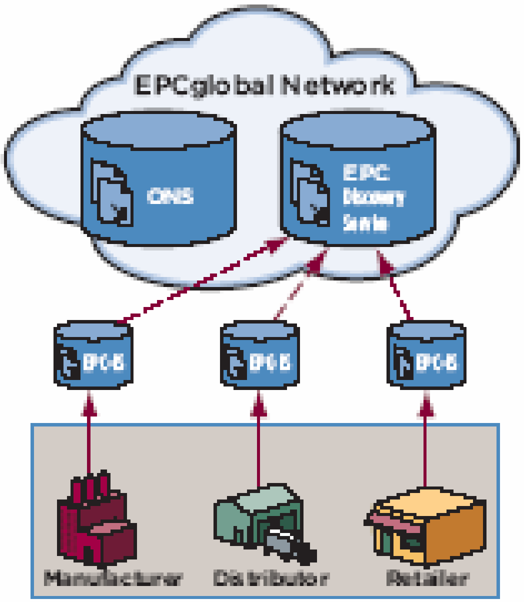
SCIS 2006: The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Mobile RFID Security Issues

Divyan M. Konidala, Kwangjo Kim
Cryptology and Information Security Lab (CAIS Lab)
Auto-ID Lab, ICU, Korea
Information and Communications Univ. (ICU)
Daejeon, South Korea

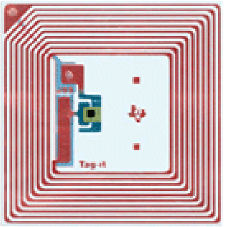
RFID Technology (1/2)

- Radio Frequency Identification (RFID): means to quickly auto-identify
  - objects, assets, pets, and people.
- So far, RFID technology: used to track inventory in the supply chain
  - Wal-Mart, P&G, HP, Prada, Gillette, GAP



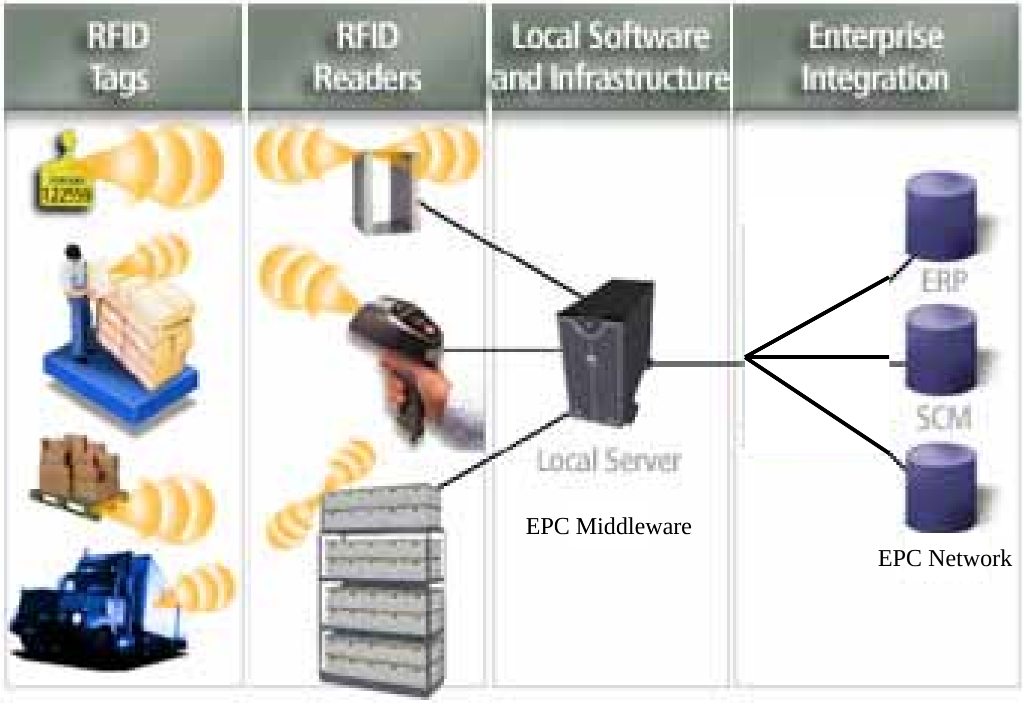
(Adapted from Source: VeriSign, "The EPCglobal Network: Enhancing the Supply Chain")

RFID Technology



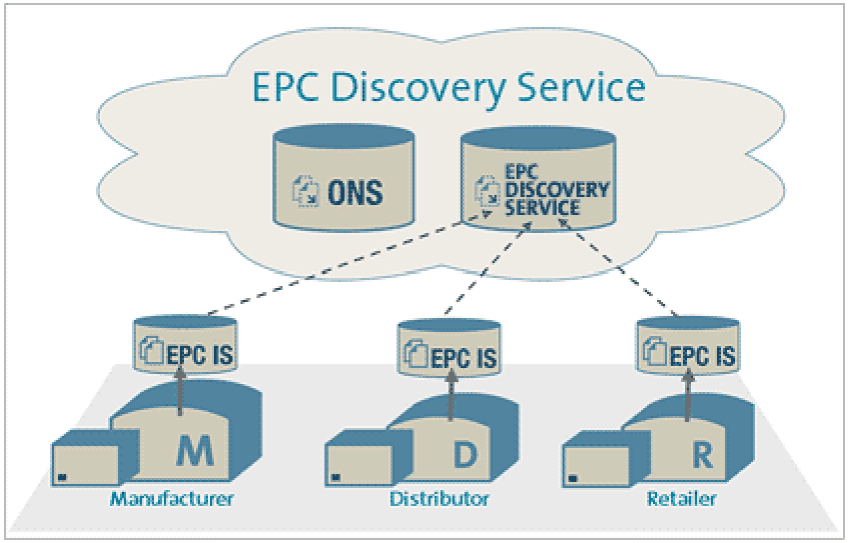
A typical RFID tag

(Adapted from Internet)

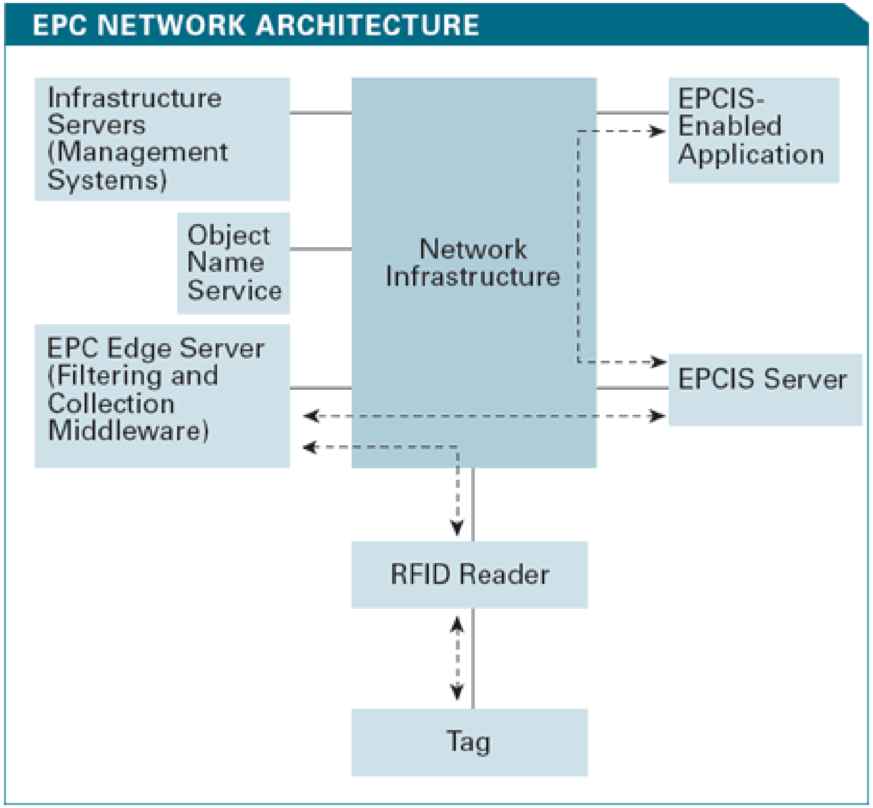


(Adapted from Source: http://www1.webmethods.com/images/solutions/webMethods_RFID_121703.jpg)

EPC Network



(Adapted from Source: VeriSign)


EPC NETWORK ARCHITECTURE
Infrastructure Servers (Management Systems)
Object Name Service
EPC Edge Server (Filtering and Collection Middleware)
Network Infrastructure
EPCIS-Enabled Application
EPCIS Server
RFID Reader
Tag

(Adapted from Source: cisco)

Mobile RFID Technology (1/2)

- RFID readers would become ubiquitous
- Get easy and quick information about
  - Movies by scanning RFID tagged posters
  - Location by scanning RFID tagged sign posts
  - Prices of RFID tagged merchandise sold at stores for Compare Shopping

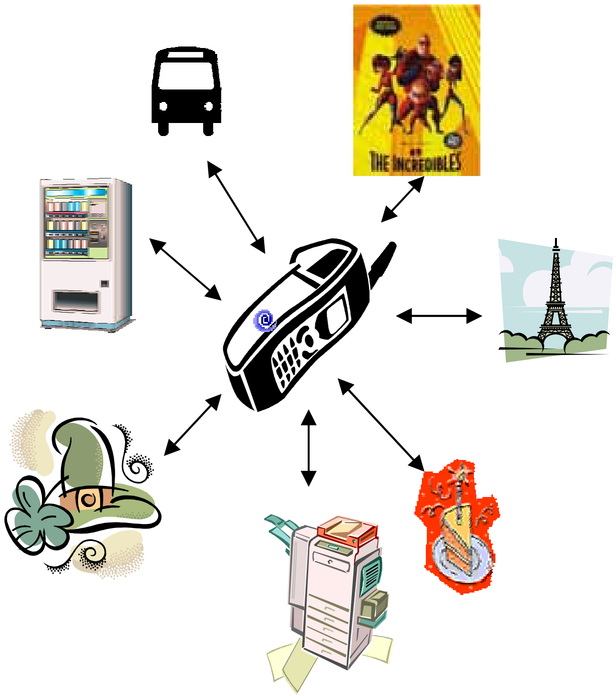
Mobile RFID Technology (2/2)

- A mobile phone or any portable device
  - Also **behaves as RFID reader**
- Integrating RFID reader chip into mobile phone
  - User friendly approach to quickly
    - Access information from other RFID tags
  - Brings the RFID technology more closer to the common users and daily life
- Nokia Unveils RFID Phone Reader

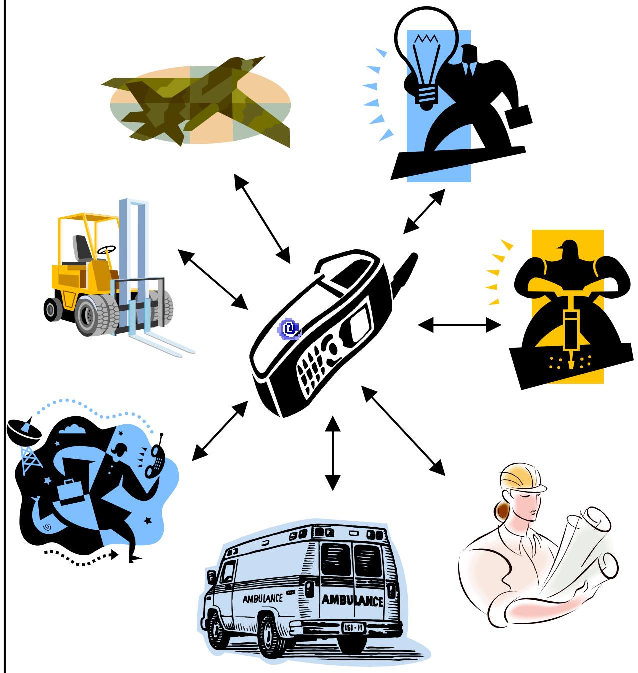
(Adapted from http://europe.nokia.com/nokia/0,,55739,00.html)

Three Application Zones of Mobile RFID

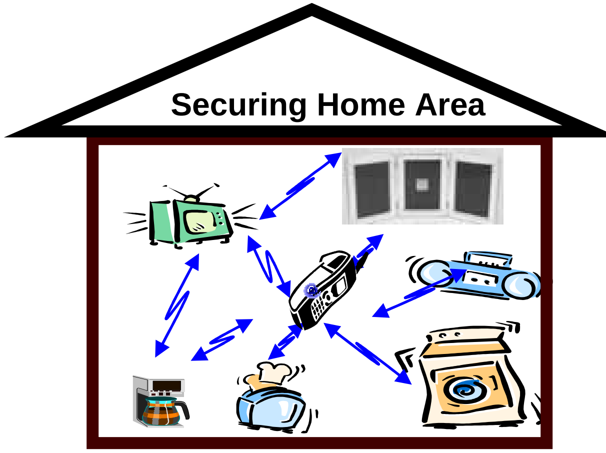
LBS Zone



Enterprise Zone



Private Zone



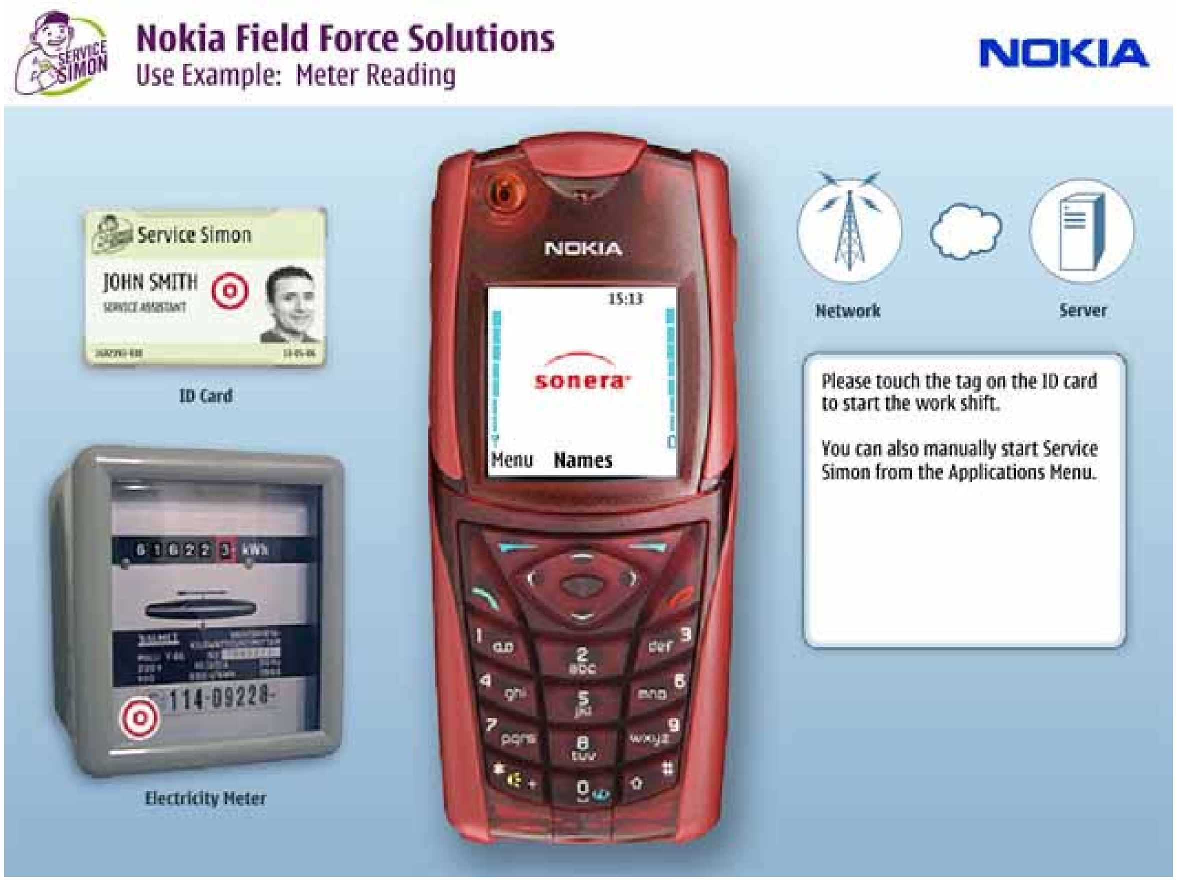
Mobile RFID Application Zones

- Location-based Services (LBS) Zone
  - Very open, unprotected zone: tags, tags everywhere
  - All RFID tagged items respond to every mobile RFID
  - No need for security between RFID tag and mobile RFID
  - Publicly available tags can be fake
  - Establishing a appropriate security architecture is very difficult.
  - Mobile RFID must contact many EPC-IS which might be either genuine or malicious.

Mobile RFID Application Zones

- Enterprise Zone
  - Proprietary and confined to the boundaries of a particular organization
    - Well-monitored zone: not very difficult to establish & enforce
      - efficient security architecture, trust model, and security & privacy policies.
  - Availability of up-to-date list of registered employees & items/products in a company;
    - designing and implementing security, moderately easy and mostly risk free when compared to LBS zone

Enterprise Zone



Please touch the tag on the ID card to start the work shift.

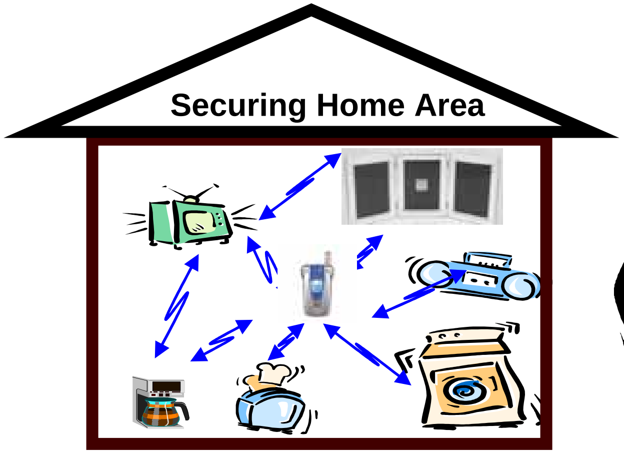
You can also manually start Service Simon from the Applications Menu.

Mobile RFID Application Zones

- Private Zone
  - Small: requires a simple security model
  - Easily deployed and maintained by the user at his home. Users in this zone can buy off- the-shelf Mobile RFID Kits.
  - These kits can contain
    - RFID tags, Mobile RFID, related hardware, and software with user-friendly GUI.

Private Zone

Private Zone



Mobile RFID

PC + S/W

GUI based Mobile RFID Kit

Security Requirements: Mobile RFID - LBS Zone

- Secure Job Delegation
- Trust Model
- Unauthorized Tag Information Access
- User Privacy Protection
- Tag Access-Control Management
- Tag Access Authorization
- Data Integrity & Confidentiality

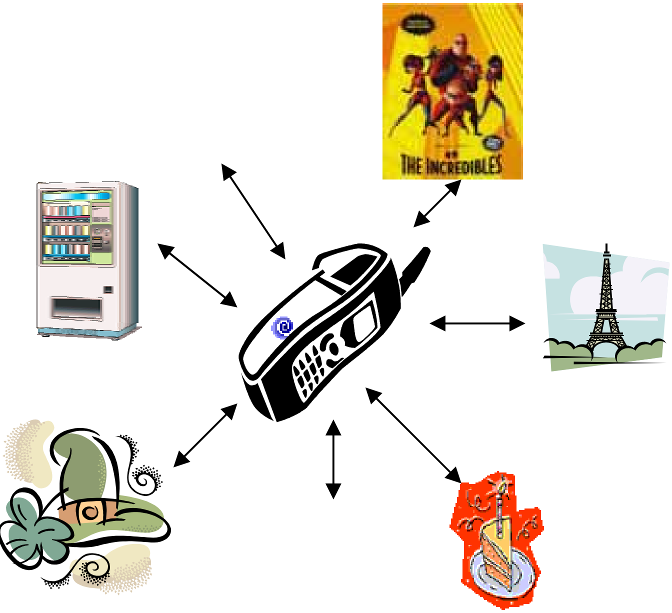
Building Blocks: Mobile RFID - LBS Zone

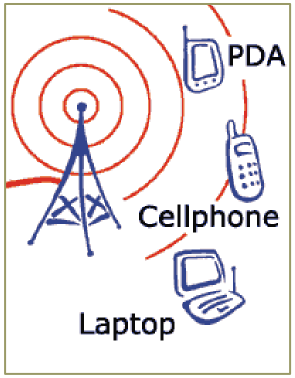
LBS Zone

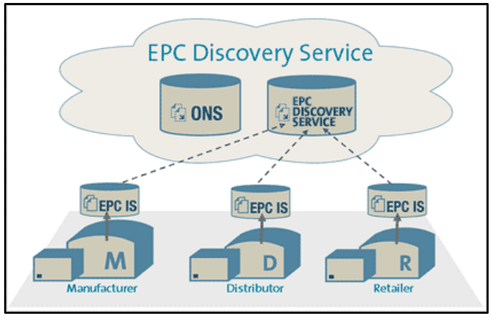
Mobile RFID

Mobile Operator

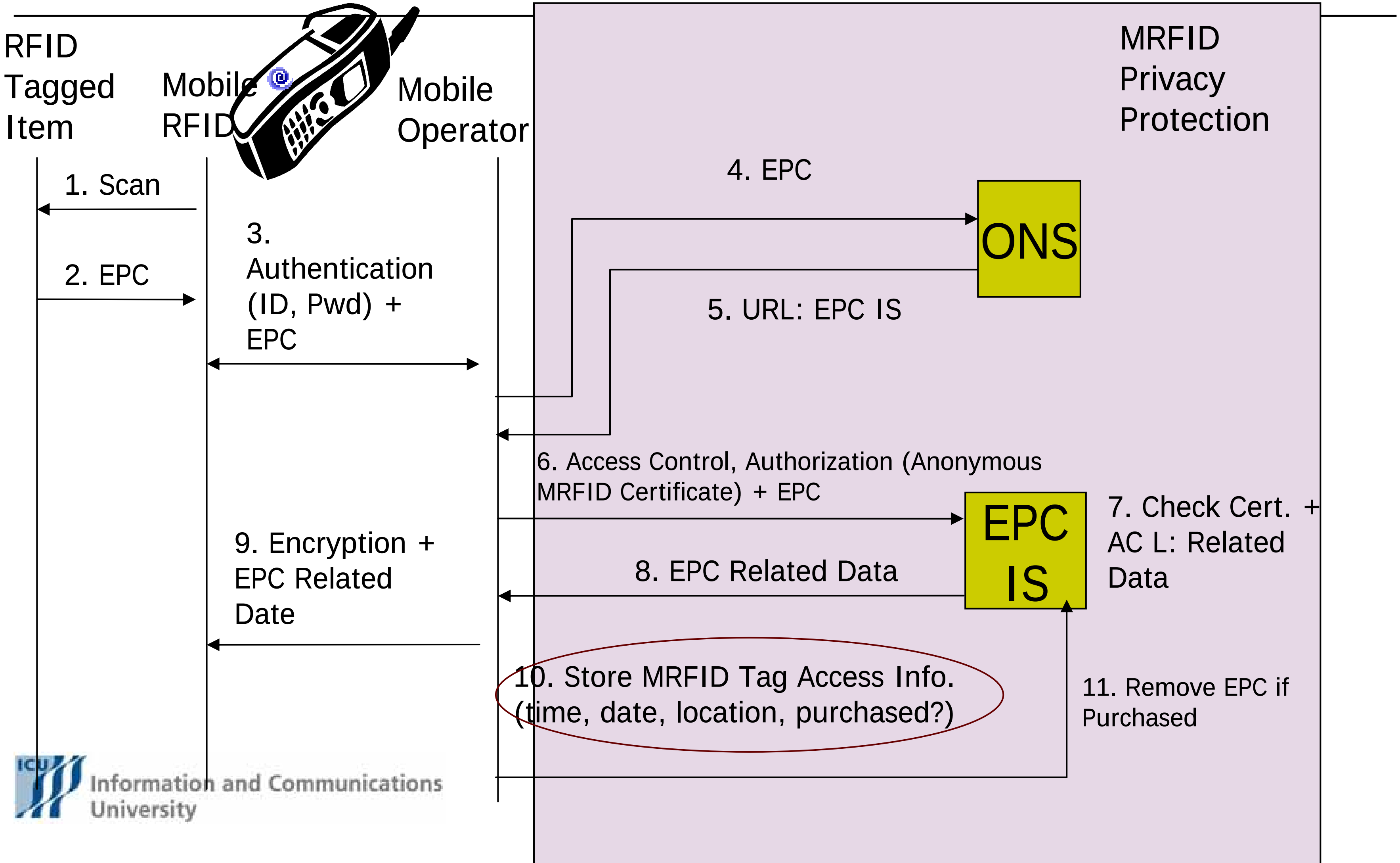
EPC Network







Security Architecture: Mobile RFID - LBS Zone



RFID Tagged Item

Mobile RFID

Mobile Operator

MRFID Privacy Protection

1. Scan

2. EPC

3. Authentication (ID, Pwd) + EPC

4. EPC

ONS

5. URL: EPC IS

6. Access Control, Authorization (Anonymous MRFID Certificate) + EPC

EPC IS

7. Check Cert. + AC L: Related Data

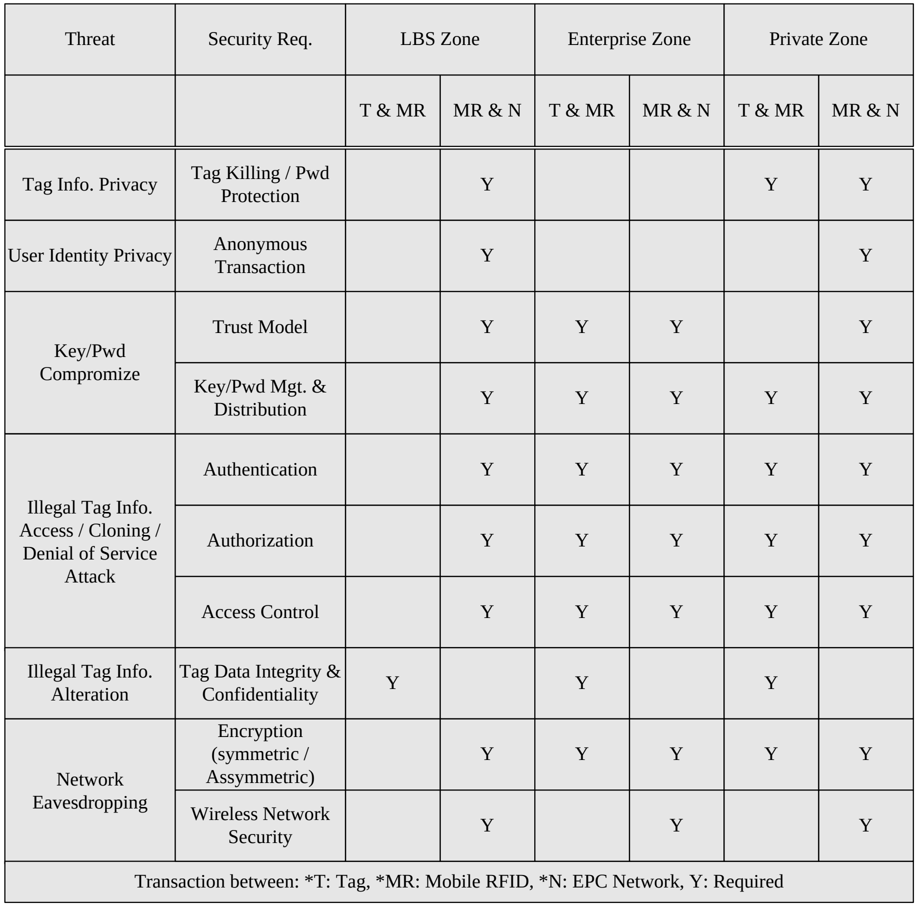
8. EPC Related Data

9. Encryption + EPC Related Date

10. Store MRFID Tag Access Info. (time, date, location, purchased?)

11. Remove EPC if Purchased

Comparison: Security Threats & Security Requirements of 3 zones



Threat	Security Req.	LBS Zone		Enterprise Zone		Private Zone	
		T & MR	MR & N	T & MR	MR & N	T & MR	MR & N
Tag Info. Privacy	Tag Killing / Pwd Protection		Y			Y	Y
User Identity Privacy	Anonymous Transaction		Y				Y
Key/Pwd Comprimize	Trust Model		Y	Y	Y		Y
	Key/Pwd Mgt. & Distribution		Y	Y	Y	Y	Y
Illegal Tag Info. Access / Cloning / Denial of Service Attack	Authentication		Y	Y	Y	Y	Y
	Authorization		Y	Y	Y	Y	Y
	Access Control		Y	Y	Y	Y	Y
Illegal Tag Info. Alteration	Tag Data Integrity & Confidentiality	Y		Y		Y	
Network Eavesdropping	Encryption (symmetric / Assymmetric)		Y	Y	Y	Y	Y
	Wireless Network Security		Y		Y		Y
Transaction between: *T: Tag, *MR: Mobile RFID, *N: EPC Network, Y: Required							

Key Security Solutions Required

- Mutual Authentication mechanism between M-RFID and MO
- Mutual Authentication mechanism between MO and EPC-IS
- Anonymous Certificates for Identity management, authentication, and authorization
- M-RFID privacy

Conclusion & Future Work

- Proposed 3 application zones for Mobile RFID
  - highlighted distinct security threats & security requirements
- User Privacy is protected from service providers
- Proposed architecture integrates with EPCglobal EPC Network
- Reduces the burden on mobile device
- Efficient trust model & job delegation: Mobile Operator
- Future Work
  - Detailed research on the security for all 3 zones
  - Apply formal Security and cryptographic primitives

References

[1] Ari Juels, “RFID Security and Privacy: A Research Survey”, RSA Laboratories, 2005

[2] EPCglobal Web site, 2005, http://www.EPCglobalinc.org

[3] Nokia, “RFID Phones - Nokia Mobile RFID Kit”, http://europe.nokia.com/nokia/0,,55739,00.html

[4] VeriSign, “The EPCglobal Network: Enhancing the Supply Chain”, White Paper 2005, http://www.verisign.com/stellent/groups/

Thank You!

Q & A