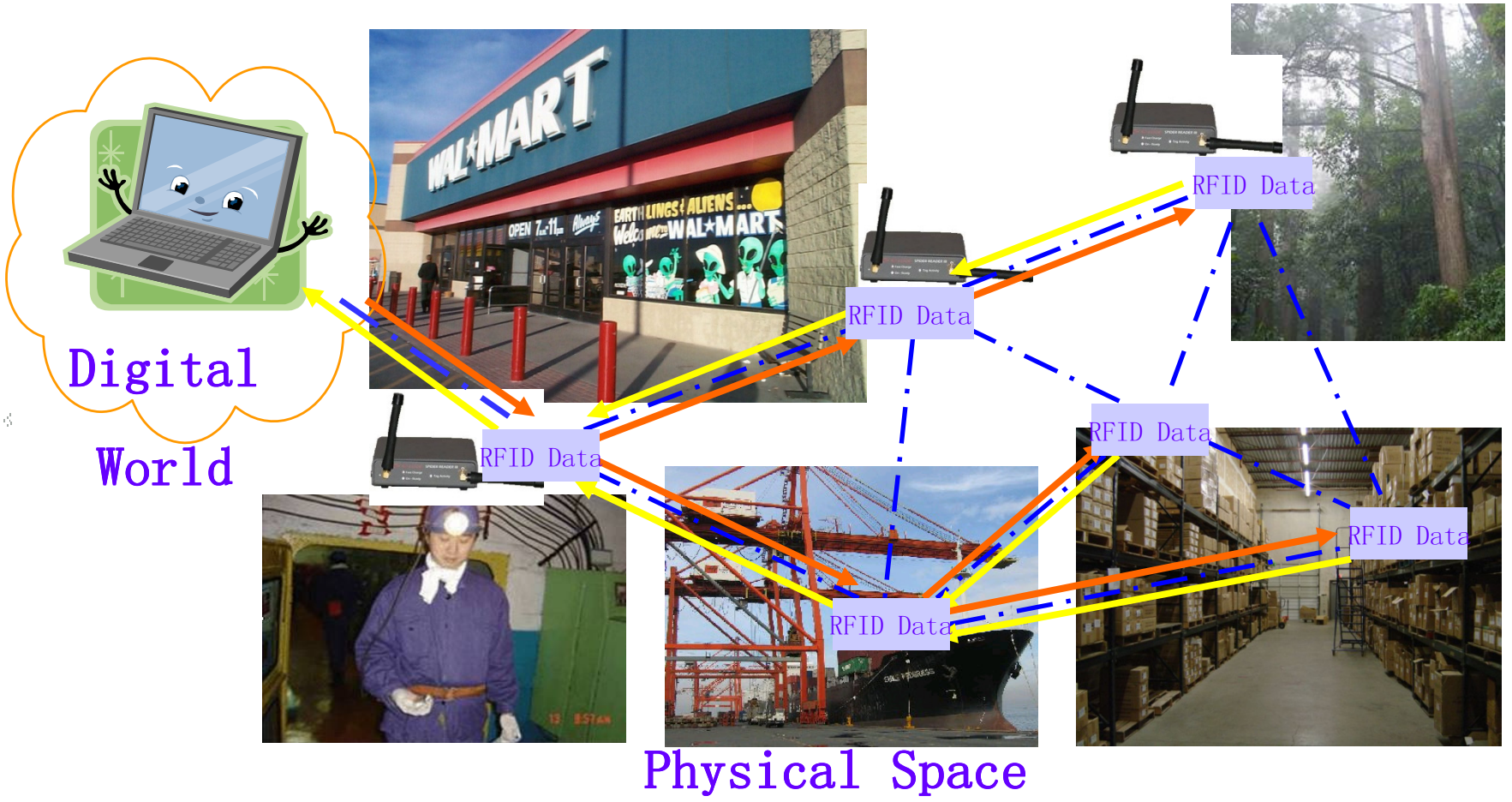
Trustworthy RFID Solutions for E-Logistics and Internet of Things

Jinsong Han
韩劲松
Hong Kong University of Science and Technology

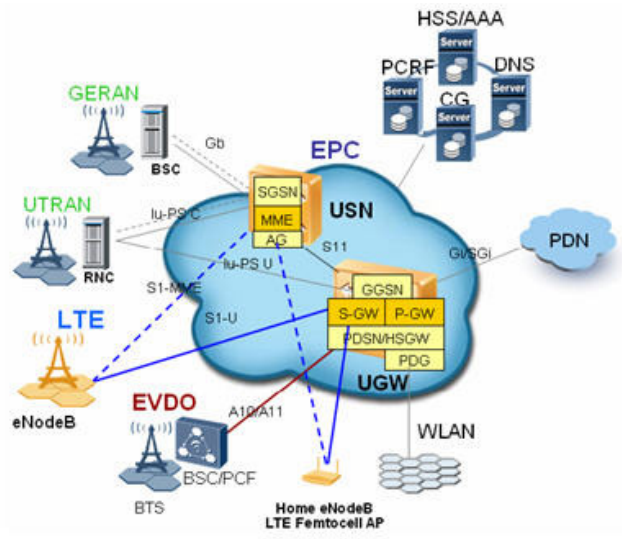
RFID System（无线电子射频识别系统）

- Bridging physical space and digital world



RFID Systems, the Future
射频识别系统的应用前景

- **Internet of things (IOT) 物联网**
  - **RFID tags and other smart devices**
  - **Each dust has an ID**
  - **Pervasive computing**
- **Any time, Anywhere, Any service, …**



E-logistics, Security, and Trust
电子物流与安全可信计算

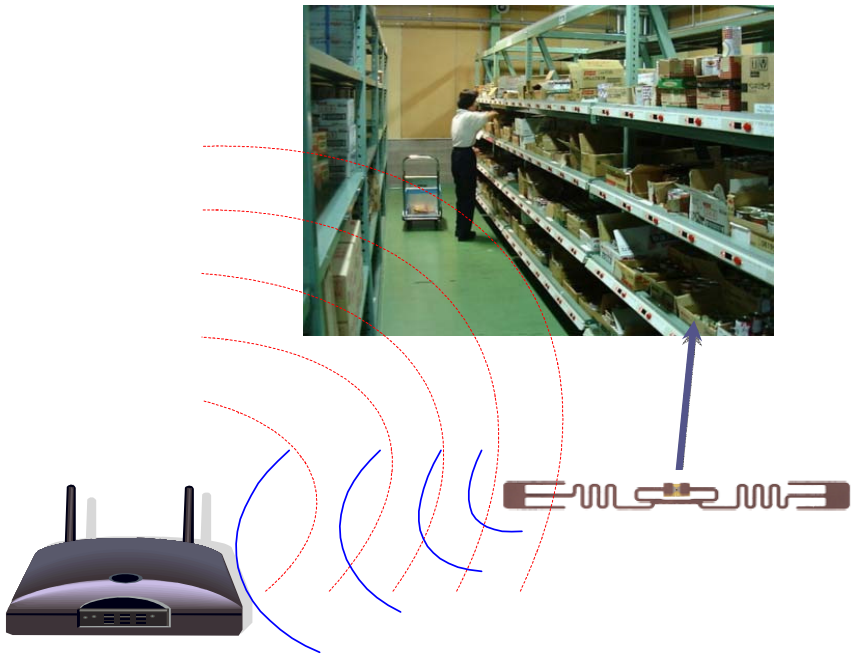
- 外部风险
  - “深圳百家物流企业在粤赣高速频遭盗抢”, 广州日报, 2009-10-26。

- 内部管理
  - 目前，我国多数物流企业货损率在2%左右，物流作业过程效率低下、差错率和货损率居高不下。
- 未来电子物流及物联网对安全可信计算的需求

Challenges and Issues
安全挑战

- Security
  - No security enhancements
  - Plaintext message
- Privacy
  - ID
  - Location
  - Number of tags
  - …

Adversary



Long-range detection

LSCM Project Overview
项目概況

- Phase I: Trustworthy RFID Technologies: Methodology and Practice, GHP/044/07LP, 2008-2010
- Phase II: Trust Solution for RFID Enabled Interoperable E-logistics, ITP/037/09LP, 2010-2012
- Sponsored by ITF in Hong Kong SAR
- Supervised by LSCM
- Platform research programs

Project Objectives
项目发展计划

- 开发基于RFID安全技术(Phase I)
  - 加解密 (En/Decryption)
  - 认证 (Authentication)
  - 隐私保护(Privacy Protection)
- 基于RFID的安全可信架构技术(Phase II)
  - 可信中心 (Trust Center)
  - 信任及信用管理 (Trust management and auditing)
  - 所有权转移 (Secure Ownership Transfer)
  - 可信合作 (Trustworthy Collaboration)

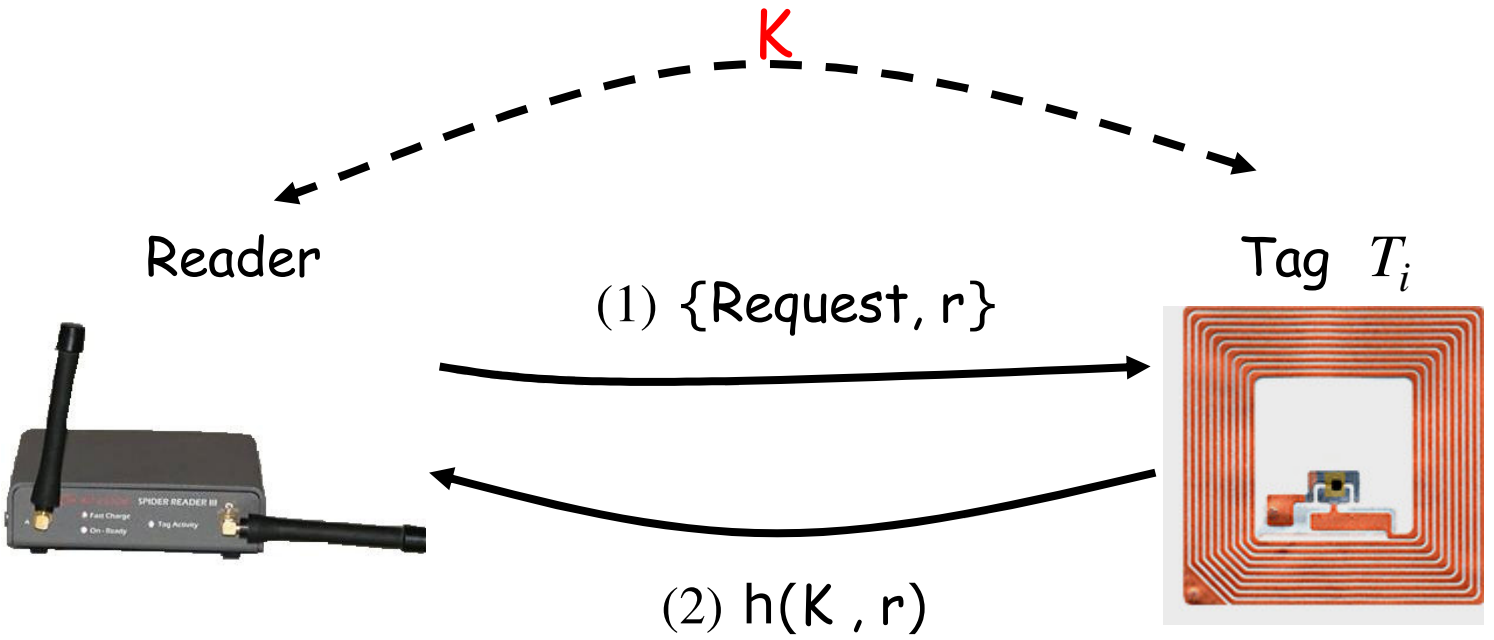
Bottlenecks of RFID Applications
可信RFID应用的瓶颈和挑战

- 认证模式
  - 一对一认证
  - 费时费力
- 识别效率
  - 基于ALOHA的识别模式
  - 底层通信模式效率低下
- 保护方式
  - 现有工作集中于应用层
  - 密码算法实现
  - 缺乏物理层保护

安全及隐私保护协议
Privacy-Preserving Authentication

Linear search, O(N). Simple, Safe, but not Scalable.

Solution: Highly efficient authentication schemes (Tree based search, Randomization, Key-updating, etc.)



批量认证——快速防伪

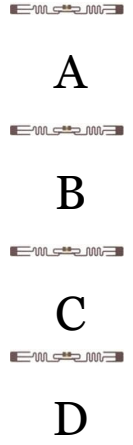
- 批

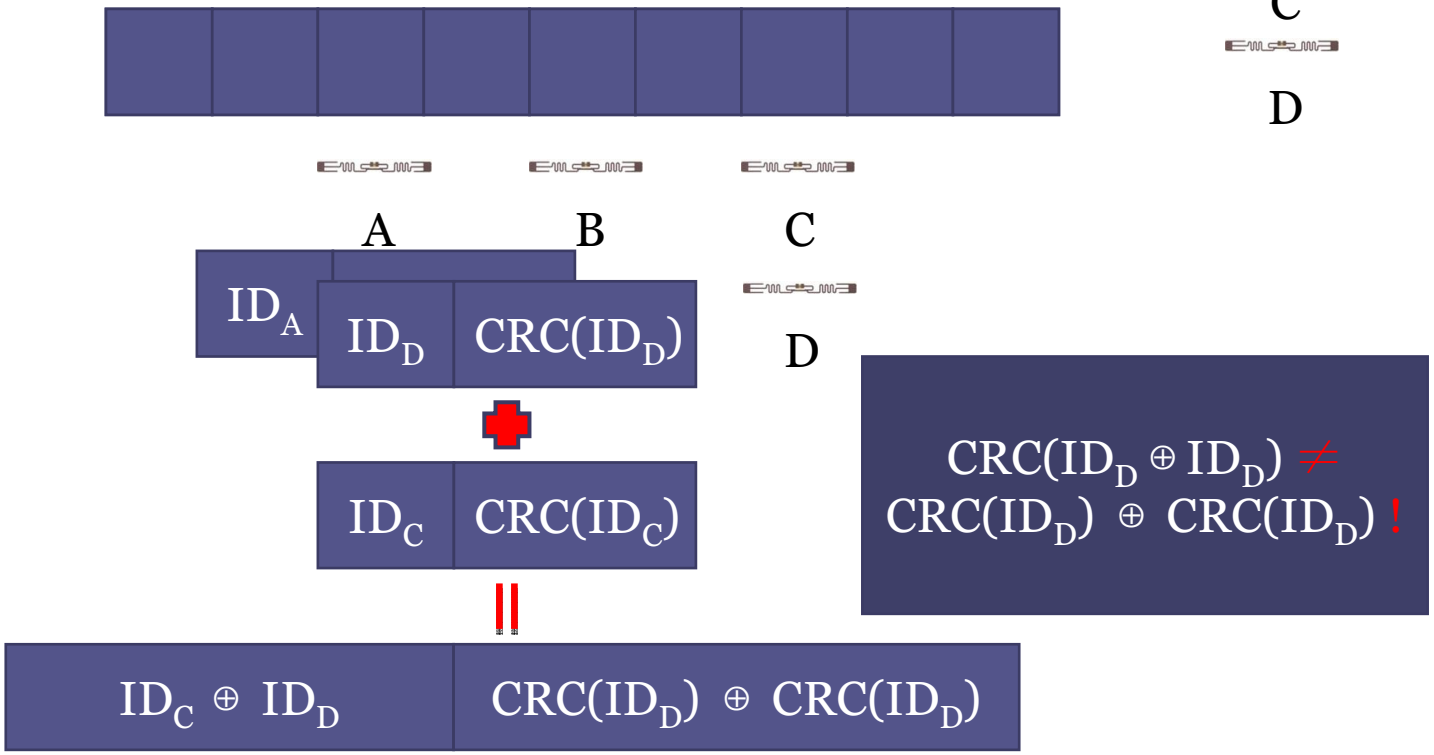
Tag size	AA	SMP	SEBA-2	SEBA-3
1000	72.95s	17.28s	15.18s	15.17s
2000	145.07s	21.30s	10.71s	10.70s
3000	213.46s	25.10s	9.192s	9.18s
4000	287.68s	29.23s	8.28s	8.27s
5000	362.26s	33.38s	7.69s	7.68s
6000	434.25 s	37.39s	7.29s	7.28s
7000	508.04s	41.50s	6.97s	6.95s
8000	579.6s	45.48s	6.72s	6.71s
9000	641.8s	48.97s	6.54s	6.53s
10000	712.48s	52.88s	6.37s	6.35s
11000	788.48s	57.12s	6.21s	6.19s
12000	866.57s	61.46s	6.07s	6.04s

n

识别效率——高效识别

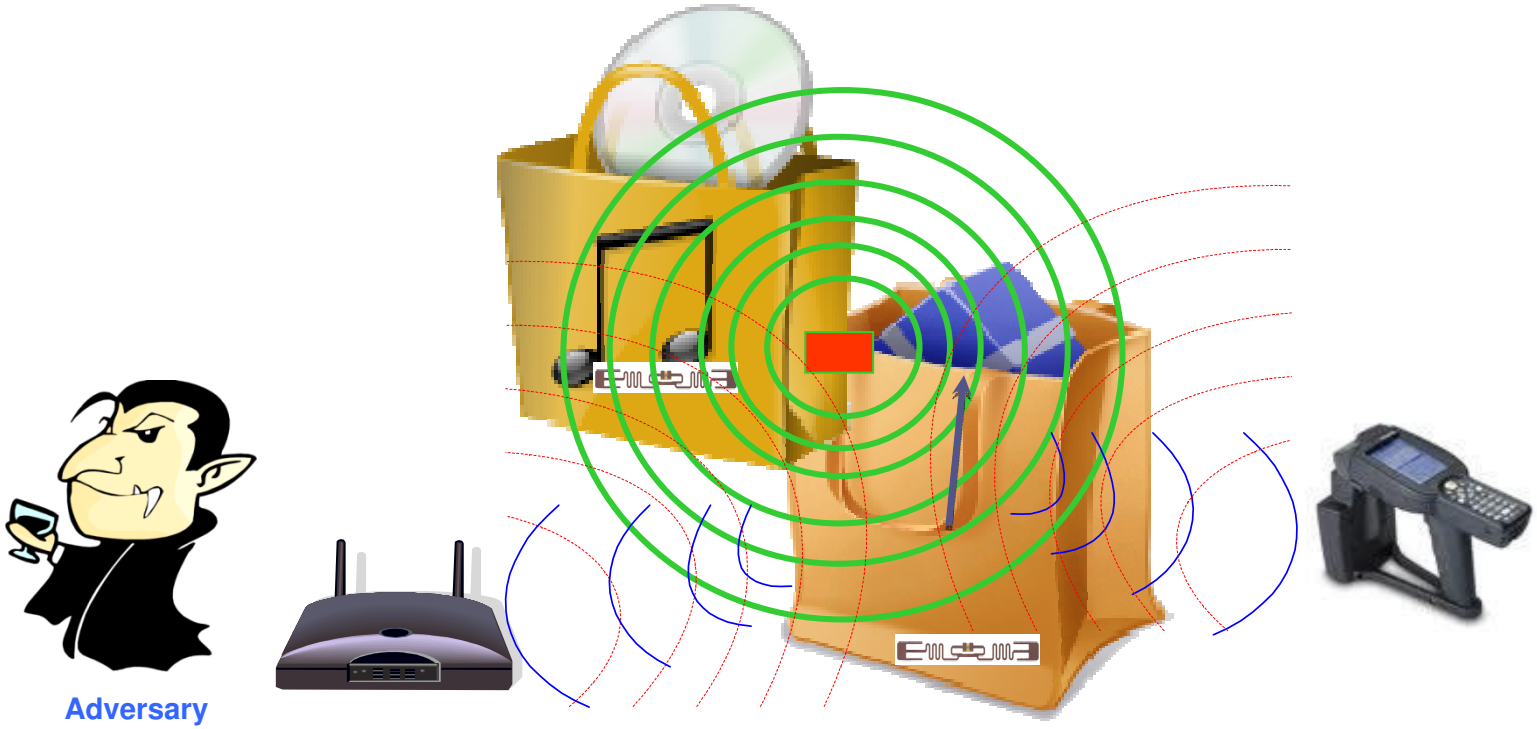
- 基于ALOHA的识别模式
  - Framed Slotted Algorithm
  - CRC Code



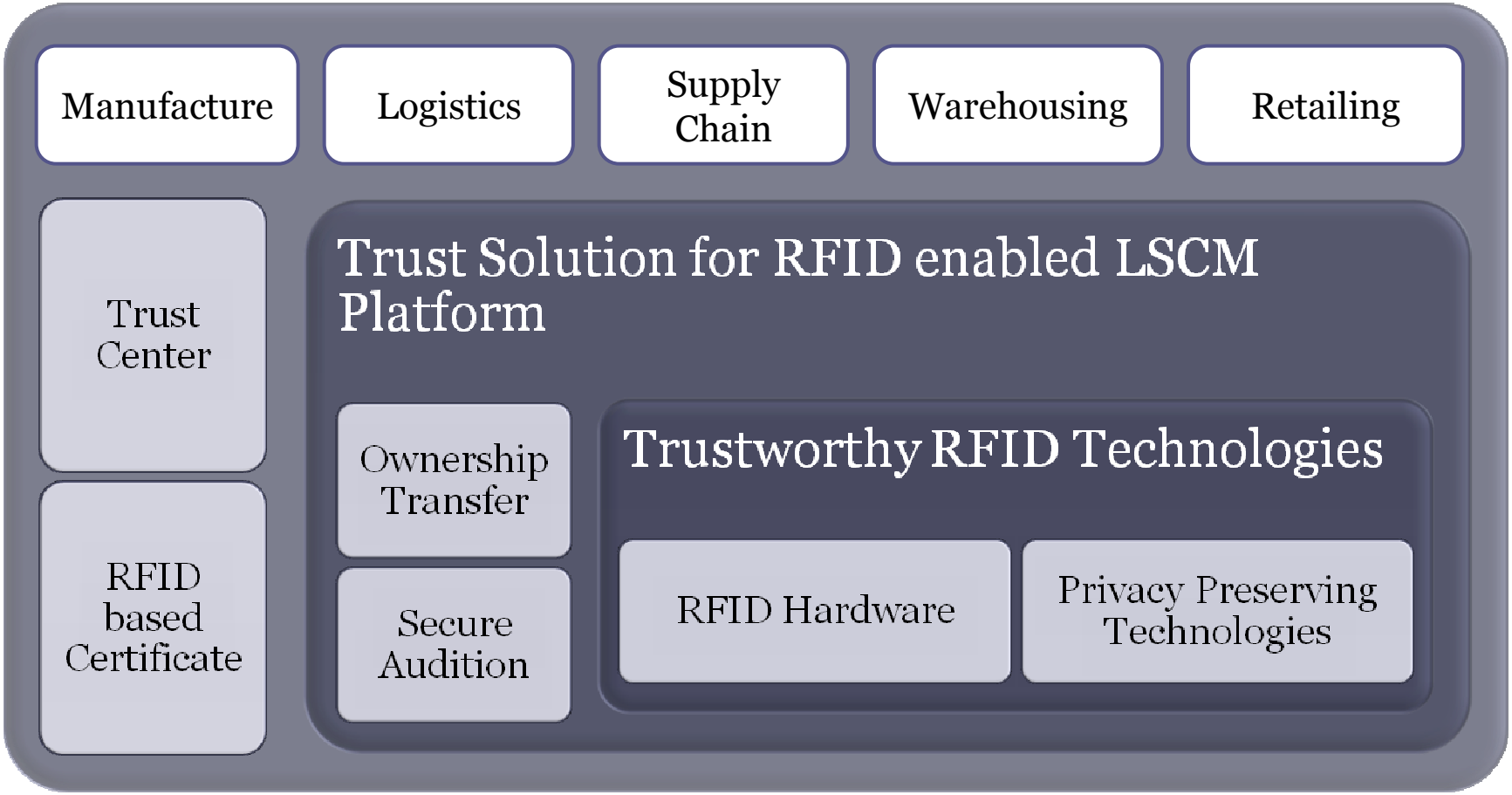


保护模式——主动式保护

- 开发主动式防护标签



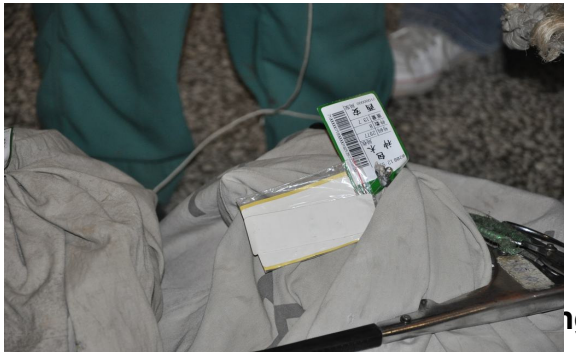
可信RFID支持下的电子物流架构
Trusted E-logistic infrastructure



Applications —— China Post
行业示范应用

- **Xi’an Postal Processing Center（西安邮政处理中心）-- One of the 7 key-processing centers in China**
  - **20 million packages of mails, 640 million letters, 32 million flat mails, 10.8 million parcel-like mails per year.**

Replacing Barcodes for Identification 替换条码技术



Automatic Processing – Efficiency
提高自动化处理效率

- **Manual process may need about 1s for each item.**
- **Using RFID can fast scan a batch of items.**

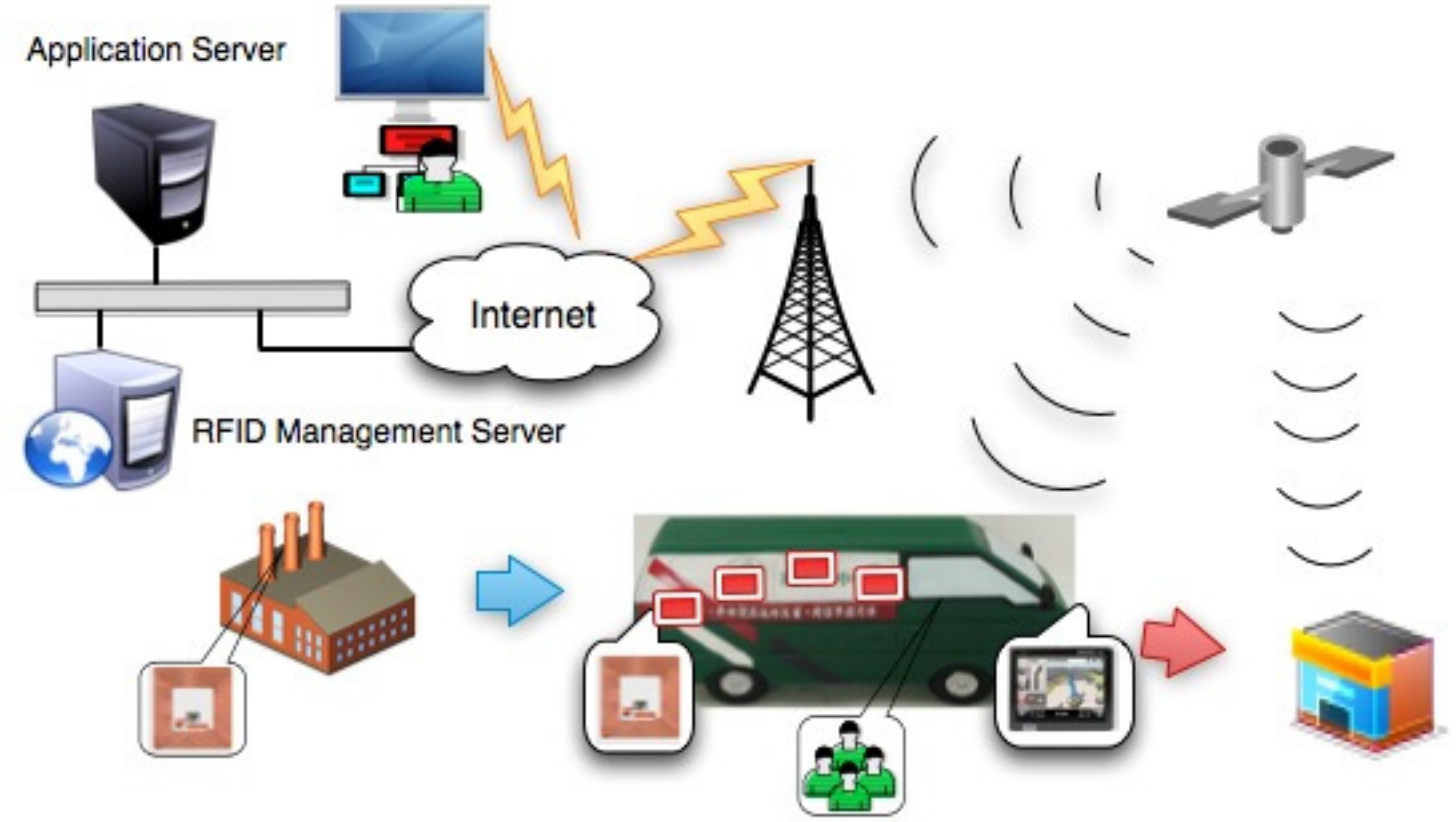
Real Time Monitoring – Reliability
实现实时可靠监控

- **Locating an item without unpacking the package**
- **Monitoring the items**

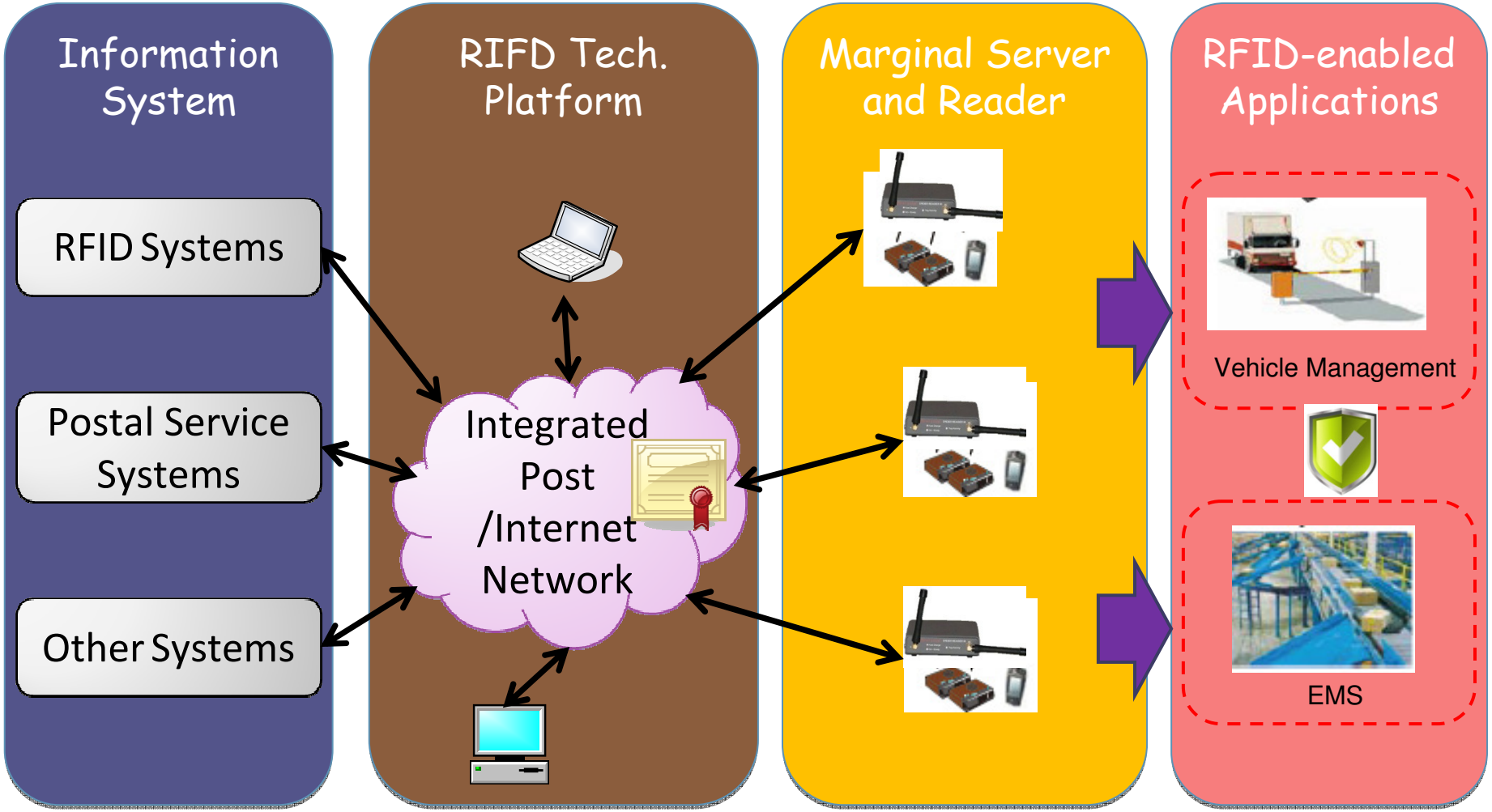





Online Tracking – Security
实现在线跟踪



Trustworthy Postal Applications
可信RFID邮政示范应用




Thank you!