



Building Radio frequency IDentification solutions for the Global Environment

Secure Supply Chain Solutions

Industry Perspectives

Andrea Soppera
BT Innovate and Design



Agenda

- **Part I – Research Challenges**
- **Part II – Our Vision**
 - Securing Data Services
- **Part III – Technology Innovation**
 - Secure Tags
 - Secure Readers
 - Secure Sharing in the IOT



© 2007



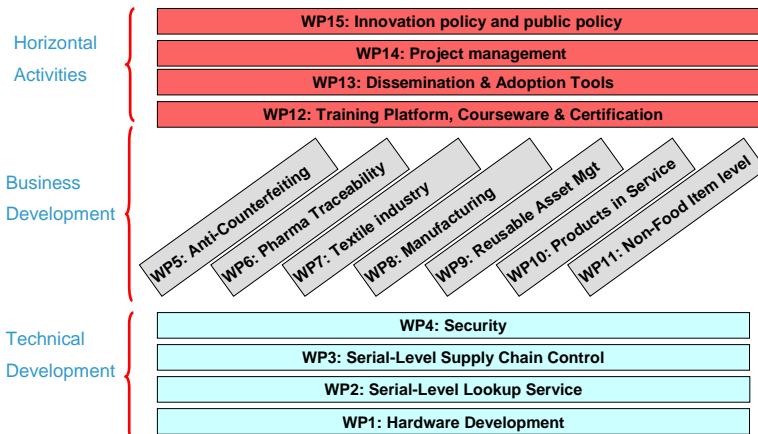


Part I – “Research Challenges”



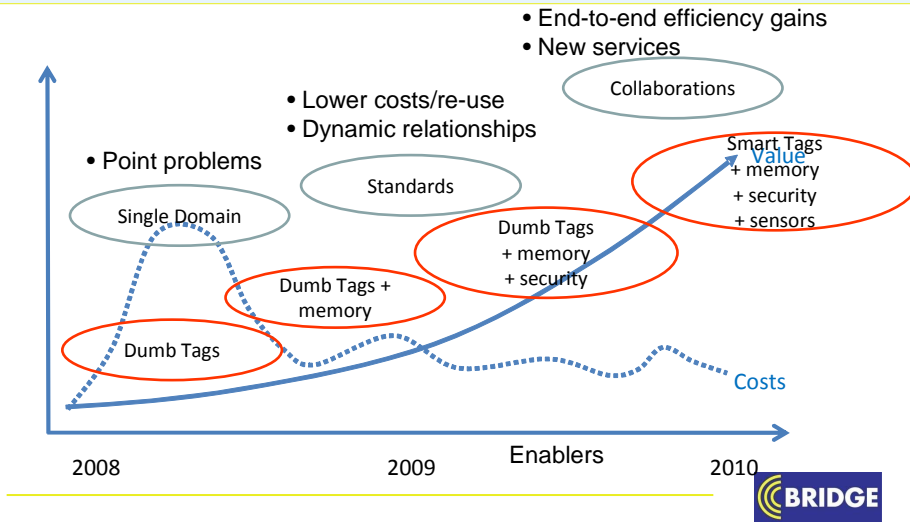
Part I – Research Challenges

Building Radio frequency IDentification solutions for the Global Environment





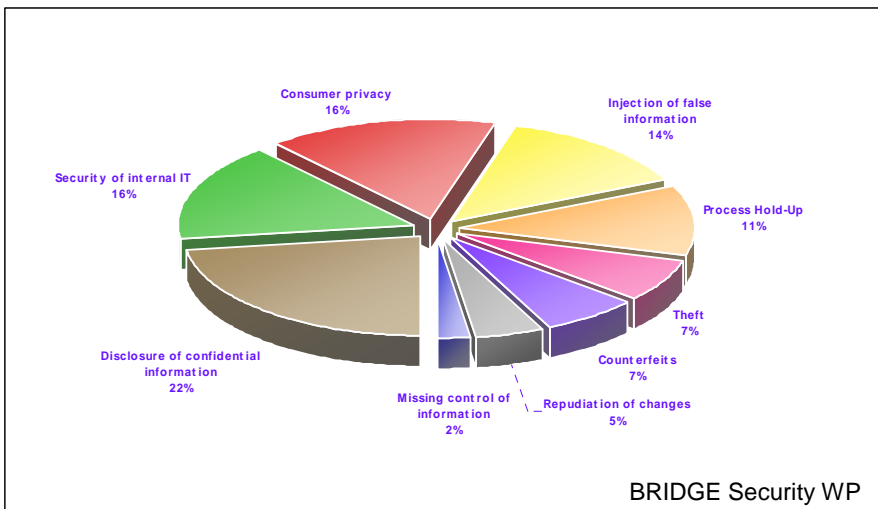
Collaborative Secure Supply Chains



© 2007



Security Concerns



BRIDGE Security WP





Top Priorities

- 1. Securing data services** – by increasing control over data sharing and devices
 - Lightweight security mechanisms for passive RFID tags
 - Policies and access control mechanisms but scalability still an issue
- 2. Collaborative Information Sharing** – ecosystem services for discovery and security
 - Heterogeneous data sources without a common data standard
 - No mechanism to search and access confidential data across heterogeneous systems
- 3. Measuring Real World Inefficiencies** - extracting knowledge of supply chain operations
 - Event detection and learning algorithms



© 2007

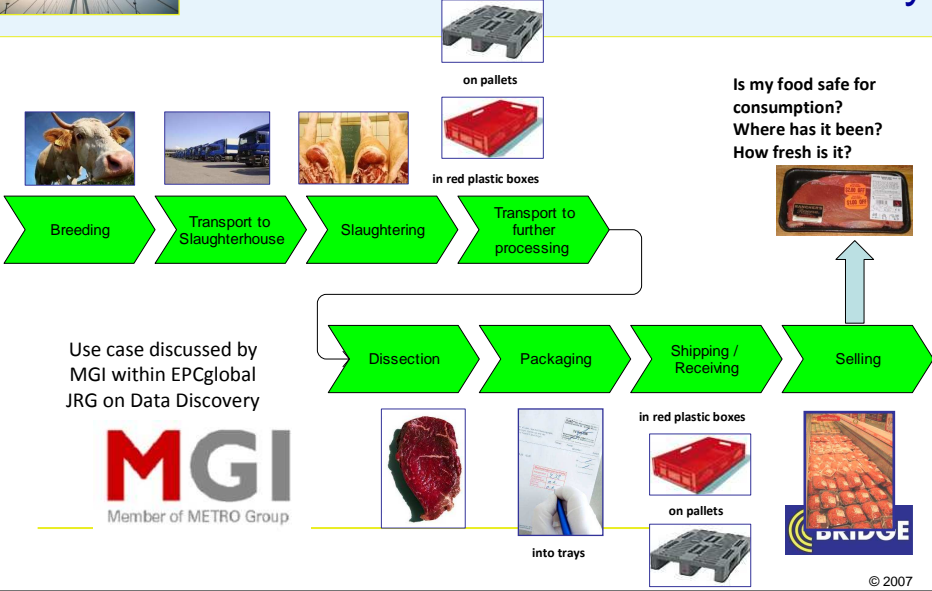


Part II – Our Vision “Securing RFID Data Services”





Use case: Fresh Meat Traceability

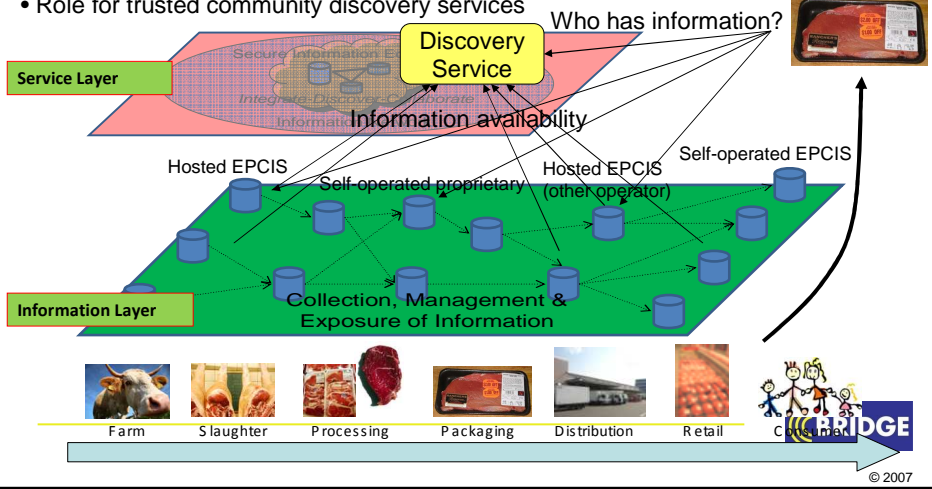


Ecosystem Services: Discovery

Finding the Correct Information

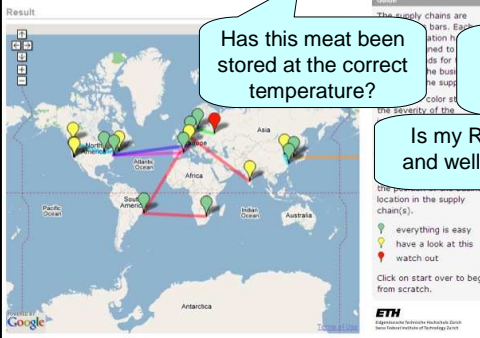
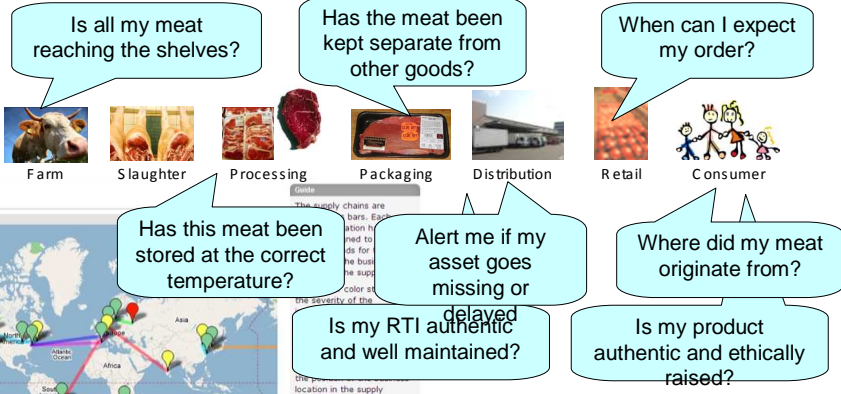
- Who has information about my products?
- Where is my asset? Is my asset authentic?
- Role for trusted community discovery services

Is my food safe for consumption? Where has it been? How fresh is it?

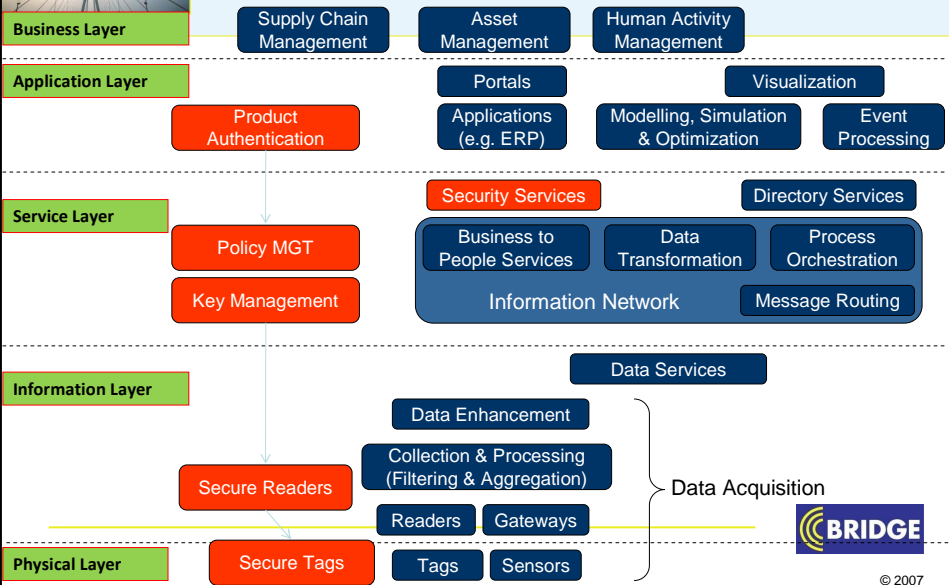




End-to-End Visibility



Technology Components






Part III – Technology Innovation and Dissemination



Part III – Technology Innovation



RFID Secure Services

Security E-Pedigree Services
Product Authentication
Identity Management
Asset Management

Is my product Authentic?
Who is the owner of this asset?

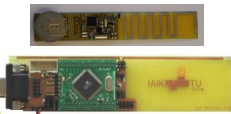

Secure Reader




Key Management Service

Policy MGT

Secure Track and Trace

Strong authentication instead of identification (proof of ID by challenge response mechanism)



Manufacturer Tag ID

Disadvantages

- Tag ID can be easily cloned and replicated
- Everybody can access Tag ID – little differentiation

Advantages

- Easy to deploy solution - Tag ID is already available
- No need to modify standards or collect/share tag history data



Secure Tag

Disadvantages

- Most solutions are based on semi-passive tags
- Increased cost of the tag reduces application space

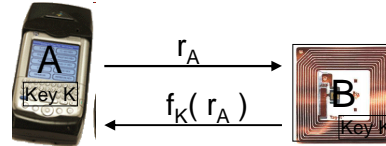
Advantages

- Enable added value services
- No modification to standards
- Can extend to cover privacy issues (e.g. beyond POS)
- Secure storage of data (e.g. aerospace maintenance records)
- Give to product a secure and unclonable identity



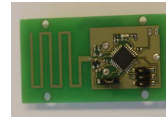
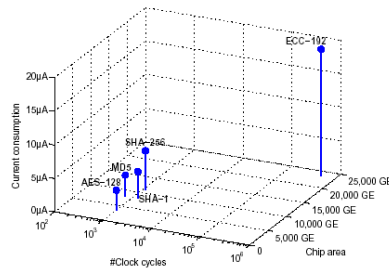
Tag Security

- Benefits of Tag Security:
Strong **authentication** instead of identification (proof of ID by **challenge response** mechanism)



So far investigated:

- AES-128
- TEA
- SHA-1
- SHA-256
- MD5
- Trivium
- Gain
- ECC-192



Need for Secure Readers

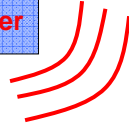
- Identification vs. Authentication
 - Need to authenticate goods
- Increase in Collaborative Systems
 - Multiple parties without strong established trust
- Privacy and Confidentiality
 - Protecting consumers and business intelligence
- Supply Chain Integrity
 - Operating critical processes
- Increase in Secure Tag usage: Key management
 - Enabling scalable deployment of secure RFID tags





RFID “Reading Policy”

RFID Reader



Readings:

- 32 Folders
- 12 Notepads.

- 1 Branded Bag
- 1 Wig
- 2 Medical Drugs



Retail ‘XY’

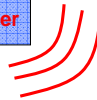


© 2007



RFID “Reading Policy”

RFID Reader



“Read unsold items but protect consumer information.”

Readings:

- 32 Bottles of wine
- 12 Bottles of Vodka.

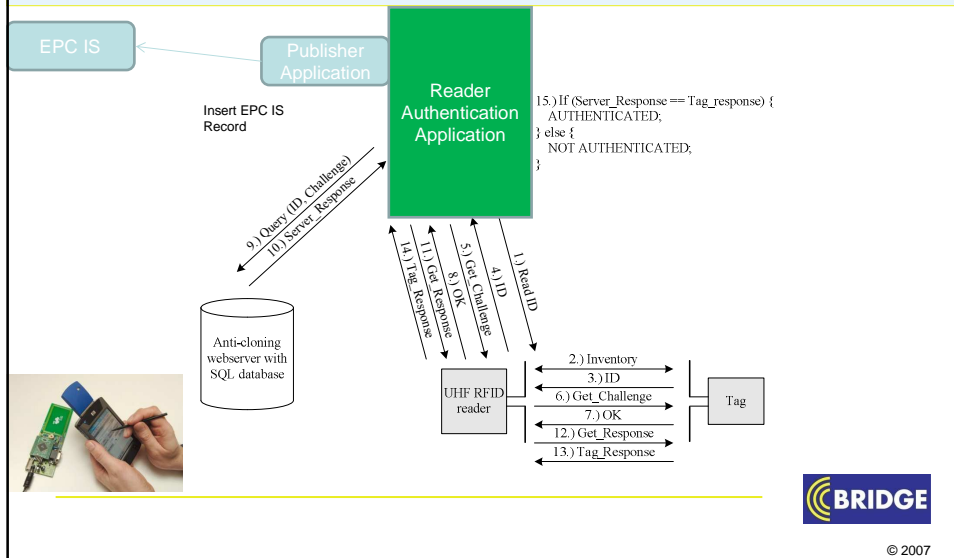


Retail ‘XY’



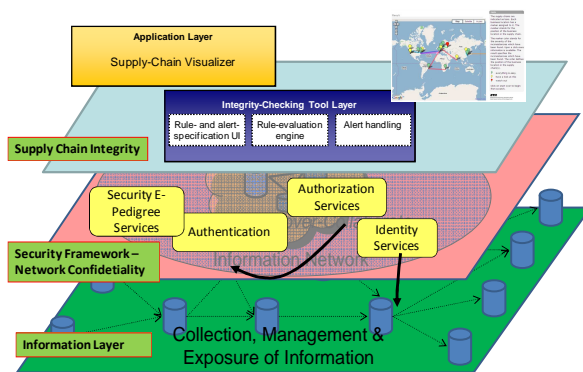
© 2007

Use of Trusted Reader for RFID Authentication



© 2007

Next Steps? Securing Sharing in the IOT



Need to discover RFID data under the control of other parties with whom no prior business relationship exists





Security Goals in the IOT

Supply chain Integrity

- **Publisher Control**
 - The resource owner should be able to control who can see their resource information (or whose queries they receive)
- **Delegation**
 - The resource owner will require delegation capabilities to allow access to previously unknown parties
- **Query Confidentiality**
 - Queries are also confidential
- **Integrity**
 - Should be able to authenticate and verify the information
- **Availability**
 - Need resource independence and consider amplification attacks



Conclusions

- **Part I – Research Challenges**
- **Part II – Our Vision**
 - Securing Data Services
- **Part III – Technology Innovation**
 - Secure Tags
 - Secure Readers
 - Secure Sharing in the IOT



© 2007





Building Radio frequency IDentification solutions for the Global Environment

Thanks

andrea.2.soppera@bt.com

