



How to Think of Security in Anti-Counterfeiting and How to Achieve it with RFID



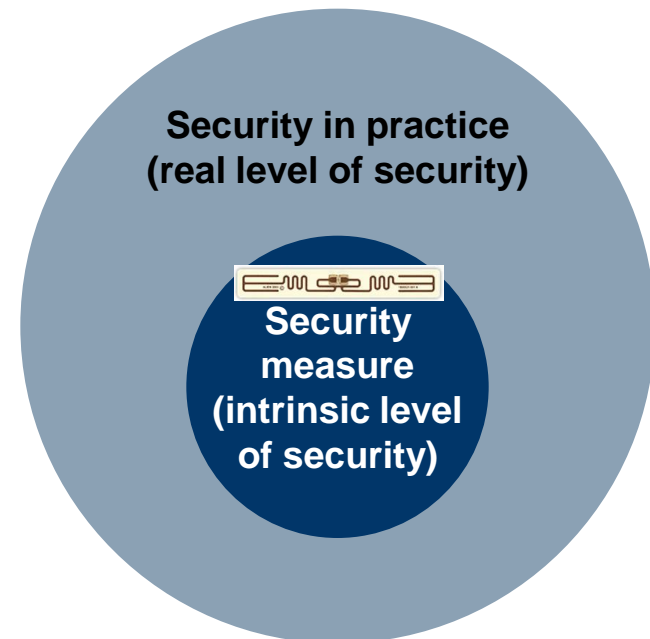
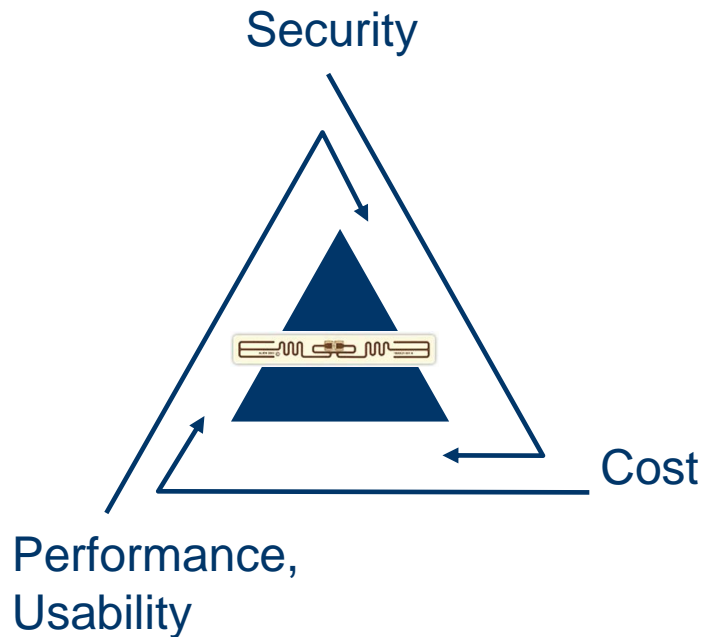
Information Society
Technologies

27.5.2009 – Mikko Lehtonen (ETH)



Sixth Framework Programme

- Security = Protection of assets against threats
 - Asset = Distribution channel
 - Threat = Counterfeit product enters distribution channel





Prevention
(Cost to break)



Detection
(Detection rate)



Response
(Expected fine)

Direct effect of security

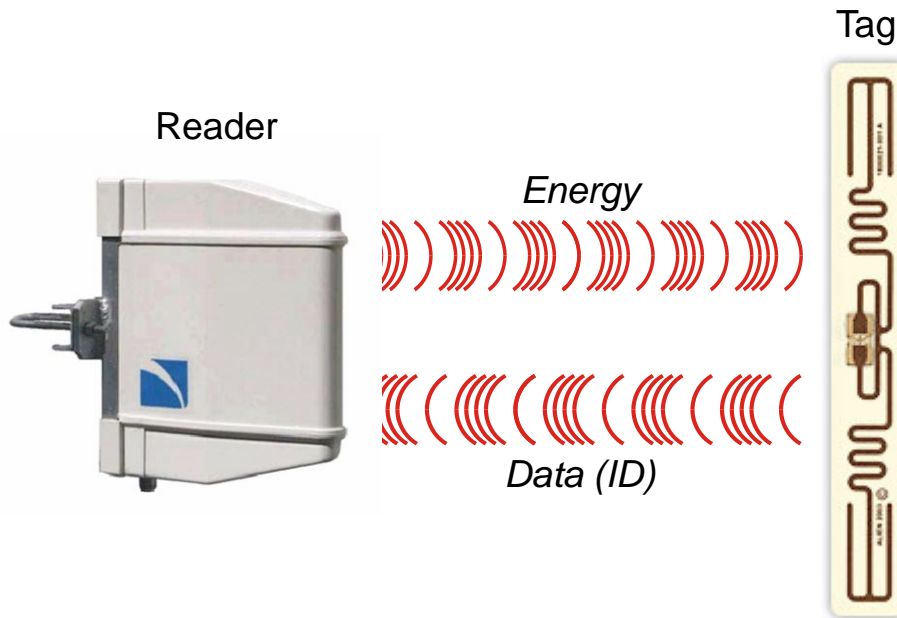
$$\text{Pr(counterfeit product detected)} = \text{Check rate} \cdot \text{Pr(counterfeit detected in a check)}$$

Target: 100%

Indirect effect of security (deterrent effect on counterfeiter)

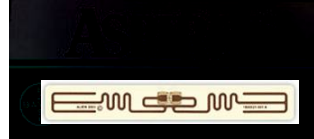
$$\text{Expected profit} = \text{Pr(counterfeit product not detected)} \cdot \text{Illicit profit - Cost to break} - \text{Pr(counterfeit product detected)} \cdot \text{Expected punishment}$$

Target: < 0



- Simple, low-cost devices
- EPCglobal vision: replace barcodes with 5¢ tags
 - Open-loop, industry-wide networks
 - Security comes only afterwards
- Frequencies
 - 13.56 MHz (HF), 862-956 MHz (UHF)

Source: Floerkemeier/Lampe

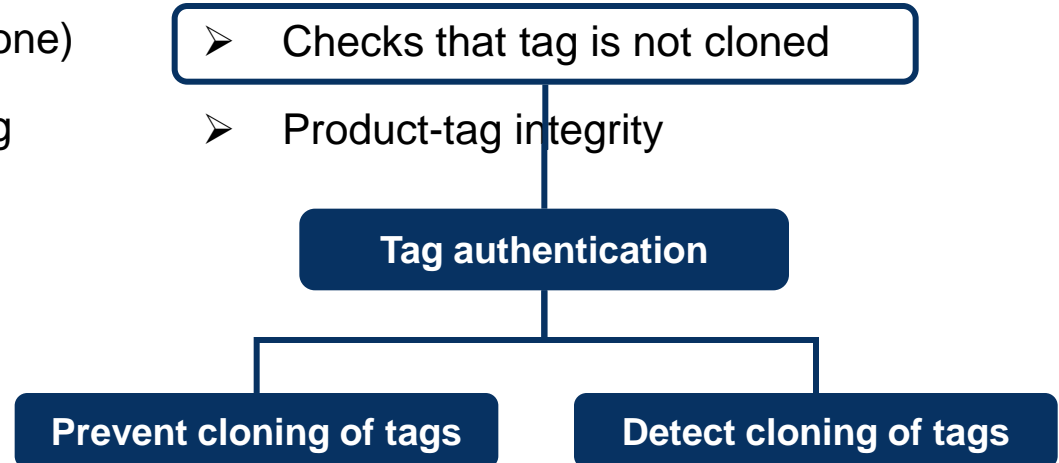


Counterfeit products (threats)

1. Counterfeit without a tag
2. Counterfeit with a tag with invalid ID
3. Counterfeit with a valid ID (clone)
4. Counterfeit with a genuine tag

Countermeasures

- Check that products have tags
- Check that tags have valid IDs
- Checks that tag is not cloned
- Product-tag integrity



Static Passwords

- *Clumsy method, only moderate security*

Unique Transponder ID (TID) Numbers

- Can be cracked with a 10€ tag impersonation device
- Programmable chips would undermine all protection
- *Little clumsy, not secure for large-scale use*

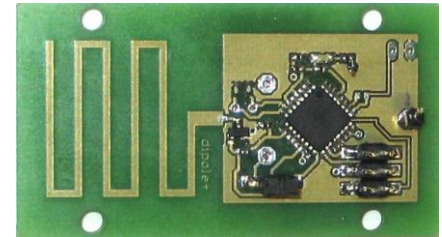
Chip Fingerprints



- Measure a unique “fingerprint” of the chip
- Possibly low-cost, high-secure
- *Promising, recently commercialized*

Strong Cryptography

- Exists in HF, has been demonstrated for UHF
- Long read time (up to seconds)
- *Technically possible, costs are decreasing*



10€ tag impersonation device (Confidex Oy)

Blacklisting

- List of copied ID numbers
- *Basic method, requires upkeeping*

EPC
18264.697441.1
18264.697441.2
18264.697441.3
18264.697441.4

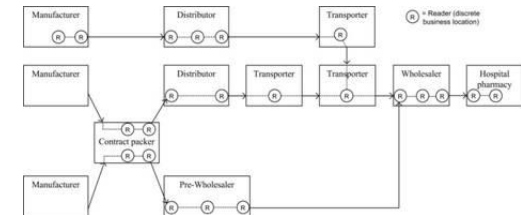
Event Counting

- *“Only first N events are generated by the genuine product”*
- *Basic method for static close-loop systems*

Track and Trace Checks



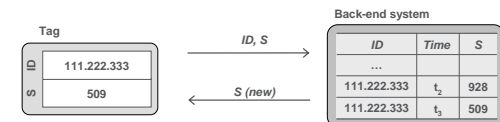
- Data mining to detect events generated by cloned tags
- Dynamic open-loop systems
- *Comes for free with visibility, can generate false alarms*



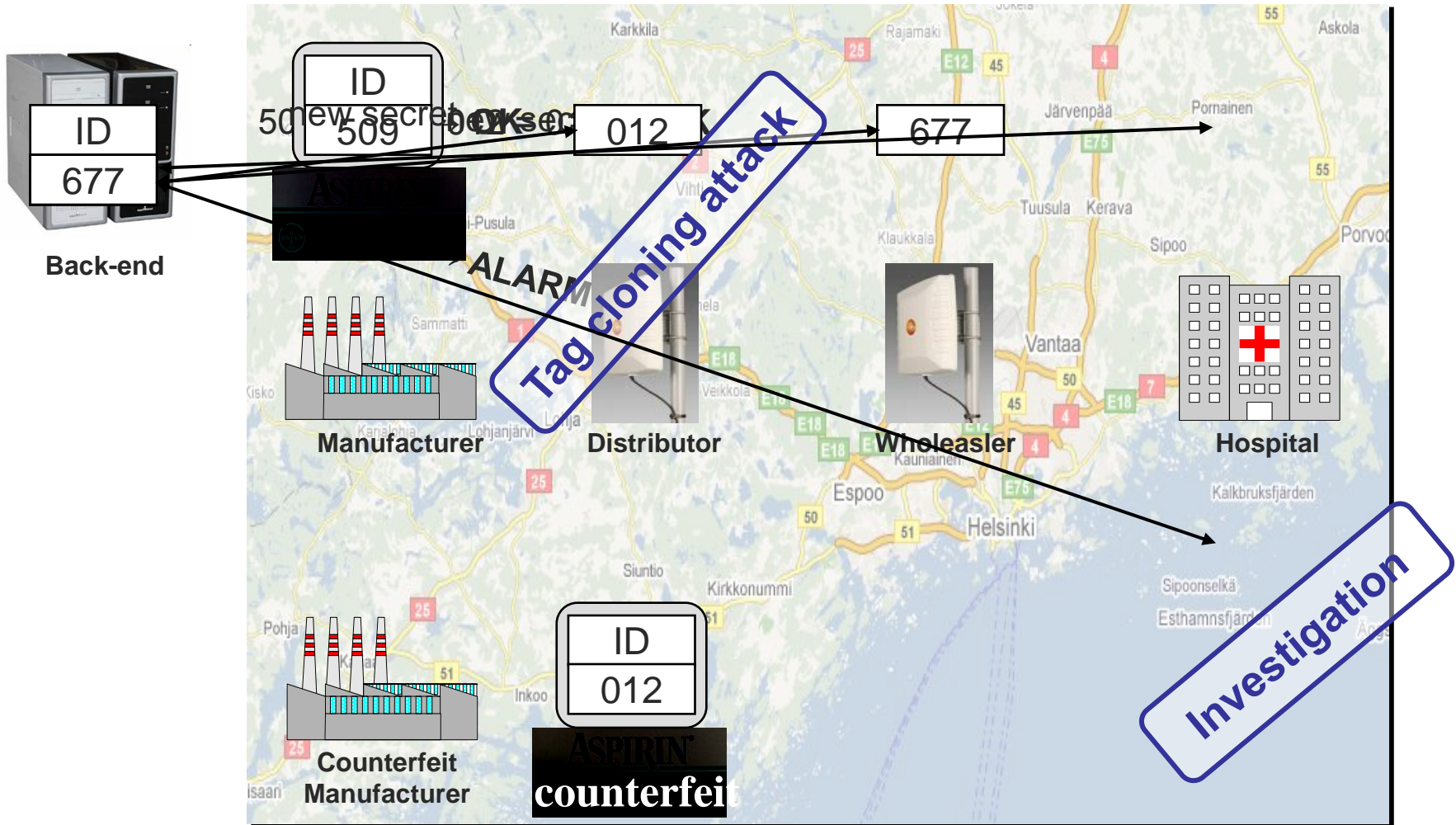
Synchronized Secrets



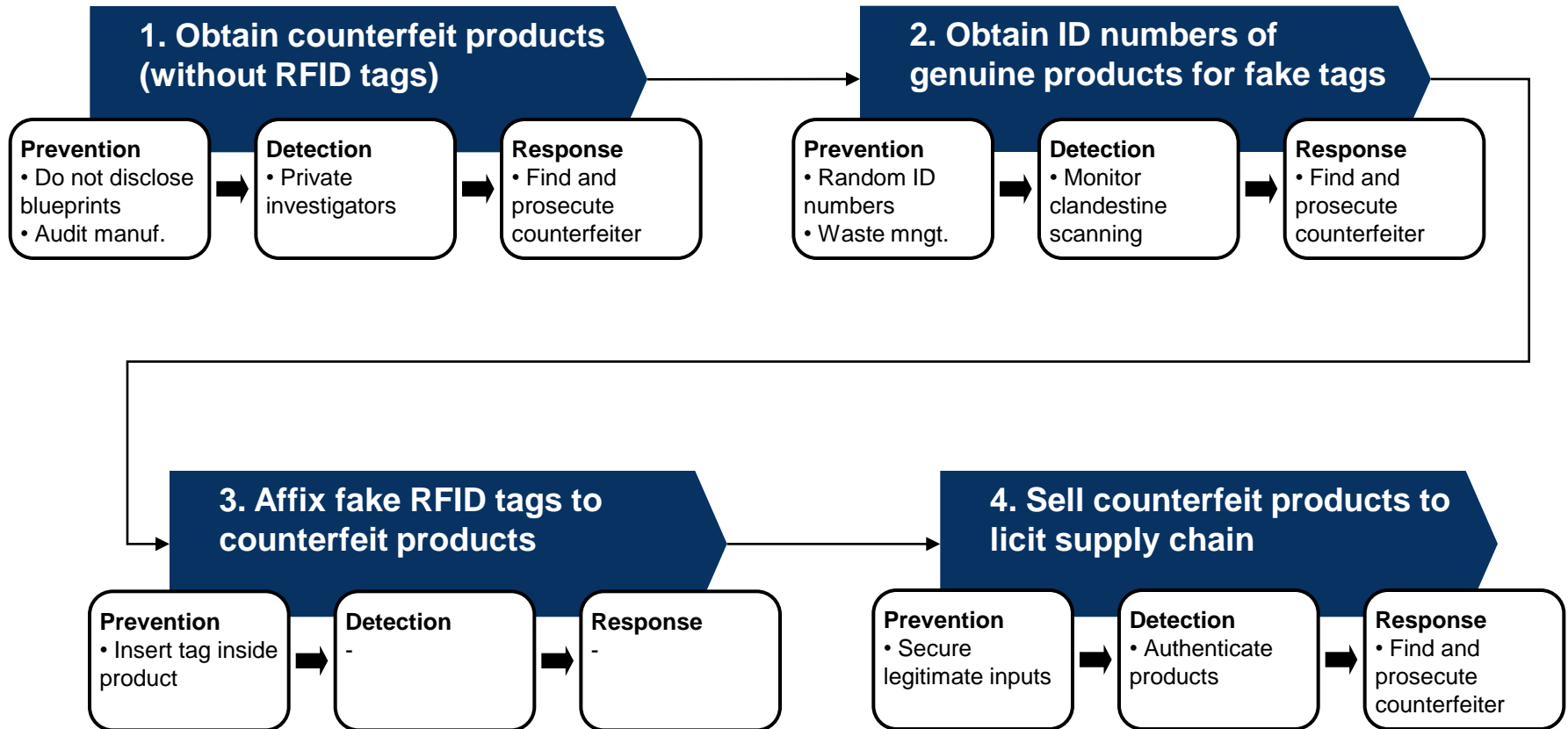
- Novel method to detect tag cloning attacks
- Requires only some rewritable memory (not for barcodes!)
- *No false alarms, but manual inspection needed*



Example: Synchronized secrets



Process of Securing a Supply Chain



- Security is the overall benefit
 - Technology is one component in the overall process of securing a supply chain
- RFID provides a platform
 - Much richer platform than 2D barcodes
- Metrics matter – goal is to detect all counterfeits
 - High check rate and tracking

