Security and RFID – Strenghtening European Expertise

Prof. Reinhard Posch
IAIK TU-GRAZ
AUSTRIA

15th November 2007

IAIK TU Graz

THE STATE OF THE PLAY

- **Main Applications**
  - **security, supply chain, assset tracking**
- **Huge increase expected**
  - **in numbers much more than in $**
- **Shift to higher frequencies**
  - **UHF to be the possible winner**
- **Revenue shift to software**
- **Privacy to be recognized**
  - http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf

IAIK TU Graz

MAJOR CHALLENGES

- **Security to the chip**
  - **the assumption that cloning is too expensive is not sustainable**
- **Protection profiles and evaluation**
  - **to ensure security in practice**
- **Europe to remain the top player**

EXISTING WEAKNESSES

The Mobil' Speedpass:

(Exxon/Mobil USA)

- **Payment at petrol stations with RFID Tags:**

System facts:

- **6 million users (tags)**
- **7.500 Exxon & Mobile stations (each 5 terminals?)**

Picture from www.catskills.com

only quality crypto can do !

IAIK TU Graz

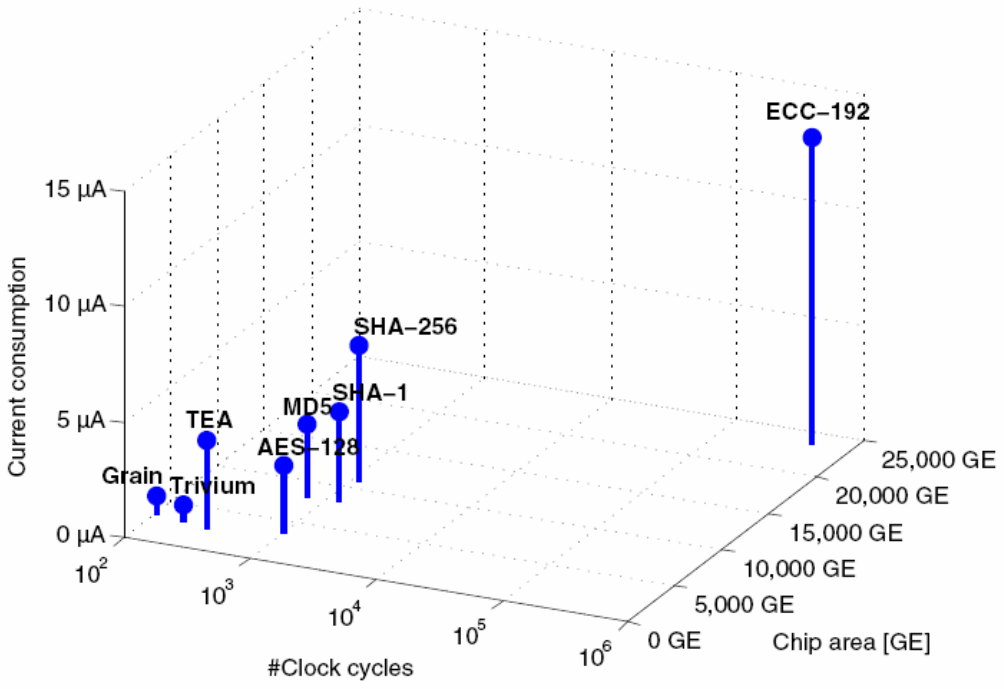
STRENGTH IN CRYPTO

- **Broken in 2005 by students from Johns Hopkins University**
- **Tags use proprietary algorithms with too short key length (40-bit) – "DST40 algorithm"**
- **Algorithm was re-engineered and hardware for key-search was implemented (costs for equipment approx. US$ 3.500.-)**

- **More info: www.rfid-analysis.org**

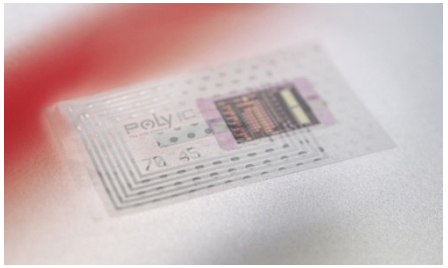
CRYPTO - AVENUES TO GO

- Energy for Crypto should be below E2PROM 1/1000 of smart card
- Area not critical
- Throughput in general feasible
- Symmetric primitives feasible with (0,25 or 0,18µm) – asymmetric (ECC) still out of focus but not very far



TECHNOLOGY CHALLENGE

- **Polymer**
  - **soluble, printing ink, low price**
- **Limits**
  - **mobility of free charge carriers much lower than, heavily reduced performance, 13.56 MHz tags prototypes**
- **Target: lowest cost tags**
- **Environmental effects to be explored**



Copyr. by PolyIC – Pic. taken from Heise online

IAIK TU Graz

ENVIRONMENTAL CHALLENGE

- **Production and disposal**
  - **pollution – separation**
- **Radiation**
  - **"Guidelines for Securing Radio Frequency Identification (RFID) Systems" NIST**
  - **result: no documented examples have been identified**
  - **RFID technology typically operates at power levels below those that would cause a concern**

IAIK TU Graz

HEALTH CHALLENGE

- **Thermal**
  - **device itself: compare energy (10µA)**
  - **effects: parasitic heating up of material in the RFID field due to EM radiation (reader)**
  - **Reader field strengths are below international accepted radiation limits**

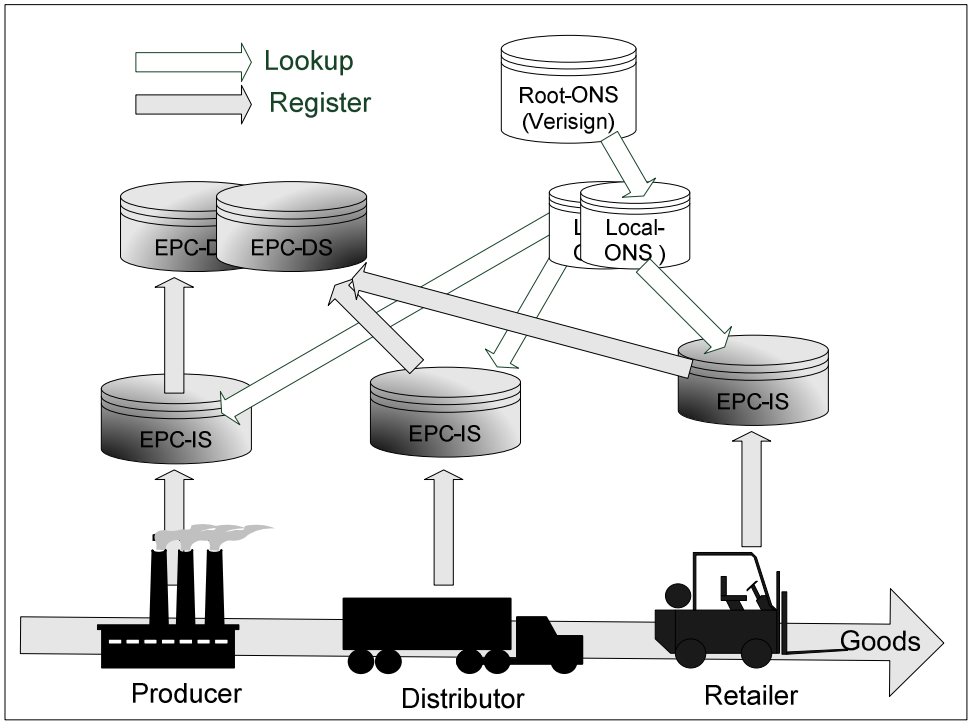
- **No damage was documented**
  - **effects to critical objects (e.g. pharmaceuticals) to be investigated**

EUROPE TO STAY AHEAD?

ONS: Object Name service: Directory for EPC lookup (similar to DNS)

EPC-IS: Information service: Repositories for EPC specific information – tag specific information about the object

EPC-DS: Directory Service: Registration service for EPC-IS



Scalability of system (billions of tags) ? Management of access rights to stored data? Central authority!

IAIK TU Graz

EPC Global

- **EPC Global: "electronic product code", successor of barcode systems (EAN.UCC)**
  item level identification!
- **To provide a standardized solution for "trading networks" e.g. supply chain solution**
- **The standardization is heavily driven by the retailer industry (Walmart, Metro, etc.)**
- **The assumption suggests to use "low cost" tags and perform all decisions on basis of information in the network!**

Quality CRYPTO could be the alternative to avoid dependence upon a single stakeholder – CHALLENGE FOR EUROPE

IAIK TU Graz

Recommendations

- Privacy discussion to contribute
- At the end the risks to be assessed at application level
- Technology needs to provide measures to deal with privacy. Application of cryptographic measures is a feasible measure
- Cryptographic measures also with low cost RFID
- Research towards "signature generating RFID tags"
- Research on standardized crypto on low cost tags
- Industry independent (to avoid conflict of interests) research on EPC-Global application and alternatives
- FOCUS AND DISSEMINIATE COMPETENCE

IAIK TU Graz

WHAT CAN EUROPE DO

- **Sustain and strengthen European competence**
  - **70% HF devices developed in Europe (area Graz)**
- **Ensuring longterm EU-effects**
  - **Despite of immediate industry interest**
- **Network/center of excellence**
  - **As a focuspoint for knowledge**
  - **Fostering security and cryptography**
  - **Envisaging European interests**

IAIK TU Graz

thank you for your attention

reinhard.posch@cio.gv.at