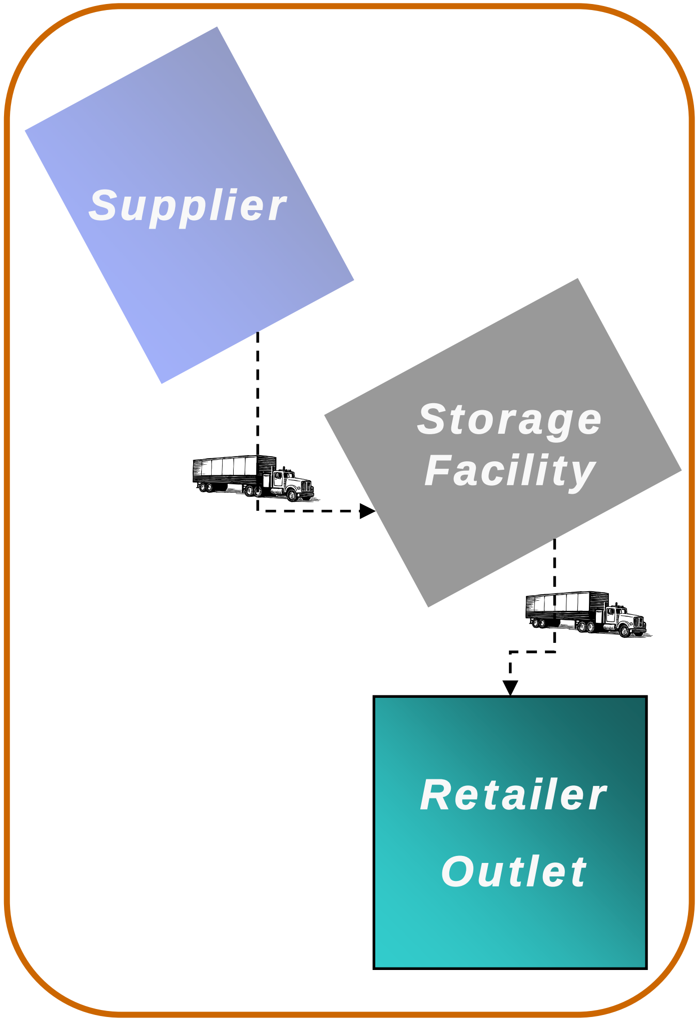
RFID Usage in Retail beyond the Point of Sale

Temporary Deactivation as a Solution for Challenges in Privacy and Security

Claus Wonnemann **Dr. Jens Strüker**
{wonnemann | strueker}@iig.uni-freiburg.de

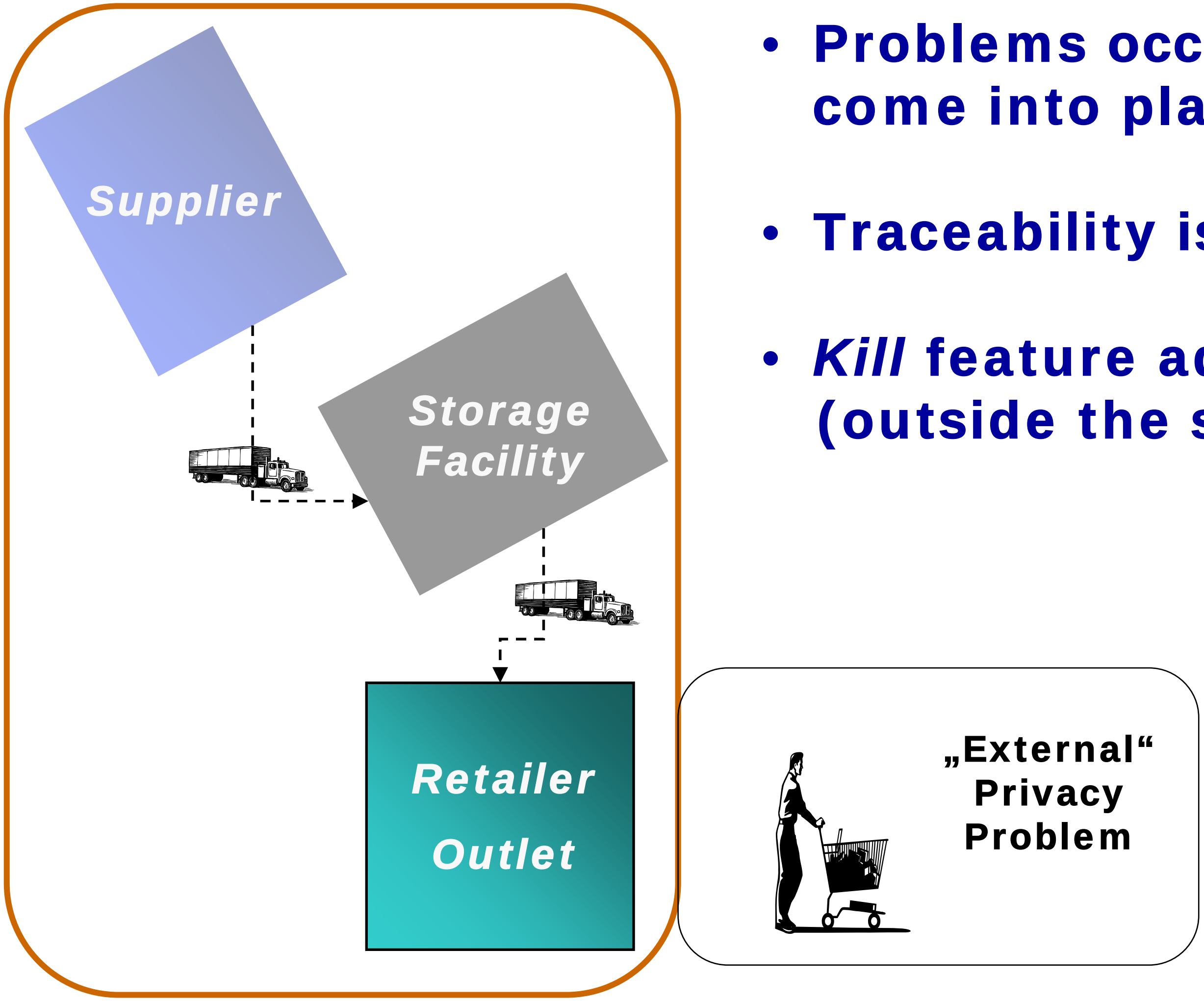
Institut für Informatik und Gesellschaft
Abteilung Telematik
Albert-Ludwigs-Universität Freiburg

RFID in Retail



- **Automatization in the supply chain is the major goal**
- **Tagging of pallets & boxes**
- **Common standard: *EPC C1G2***

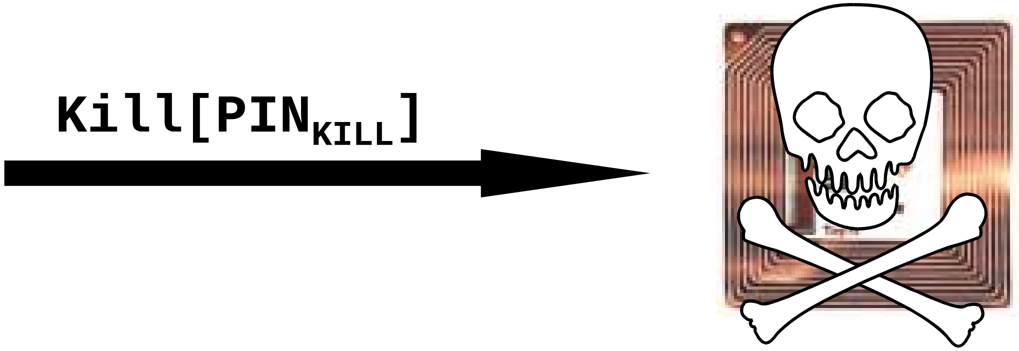
RFID in Retail – Privacy Challenges



- Problems occur when customers come into play
- Traceability is the major threat
- *Kill* feature addresses problem (outside the shop)

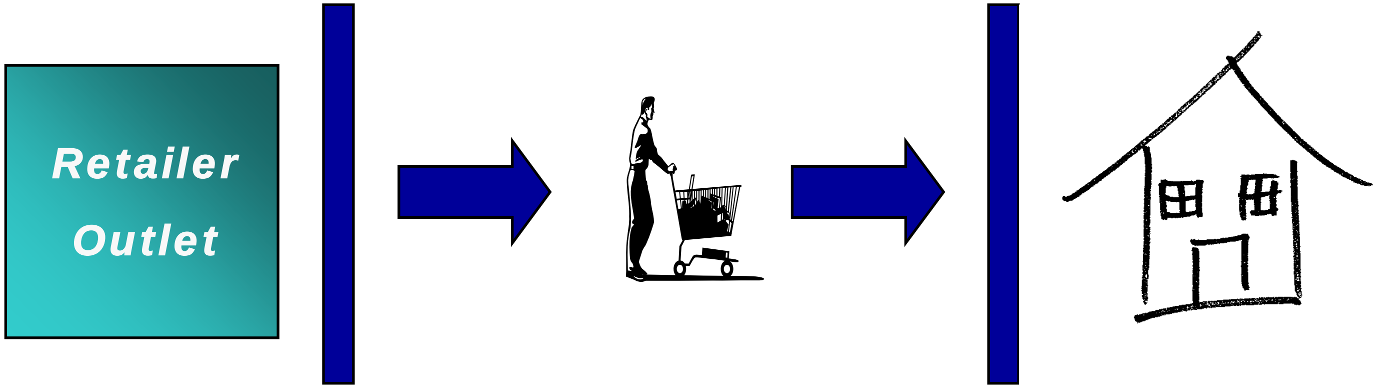
The Kill Feature

- Only mandatory privacy feature in EPC C1G2
- Causes tags to self-destruct
- Solves privacy problem (in a quite radical way, though)
- But: Prohibits use of extended RFID-based services



A Re-Activation Approach

- Tags are deactivated at the checkout
- Non-Traceability on the way home
- Re-Activation in a „secure surrounding“



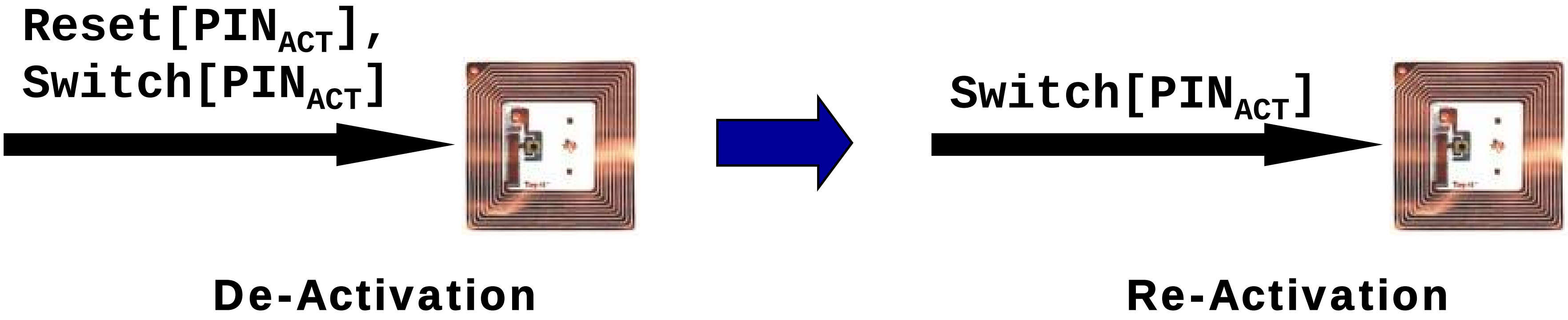
Retailer Outlet

De-Activation

Re-Activation

A Re-Activation Approach (2)

- Activation switch protected by PIN_{ACT}
- Value of PIN_{ACT} is set to customer-chosen value
- Re-Activation through subsequent call $\text{Switch}[\text{PIN}_{\text{ACT}}]$



$\text{Reset}[\text{PIN}_{\text{ACT}}]$,
$\text{Switch}[\text{PIN}_{\text{ACT}}]$

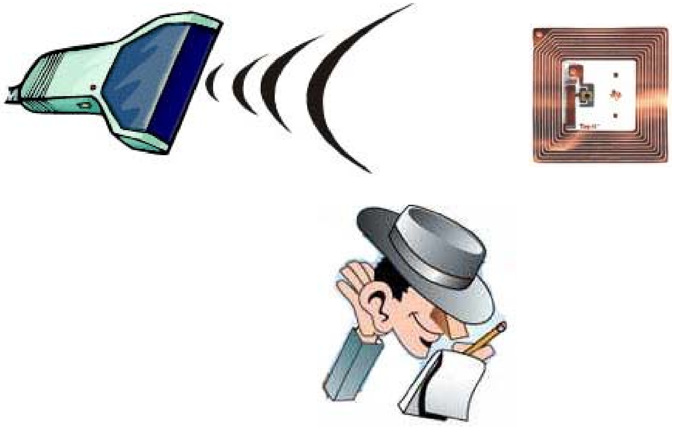
$\text{Switch}[\text{PIN}_{\text{ACT}}]$

De-Activation

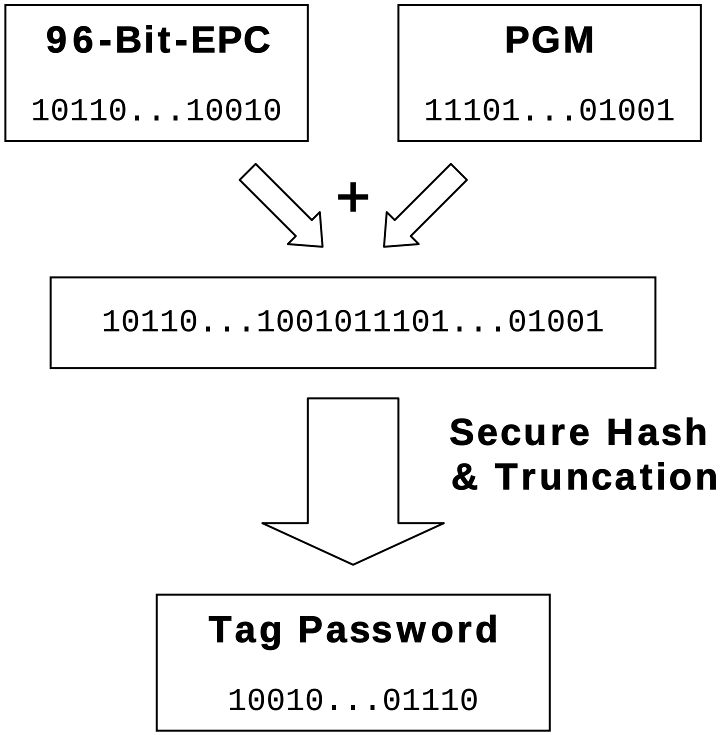
Re-Activation

Individual Passwords per Tag

- Passwords are not secure (Eavesdropping, Side Channel Attacks, ...)
- Potential damage in case of broken password has to be minimized
- PIN_{ACT} must be different for each tag!



Password Generation



96-Bit-EPC

10110...10010

PGM

11101...01001

+

10110...1001011101...01001

Secure Hash
& Truncation

Tag Password

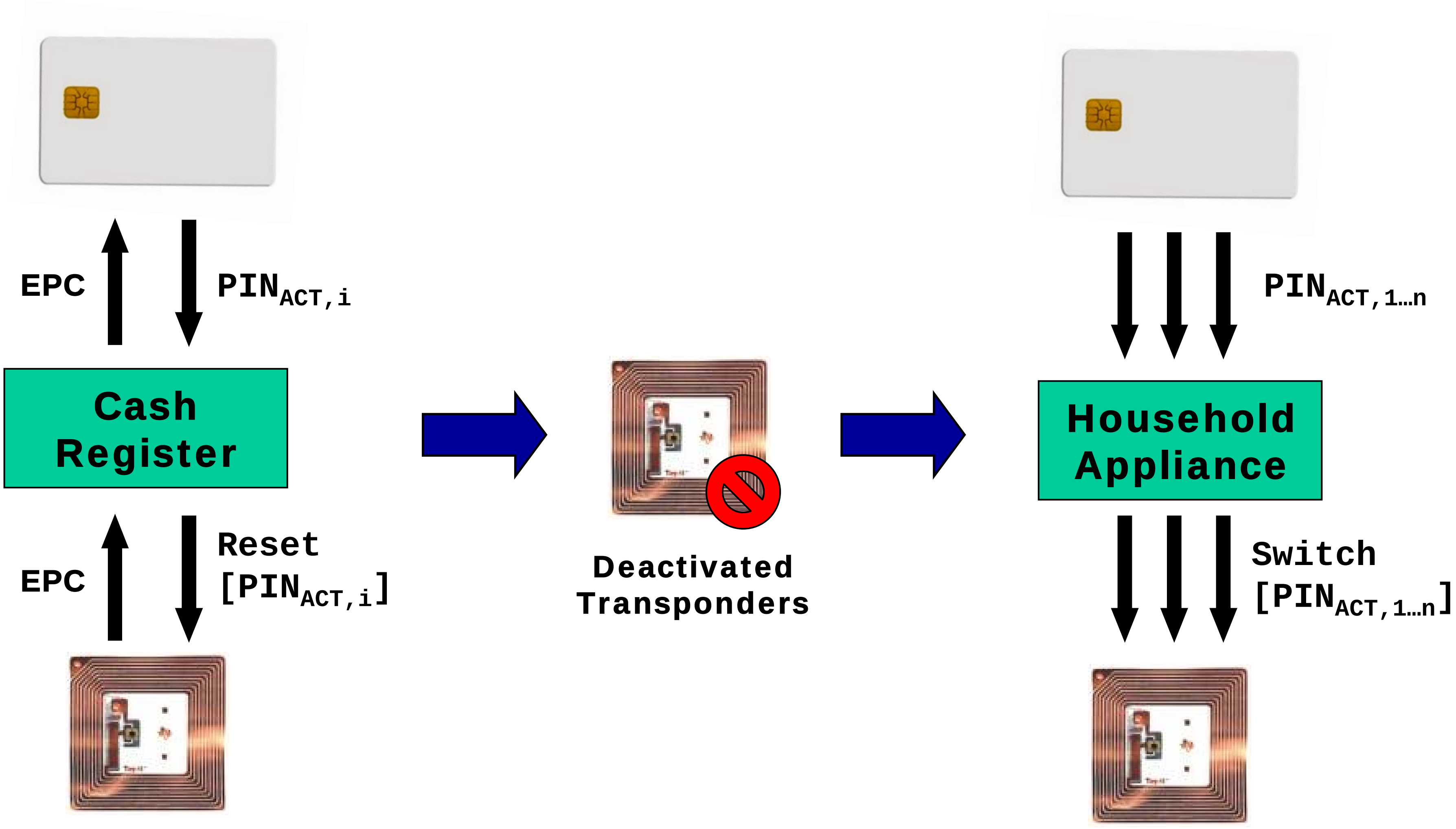
10010...01110

- Generation of tag passwords from a single secret (PGM)
- Secure hash on concatenated string EPC + PGM
- Smart Card (e.g. loyalty card) as a generation device

Re-Activation

- Smart Card stores EPCs of purchased goods
- Re-Activation by transmitting passwords
- Password management either trough central device or de-centralized

Scenario



EPC

$\mathrm{PIN}_{\mathrm{ACT},i}$

Cash Register

EPC

Reset $[\mathrm{PIN}_{\mathrm{ACT},i}]$

Deactivated Transponders

$\mathrm{PIN}_{\mathrm{ACT},1\ldots n}$

Household Appliance

Switch $[\mathrm{PIN}_{\mathrm{ACT},1\ldots n}]$

Wrap-up

- Tags must not be killed to enable extended services
- Re-Activation makes tags temporarily untraceable
- Individual Passwords balance the trade-off between password security and cost
- Password Generation from a single secret makes management feasible

Thank you!