

## Security and privacy challenges in IoT applications



**gemalto**  
security to be free

Jean-Pierre Tual

Celtic proposer's day, Issy Les Moulineraux, June 29th, 2015

# Agenda

Trends and Problem statement

Introduction to Security  
Technologies

Risks/threats on IoT will derive from  
those facing the Mobile world

Examples from the automotive  
Industry

Examples from the Energy Industry

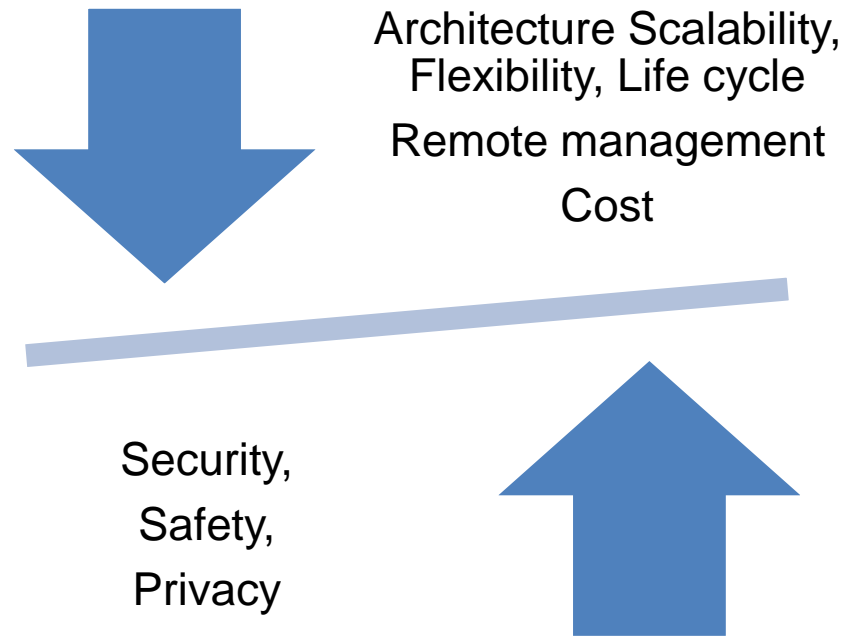
# The trends :

... large scale deployment of **Embedded Systems**

- 
- ✦ High Bandwidth Wireless Connected World
  - ✦ Smart objects: phones, tablets, wearables
  - ✦ Internet of Things / M2M explosion
  - ✦ Cloud Computing & **DIGITAL** Everything as a Service
  - ✦ Data explosion & Big data
  - ✦ HW/SW Virtualization **REVOLUTION**
  - ✦ Networks convergence (IP, WAN, LAN ...)
  - ✦ Open Source SW
  - ✦ Security and Privacy management

# Embedded Systems & IoT major issue...

... find the right trade off between :



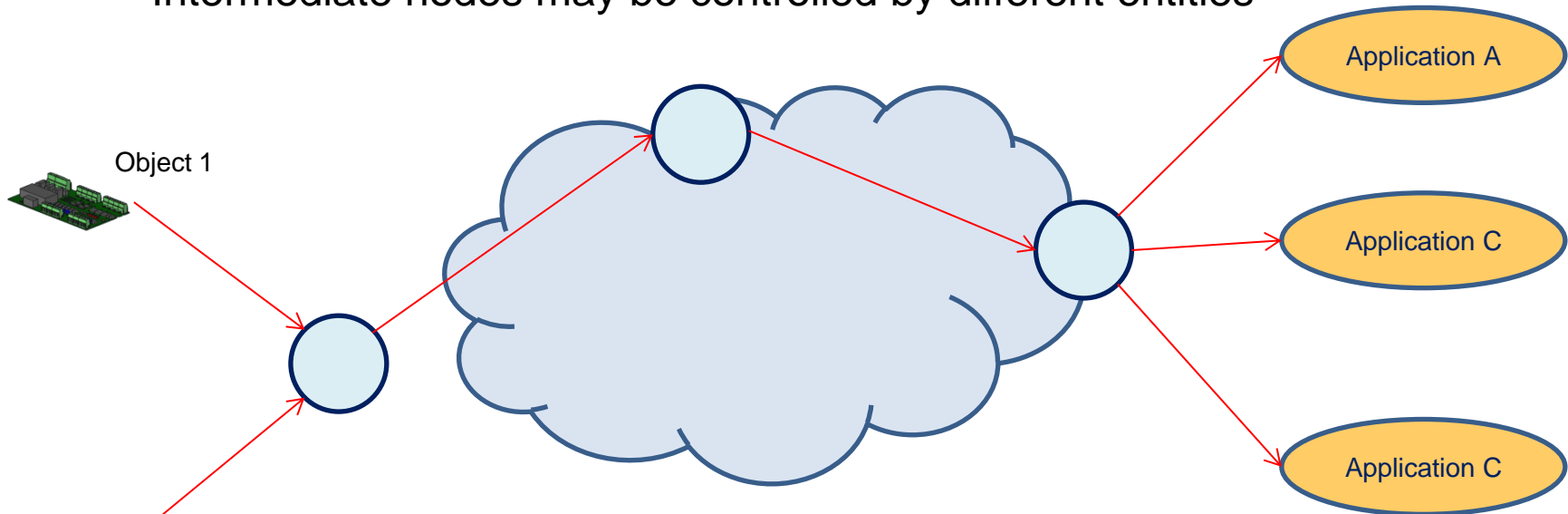
... that matches **end user** and **market** requests & expectations

(service providers, manufacturers, distributors and regulators)

# IOT applications: heterogeneity is the Rule

IOT applications often involve several communication hops, capillary networks

Intermediate nodes may be controlled by different entities

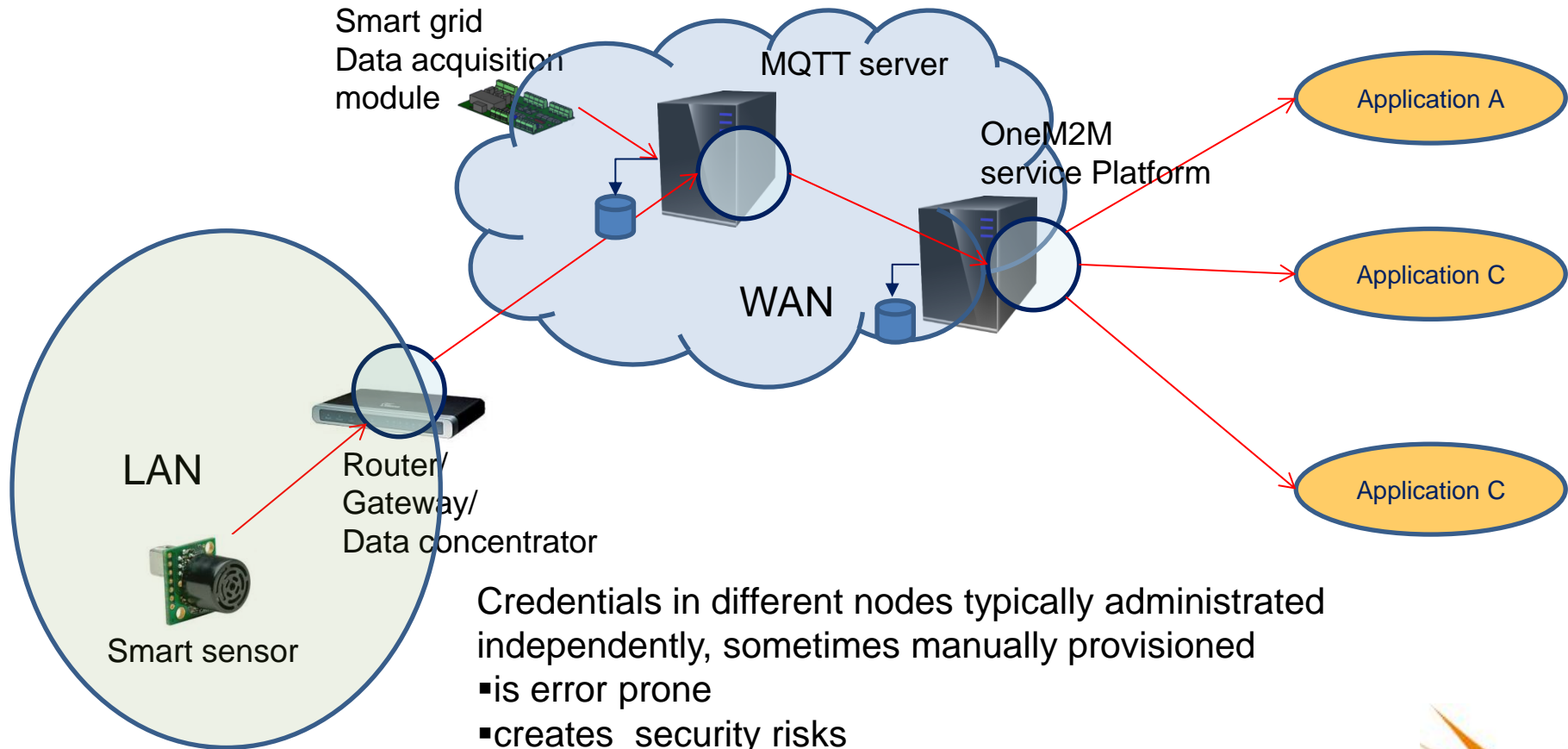


## Challenges:

- Authenticate entities and secure every single hop of the communication path
- Possibly secure communication from source to destination with a single set of credentials
- Manage authorizations (fine grain) in every node

# Real case example

IOT applications often involve several communication hops  
Not all controlled by the same entity



Credentials in different nodes typically administrated independently, sometimes manually provisioned

- is error prone
- creates security risks

=> Need to find a way to link credentials and authorizations in the different nodes





# SECURITY the Bottleneck for large scale deployment

✧ In the past for :

Financial Institution → Banking Card

Mobile Communication → SIM / UICC

Governmental solution → National Id Card

→ By a Removable Security Token

✧ For M2M / IoT solutions :

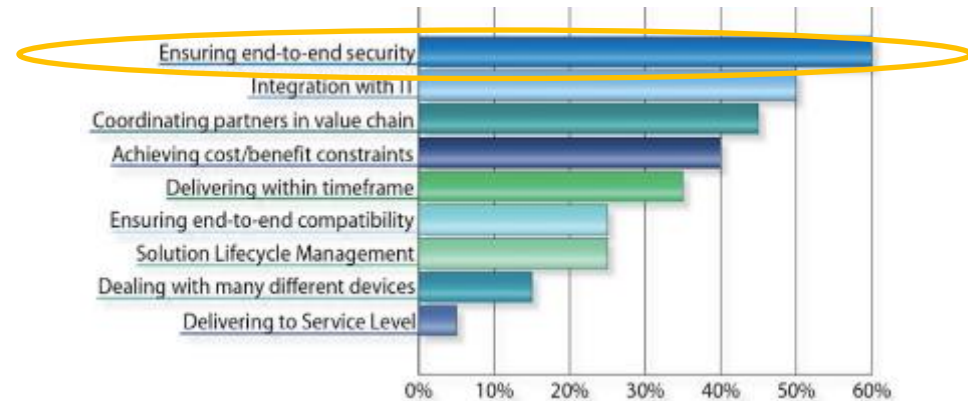
Mobile Industry

Automotive Industry

Energy industry

...

New challenges → Looking for alternative solutions



Survey from Beecham Research November 2013

# Les Echos

ÉNERGIE

Le ministre de l'Énergie, Eric Besson, souhaitait annoncer sa généralisation des compteurs Linky avant la fin de l'été. Il a décidé d'attendre les élections sénatoriales, qui ont lieu ce week-end. Avec la présidentielle, la fenêtre de tir se resserre.

## Le gouvernement hésite à déployer le compteur Linky

La généralisation des compteurs Linky peut être décidée dès maintenant. La conclusion du rapport rédigé par Jean-Claude Lenoit, député de l'Orne, et Ladislas Poniatowski, sénateur de l'Eure, dans le cadre du comité de suivi de l'expérimentation sur les compteurs électriques communicants, le mérite d'être claire. Pourtant, le gouvernement hésite sur la méthode de déploiement du fameux compteur intelligent. L'approche de l'élection présidentielle, la fenêtre de tir se resserre. Au départ, le ministre de l'Énergie, Eric Besson, souhaitait annoncer la généralisation avant la fin de l'été. Il a ensuite décidé d'attendre les élections sénatoriales du 25 septembre. « Il vient de recevoir le rapport Lenoit-Poniatowski et veut maintenant réfléchir aux décisions à prendre », selon une source proche du ministre. Après le mois d'octobre, le gouvernement sera soumis à un devoir de réserve sur les grands enjeux. Estimé à plus de 4 milliards d'euros, le projet Linky en fait partie. Tour d'horizon des questions en suspens.

La fabrication et l'installation du compteur Linky ne seront pas facturées au consommateur d'électricité. Pour Eric Besson, c'est clair, le compteur intelligent ne sera pas couvert par les tarifs d'électricité. Le devoir d'achat obligatoire d'ERDF est le meilleur moyen de garantir la rentabilité de l'investissement et de bénéficier de l'économie induite par le projet. Les recettes induites par le projet, telles que la disparition des fraudes ou d'une meilleure gestion de son réseau. Mais si on doit évaluer les 4 milliards, il faut qu'on sécurise les recettes liées à Linky, souligne un proche de l'entreprise.

Le projet Linky vise à équiper 35 millions de foyers en compteurs intelligents à l'horizon de 2020.

Impose l'ouverture à la concurrence, y compris dans l'énergie », souligne Jean-Luc Dupont, président du syndicat intercommunal d'énergie d'Indre-et-Loire, où a eu lieu une expérimentation. D'autres pays, comme la Grande-Bretagne ou l'Italie, ont inscrit dans la loi les durées de concessions.

Les services liés au compteur Selon la Commission de régulation de l'énergie, « une généralisation du compteur communicant Linky bénéficierait aux consommateurs ». Le régulateur évoque notamment la stabilité des réseaux d'électricité ou la relève à distance. Un point de continuité de service : la maîtrise de la demande d'énergie (MDE) et le mode d'affichage de la consommation. L'Agence de l'environnement

### UN PROJET PHARE

Le distributeur ERDF a lancé en 2007 le projet Linky. Objectif : équiper 35 millions de foyers en compteurs communicants à l'horizon 2020, pour un coût de 4 milliards d'euros. En février 2010, la Commission de régulation de l'énergie a autorisé l'expérimentation en Île-de-France, en Loire et à Lyon avec l'installation de 300.000 compteurs. Le 2 septembre 2010, le ministre de l'Énergie, Jean-Louis Borloo, signe un décret annonçant un déploiement dès le 1<sup>er</sup> janvier 2012. Le 15 septembre, il prolonge l'expérimentation jusqu'à mars 2011.

### La confidentialité et la sécurité

« A partir d'une courbe de charge extrêmement précise, nous pouvons connaître la vie privée d'un consommateur », prévient Christophe Alexandrie, directeur des Affaires juridiques à la Commission nationale de l'informatique et des libertés (CNIL). Pour lui, les consommateurs doivent en être conscients. Dans un rapport présenté le 7 juillet, la commission s'interroge par ailleurs sur la sécurité de l'infrastructure Linky et sa résistance aux prises de contrôle externes, via une cyberattaque. Toutes les garanties nécessaires aux interventions de sécurité et de confidentialité des données », reconnaît le comité de suivi.

Alors que Linky pourrait assurer 10.000 emplois par an pendant sept ans, selon ERDF, ce dernier veut aller vite. Le gouvernement pourrait publier un arrêté prochainement, quitte à préciser certaines modalités plus tard. « On peut lancer le projet avec ses limitations parce que des spécificités », défend-on à Bercy. Reste à savoir si un arrêté « light » suffirait à ERDF pour lancer son appel d'offres.

10.000 / AN

Le nombre d'emplois que le projet Linky pourrait assurer pendant sept ans, selon ERDF.

THIBAUT MARÉLAIN

Regulations

Privacy

Safety  
Cyber attack

Security  
Fraud

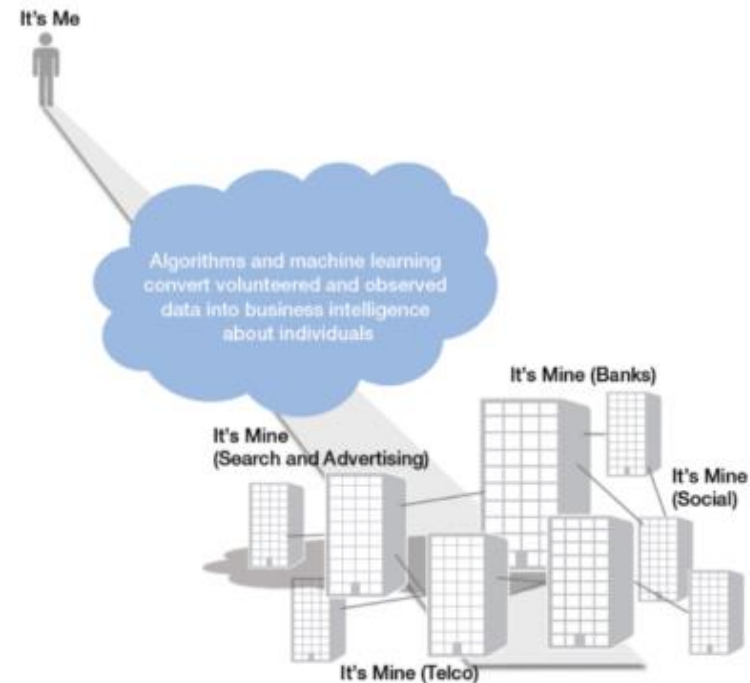


# Everything that can be hacked *will* be hacked



# Is privacy a problem ?

- ✧ We are talking about what is concerning you data, ongoing inside your house !
- ✧ Who wants to monitor your load profiles
  - police ? robbers ? tax administration ? tabloids ? immigration service ? and **most probably advertising people !**
- ✧ There are some existing regulations
  - Need to know principle should apply
  - Explicit consent should apply
  - Privacy enabling technologies can help
- ✧ More generally privacy applies to all stakeholders



Source: BCG

# Agenda

Trends and problem statement

Introduction to Security  
Technologies

Risks/threats on IoT will derive from  
those facing the Mobile world

Examples from the automotive  
Industry

Examples from the Energy Industry

# Basic security technology building block in embedded or IoT security:

- ✧ Smart cards / security elements (SE)
- ✧ Trusted Execution Environment
- ✧ OTA servers
- ✧ Trusted service manager
- ✧ Device remote personalization



# Removable versus Non Removable SE

## ✧ Removable Secure Element

- As soon as the SE is used with **multiple** “readers” then the SE is still standalone.
- Banking Cards,
- GP cards (ID, Licences, CPS, Passports)

## ✧ Non removable Secure Element

- As soon as the SE is used into a **single** device then :
  - Step 1: The SE is soldered in becoming an embedded SE.
  - Step 2: The SE is embedded in a TEE or a SOC (System On Chip)
- Full remote personalization is required



# Removable SE Constraints on SW components

## ✧ The software provisioning rules :

- Secure production process from chip manufacturer to device issuer (bank, operator)
- Scalability of deployment schemes
- Late personalization even after customer issuance limited to application
- Full Remote personalization is not possible
- Long life cycle management

## ✧ Mobile adaptation and evolution to address these constraints:

- OTA, TEE, TSM, eSE



## Classical security model (Server, PC,..)



- ✘ Protected environment
- ✘ Trusted users
- ✘ Direct access to data

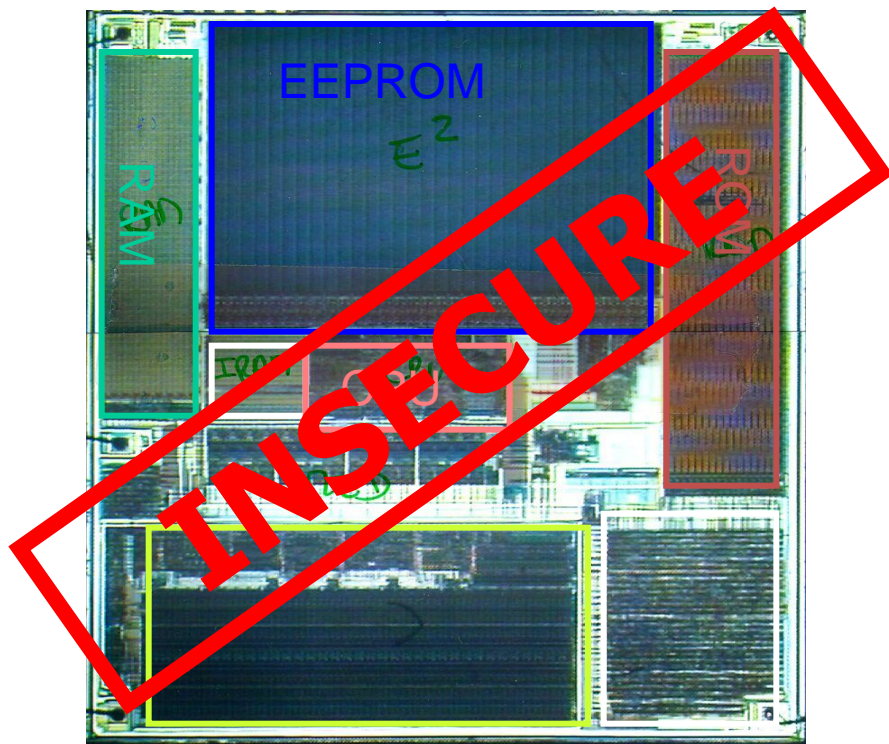
## Embedded security model (M2M, IoT,....)



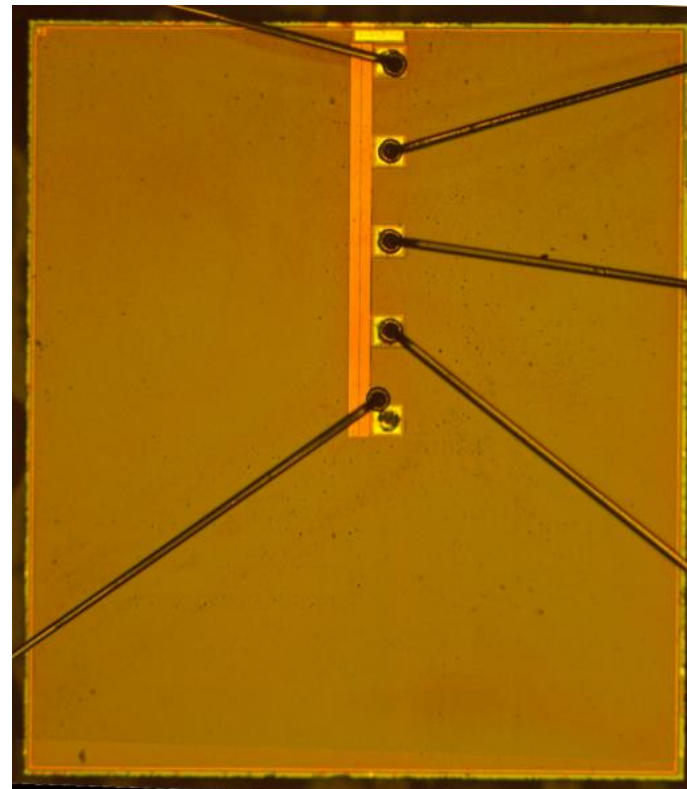
- ✘ Unprotected environment
- ✘ Non trusted users
- ✘ No direct access to data
- ✘ **Tamper resistant devices**

# What does it means for SE ?

# Tamper resistance at chip level



- ✘ Blocks can be easily identified
- ✘ No shield
- ✘ No glue logic
- ✘ Buses clearly visible

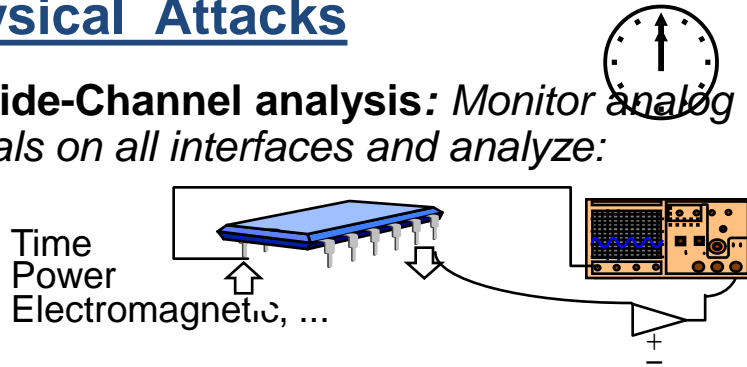


- ✘ Shield
- ✘ Glue logic
- ✘ No Buses visible
- ✘ Memories and buses encryption
- ✘ Sensors

# Secure Elements: expected resistance to Physical and Logical attacks

## Physical Attacks

- ★ **Side-Channel analysis:** Monitor analog signals on all interfaces and analyze:



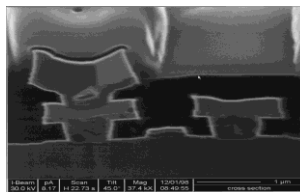
- ★ **Fault injection:** use of Laser, Glitchers, Flash light...

to bypass protections and infer secrets.



- ★ **Invasive manipulation:**

Chip observation  
Deposit probe pads on bus lines  
Reverse ROM mapping  
Disconnect RNG  
Cut tracks



## Logical Attacks

- ★ **Aggressive software:** Buffer overflow, Aggressive applets, Trojan Horses, Viruses, Cryptography,...



- ★ **Environment:** Servers, PCs, readers and handsets configurations:



- ★ **Protocols and stack implementations:**



# Impact on SW components

- ✧ The software provisioning must to the following rules
  - Late personalization even after customer issuance
  - Full Remote update because the components are soldered/embedded and cannot be changed
  - Scalability of deployment schemes
  - Possibly two level of SW bootstrap (one bundled, for OS downloading, one bundled with OS for patches, upgrades)
  - Embedded local security, often with low footprint
  - Long life cycle management (bugs and security patches)
  - Flexibility according to the country and the field actors (late customization after issuance to the final customer)
- ✧ Emerging concepts from the Mobile world can be customized on purpose
  - TEE
  - OTA
  - TSM



# Enforcing Security: Trusted Execution Environment (TEE)

Open to

malware

any user modification  
(e.g. "Jailbreaking"/  
"Rooting")



Main OS Environment

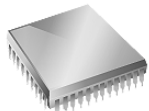


APPLICATIONS

TEE Client API



Operating System



Gateway Processor

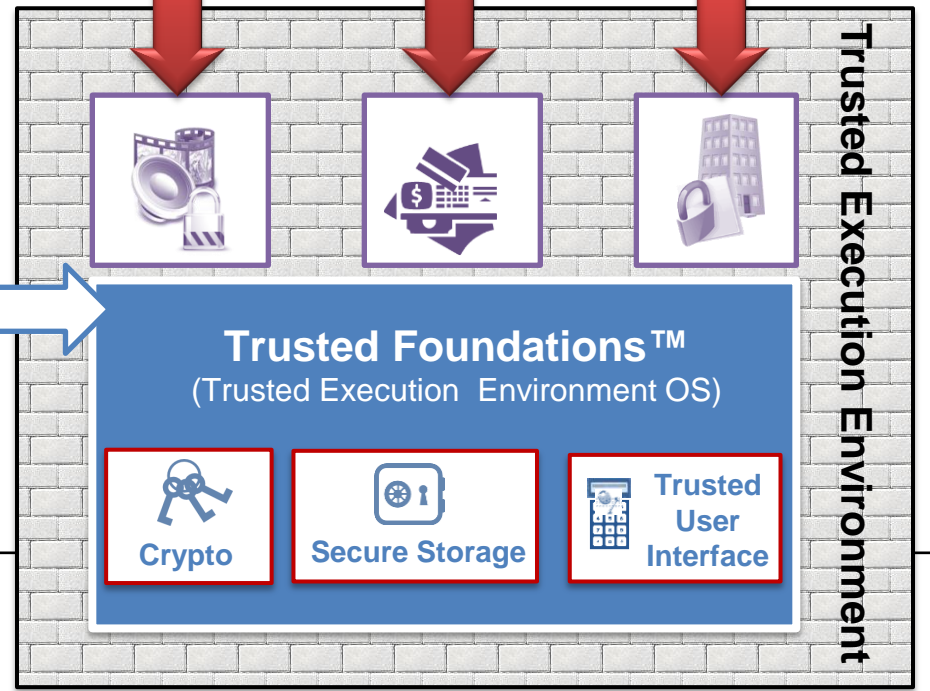
Protection of

- Payment engine
- Bank authentication

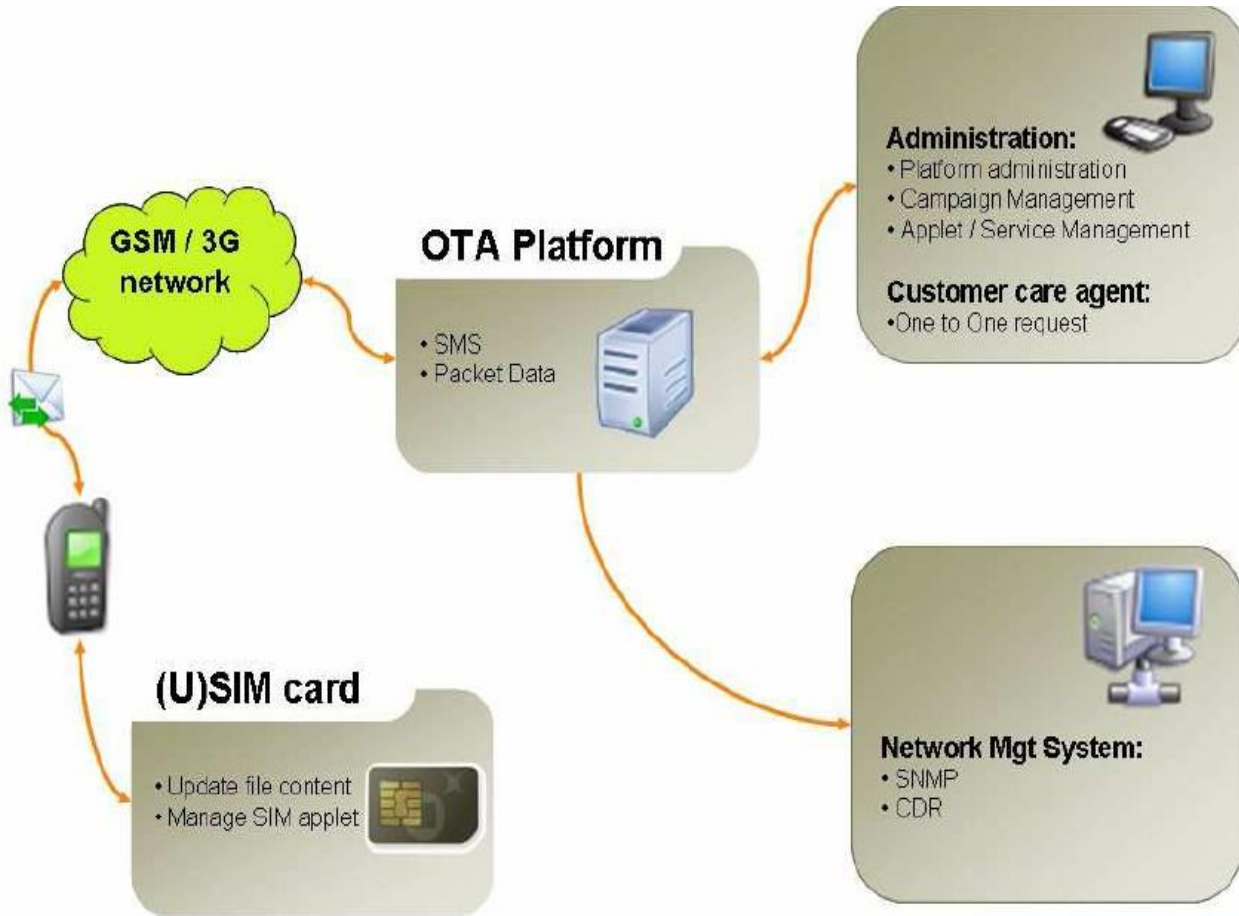


Premium content  
Management & Protection

- Device integrity and management
- Corporate service
- Sensitive user data

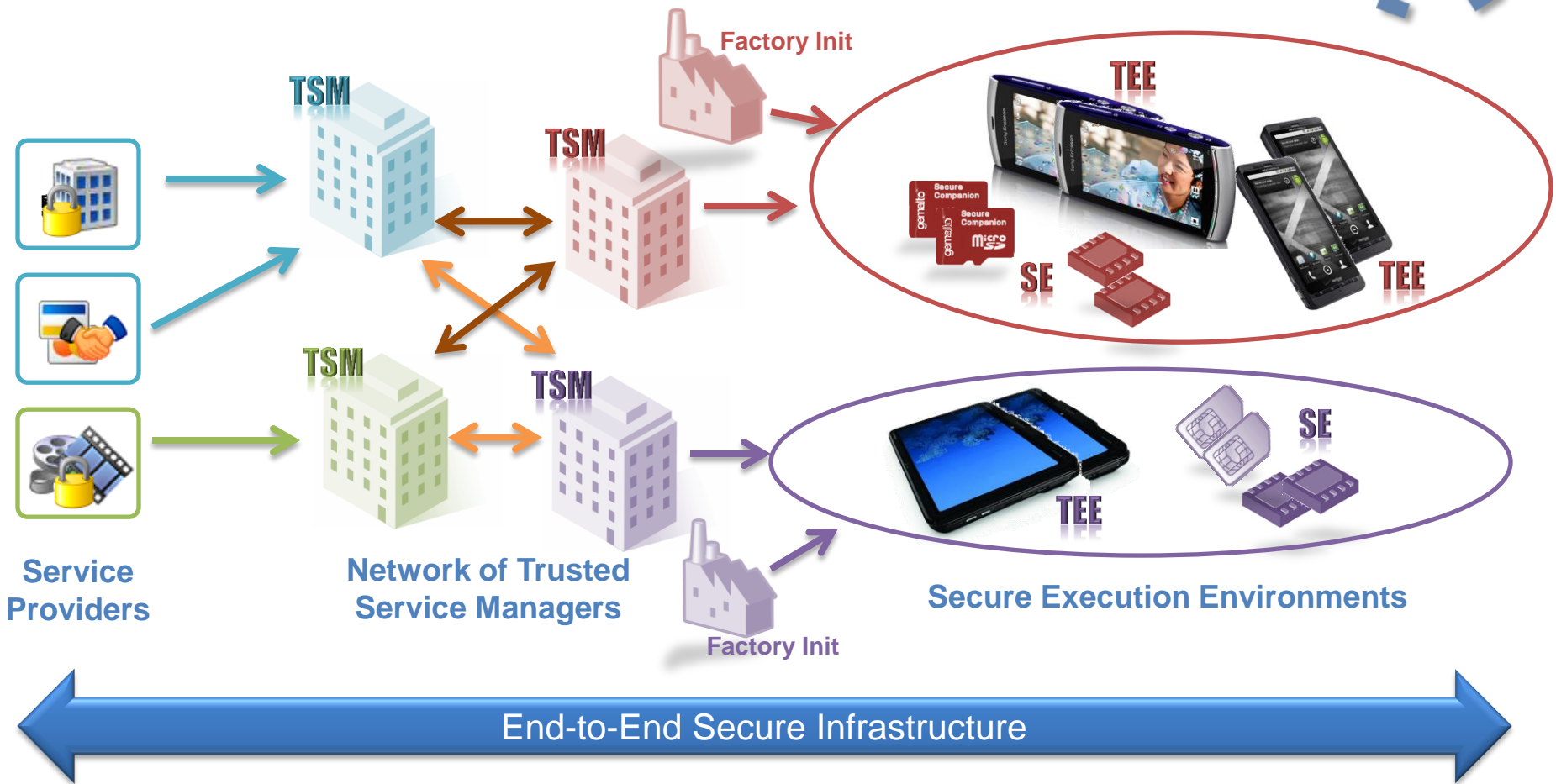


# Remote management of devices by millions



Create Screen Clipping (Windows+F5)

# TEE and SE remote Administration



- Same remote administration architecture for TEE and Secure Elements
- Complementary of TEE and SE

# Agenda

Trends and problem statement

Security technologies

Risks/threats on IoT will derive from those facing the Mobile world

Examples from the automotive Industry

Examples from the Energy Industry

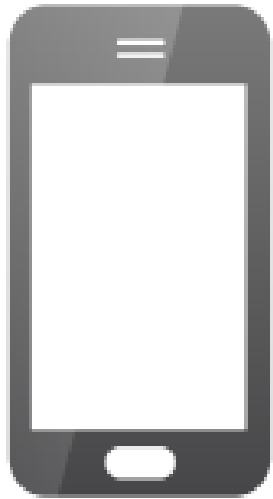
# The threats



Supply chain



Enrolment



Device



User



Networks



# Threats in product life cycle

## ✧ The supply chain.

- Weak root keys generation
- Insider knowledge (keys, debug protocols,...)
- HW and SW Trojan
- Bugs (e.g. in OEM code)



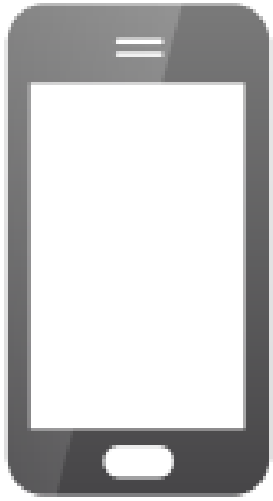
## ✧ Enrolment and provisioning.

- Weak user authentication
- Weak device authentication
- Alternative app stores
- Fake apps
- Trojans



## ✧ Usage...





Device

**HW**

Peripherals: Biometric sensors, USB, Camera...  
Local storage: dump of Flash memory  
JTAG  
Physical attacks (Side-channel, Fault injections...)

**Boot**

Bypass Secure boot sequence

**Baseband**



**OS**

Kernel:  
Libs/APIs, Drivers, System Apps.  
Privilege escalation, KeyLogging, MiTM

**App**

Local Storage  
Run Time injection  
DoS  
Fake App

**Browser**

Local Storage (Keys, Cookies)  
Framing  
Click Jacking



Fake Access Points: Fake BTS, WiFi,...

MiTM

Relay Attacks

DNS Poisoning



Phishing  
Social engineering

Jailbreaking

ID theft

# Agenda

Security technologies

Examples from the Mobile Industry

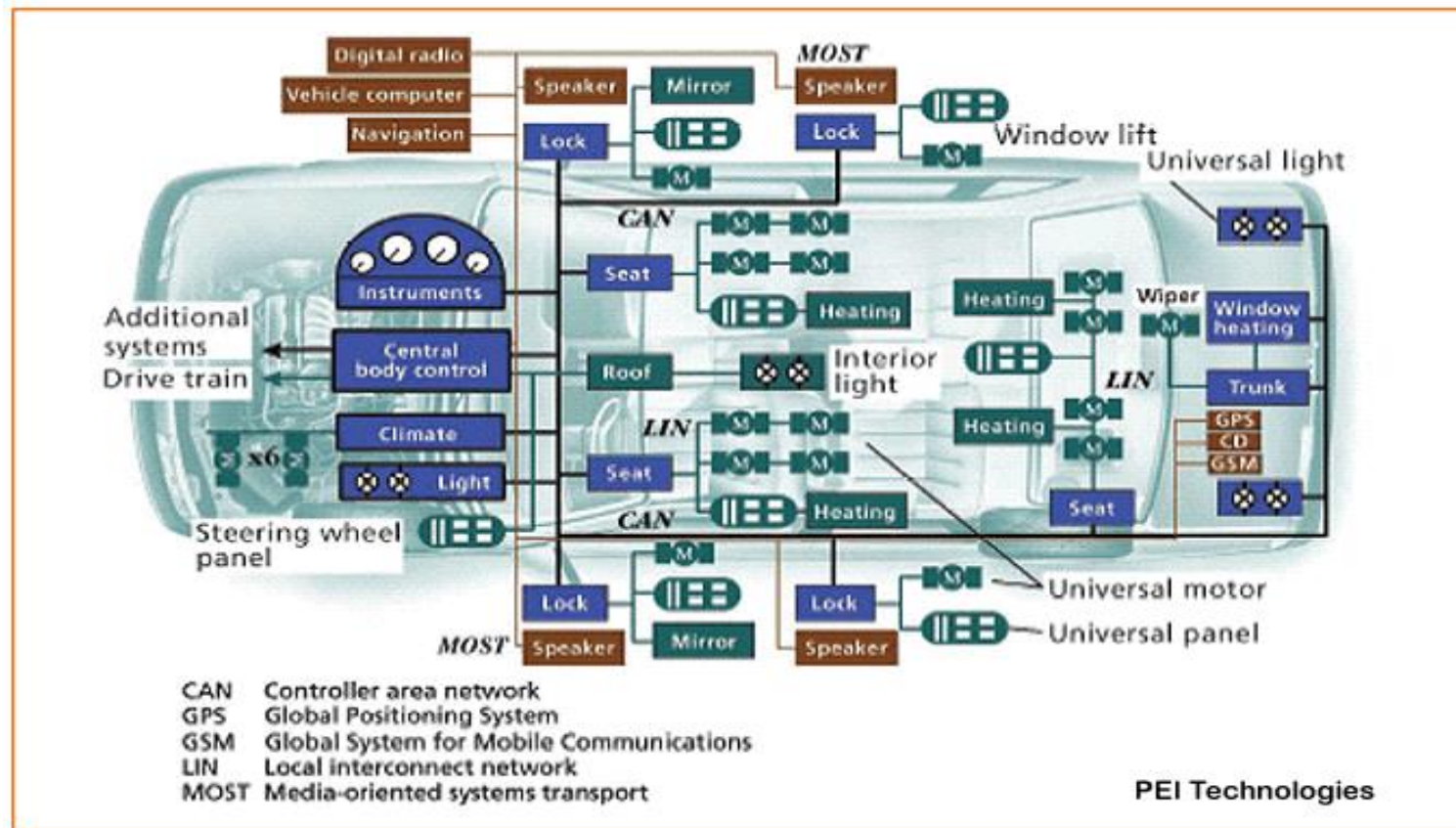
Examples from the automotive Industry

Examples from the Energy Industry

Security and privacy preserving design principles

# Security issues in a modern car

- ✧ Modern cars have over 80 ECUs connected to the CAN bus



# Security issues

- ✘ CAN is an insecure low-level protocol
- ✘ More recent CANs contain wireless components
  - Massive security implications
- ✘ Every message is an unencrypted plain-text broadcast to every device on the CAN
- ✘ Possible messages and communication procedures are often documented and made available freely
- ✘ No component authentication
- ✘ Any device can send a command to any other devices
  - E.g. Attacker could use tire pressure gauge to turn off brakes





# Consequences

- ✧ Demonstration by researchers (\*) of a sniffer/injection tool, introduced into the CAN by simply plugging a device in to the car's federally mandated universal *OBD-II* diagnostics
- ✧ Example of attacks made possible including at 45 mph speed
  - Disable brakes
  - Engage brakes
  - Disable wipers and continuously spray fluid
  - Permanently activate horn
  - Kill engine
  - Unlock all doors
- ✧ Most attacks made also possible wireless

(\*) University of California and Washington

[http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5504804&tag=1](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5504804&tag=1)

<http://dl.acm.org/citation.cfm?id=2018396>



# Next threat: car as a programming platform

- ✧ Services are provided as apps
- ✧ The car needs to provide a rich API in order to be an attractive platform for developers
  - Case study: RelayRides app on OnStar

The infographic is divided into two main panels. The left panel, titled 'GM vehicle owners can rent out their vehicle with RelayRides', shows a man standing next to a red car. It features logos for RelayRides (Neighbor-to-Neighbor Carsharing) and OnStar. The right panel, titled 'I need a car:', shows a woman in a pink dress using a smartphone app to rent a car. It features logos for RelayRides and OnStar, and a red car. The background is a light blue sky with white clouds and a green ground.

**GM vehicle owners can rent out their vehicle with RelayRides**

**I have a car:**

- Enroll:** A GM car owner decides to enroll his car in RelayRides
- Schedule:** He sets both the car's availability and the rates
- Drive:** He sits back, and makes the easiest cash he's ever earned

**I need a car:**

- Enroll:** A woman living without a car signs up with RelayRides to gain access to affordable wheels in her neighborhood
- Schedule:** she searches RelayRides' online marketplace for available cars that meet her needs
- Drive:** She can use an application\* on her phone to unlock the car through OnStar technology
- Everybody Wins:** He earns some much needed cash. She gets access to wheels when she needs them. Everybody wins!

\*mobile app available early 2012

# Hardware factorization in cars



Navigation



speed radar locator



Open android platform



Ecodriving



Multimedia

A smart phone with 4 wheels ?

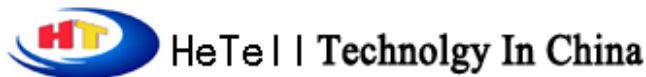
# Example of hobbyist at work





# Example of professionals at work

PCB Reverse, PCB Clone, MCU Reverse, Chip Crack, PCB Manufacturing, PCB Designing, PCB Cloning, PCB fabrication, PCB Rework, PCB Assembly



Great Service ♦ Highest Quality ♦ Competitive Pricing

086-0755-61327568 && 086-0755-61327569

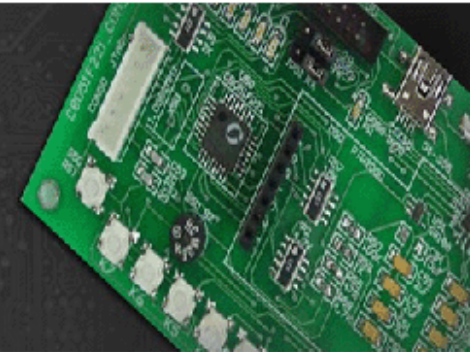
pcbhetell@gmail.com hetelltech@gmail.com skype:hetell0755

Home | About | PCB Cloning | PCB Designing | MCU Crack | PCB Assembly | Contact US | PCB layout

8051 MCU Code Extraction    ARM MCU Crack  
MASK Rom MCU Attack    DSP Chip decryption



PCB Design  
PCB Manufacturing  
& PCB Assembly



## Products & Services

- ◆ PCB Reverse Engineering
- ◆ Altera Chip decryption
- ◆ Atmel MCU Crack
- ◆ CYPRESS MCU Attack
- ◆ Dallas MCU Code Extraction
- ◆ EMC IC Code Extraction
- ◆ Freescale IC Crack
- ◆ Heltak IC Break

## AT89C51RB2 MCU Attack, Atmel AT89 IC Code Extraction

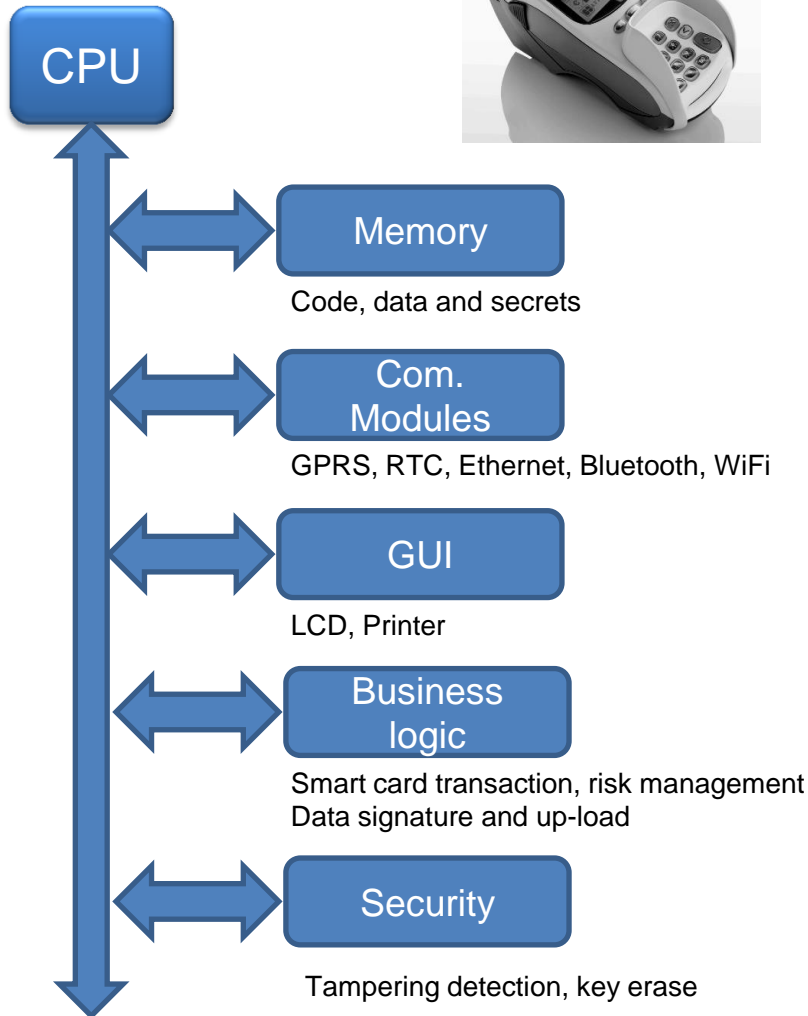
For AT89C51RB2 MCU Code Extraction, AT89C51RB2 IC Crack, AT89C51RB2 MCU Break, and other Atmel IC Attack, we use high-end technologies and the latest laboratory equipment to perfect the technique of microcontroller code recovering (extracting the code from locked microcontrollers). We had analyzed a wide variety of chip types which are commonly used in different industries, which enable us to open the chips and extract the program inside with quick speed and accuracy, and thus help launching your project quicker and cheaper.

### Description

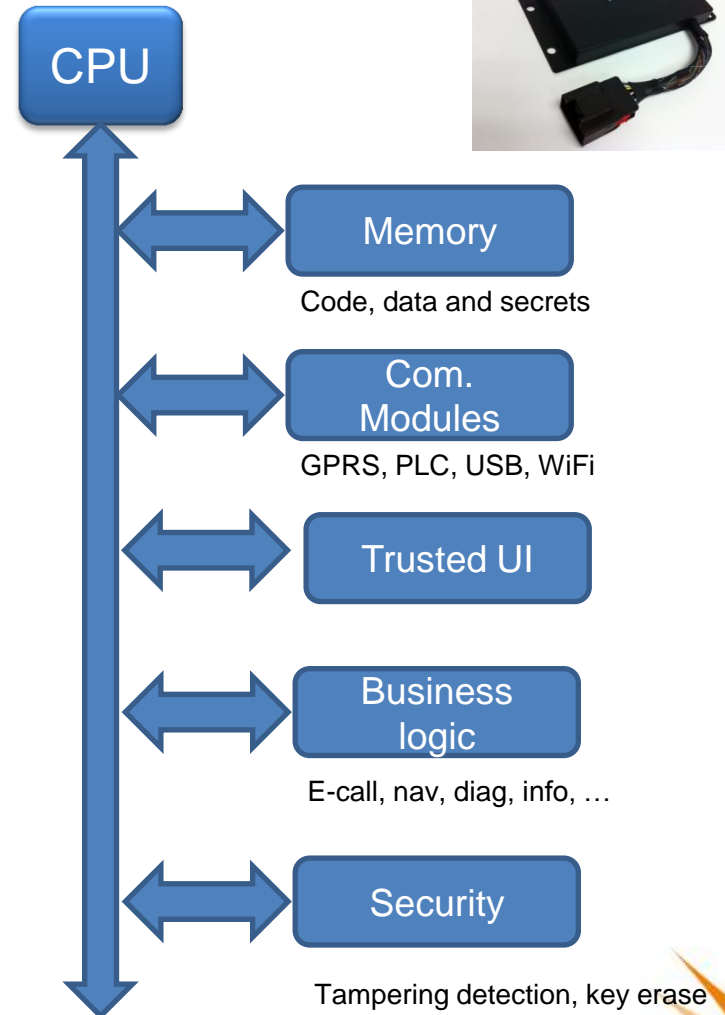
The AT89C51RB2 is a high-performance Flash version of the 80C51 8-bit microcontrollers. It contains a 16K Bytes Flash memory block for program and data. The Flash memory can be programmed either in parallel mode or in serial mode with the ISP capability or with software. The programming voltage is internally generated from the standard VCC pin.

### Features

# Point of Sale terminal

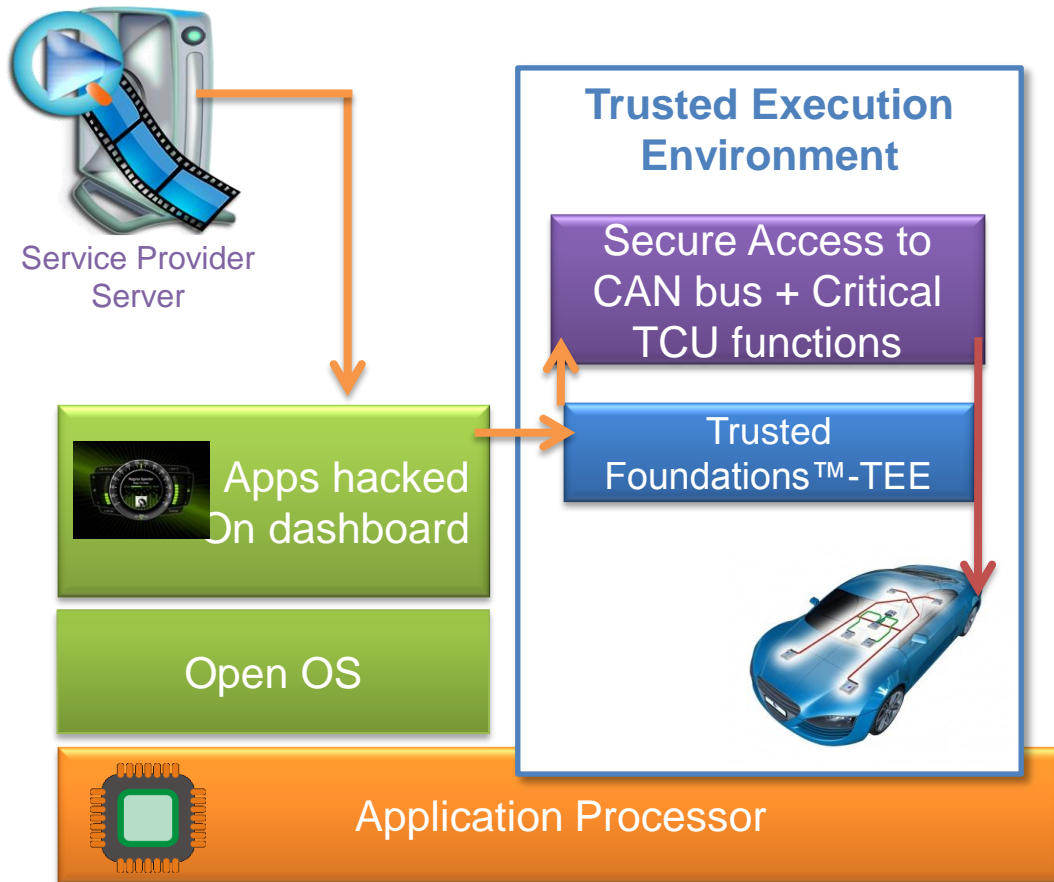


# Telematic Control Unit





# Guidelines for security improvement in cars



- **Controller authentication**
  - Only valid controllers can communicate on the CAN
- **Encrypted communication**
  - Must be high performance, so use symmetric key
  - Distribute symmetric key using asymmetric encryption during authentication
- **TEE for ECU Protection (firewall)**
- **Solution to protect Automotive asset against the attacks like:**
  - Malicious Application
  - Deny of Services
  - ECU malicious update

# Agenda

Security technologies

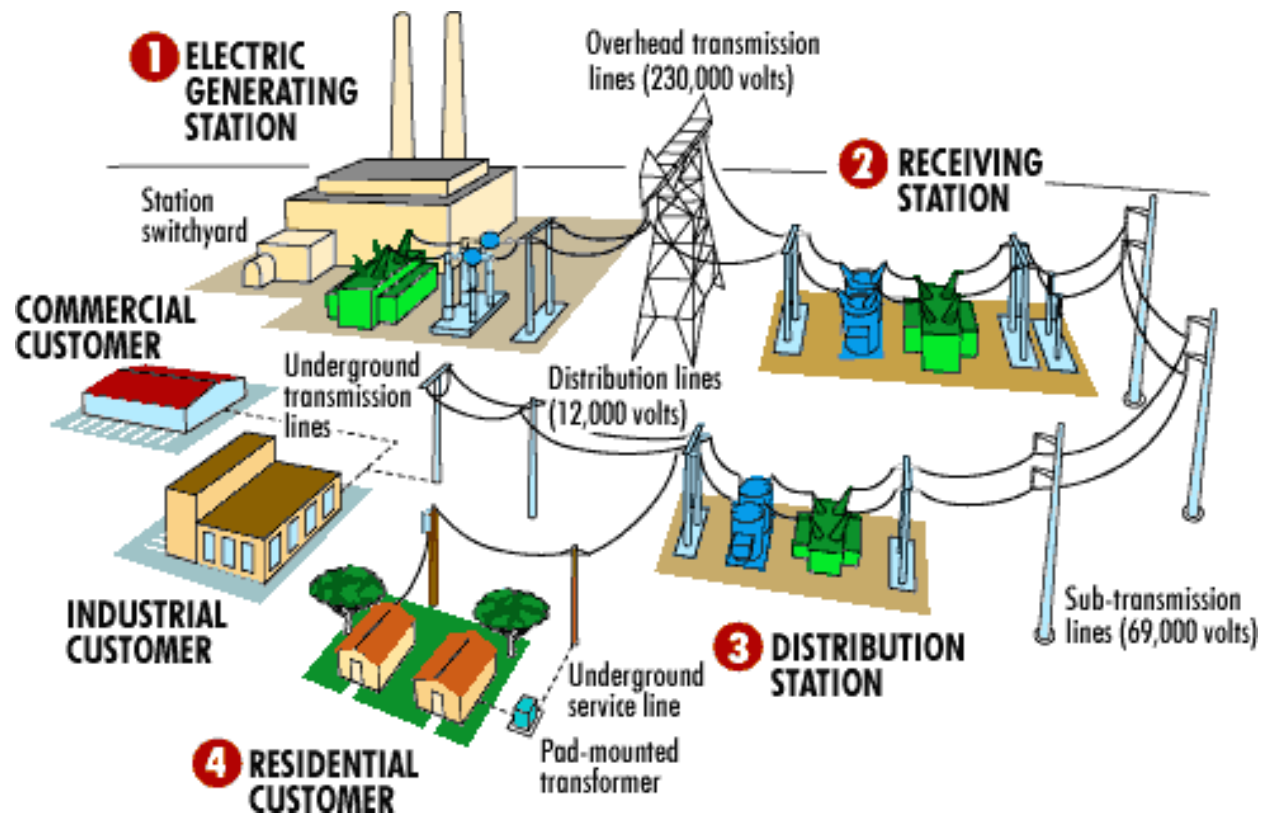
Risks/threats on IoT will derive from those facing the Mobile world

Examples from the automotive Industry

Examples from the Energy Industry

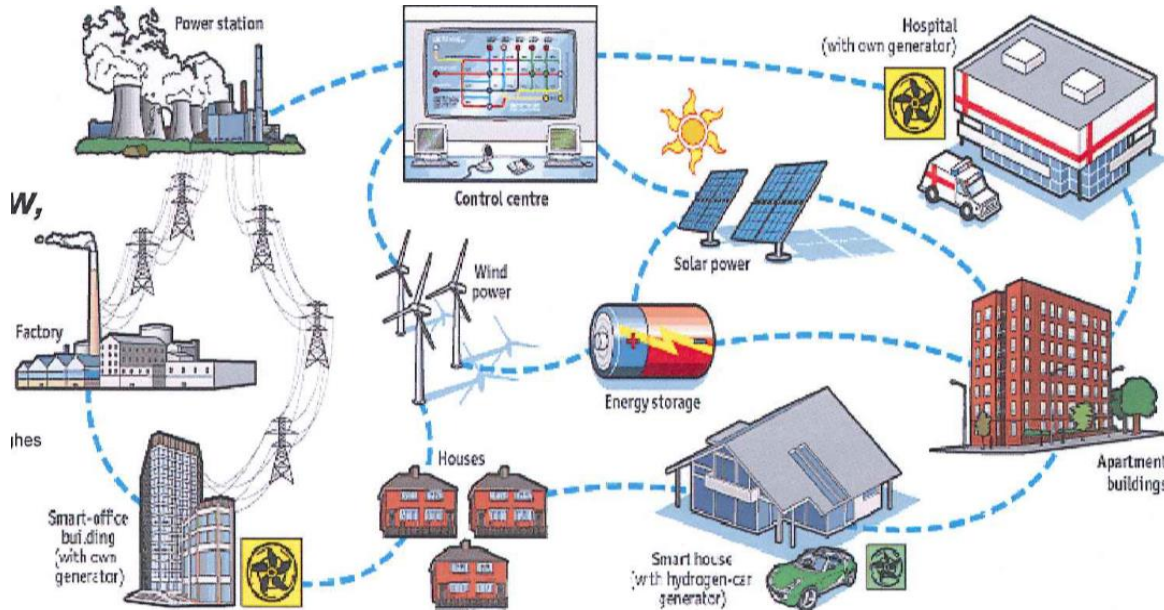
Security and privacy preserving design principles

# From grid ....



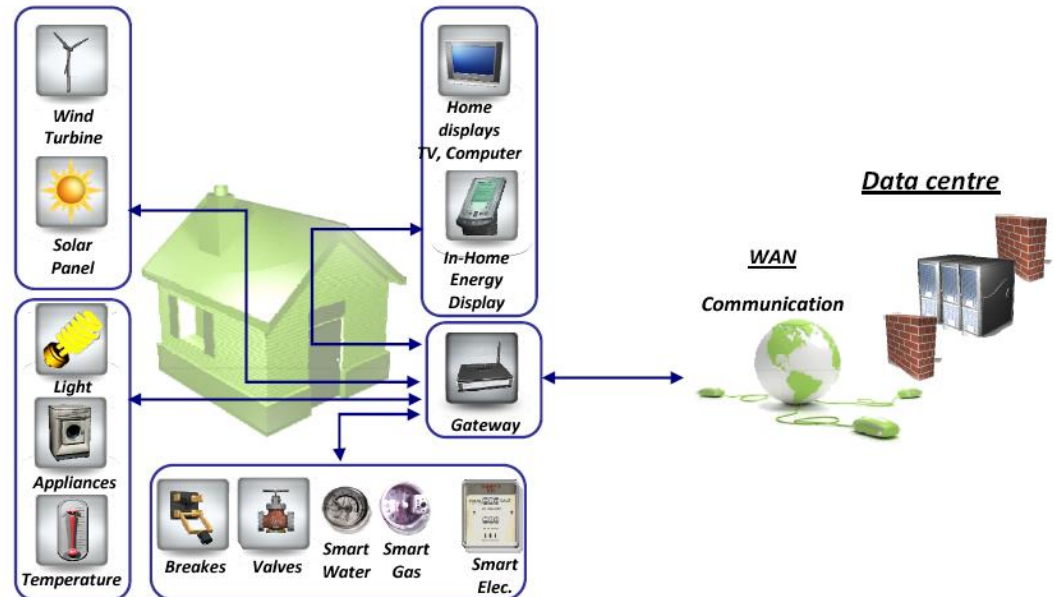
- ✦ One way energy flow
- ✦ Centralized, bulk generation
- ✦ Few actors, central information system

# ... to smart grid

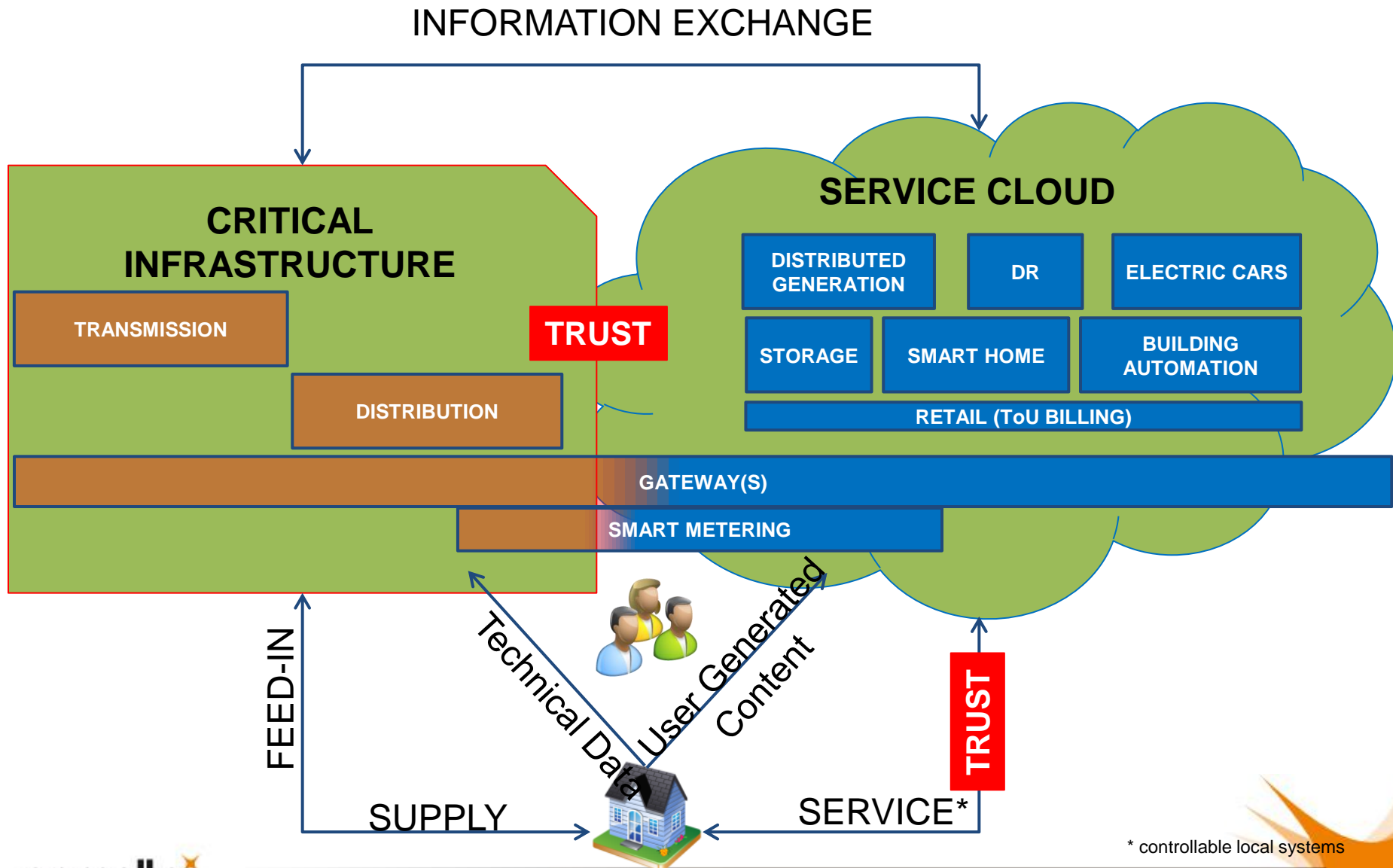


Sources: The Economist; AEB

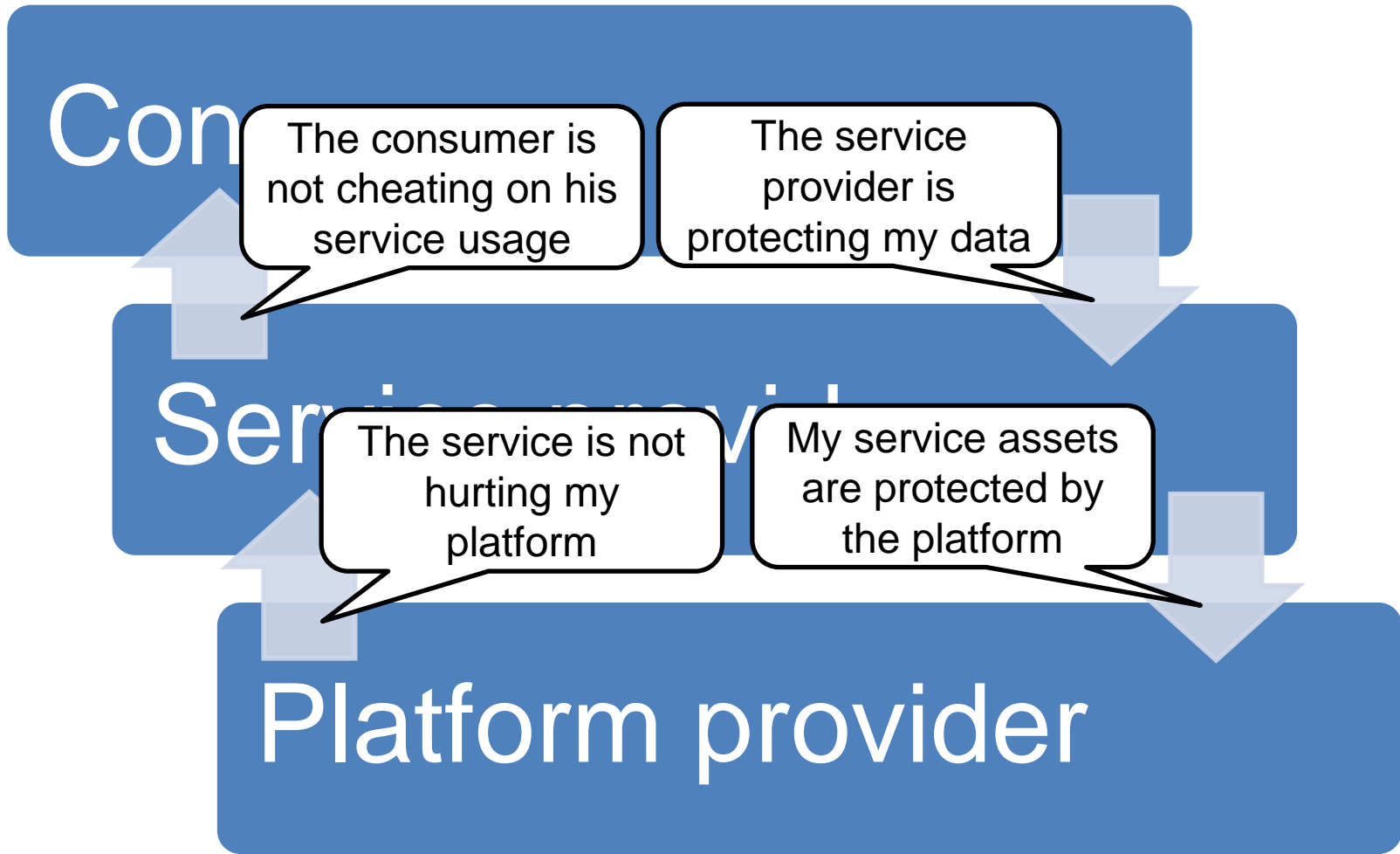
- ✧ Bi-directional energy flow, distributed production
- ✧ Numerous actors
- ✧ Open information system which is critical for grid management



# Trust will be the key enabler for a smart energy ecosystem

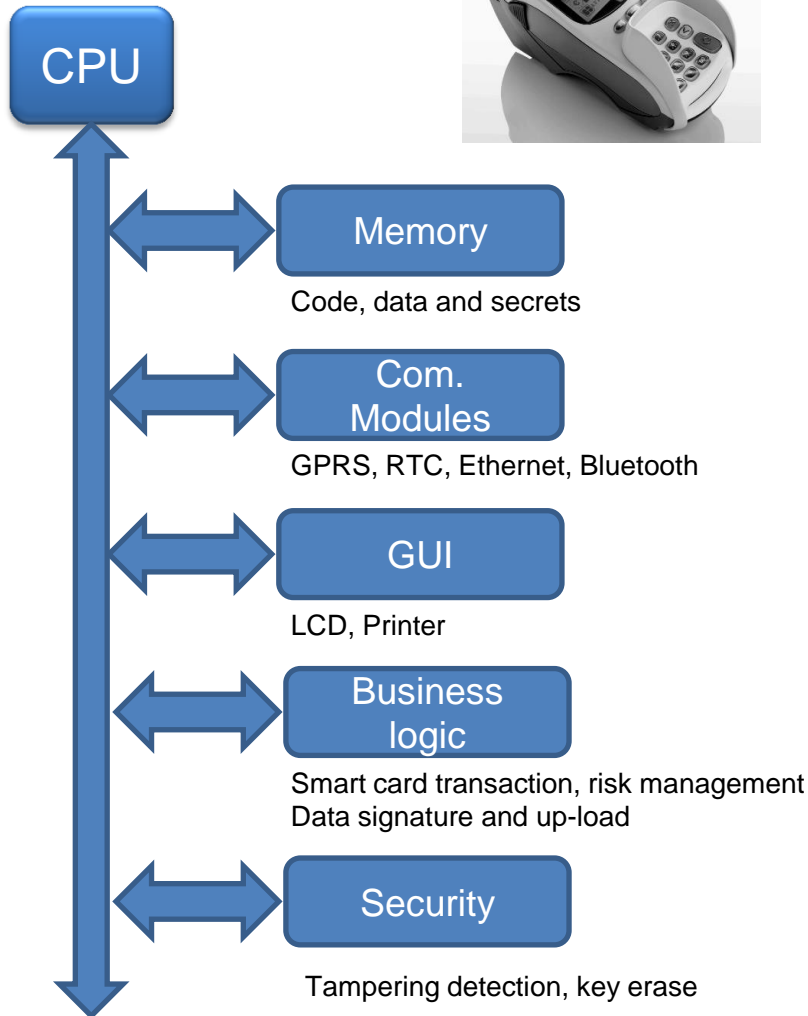


# Trust relationships

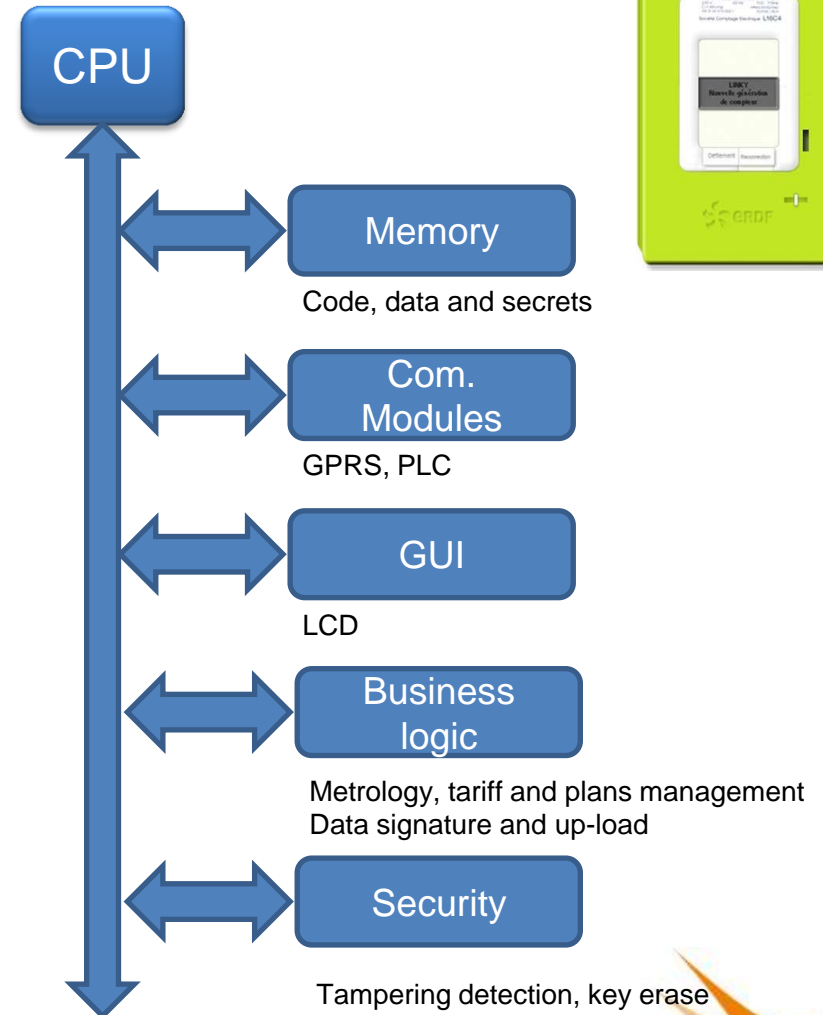




# Point of Sale terminal



# Smart Meter

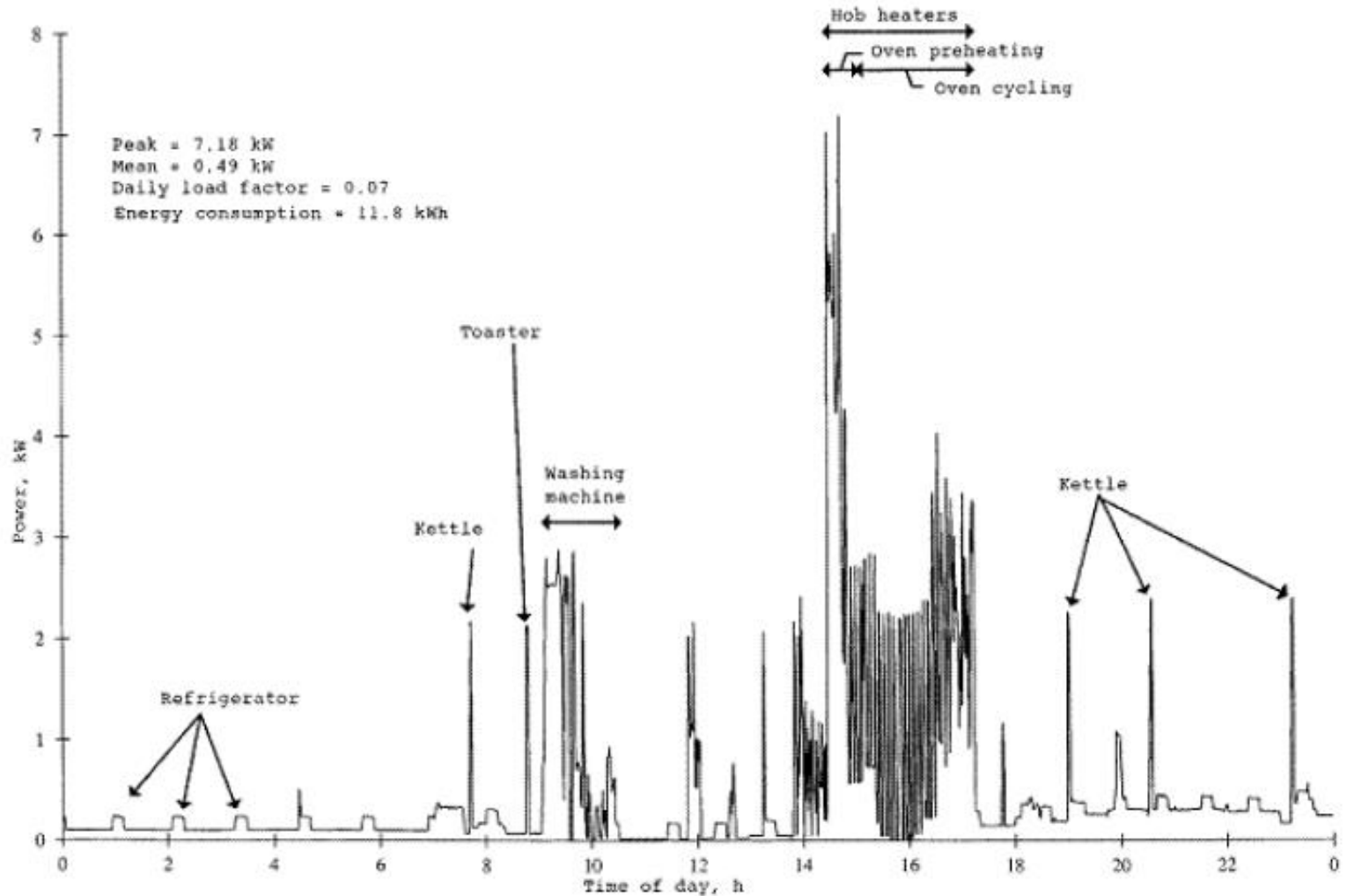


# HW Attack examples on smart meters

- ✦ Attack on a terminal not equipped with sensors
- ✦ Attack by a wire hidden in the rear cover
- ✦ Attack by a niddle in the rear cover
- ✦ Attack by unplotting the epoxy
- ✦ Imagine what can be done with SW attacks !



# House load curve over 24 hours



# Attacks always get better !



Fachhochschule  
Münster University of  
Applied Sciences



## Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“

Arbeitspapier<sup>1</sup> – Technischer Report, Status: ENTWURF, Version 0.6, Greveler, 20. Sep. 2011

Labor für IT-Sicherheit der FH Münster: Prof. Dr.-Ing U. Greveler, Dr. B. Justus, D. Löhr MSc.  
Forschungsprojekt DaPriM ([www.daprim.de](http://www.daprim.de))

**English Abstract:** Advanced metering devices (smart meters) are being installed throughout electric networks in Germany (as well as in other parts of Europe and in the United States). Unfortunately, smart meters are able to become surveillance devices that monitor the behavior of the customers leading to unprecedented invasions of consumer privacy. High-resolution energy consumption data is transmitted to the utility company allowing intrusive identification and monitoring of equipment within consumers' homes (e. g., TV set, refrigerator, toaster, and oven). Our research shows that the analysis of the household's electricity usage profile does reveal what channel the TV set in the household was displaying. Moreover, the data being transmitted via the Internet is unsigned and unencrypted. All tests were performed with a sealed, operational smart meter used for electricity metering in a private home in North Rhine-Westphalia, Germany.

# How about hardware sharing ?



Demand response: gateway



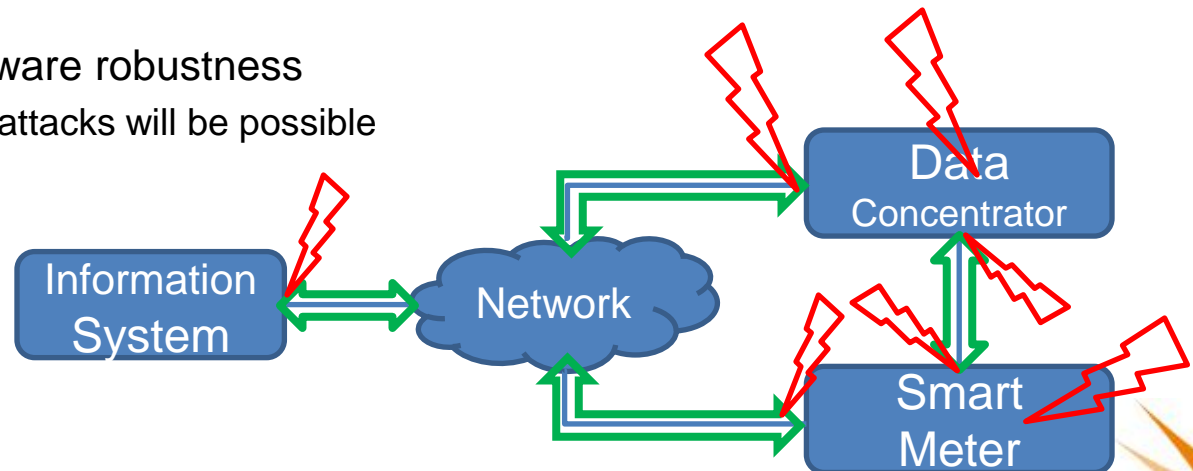
Home energy management



PV array management

# Security mechanisms & weaknesses

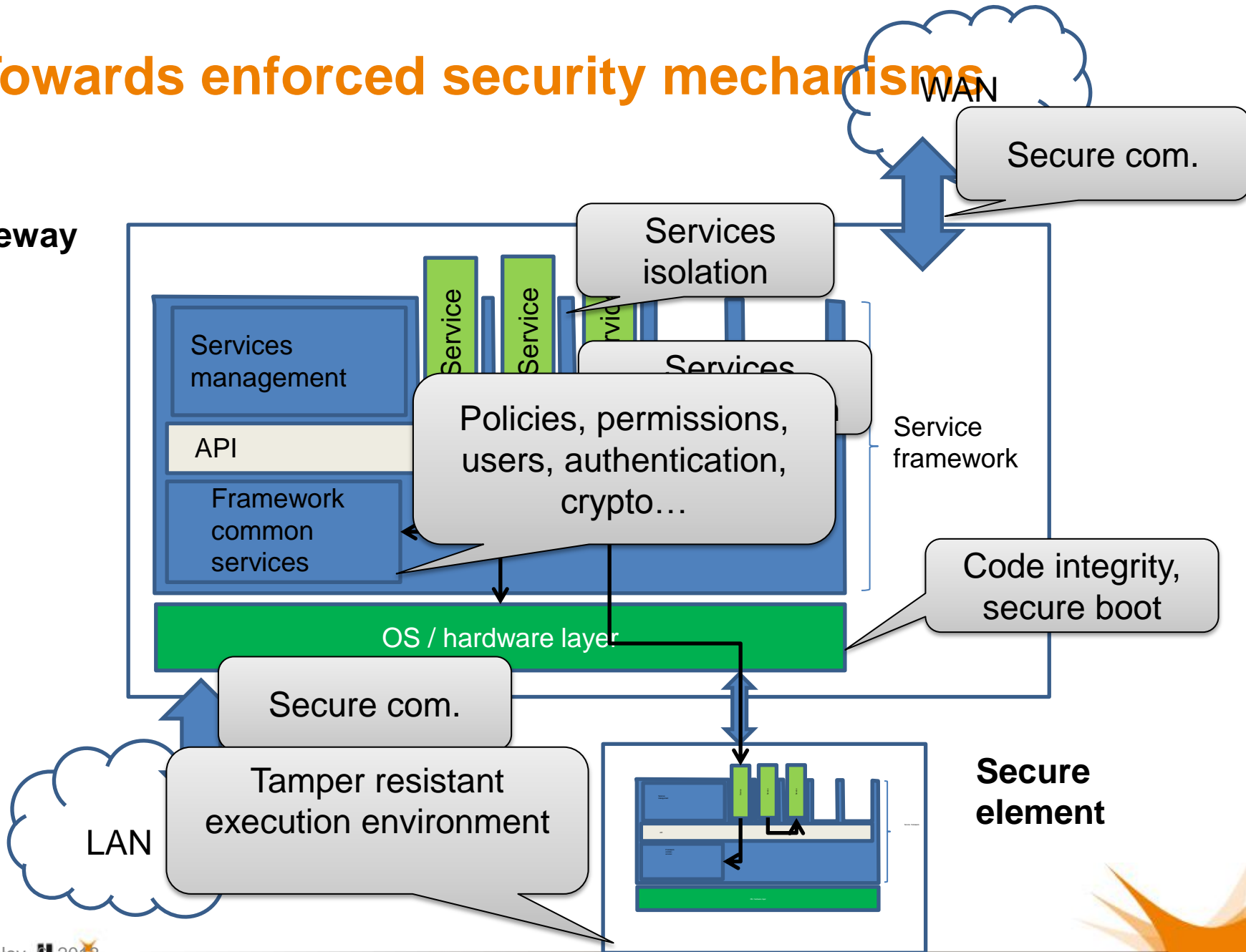
- ✧ Cryptographic mechanisms start to be introduced
  - Communication encryption
  - Data integrity (e.g. consumption measurements, firmware upgrade)
- ✧ But end-points remain vulnerable
  - Very limited physical protection
    - No tamper resistance
    - Limited tamper evidence
  - Limited software robustness
    - Remote attacks will be possible





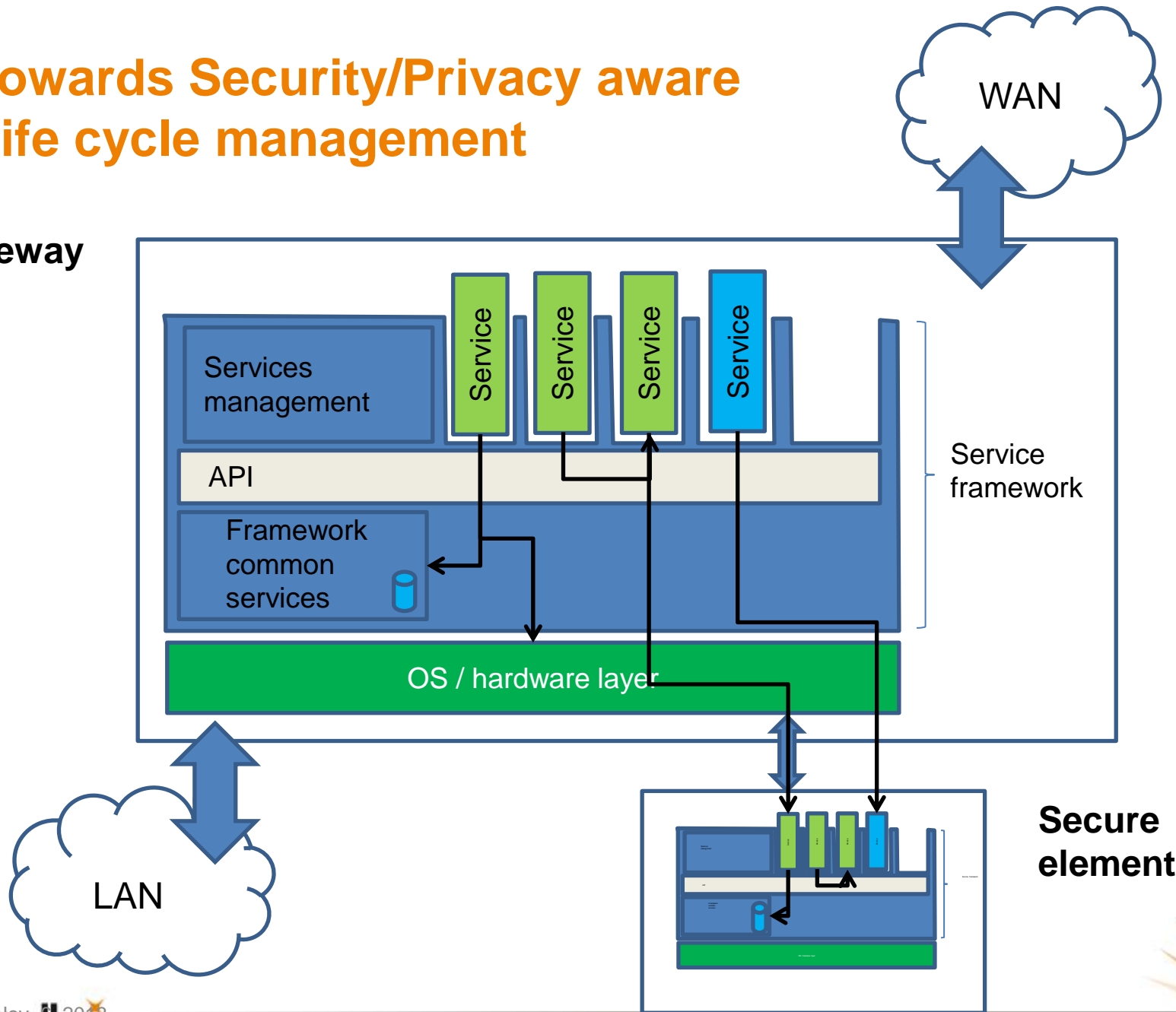
# Towards enforced security mechanisms

Gateway



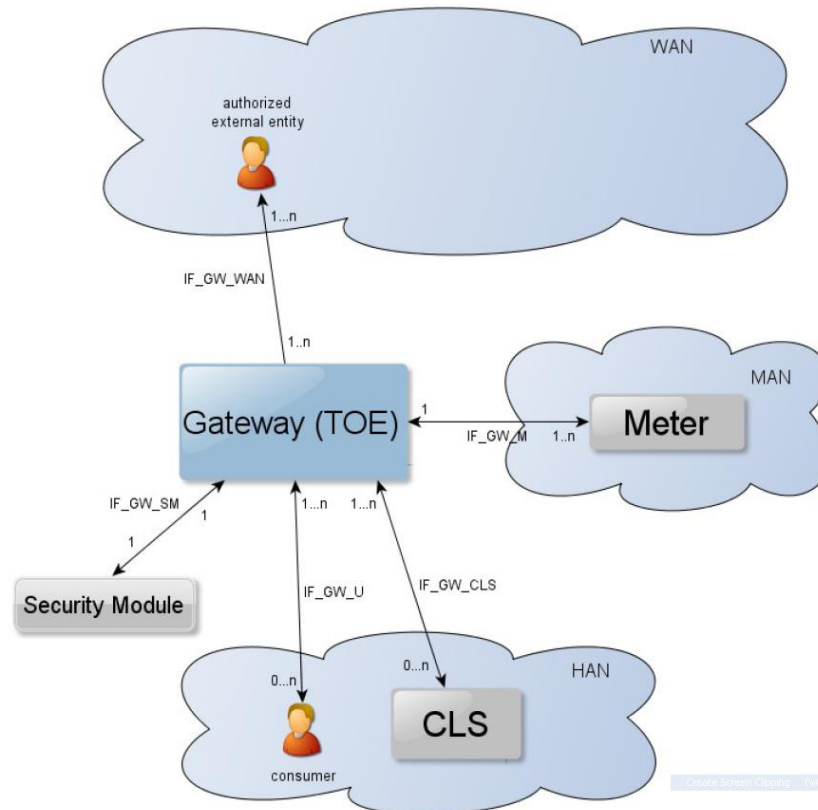
# Towards Security/Privacy aware Life cycle management

Gateway



# Certification vision in Germany (BSI)

- ✧ Protection Profile for the Gateway of a Smart Metering System (EAL4+)



- ✧ There will be another PP for the security module (EAL4+)
- ✧ No security constraint on the smart meter !

# Agenda

Security technologies

Risks/threats on IoT will derive from those facing the Mobile world

Examples from the automotive Industry

Examples from the Energy Industry

Security and privacy preserving design principles

# A security/privacy keeping framework is needed

- ✧ Permissions need to be managed based on
  - Service provider / developer identity
  - Certification status
  - User authentication
  - Device (e.g. Car) life cycle state (e.g. in maintenance)
  - Real time context (e.g. speed)
- ✧ Of course we need permissions on API
  - But it's not so simple
  - Avoid the “Click I accept” syndrome
- ✧ Apps and services will also need
  - Users and device (car!) authentication
  - Billing framework



# Security Process

## ✧ Detailed risk analysis

- Identification of attackers and assets
- Threats and attack scenarios
- Risk quantification for each scenario

## ✧ Validation plan to check equipment against the risks

- Test list to cover each threat
- Detailed procedure for each test

## ✧ Use/adapt equipment testing in hardware and software attack lab





# Identification and authentication

## ✧ Management of identities and roles

- Ex of Roles in Automotive = owner, driver, passenger, shift manager, fleet manager, maintainer, ...

## ✧ Flexible authentication methods

- Biometrics
- Cryptography
- Hardware based

## ✧ Flexible security levels

- Not the same level needed for kids screen skinning and door opening

## ✧ Various form factors

- USB tokens, SD cards, mobile phone, key fob, driving license, ....



# Risk analysis is the most sensitive step

## ✧ Who will be the attacker ?

- Do you protect the consumer or from him ?
- In cars: owner, driver, passenger, shift manager, fleet manager, maintainer
- Should we take into account cyber attacks ?
- Built your own threat model and be prepared to adapt it !

## ✧ Quantitative evaluation is difficult

- How to evaluate the equipment cost ?
  - How about rental, how about new techno (e.g. OpenBTS)
- How to evaluate the man power ?
  - Hackers teams have an almost infinite man power pool
- How to evaluate the attack knowledge ?
  - More and more public papers and open source

## ✧ Take into account complex/new use cases

- P2P rental, fleet management, BYOD, open or secure environment

## ✧ Take into account the full product life cycle

- Provisioning, maintenance, reconditioning, ownership change, upgrade, patch, dispose

# Attacker Model

## ✧ Hacker

- No physical access to the vehicle

## ✧ Malicious Driver

- Some access to the vehicle

## ✧ Malicious Car Repairer

- Complete access to the vehicle

## ✧ Terrorist Organization

- Attack on the infrastructure



# Some points worth thinking

- ✧ Avoid security by obscurity
  - Anything can be reverse engineered
  - Examples: Comp128-1 vs Milenage, Mifare vs DesFire
- ✧ Design for the unknown
  - Creativity of attackers (e.g. DPA)
- ✧ Consider end-to-end security
  - Build your own security (e.g. relying on network security only is risky)



# Threats (example)

- ✧ Threat 1: Attacker can control some physical elements (ECUs) of a car (locally/remotely)
  - [TH 1.1] Attacker can control some physical elements of a non running car
    - [TH 1.1.1] Attacker can open/close the door of the car (BCM)
      - Locally can mean through a wireless mean
    - [TH 1.1.2] Attacker can start the car engine (ECM)
    - [TH 1.1.3] Attacker can switch off/on the headlights
  - [TH 1.2] Attacker can control some physical security elements of a running car and have an impact on the car safety
    - [TH 1.2.1] Attacker can speed up / slow down the car (SCU)
    - [TH 1.2.2] Attacker can stop the engine (ECM)
    - [TH 1.2.3] Attacker can force the car to brake or can prevent the car to brake (BrCM)
    - [TH 1.2.4] Attacker can launch the AirBag
    - [TH 1.2.5] Attacker can switch off the ABS
    - [TH 1.2.6] Attacker can switch off/on the headlights
    - [TH 1.2.7] Attacker can modify some driving parameters (hardness of brake, softness of direction)
    - [TH 1.2.8] Attacker can modify some comfort elements (massage automatic chair)

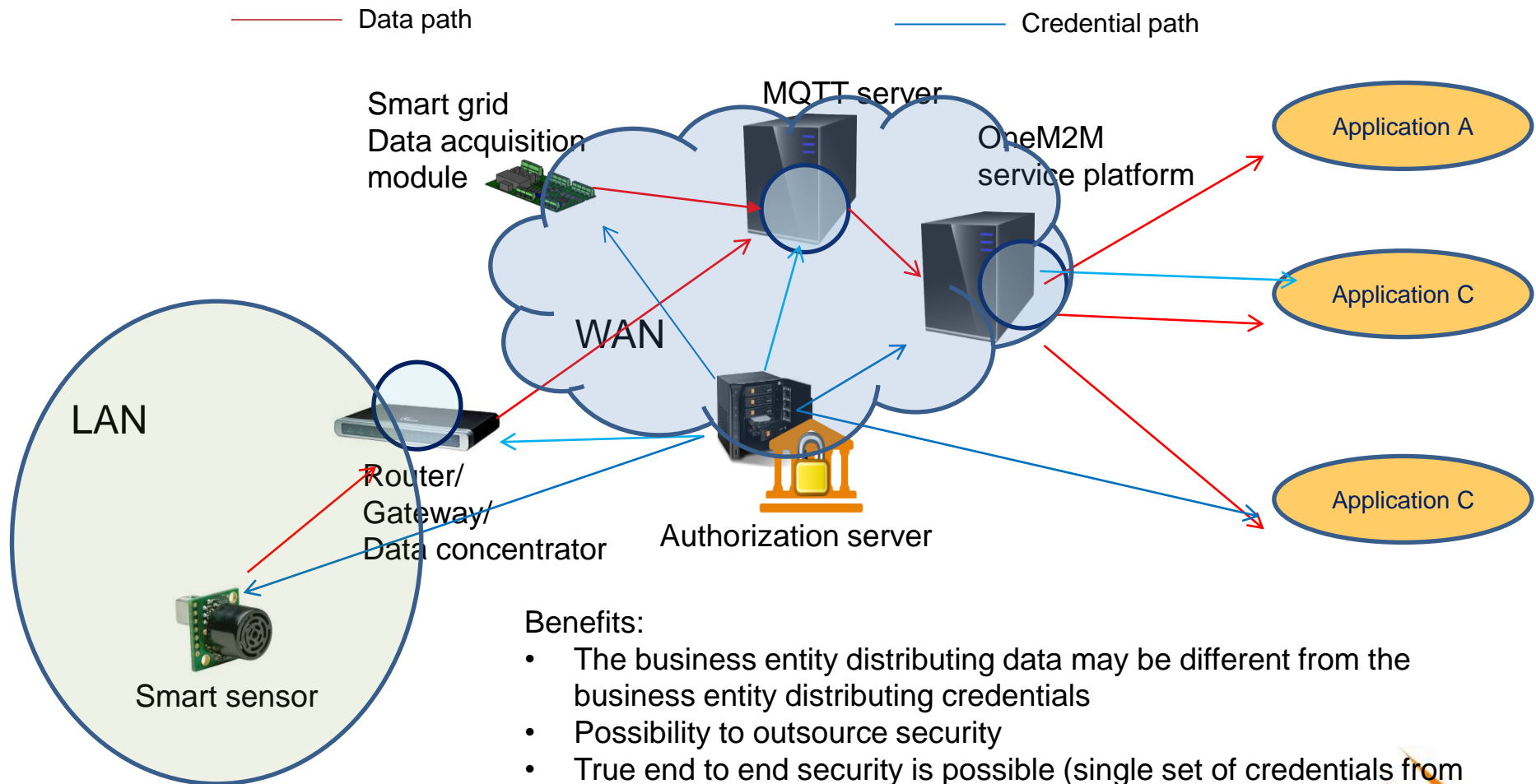
# Privacy by design Principles

- ✦ 1. Proactive not Reactive; Preventative not Remedial
- ✦ 2. Privacy as the Default Setting
- ✦ 3. Privacy Embedded into Design- Not an add-on
- ✦ 4. Full Functionality — Positive-Sum, not Zero-Sum
- ✦ 5. End-to-End — Full Lifecycle Protection
- ✦ 6. Visibility and Transparency — Keep it Open
- ✦ 7. Respect for User Privacy — Keep it User-Centric



# New way: delegated security management

Principle: separate data and credentials distribution paths



## Benefits:

- The business entity distributing data may be different from the business entity distributing credentials
- Possibility to outsource security
- True end to end security is possible (single set of credentials from Source to Destination)

# Conclusion

✧ Embedded security/privacy problems start to be understood

✧ Several initiatives in the mobile

- » Samsung Knox
- » Secure Enclave
- » SE Linux



✧ Other domains still embryonic

✧ Innovative solutions are emerging on the market: TEE, whitebox cryptography, homomorphic VM, delegated security management, “bitcoin” like approaches

✧ Secure Elements are part of the pictures

✧ Research collaboration between academics and industry is the next MUST

**Thanks for your attention !**