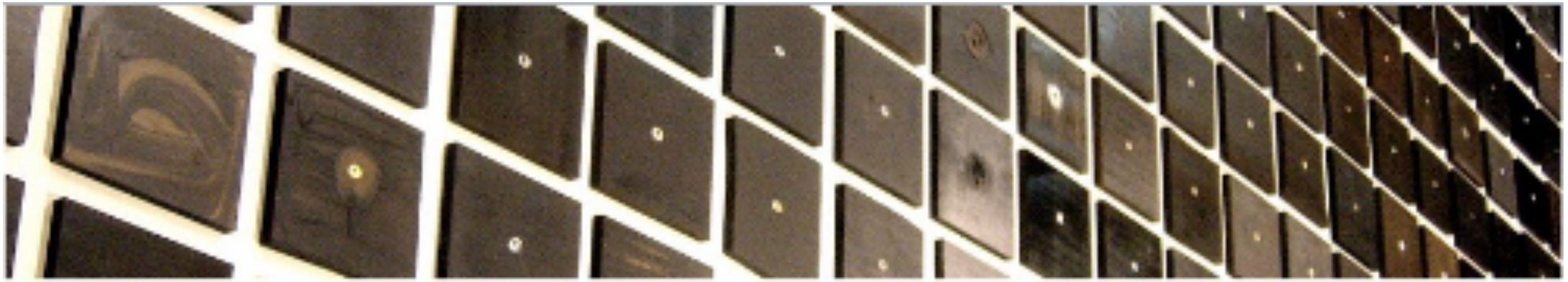


UiO : Universitetet i Oslo

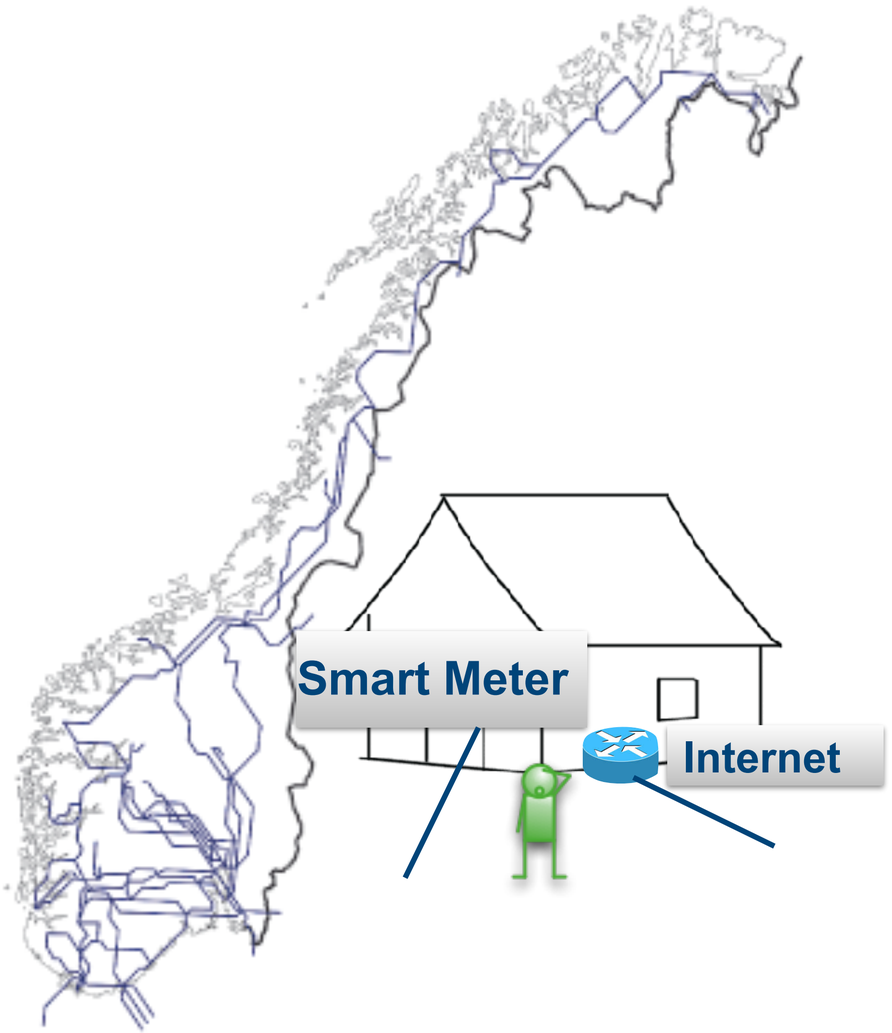
ESRO Fagdag “Risikostyring i fremtidens avanserte samfunn”, Oslo, 1Jun2017

Smart energisektor - hvordan etablere og sikre tillit?

Josef Noll
josef@jnoll.net, @josefnoll, m: +47 9083 8066
Project leader IoTSec.no -Security in IoT for Smart Grids
Professor at University of Oslo, Department of Technology Systems

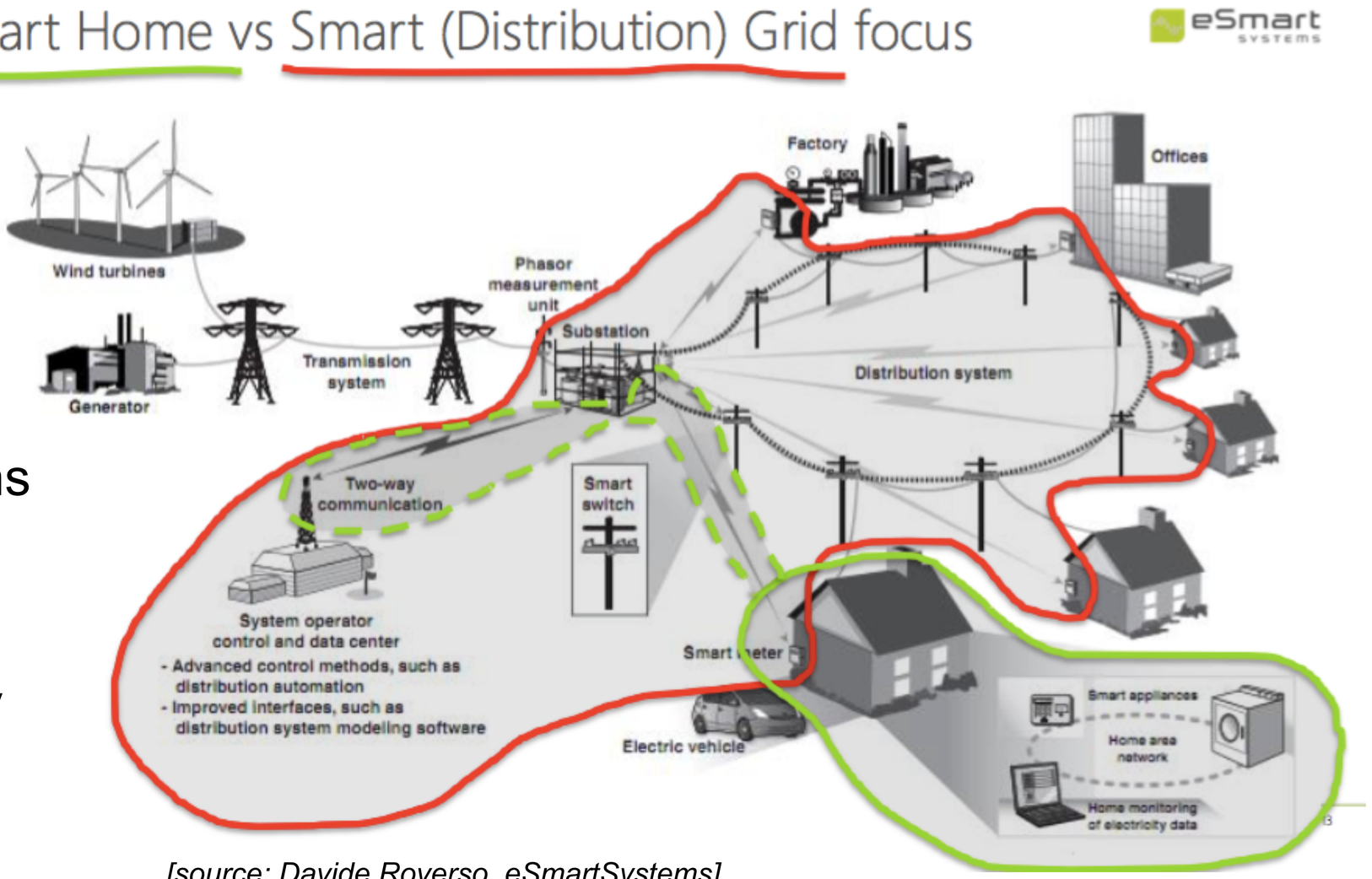
"Our Journey of Today"

- "The last time we were connected by wire was at
- Smart Grid
  - Regulations, Challenges
- Internet of Things (IoT)
  - IoT, Security & Privacy
- Postulation and Discussion
  - Demand Security
  - Privacy Labelling



Smart Electrical Grid

- Regulations
  - Soft fuse
  - Remote Switch off
- Intelligent Smart Grid
  - Attack surface
  - Remote control of Operations
  - Autonomous operations
  - Efficiency, online monitoring
- Trust, Security and Privacy

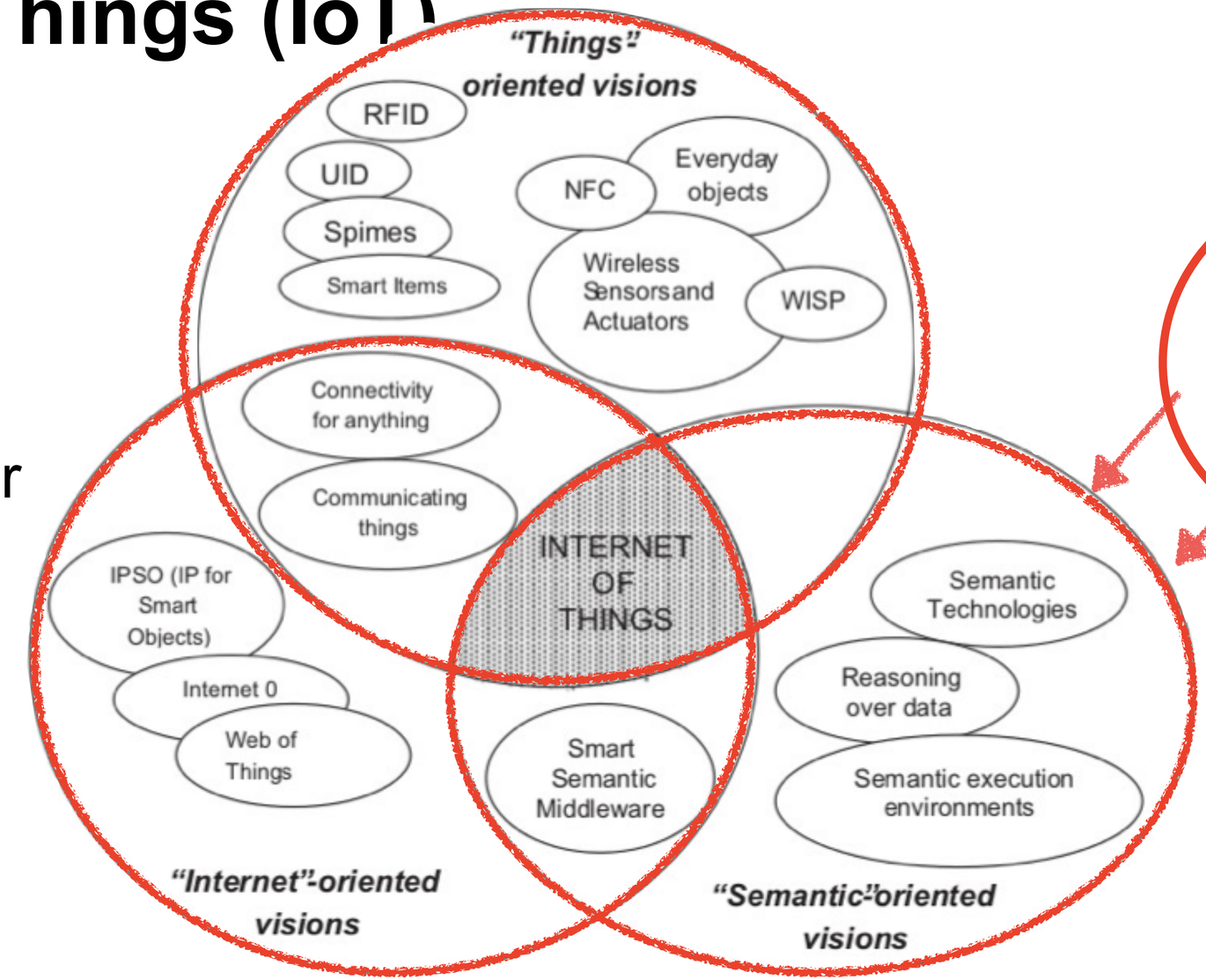


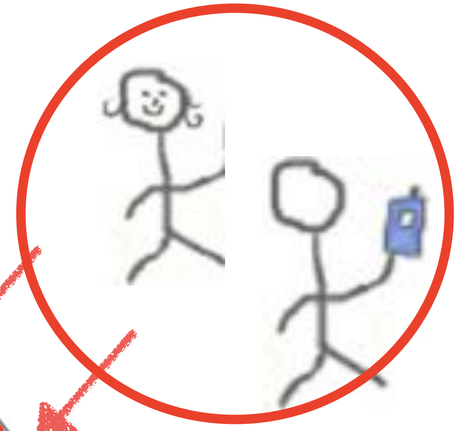
[source: Davide Roverso, eSmartSystems]

Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/

The Internet of Things (IoT)

- IoT =
  - Things +
  - Internet +
  - Semantics
- Tingene som snakker
  - med en datamaskin,
  - som forstår hva det dreier seg om,
  - og tar selvstendige beslutninger





* security
* privacy
* dependability
* context-aware
* personalised

Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

IoT threats

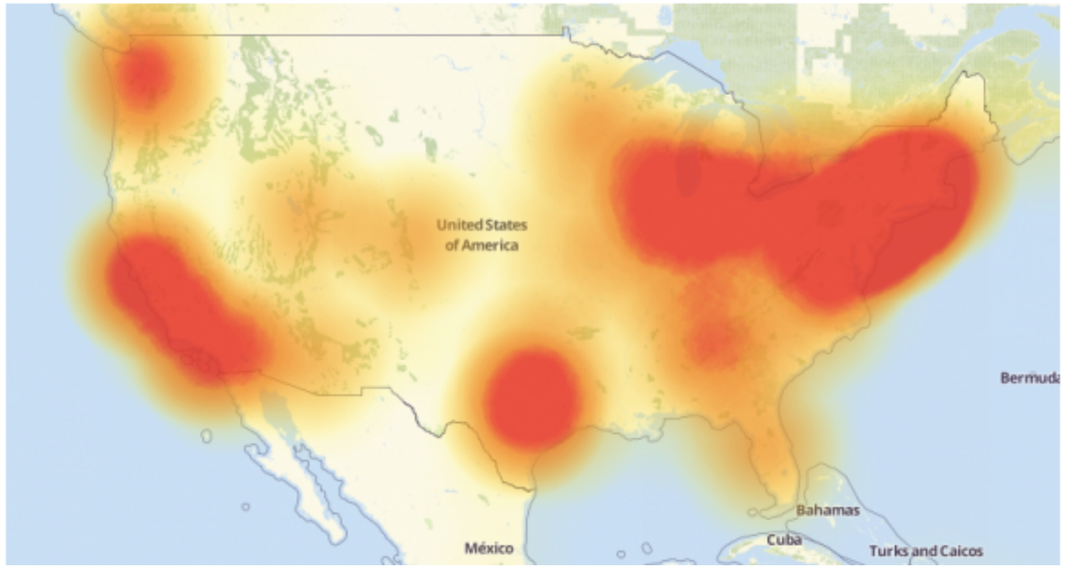
- First massive attack from IoT devices
  - 16Oct2016 IoT botnet attack on Dyn
  - Camera (CCTV), video recorder, TV,…
  - 1.2 Gbps Denial-of-Service attack

- How?
- All using Linux BusyBox for authentication
  - admin - admin, root - root, admin - 1111…
  - simple “test” was enough to convert IoTs into botı

21 OCT 16 Hacked Cameras, DVRs Powered Today’s Massive Internet Outage 16Oct

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



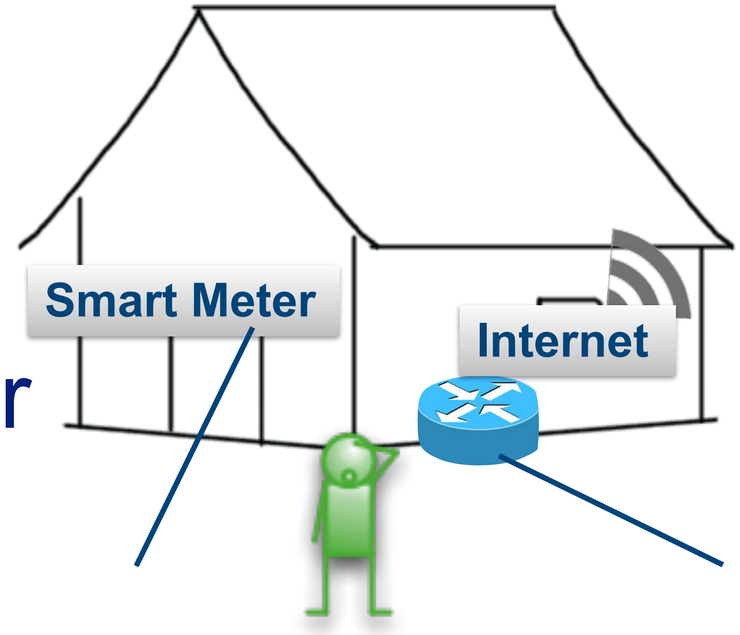
[Source: https://krebsonsecurity.com/2016

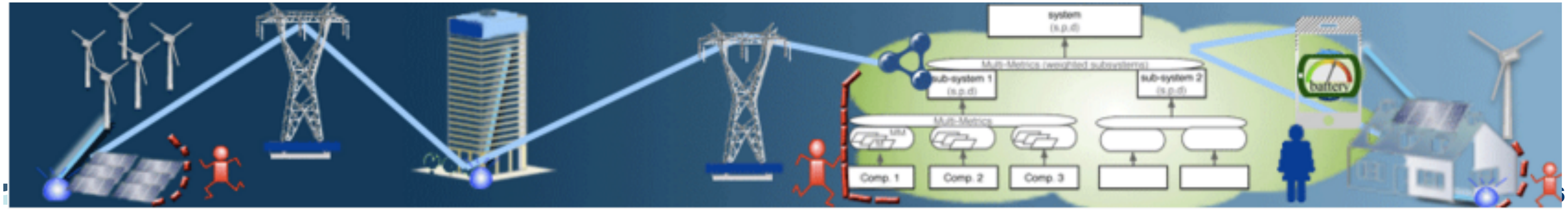
Communication & IoT for society

IoTSec.no

"Research on IoT security"
"Building the national Security Centre for Smart Grid"

http://IoTSec.no

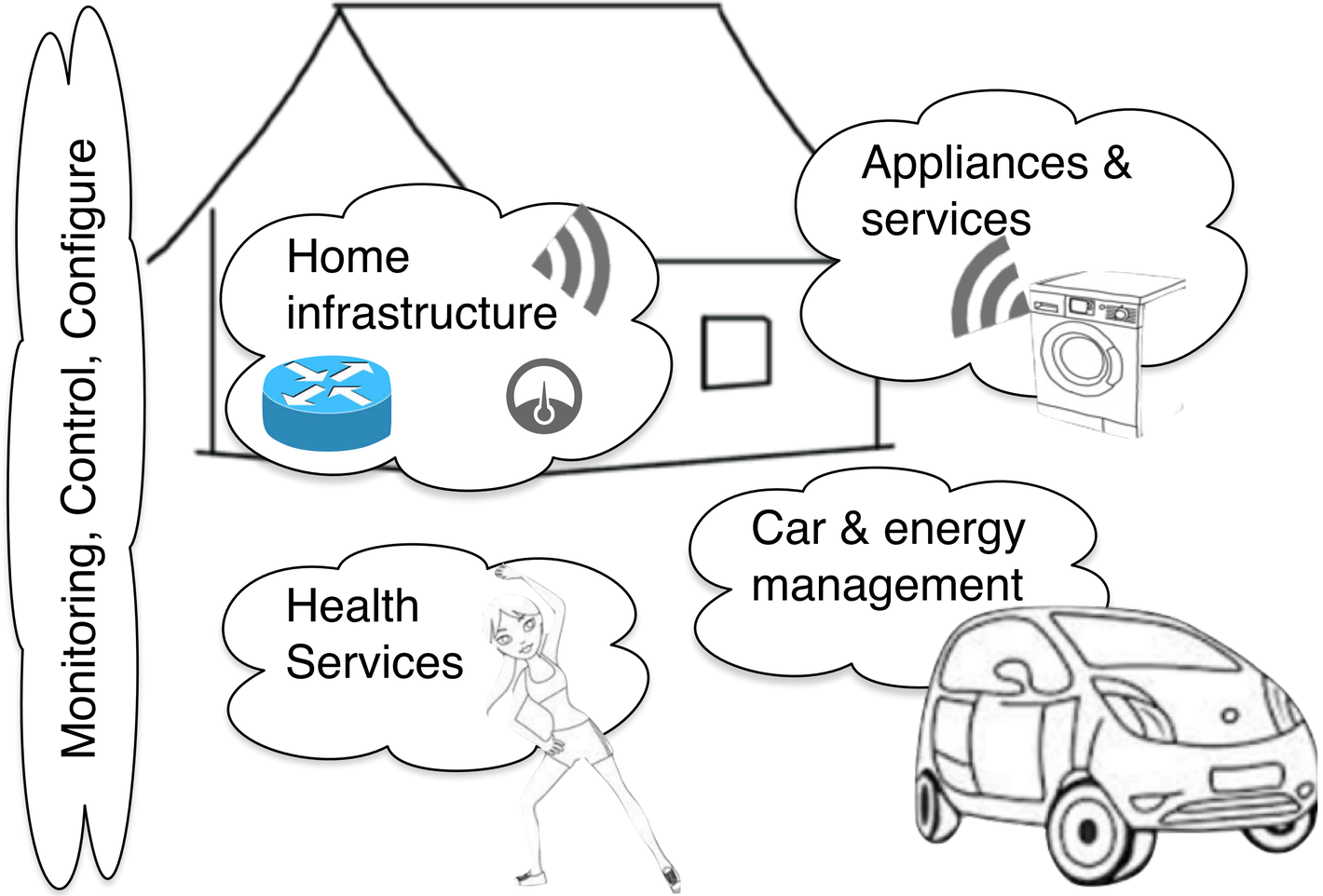




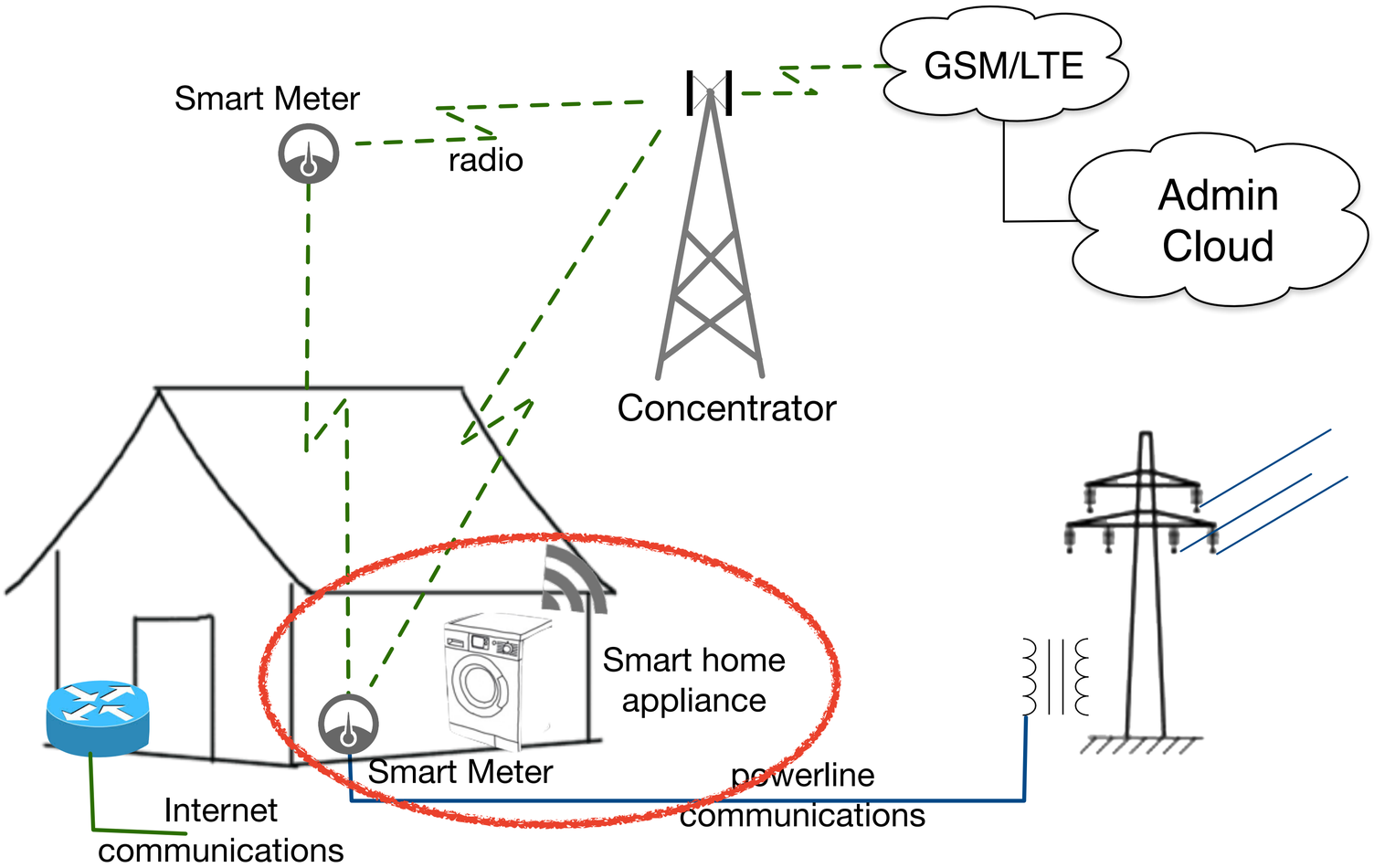
Considerations for Services in the Smart Home

- A variety of services
- Security and Privacy requirements

- Novel trends, flexibility
- My Home is everywhere



Who is going to manage the home?

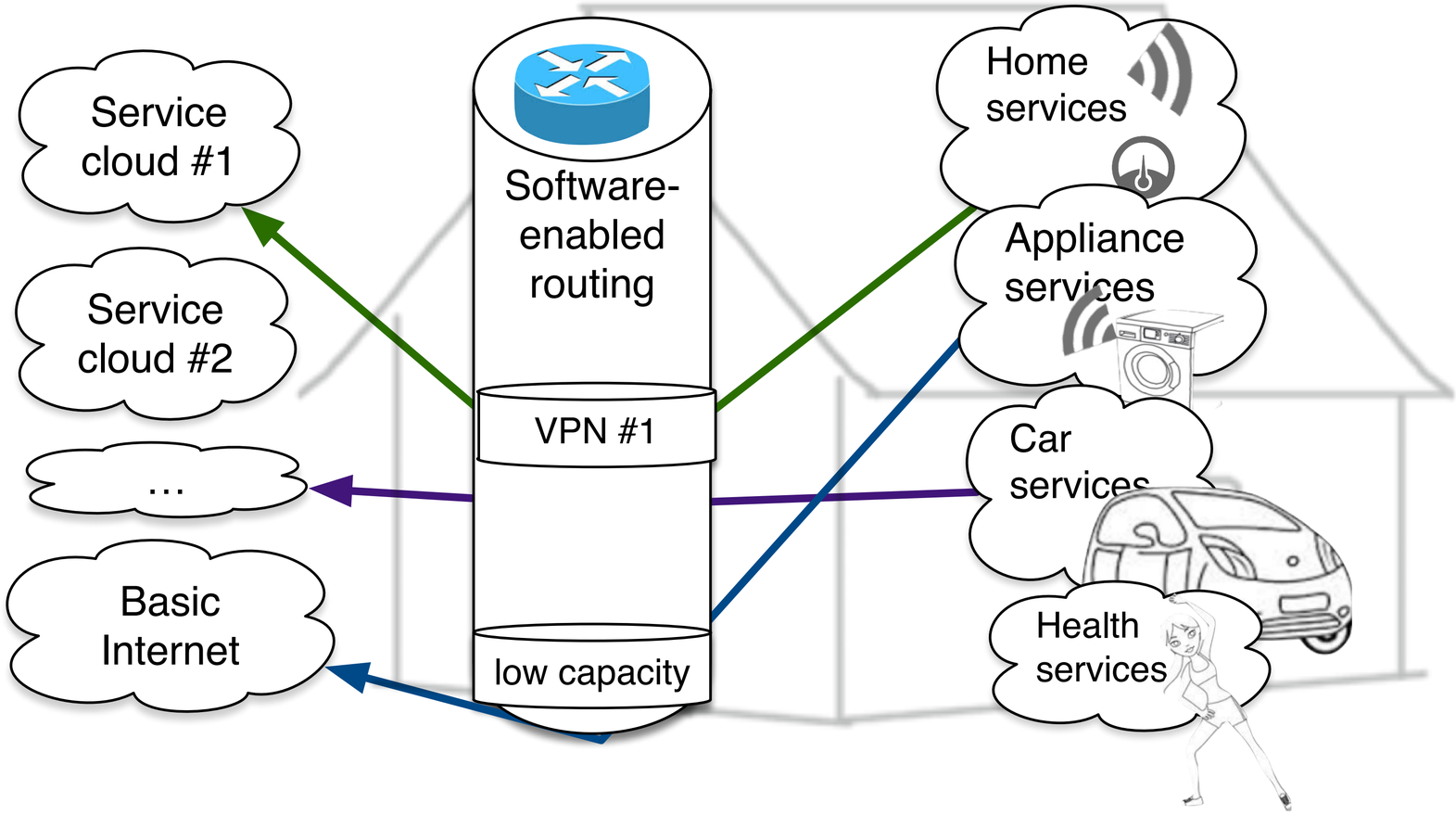


Security & Privacy?

And who is going to pay?

Learn from Industrial Automation and Mobile Networks

- "What to secure?"
- Network segregation
  - ➡ *Network slicing*
- From Confidentiality, Integrity, Availability (CIA)
- to Availability, Integrity, Confidentiality (AIC)

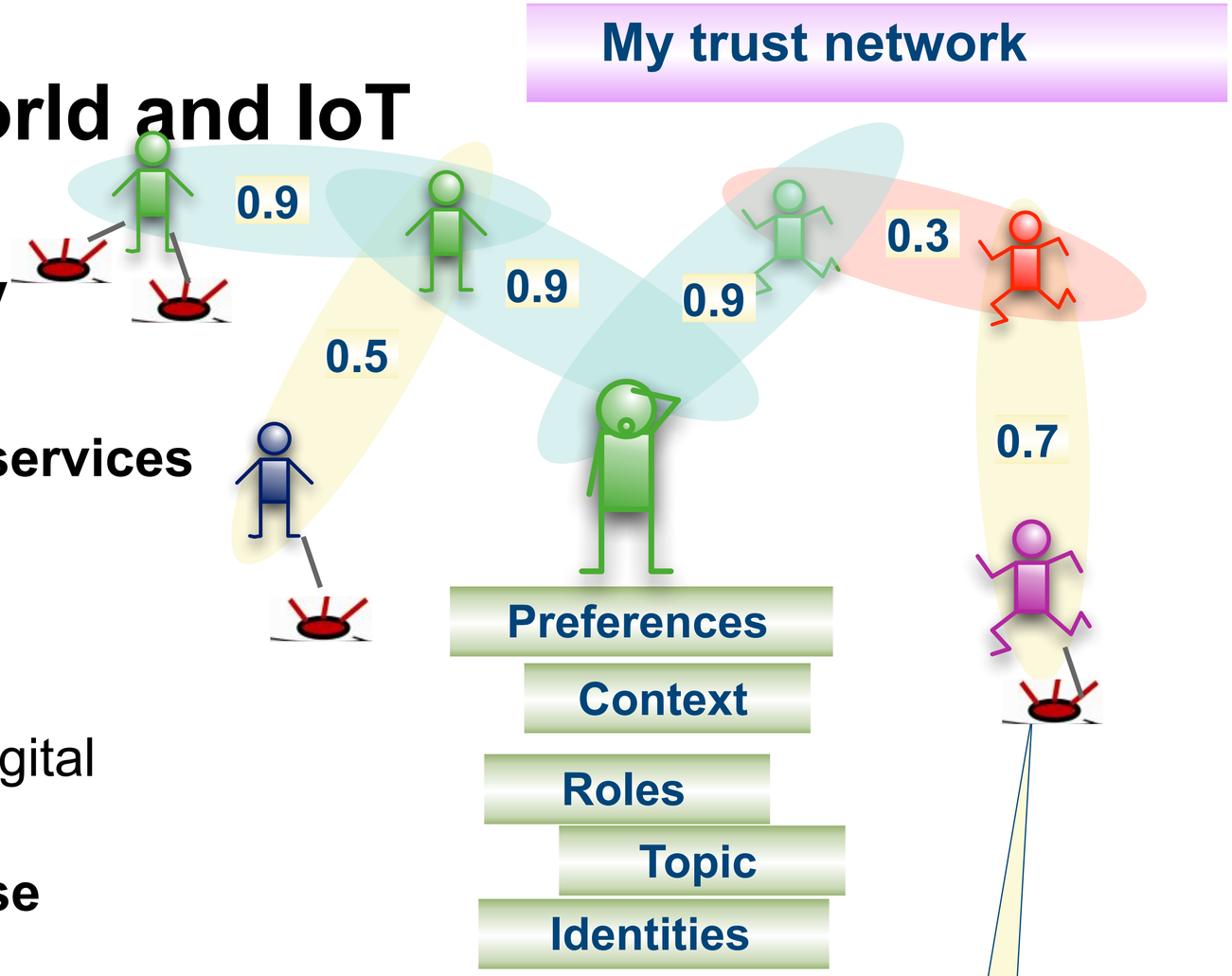


Paradigm change for The Internet of the Real World and IoT

- Trust related privacy
  -> **Representing the user adequately**

- Connecting to **sensors**, **devices** and **services**
  -> **Provide privacy and ensure trust relations**

- An ever increasing complexity in the digital environment
  -> **Hiding the complexity from the use**



Thanks to Vladimir Oleshchuk for ideas and discussions

The trust matrix

- trust as a positive user attitude
  - ➡ engaging voluntarily
- security based trust issues
  - ➡ building trusted systems
- technological factors
  - ➡ data storage, distribution
  - ➡ insight
- human/societal factors
  - ➡ government
  - ➡ family, friends

SCOTT
Secure Connected Trustable Things

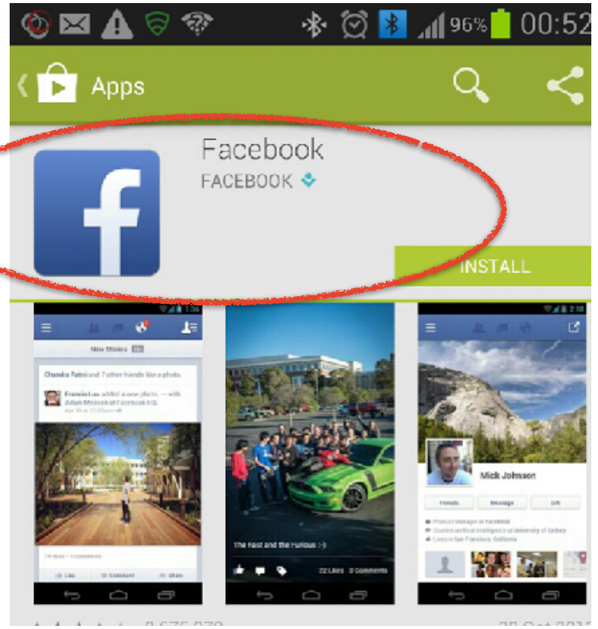
http://SCOTT.IoTSec.no

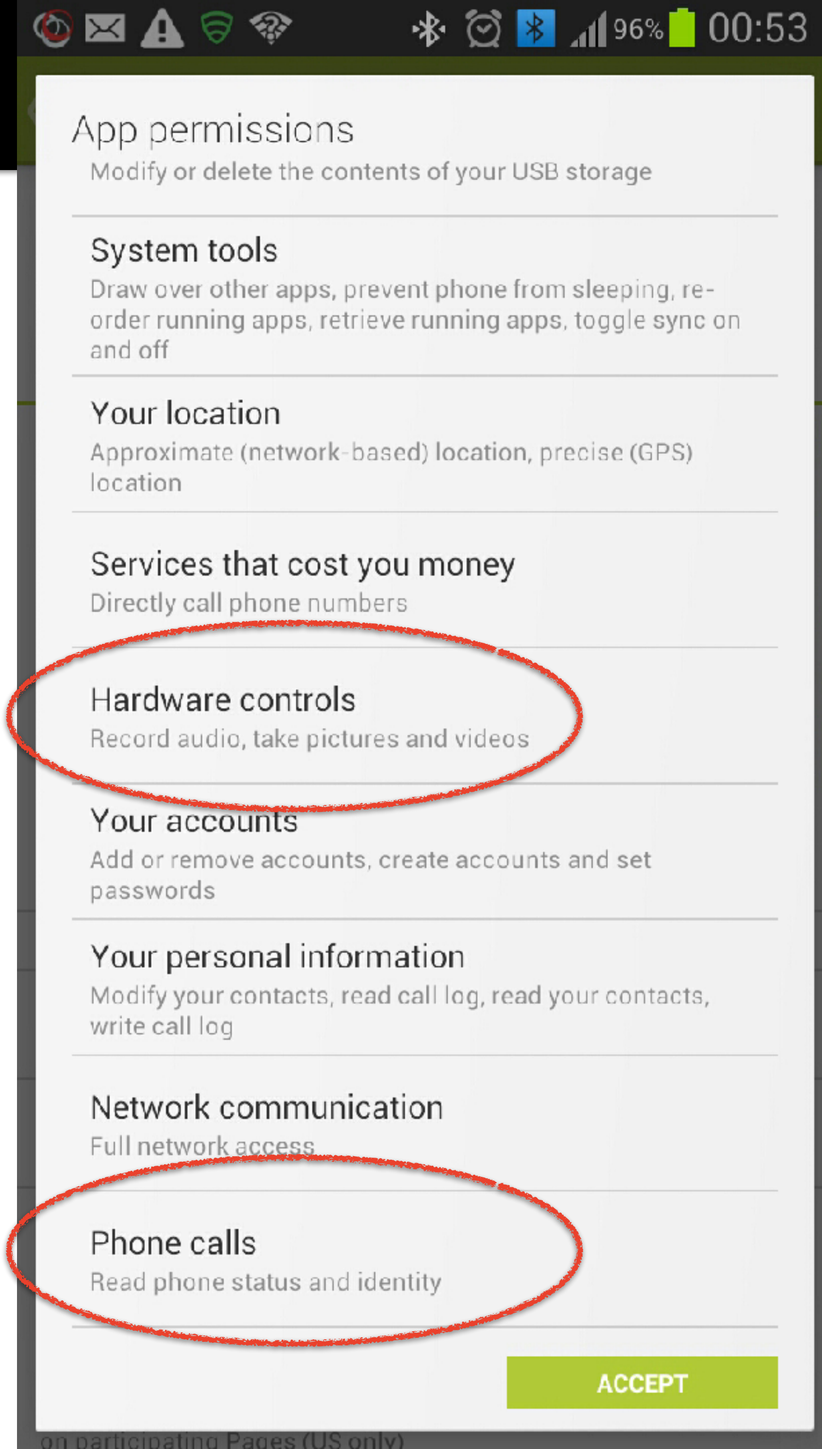
http://SCOTT-project.eu

Trust factor
Security
Privacy (social)
Acceptability
Usability
Reliability
Availability
Maintainability
Safety
Integrity
Confidentiality
Predictability
Reputation (social)
Configurability (social)
Consistency
Functionality

Do I trust Facebook?

- IoT & Mobile merge
  - health applications
  - puls meter
  - blood sugar meter
- Facebook example:
  - record audio
  - read phone status and identity
- For what?





Postulations for a trusted IoT future:

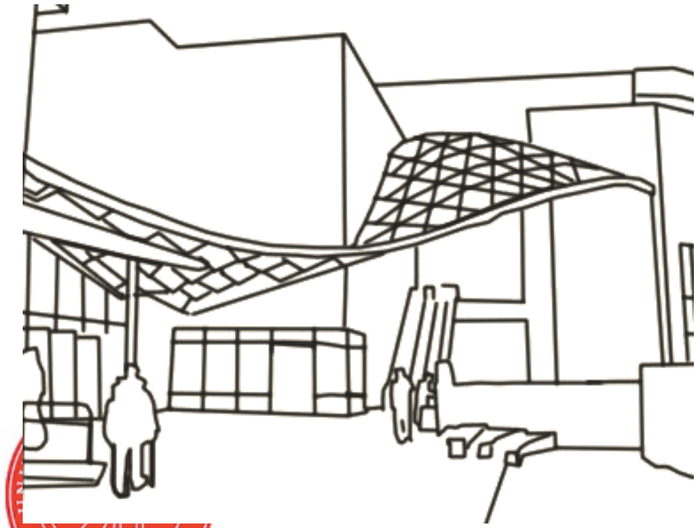
1. Establish secure mechanisms for IoT devices

2. Privacy Labelling for Services and Devices

Addressing the challenges of IoT connectivity

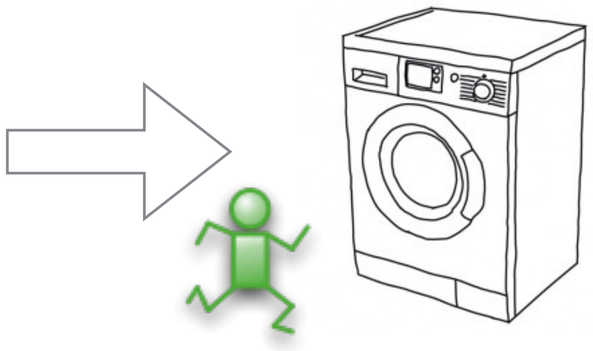
Device ownership

- who owns the device
- which data are going to whom
  - ➡ maintenance



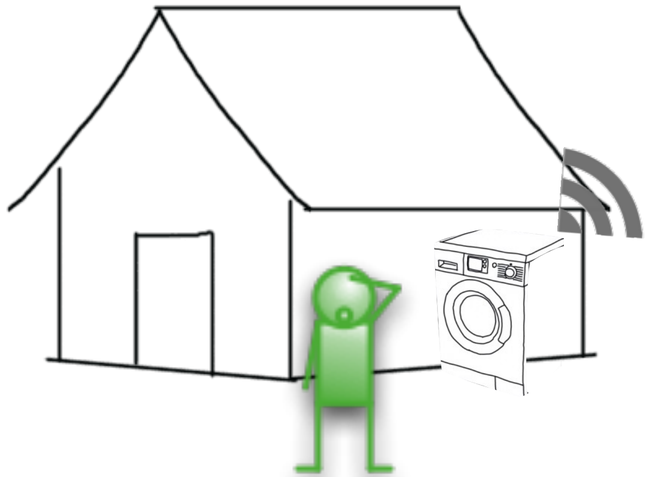
Easyness Setup

- 1. step ownership
- take control



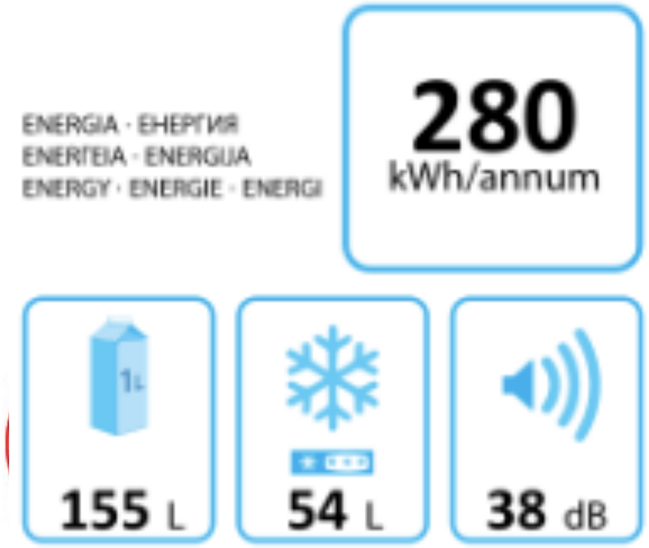
Scalability

- business model for SIM/device not scalable
- free wireless for IoT data



Towards Measurable Privacy - Privacy Labelling

- "Measure, what you can measure - Make measurable, what you can't measure" - Galileo
- Privacy today
  - ➡ based on lawyer terminology
  - ➡ 250.000 words on app terms and conditions
- Privacy tomorrow
  - ➡ A++: sharing with no others
  - ➡ A: …
  - ➡ C: sharing with ….
- The Privacy label for apps and devices

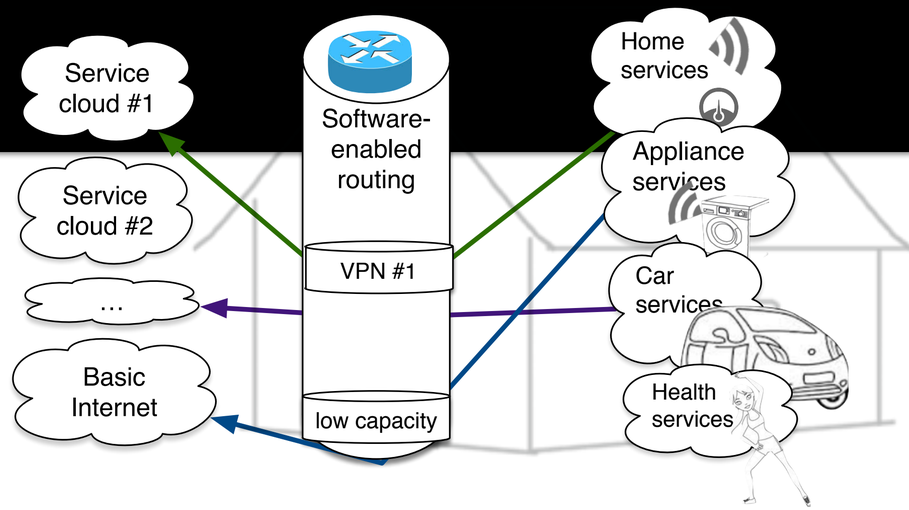


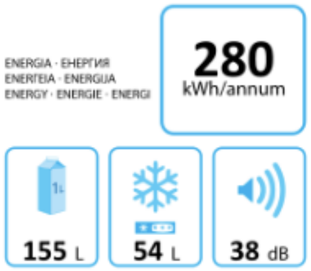
Appfail Report – Threats to Consumers in Mobile Apps

The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.

Conclusions

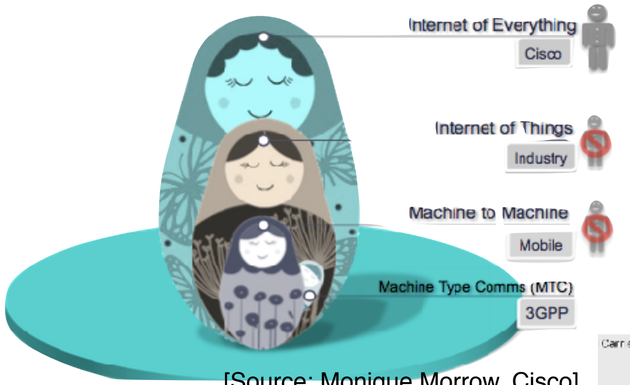
- Things (IoT) are driving the digital societies
- Novel services at home
  - Internet + Semantics + Things = IoT
  - Digitisation of the Society
- IoT Security and privacy
  - privacy/security through network slicing
  - Privacy label (A++, A+…D)
- Free access to basic information: InfoInternet
  - addressing the UN Sustainable Development Goals (SDG 2030)





Conclusions

- Internet of Things (IoT) is a game changer
  - ➡ Unfair advantage in the Nordics
  - ➡ Converting Trust into IoT
- Collaborative approach for a (more) secure society
  - ➡ partnership for secure and privacy-aware applications
- Innovation ecosystem with security and privacy
  - ➡ “let the sensors speak Norwegian”
  - ➡ Pilots for Procedures, Norms & Policies



[Source: Monique Morrow, Cisco]