Universitetet i Oslo

NEMKO Direct: A Global Perspective, 13-15Jun2016, Oslo

Measurable security and privacy for the Internet of Things (IoT)

Josef Noll

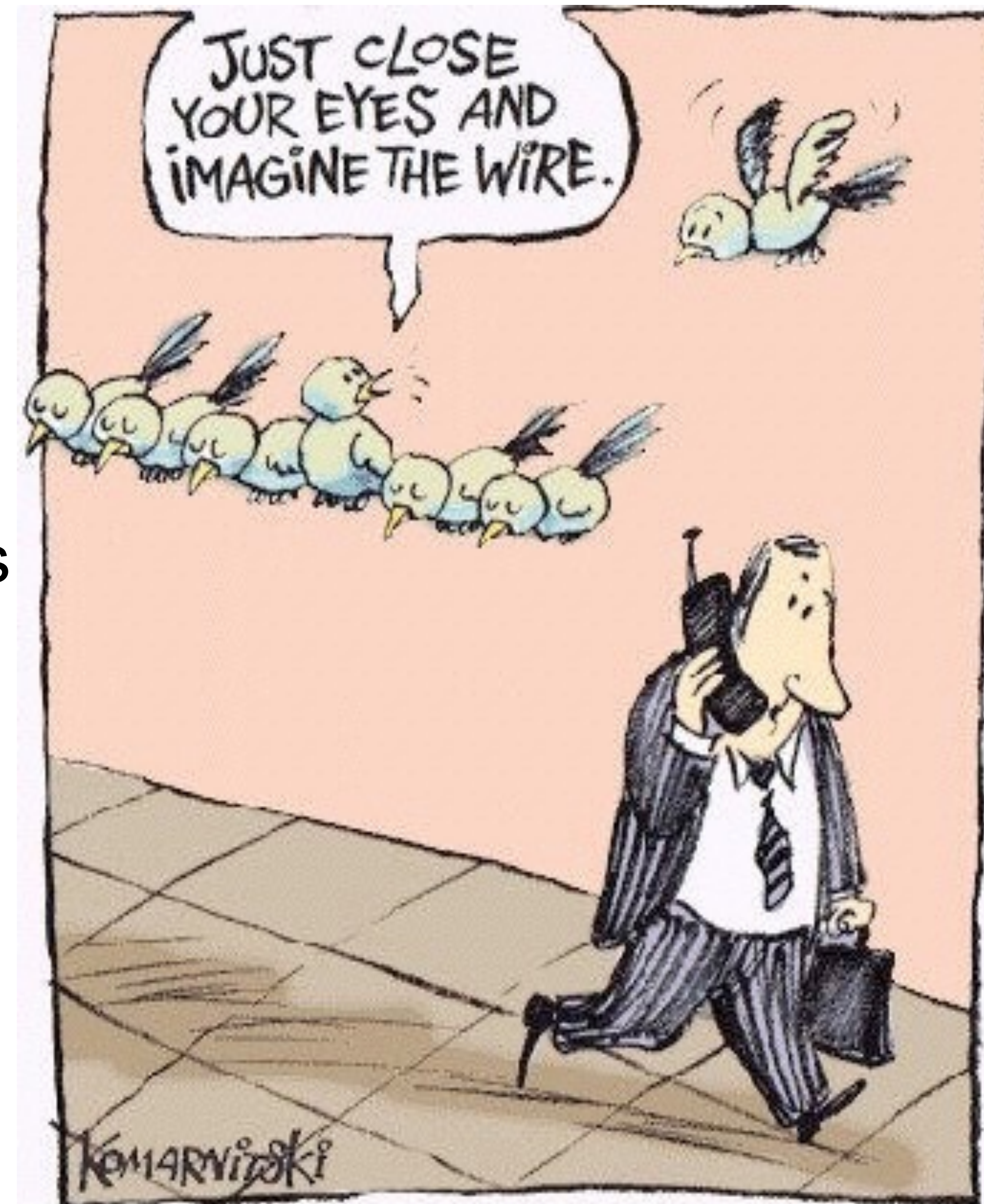Co Founder and Visionary at **Basic Internet Foundation**

Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)

Head of Research at Movation AS

Norway

1

"Our Journey of Today"

- "The last time we were connected by wire was at birth!" [Motorola]
  - ➡ Wireless is everything
  - ➡ The Internet of Things (IoT) challenges
- Smart Grid, Smart Homes, Smart Infrastructures
  - ➡ Scalability in IoT
  - ➡ Measurable Security & Privacy - IoTSec.no
  - ➡ Logic, Cloud,
- "*Some meat for discussion*"
  - ➡ Privacy labelling
  - Basic Internet Foundation

JUST CLOSE YOUR EYES AND IMAGINE THE WIRE.

KOMARNIDSKI

IoTSec.no - Measurable Security and Privacy

Nordic Mobile Plansammling, 8Jun2005

telenor

4G and disruptive technologies

Josef Noll

Researcher, Telenor R&D, N-1331 Fornebu

Prof. stip., Univ. graduate studies, UniK, N-2027 Kjeller

josef@unik.no

what has happened in the last 11 years?

and what is my vision for 2026?

Reality in 2016: Bad indoor coverage

- Telenor will solve challenges of indoor coverage
  - ➡ Voice over Wifi (VoWifi)
  - ➡ Voice of LTE (VoLTE)

VOLTE & VOWIFI

Telenor Norge vil løse innendørsdekningen

Med dårlig innendørsdekning fra mobilnettet vil WiFi redde situasjonen.

AV: ODD RICHARD VALMOT | TELE-KOMMUNIKASJON | PUBLISERT: 24. FEB. 2016 - 09:03

f Facebook   0   Twitter

BARCELONA (digi.no): Telenor Norge benyttet anledningen under Mobile World Congress til å annonsere slutten på dårlig innendørsdekning. Ikke bare vil de løse problemet ved å la telefonene kommunisere via kundenes egne mobiltelefoner, de vil også gi dem veldig mye bedre samtalekvalitet.

http://www.digi.no/artikler/telenor-norge-vil-lose-innendorsdekningen/320592

TU JOBB
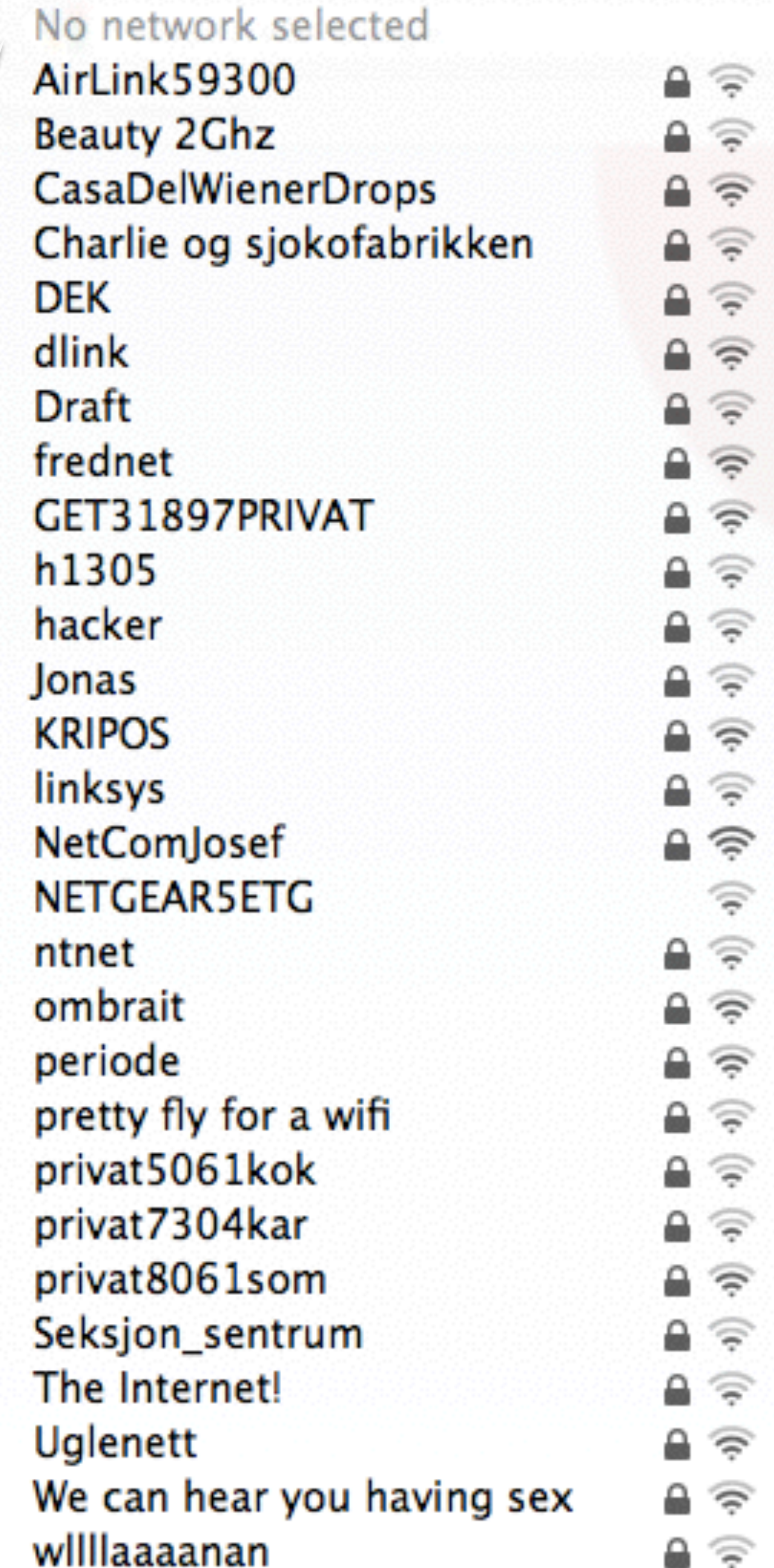
Finn din neste jobb

The world of 2016

Wifi at "Legevakten" Feb2011

- Interference-limited Wifi
  - ➡ increased demand on customer services
  - ➡ "meaningless discussions" on "Wifi"
- Operators in the need of becoming "Digital Companies"
  - ➡ Revenue, Investors?
  - ➡ Digital Ecosystem: Identity, Federation
- 5G dilemma
  - ➡ revenue versus costs
  - ➡ network infrastructure (core vs access network costs)
- Societal challenges
  - Energy, Health, "Internet for all"
  - Security, Privacy, "Digital Societies"

No network selected
AirLink59300
Beauty 2Ghz
CasaDelWienerDrops
Charlie og sjokofabrikken
DEK
dlink
Draft
frednet
GET31897PRIVAT
h1305
hacker
Jonas
KRIPOS
linksys
NetComJosef
NETGEAR5ETG
ntnet
ombrait
periode
pretty fly for a wifi
privat5061kok
privat7304kar
privat8061som
Seksjon_sentrum
The Internet!
Uglenett
We can hear you having sex
wIIIlaaaanan

Addressing the Threat Dimension for IoT

- Hollande (FR), Merkel (DE) had their mobile being mo
- «and we believe it is not happening in Norway?

18. Dezember 2014, 18:14 Uhr   Abhören von Handys

So lässt sich das UMTS-Netz knacken

[source: www.rediff.com]

[source: Süddeutsche Zeitung, 18Dec2014]

Zwei Hacker zeigen
UMTS-antenne lassen
sich knacken (Foto gpa)

Example: Smart Grid Infrastructure

- Smart Meter (customer home)
  - ➡ connected via mesh or directly
  - ➡ proprietary solution (433, 800 MHz band, power line)
- Collector
  - ➡ collects measures
  - ➡ communicates via mobile network
- Mobile Network
  - ➡ as a transmission network
- Cloud (Provider)
  - entry point for remote access
  - Application platform

< Mobile <

Smart Meter
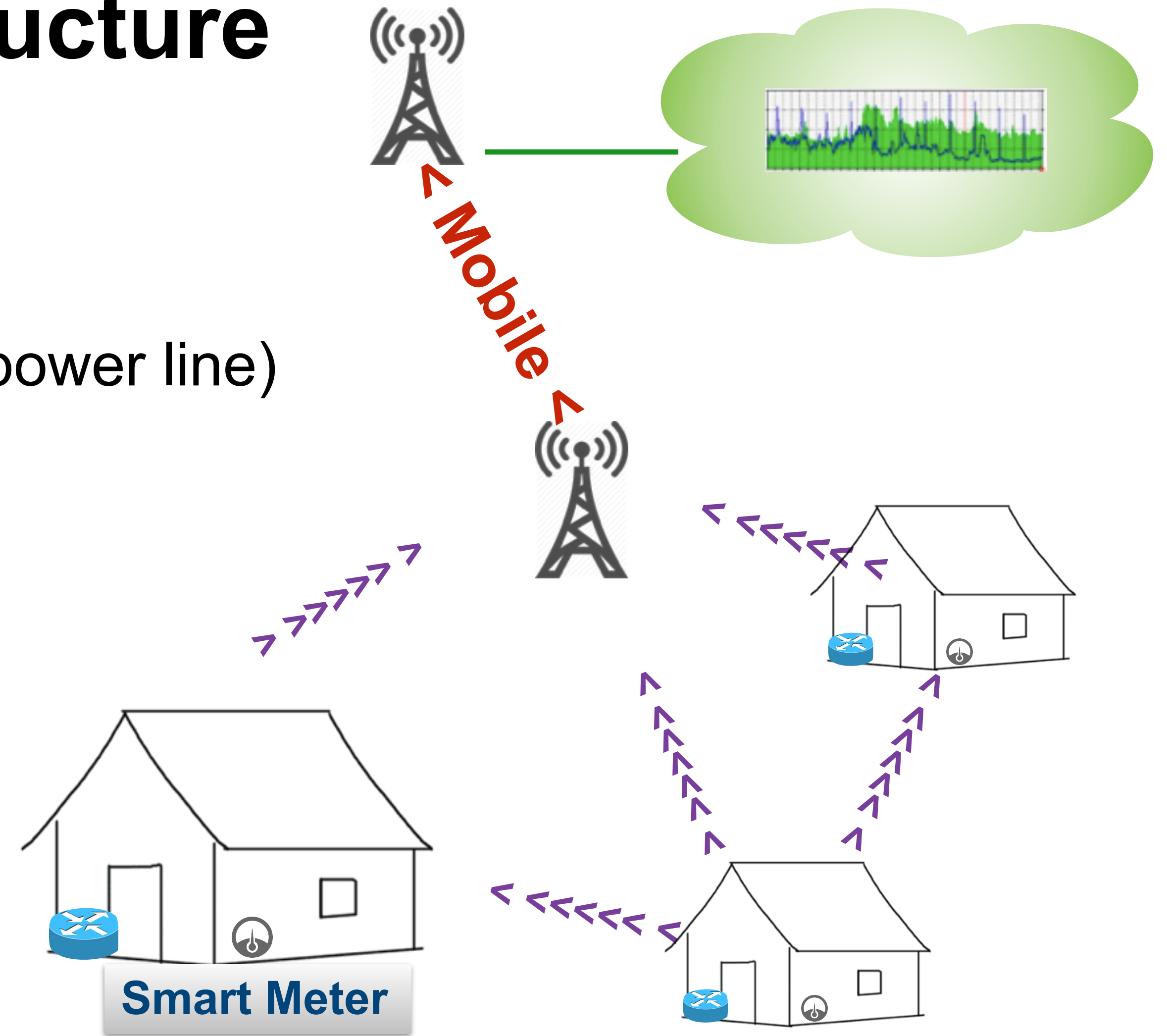
Future Smart Grid operation, § 4-2 functional requirements
"Forskrift om måling, avregning, fakturering av nettjer   mv."

1. Store measured values, registration frequency max 60 min, can configure to min 15 min.
2. **Standardised interface (API) for communication with external equipment using open standards**
3. Can connect to and communicate with other type of measurement units
4. Ensures that stored data are not lost in case of power failure
5. **Can stop and reduce power consumption in every measurement point** (exception transformator)
6. Can send and receive information on electricity prices and tariffs. Can transmit steering information and ground faults
7. Can provide security against miss-use of data and non-wished access to control-functions
8. Register flow of active and re-active power flow in both directions

§ 4-2. Funksjonskrav

AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,

b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,

c) kunne tilknyttes og kommunisere med andre typer målere,

d) sikre at lagrede data ikke går tapt ved spenningsavbrudd,

e) kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg,

f) kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordfeilsignal,

g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og

h) registrere flyt av aktiv og reaktiv effekt i begge retninger.

Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

0   Tilføyd ved forskrift 16 jan 2012 nr. 75 (i kraft 20 jan 2012).

https://lovdata.no/dokument/SF/forskrift/1999-03-11-301

Application Scenarios for Smart Meters

- Monitoring the grid to achieve a grid stability of at least 99,96%,

- Alarm functionality, addressing
  - ➡ failure of components in the grid,
  - ➡ alarms related to the Smart Home, e.g. burglary, fire, or water leakage,

- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,

- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,

- Remote home control, interacting with e.g. the heating system

- Fault tolerance and failure recovery, providing a quick recovery from a failure.

  - Future services
  - ➡ Monitoring of activity at home, e.g. "virtual fall sensor"

GSM/LTE

Admin Cloud
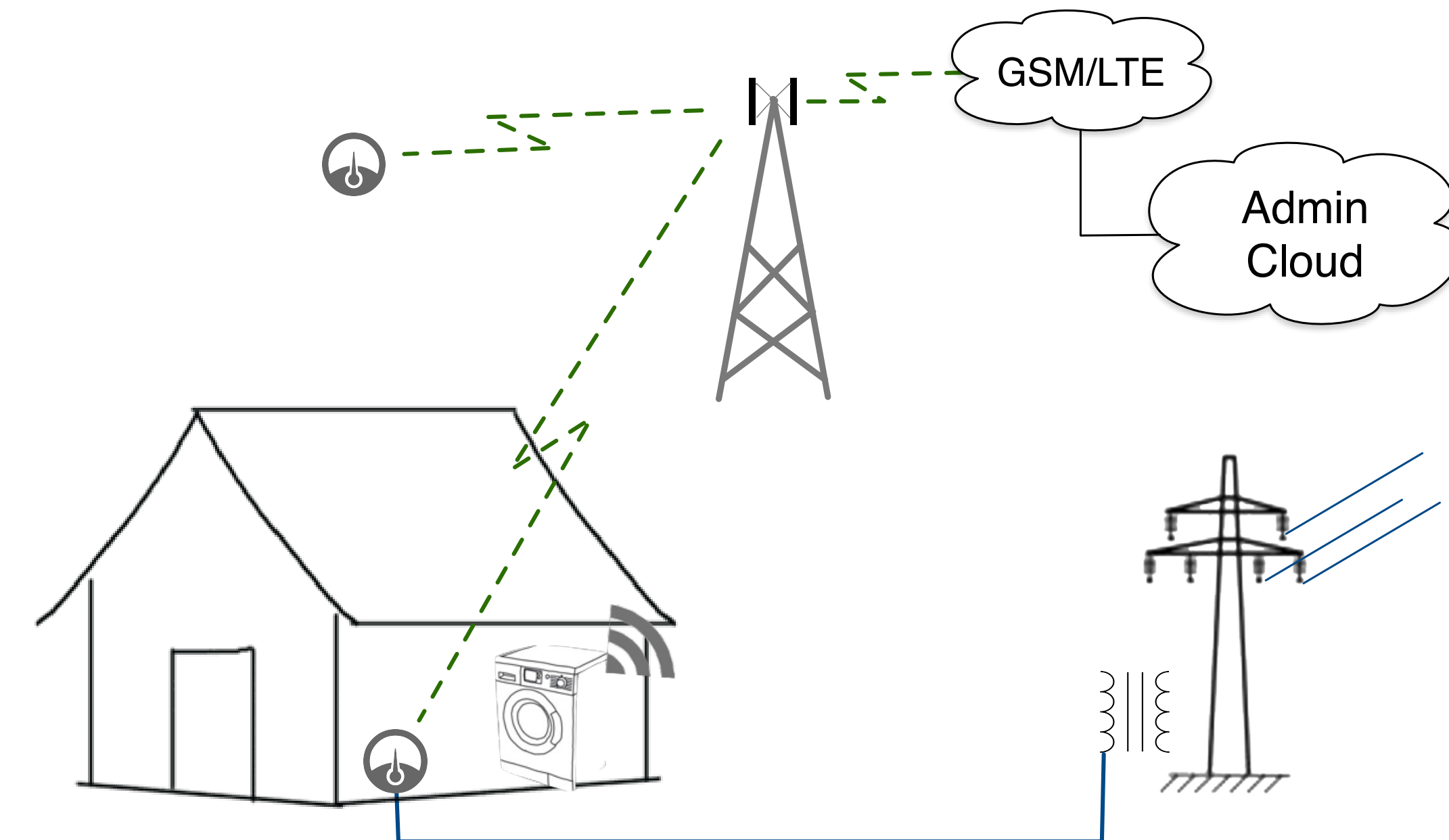
National initiative for a more secure future in IoT
IoTSec.no - Security for IoT for Smart Grids

Home | Research Areas | Security Centre | Publications | About us

The **IoTSec - Security in IoT for Smart Grids** initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Josef Noll Nov
@josefnoll

NCE Smart Partnerkonferansen @KristinHalvorsen og Nasjona...er for Sikkerhet i SmartGrid #IoT...
pic.twitter.com/FLLua94...

«Open World Approach»
everything that is not declared closed is open

Norge Norway
Gjøvik
Kjeller
Oslo
Halden

IoTSec.no - Measurable Security and Privacy

Partners and Collaborations

- UiO
- UNIK
- NR
- Simula
- NTNU

Academia

- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

Industry

- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet

Interest Org.

- EyeSaaS
- mnemonic

Industry

- Mondragon Unibersitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo
- H2020 and ECSEL projects

International

Topics for potential Master Thesis?

Topics for Master Thesis [edit]

Open Master Thesis related to IoTSec

- Privacy labels for IoT consumer products (Supervisor(s): Josef Noll, Hanne Brostrøm)
- Building an Attack Simulator on the Electric Grid Infrastructure (Supervisor(s): György Kálmán,
- Security challenges of open low-capacity wifi access (Supervisor(s): Josef Noll)
- Semantic Modeling of a Smart Home Infrastructure (Supervisor(s): Josef Noll, Christian Johans
- Risk Assessment tool analysis for Industrial Automation and Control Systems (Supervisor(s): N Chowdhury, Judith Rossebø, Josef Noll)
- Prosumers for the future smart electricity grid (Supervisor(s): Josef Noll)
- Measurable Security for Sensor Communication in the Internet of Things (Supervisor(s): Josef Chowdhury)

IoTSec

| Home | Research | Security Centre | Publications | Student corner |

Student Corner for IoTSec [edit]

Please be welcome to the Student Corner for *Security and Privacy in the Internet of Things (IoT)*.

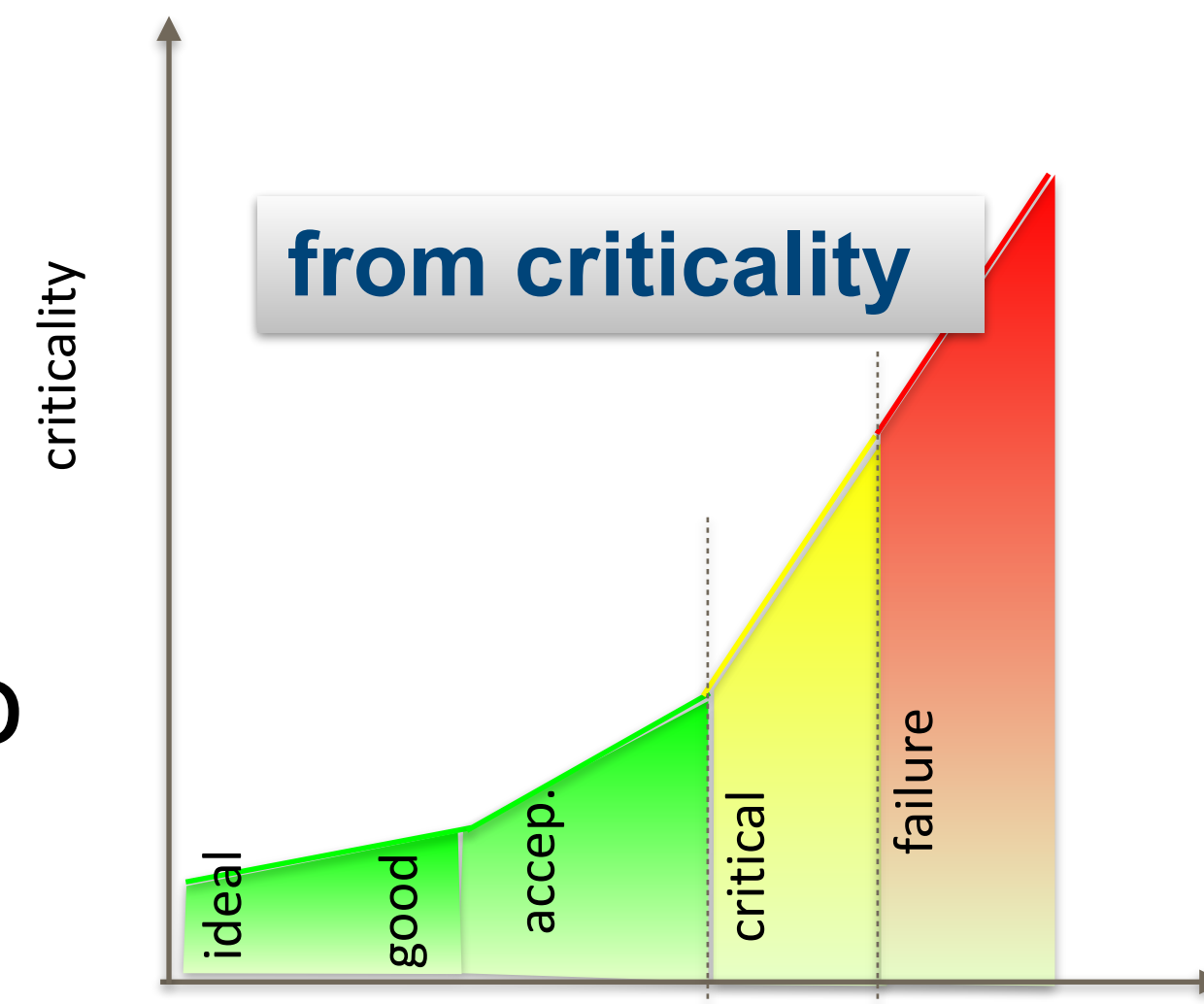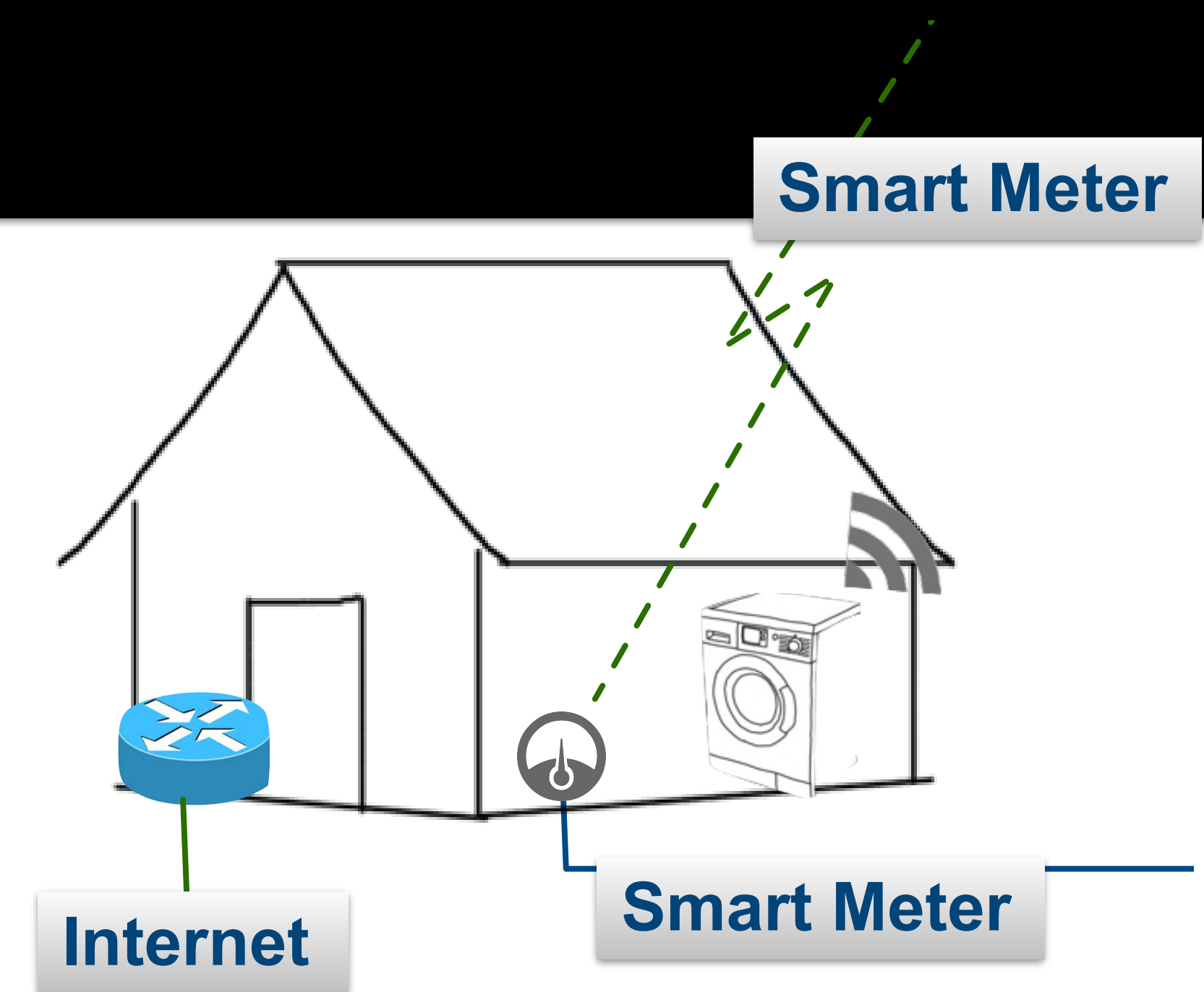Feel free to have a look at UNIK4750 course related to the project.

Ongoing Master Thesis related to IoTSec

- Smart Meter Security Analysis (Editor: Christian Resell, Hans Jørgen Furre Nygårdshaug, Mehdi Noroozi)
- The human aspect in Smart grids (from Security and Privacy point of view) (Editor: Linn Eirin Paulsen)
- Pervasive computing in smart electricity grid (Editor: Kaniz Fatema Tuly)

Upcoming Infrastructure

- ## Smart Meter
  - ➡ read and control
  - ➡ logic?

- ## Smart Home
  - ➡ intelligent devices
  - ➡ on-demand regulation

- ## Challenges
  - ➡ Logic: Centralised <—-> Fog
  - ➡ Smart Meter: Information <—> Control
  - ➡ Smart Grid Information <—> Internet Info

Smart Meter

Internet

Smart Meter

from criticality

criticality

ideal | good | accep. | critical | failure

to measurable: security, privacy and dependability

SPD level	SPD vs SPD$_{Goal}$
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)

Towards Measurable Privacy - Privacy Labelling

ENERGIA · ЕНЕРГИЯ
ENEΡΓΕΙΑ · ENERGIJA
ENERGY · ENERGIE · ENERGI

280 kWh/annum

155 L   54 L   38 dB
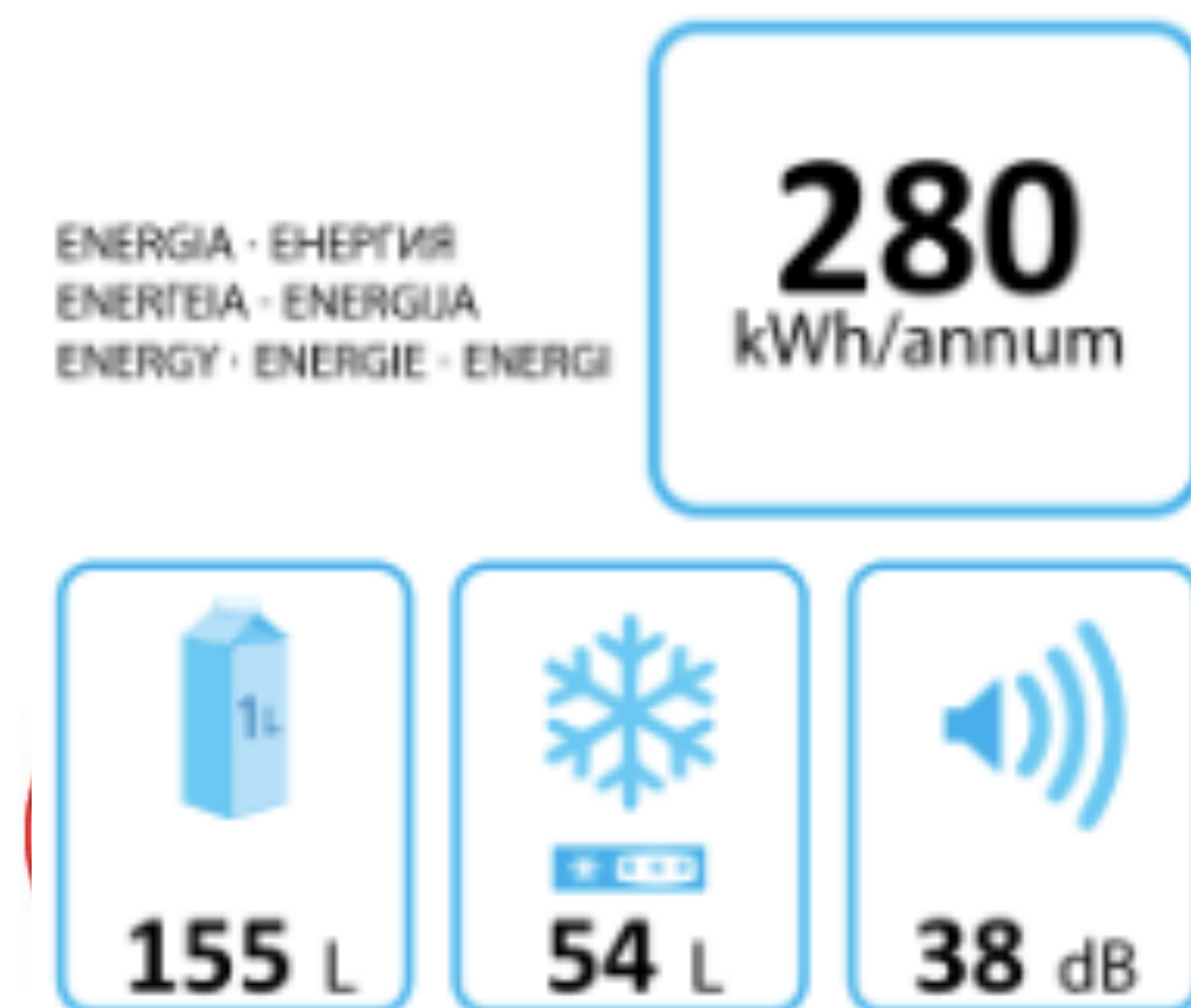
- "Measure, what you can measure - Make measurable, what you can't measure" - Galileo
- Privacy today
  - ➡ based on lawyer terminology
  - ➡ 250.000 words on app terms and conditions
- Privacy tomorrow
  - ➡ A++: sharing with no others
  - ➡ A: …
  - ➡ C: sharing with ….
- The Privacy label for apps 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.

Addressing the challenges of IoT connectivity

Device ownership

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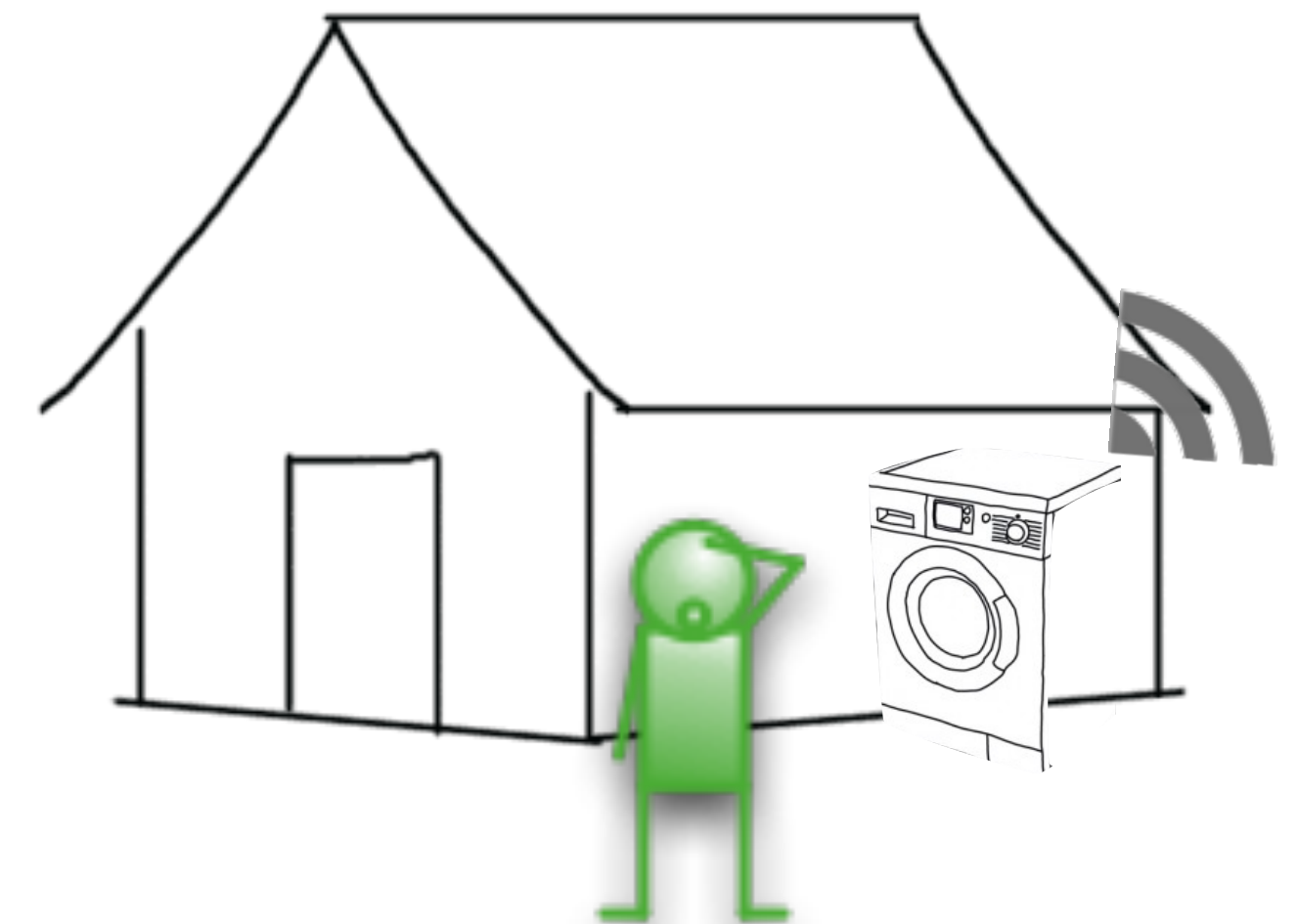- which data are going to whom
  - ➡ maintenance

Easyness Setup

- 1. step ownership
- take control

Scalability

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

Future Service Requirements (in a wireless infrastructure)

- *"we have no control of what is going on in Wifi"*
- "only 25% of broadband customers experience the speed they got promised"
- more than 75% of all calls to ISPs is related to wireless
- over 90% of boxes sent to ISP are fully functionable
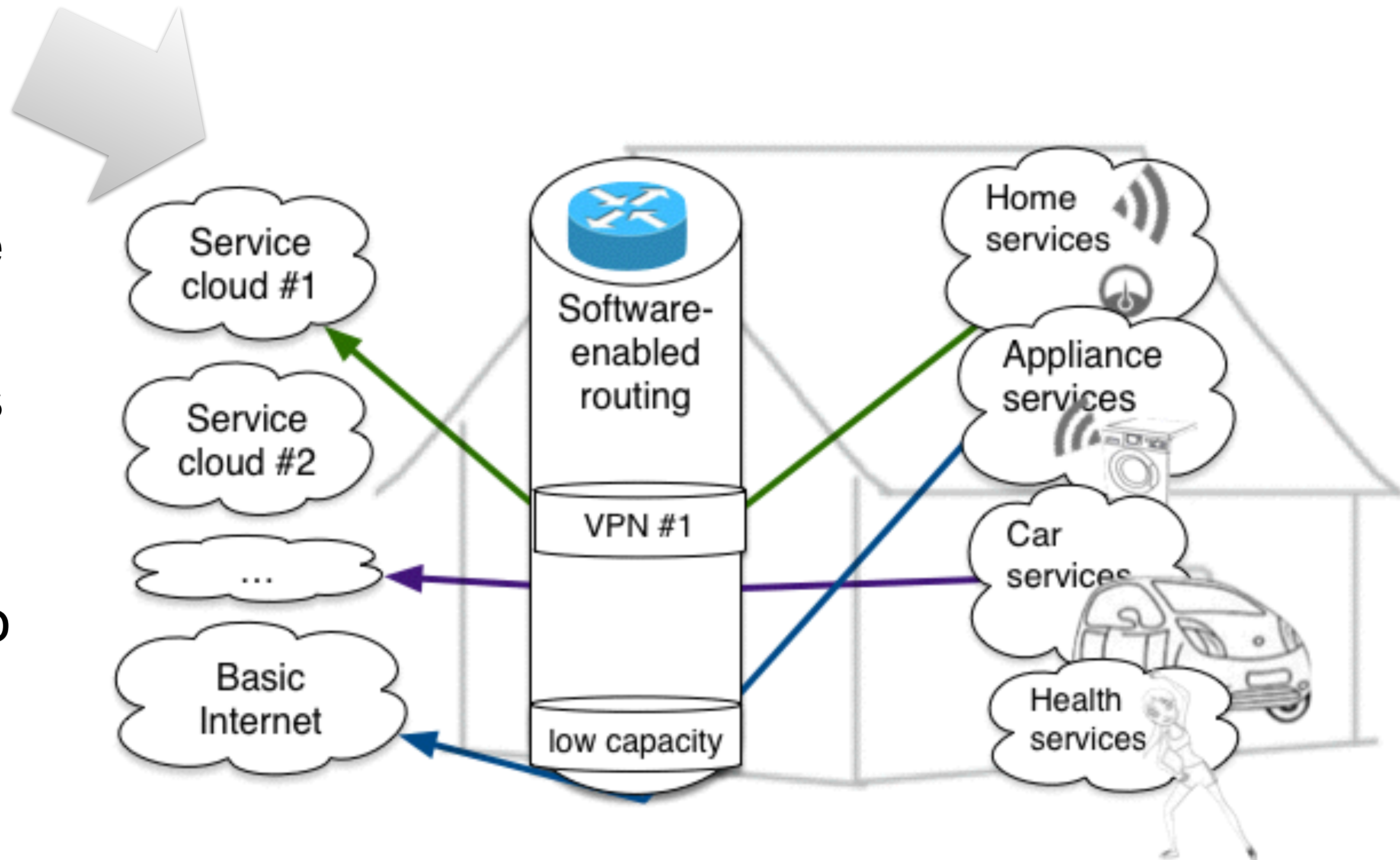
Motivation
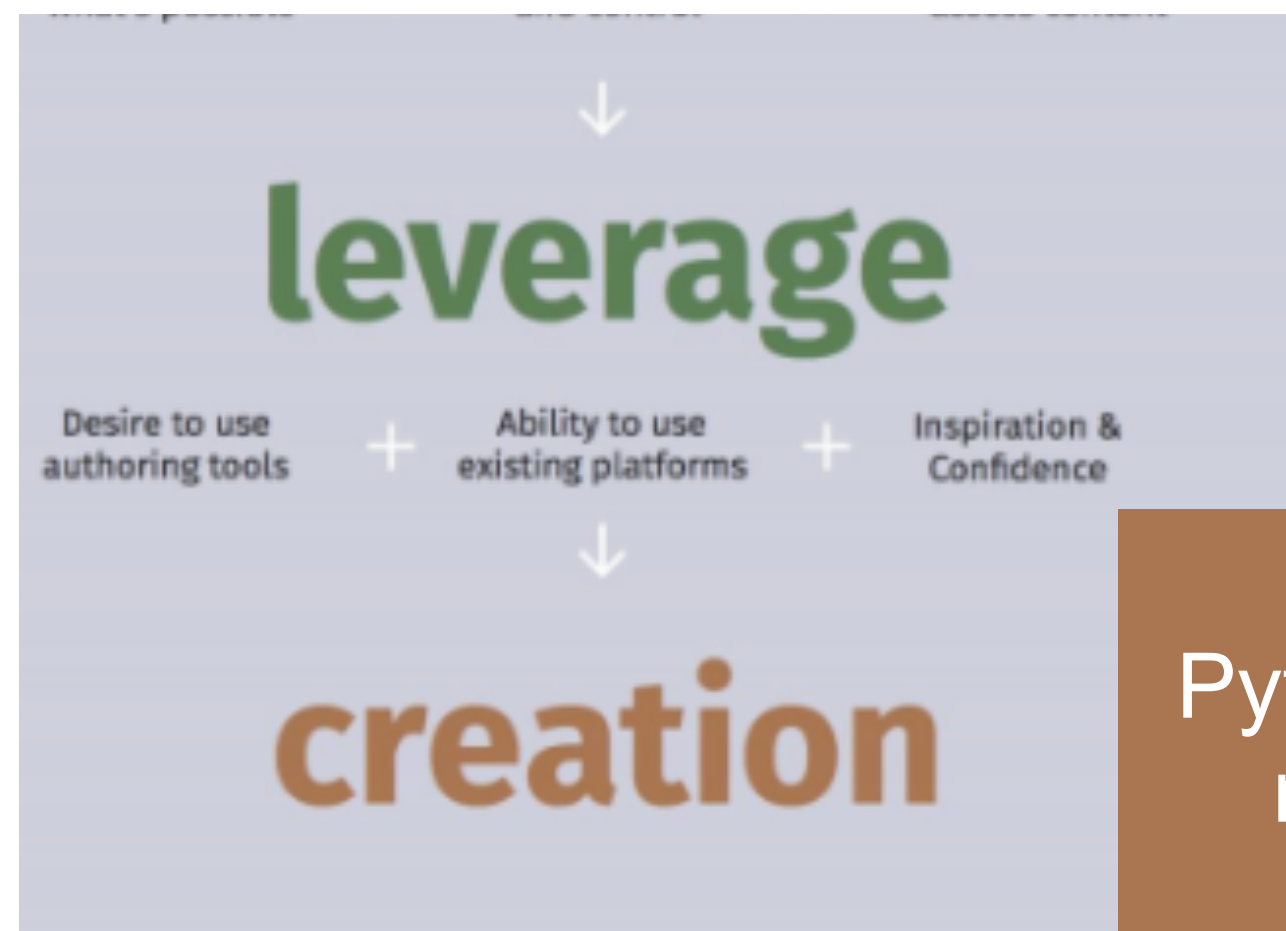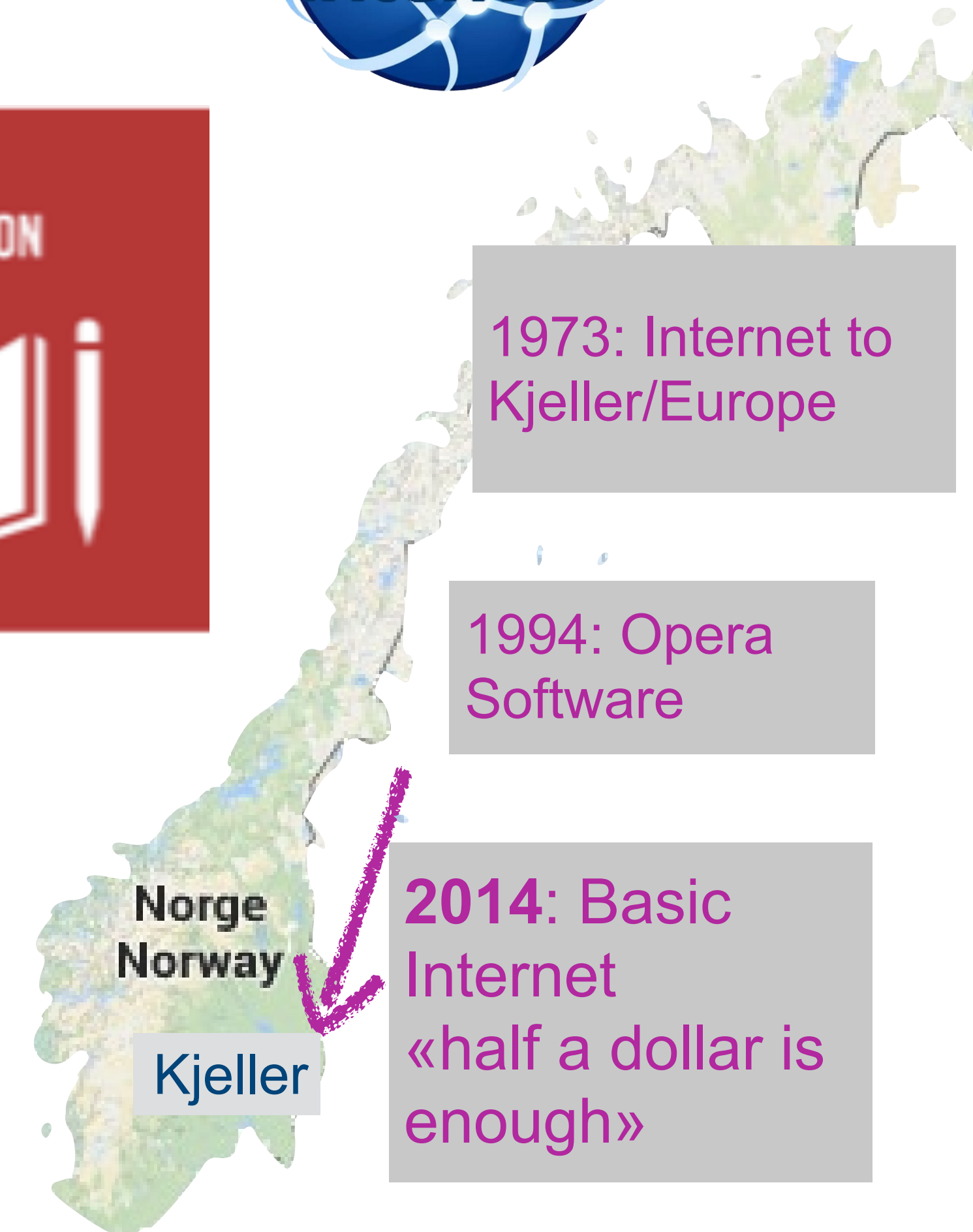# "Need to close the digital gap"

- The Global Goals:
  Norway is the secretariat for
  Quality Education

- Internet history
  - 1973 Europe through Kjeller
  - 1994 Opera Software
  - 2014 Basic Internet Foundation

THE GLOBAL GOALS
For Sustainable Development

4 QUALITY EDUCATION

Basic Internet

1973: Internet to Kjeller/Europe

1994: Opera Software

Norge Norway

Kjeller

2014: Basic Internet «half a dollar is enough»

leverage

Desire to use authoring tools + Ability to use existing platforms + Inspiration & Confidence

creation

"Internet is my teacher"

"I'm currently learning Python and HTML, so I can make a website for my parents' business"

June2016, Josef Noll   **16**

The vision of 2026

- "Digital and Inclusive Society"
- Networks adopting to service needs
  ➡ Security, privacy, dependability
- "the Road Network Infrastructure"
- Low-capacity Internet
  ➡ free and open access
- Broadband services
  ➡ authenticated access

or
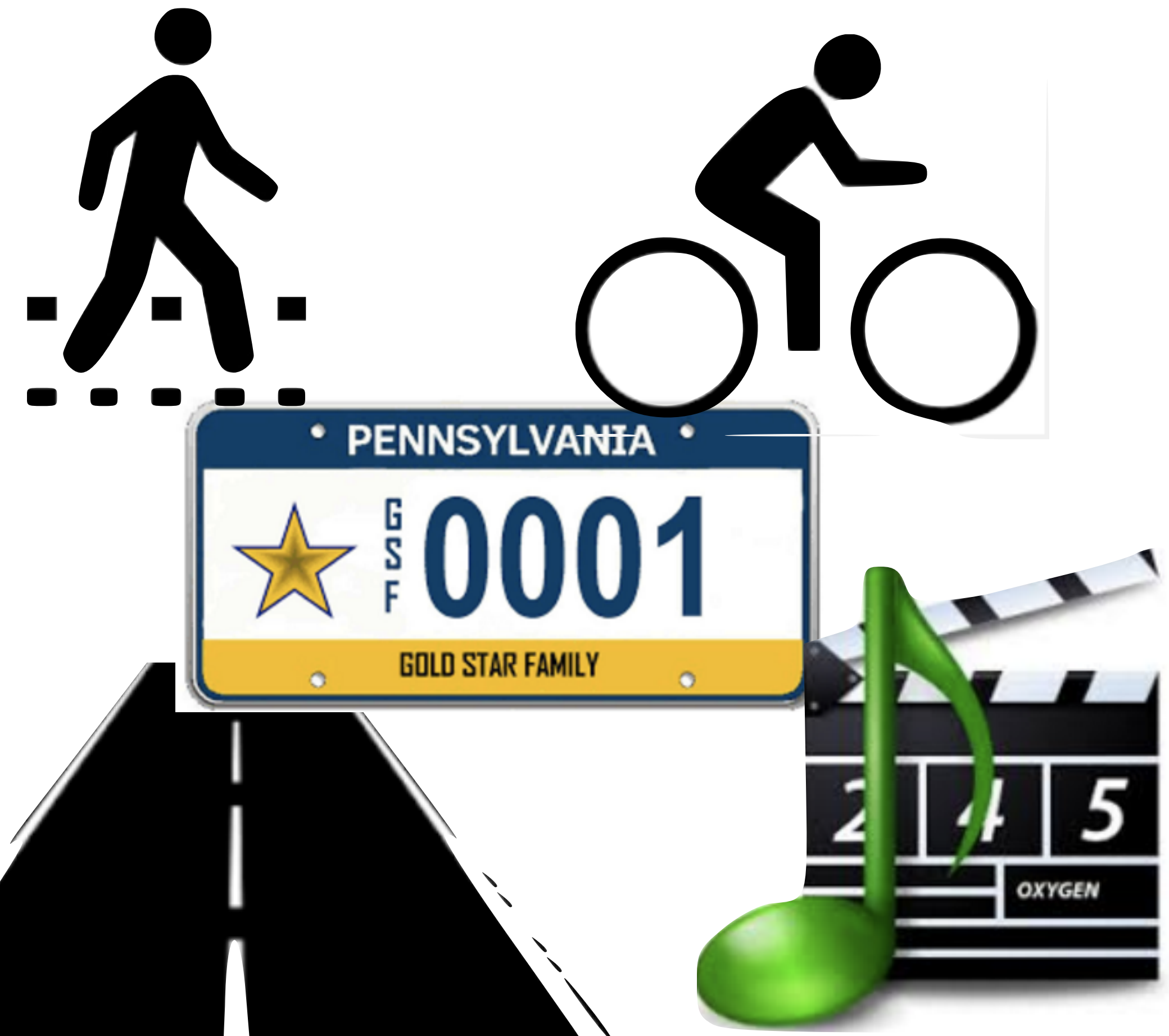
Conclusions

- Internet of Things (IoT) is a game changer
  - ➡ Everything is wireless: Smart Infrastructures
  - ➡ Autonomous systems, Critical Infrastructure
- Collaborative approach for a (more) secure society
  - ➡ trust is not enough, need for measurable
  - ➡ partnership for security: threats, measures, counter activities
- Measurable Security and Privacy for IoT
  - ➡ IoTSec.no - Security for Smart Grid
  - ➡ Industrial impact: Security Centre for Smart Grid
  - ➡ Privacy labelling for apps and devices
- Innovation ecosystem for the IoT
  - Reducing the digital gap
  - Providing Basic Internet to everyone

SPD level	SPD vs SPD$_{Goal}$
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)