Center for Wireless Innovation Norway
cwin.no

CWI
Norway

UNIK
UNIVERSITY GRADUATE CENTER

Int. Conference on Mobility 2012, Venice, Oct2012

Security, Privacy and Dependability in Mobile Networks

Josef Noll, Sarfraz Alam, Zahid Iqbal, Mohammad M. R. Chowdhury

Prof. at University of Oslo/UNIK

Member of CWI Norway

josef@unik.no

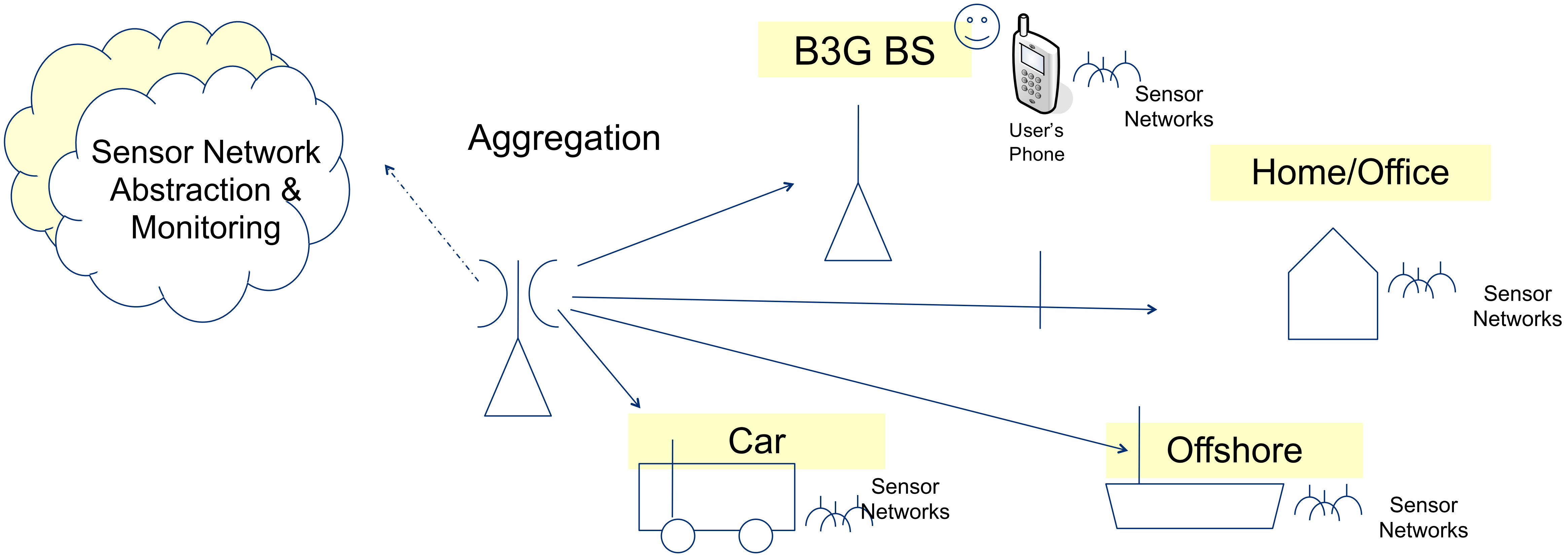
Outline

- About the author
- Security in Mobile Netwo
  - Privacy
  - Dependability
- The way ahead: Internet of Things
  - connection of sensors to mobile
  - business decisions based on information
- Security Challenges
  - BYOD “bring your own device”
  - Be aware of the value of information
  - Measurable security
- Use case for
  - From Entertainment to Socialtainment
  - Sensor data fusion
- Conclusions

Josef Noll, Oslo - CTO
Steering board member, Norway section at MobileMonday
Chief technologist at Movation AS, Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)
IARIA Fellow, Chairman of IARIA’s Intern. Conf. on Mobility
Past: Research Manager/Researcher at Telenor R&I (R&D)
Staff member at ESA ESTEC
Chip designer at SIEMENS

Center for Wireless Innovation

A facilitator for industry and seven research institutions to form strategic partnerships in wireless R&D



Høgskolen i Telemark

NTNU

UNIK
UNIVERSITETSSTUDIENE PÅ KJELLER

Universitetet i Stavanger

UNIVERSITETET I AGDER

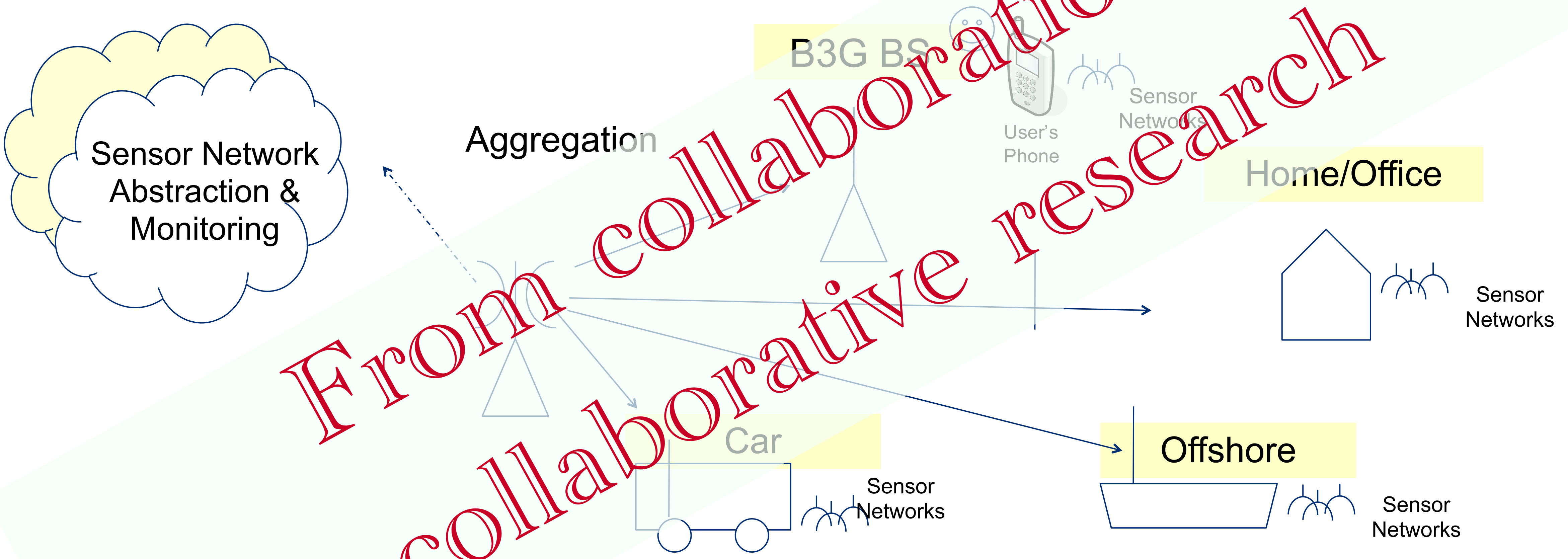
UNIVERSITETET I OSLO

HØGSKOLEN I BERGEN

Center for Wireless Innovation

CWI

A facilitator for industry and seven research institutions to form strategic partnerships in wireless R&D



From collaboration to collaborative research

Høgskolen i Telemark

NTNU

UNIK UNIVERSITETSSTUDIENE PÅ KJELLER

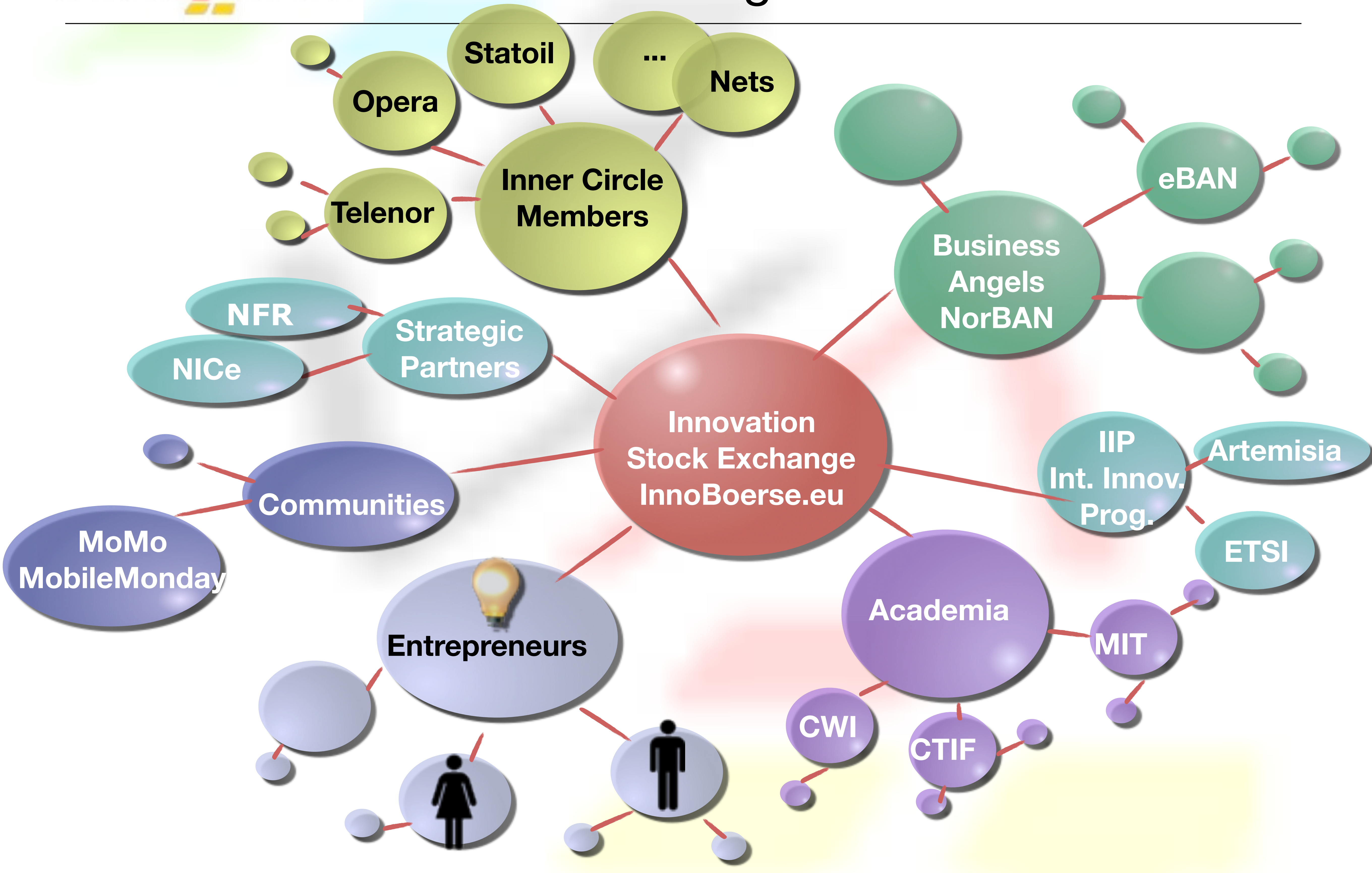
Universitetet i Stavanger

UNIVERSITETET I AGDER

UNIVERSITETET I OSLO

HØGSKOLEN I BERGEN

Innovation through Collaboration

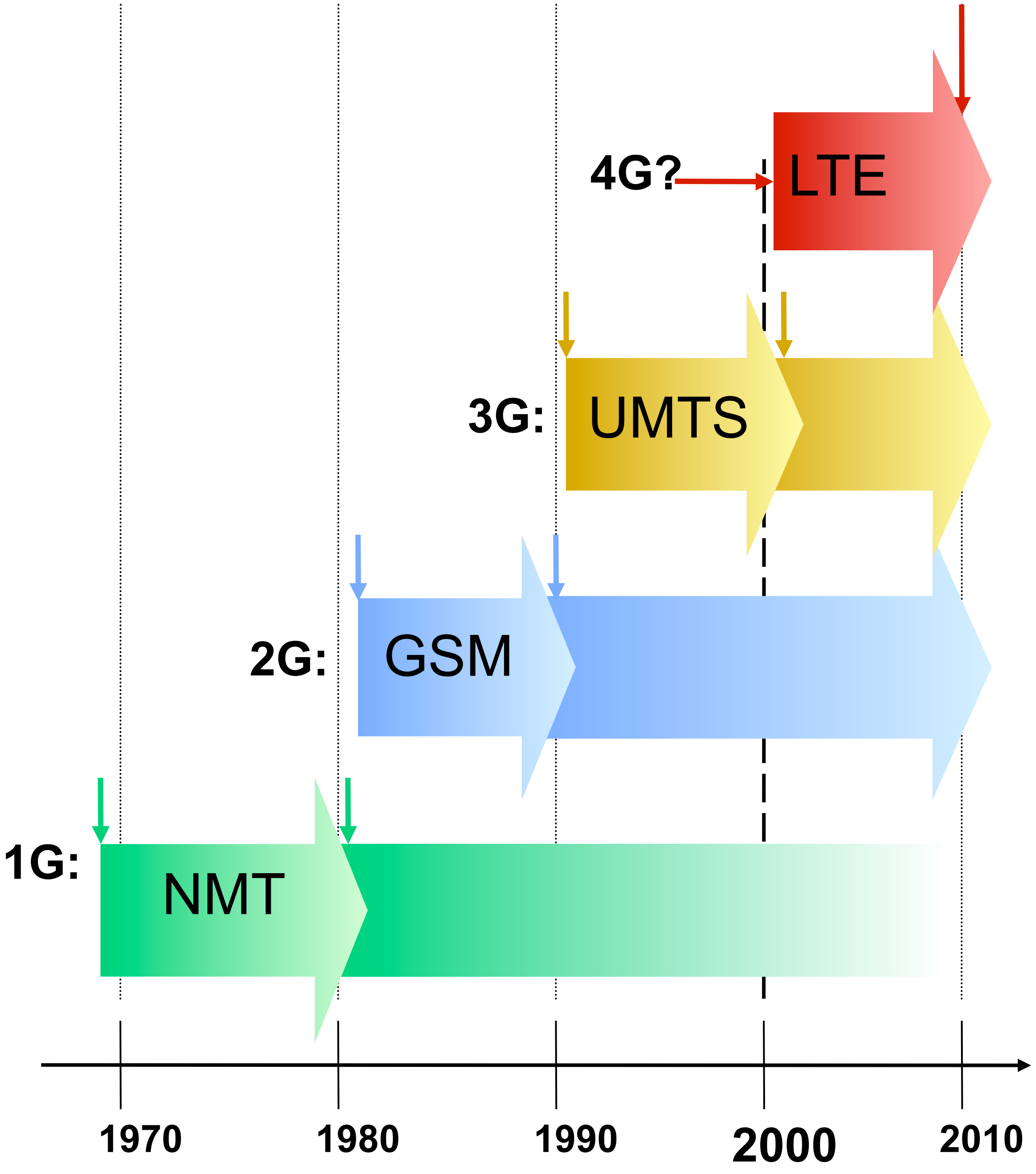


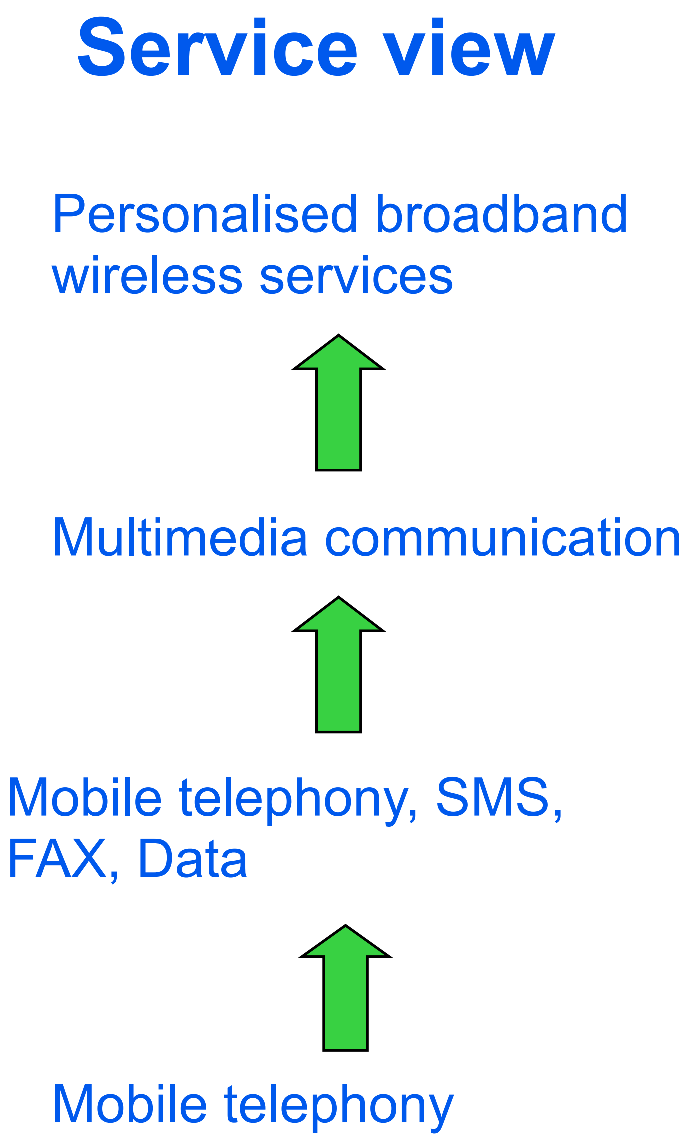
Providing the infrastructure for open collaboration

Outline

- About the author
- Security in Mobile Networks
  - Privacy
  - Dependability
- The way ahead: Internet of Things
  - connection of sensors to mobile
  - business decisions based on information
- Security Challenges
  - BYOD “bring your own device”
  - Be aware of the value of information
  - Measurable security
- Use case for
  - From Entertainment to Socialtainment
  - Sensor data fusion
- Conclusions

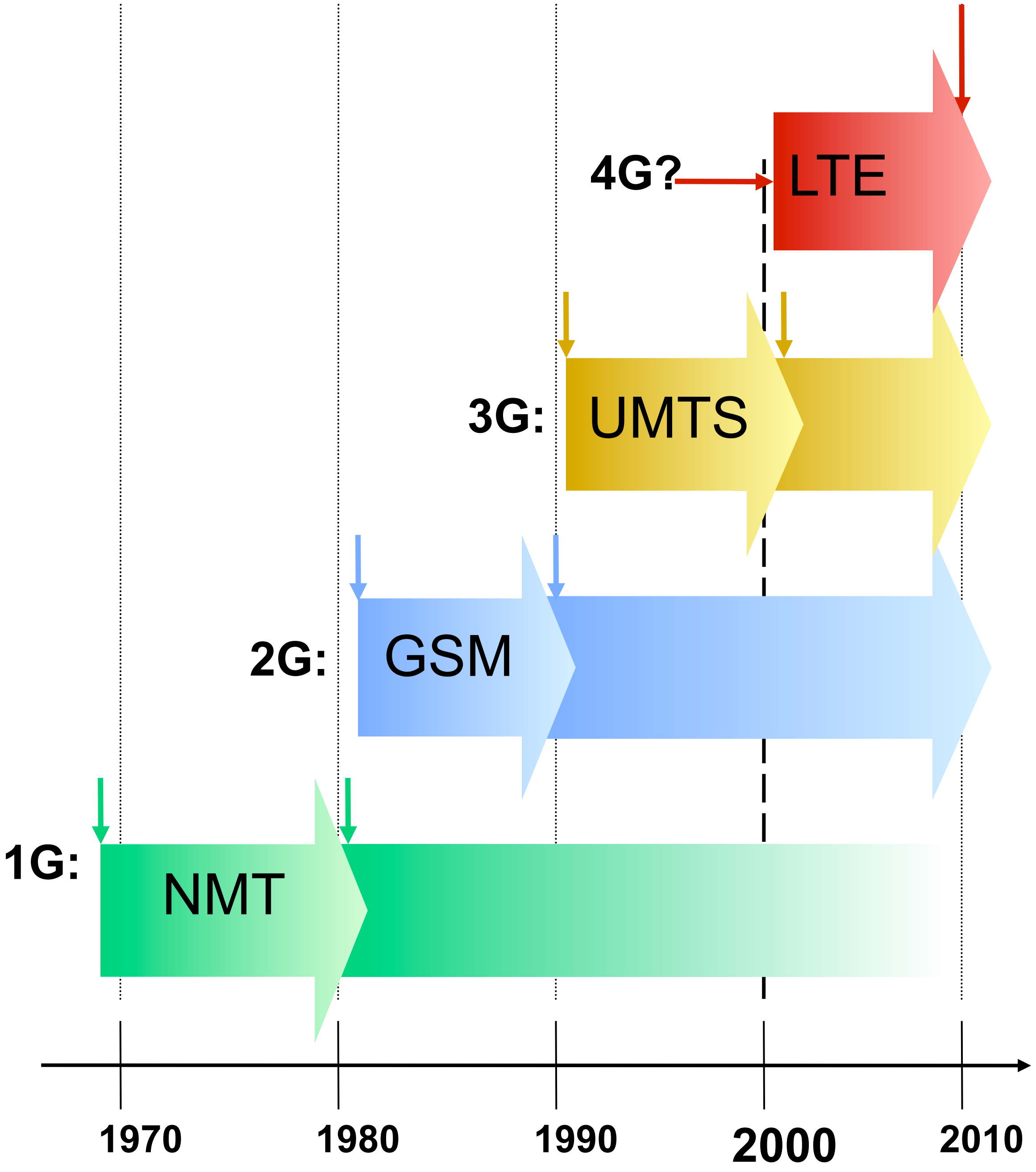
Generations of Mobile Networks




Service view
Personalised broadband wireless services
Multimedia communication
Mobile telephony, SMS, FAX, Data
Mobile telephony

[adapted from Per Hjalmar Lehne, Telenor, 2000]

Generations of Mobile Networks



Service view

Personalised broadband wireless services

Multimedia communication

Mobile telephony, SMS, FAX, Data

Mobile telephony

Security view

IP security with heterogeneous access, sensors

Open, modular security architecture - force 2G

One way authentication, encryption visibility, “obscurity”

tap the line, connect in

[adapted from Per Hjalmar Lehne, Telenor, 2000]

Security in Mobile Networks

- NMT
  - tap the line
- GSM
  - No authentication of network: IMSI catcher pretend to be BTS and request IMSI
  - Undisclosed crypto algorithms
- UMTS
  - adds integrity and freshness checks on signalling data from network to MS
  - forced attack to 2G
- LTE
  - full IP security package
  - heterogeneous access networks

[Source: Lars Strand: "Security Architecture for Mobile Telephony Systems", PhD presentation, UiO, 2011]]

Summary of Mobile Security

Threats/attacks	Security services	Security mechanisms
GSM		
Cloning	Authentication	Authentication mechanism (challenge-response with a shared secret)
Eavesdropping (voice sent in clear)	Confidentiality	Encryption of call content (A5/1, A5/2, A5/3)
Spying (identity tracking)	Confidentiality	Location security (TMSI)

[adopted from: Lars Strand: "Security Architecture for Mobile Telephony Systems", PhD presentation, UiO, 2011]]

Summary of Mobile Security

Threats/attacks	Security services	Security mechanisms
GSM		

Threats/attacks	Security services	Security mechanisms
UMTS		
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

[adopted from: Lars Strand: “Security Architecture for Mobile Telephony Systems”, PhD presentation, UiO, 2011]]

Summary of Mobile Security

LTE

Threats/attacks	Security services	Security mechanisms
GSM		

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	fast re-authentication? different access network?

[adopted from: Lars Strand: “Security Architecture for Mobile Telephony Systems”, PhD presentation, UiO, 2011]]

Summary of Mobile Security

GSM

Threats/attacks	Security services	Security mechanisms
Cloning	Authentication	Authentication mechanism (challenge-response with a shared secret)
Eavesdropping (voice sent in clear)	Confidentiality	Encryption of call content (A5/1, A5/2, A5/3)
Spying (identity tracking)	Confidentiality	Location security (TMSI)

UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

LTE

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	fast re-authentication? different access network?

[adopted from: Lars Strand: “Security Architecture for Mobile Telephony Systems”, PhD presentation, UiO, 2011]]

Security in Mobile Networks

- Main focus so far on accountability (for billing)
- End-to-end encryption is a challenge
  - Interoperability: variety of access networks, coding
  - key handling in TLS
  - application specific solutions: SIP
- Privacy
  - personal privacy
  - business value privacy
- Dependability, reliability
  - infrastructures
  - systems of systems

[Source: Lars Strand: “Security Architecture for Mobile Telephony Systems”, PhD presentation, UiO, 2011]]

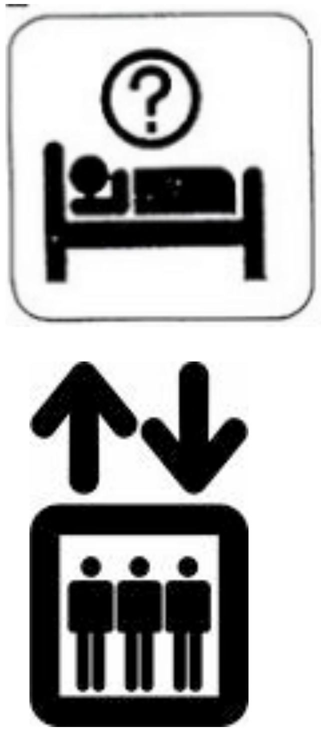
Physical vs Organisational privacy

- don’t touch me
- don’t invade
- preferences

- locations

Physical vs Organisational privacy

- don't touch me
- don't invade
- preferences



- locations

- What is in Coca Cola?
- When will VW launch the new Golf?

Value of Information

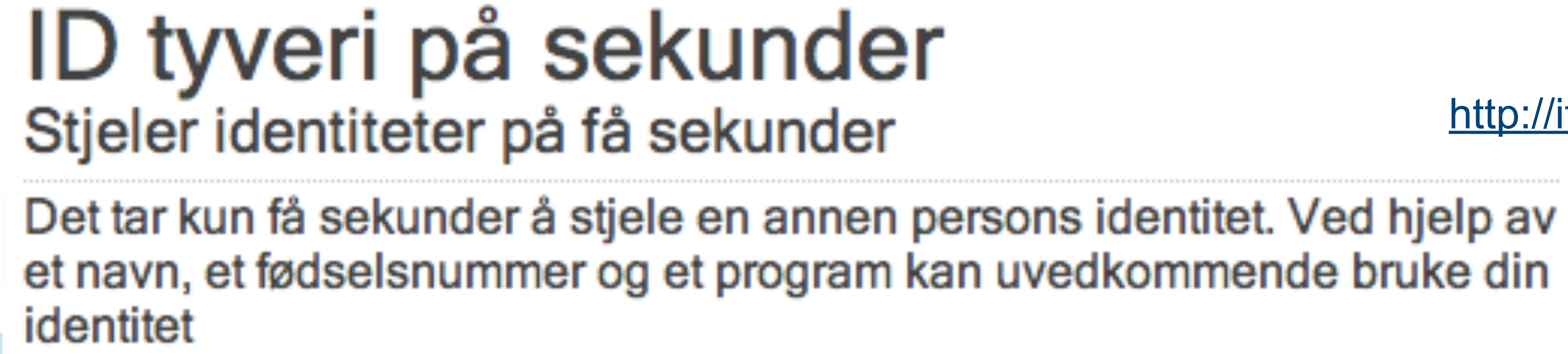
- Access to fingerprints of all people

Protecting the identity?

- 8 million US residents victims of identity theft in 2006 (4% of adults)
- US total (known) cost of identity theft was $49 billion
  - ~10% was paid by customers
  - remaining by merchants and financial institutions

- Average victim spent $531 and 25 hours to repair for damages

Source: Lasse Øverlier & California Office of Privacy Protection



ID tyveri på sekunder

Stjeler identiteter på få sekunder

Det tar kun få sekunder å stjele en annen persons identitet. Ved hjelp av et navn, et fødselsnummer og et program kan uvedkommende bruke din identitet

ID theft in seconds
http://itpro.no/art/11501.html

Outline

- About the author
- Security in Mobile Networks
  - Privacy
  - Dependability
- The way ahead: Internet of Things
  - connection of sensors to mobile
  - business decisions based on information
- Security Challenges
  - BYOD “bring your own device”
  - Be aware of the value of information
  - Measurable security
- Use case for
  - From Entertainment to Socialtainment
  - Sensor data fusion
- Conclusions

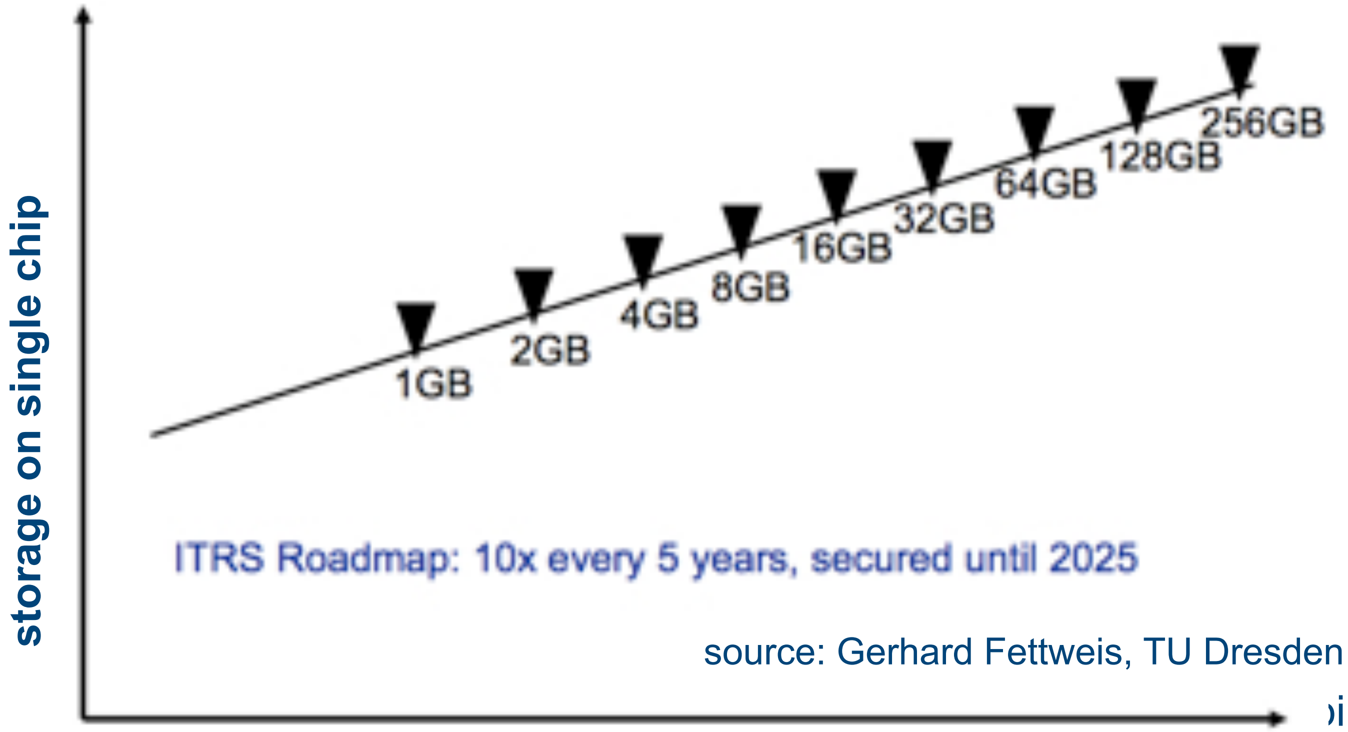
IoT paradigm

- The present "Internet of PCs" will move towards an "Internet of Things" in which 50 to 100 billion devices will be connected to the Internet by 2020. [CERP-IoT, 03.2010]
- “We are entering a new paradigm where things have their own identity and enter into dialogue with both other things and humans mediated through processes that are being formed today. [IoT Europe 2010 conf., 06.2010]

"Now we have roughly 5.2 Mio mobile subscribers. In some year we will have 30...50 Mio devices on the mobile network”
– *Hans Christian Haugli, CEO, Telenor Objects* *2010*

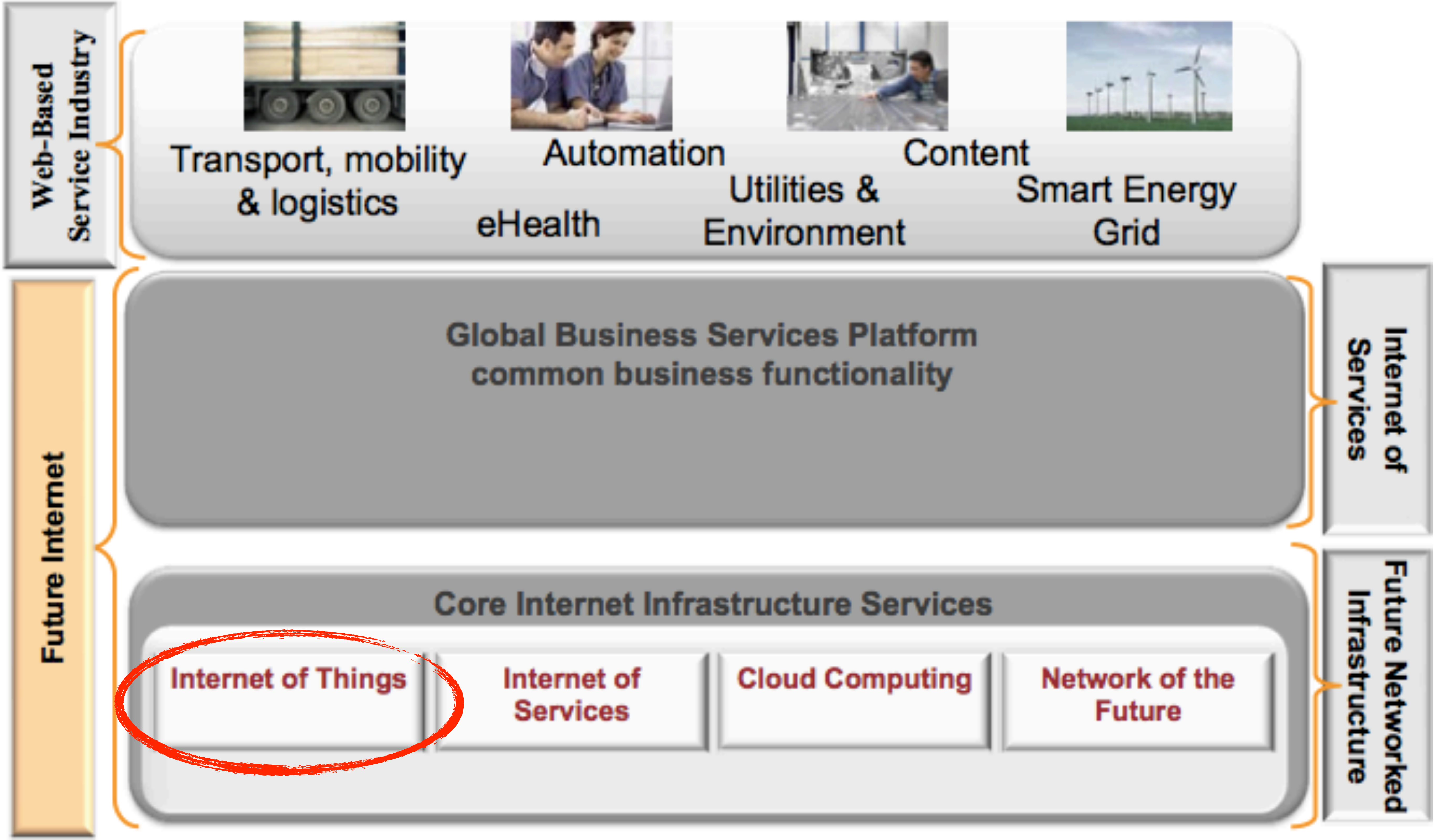
“In 2012 there were more devices than people on the mobile network of Telenor”.
– *Hans Christian Haugli, CEO, Telenor Objects*

The speed of development



source: Gerhard Fettweis, TU Dresden

Principal Objective of the FI PPP - A Holistic Global Service Delivery Platform


Web-Based Service Industry
Transport, mobility & logistics
Automation
eHealth
Content
Utilities & Environment
Smart Energy Grid
Future Internet
Global Business Services Platform common business functionality
Internet of Services
Core Internet Infrastructure Services
Internet of Things
Internet of Services
Cloud Computing
Network of the Future
Future Networked Infrastructure

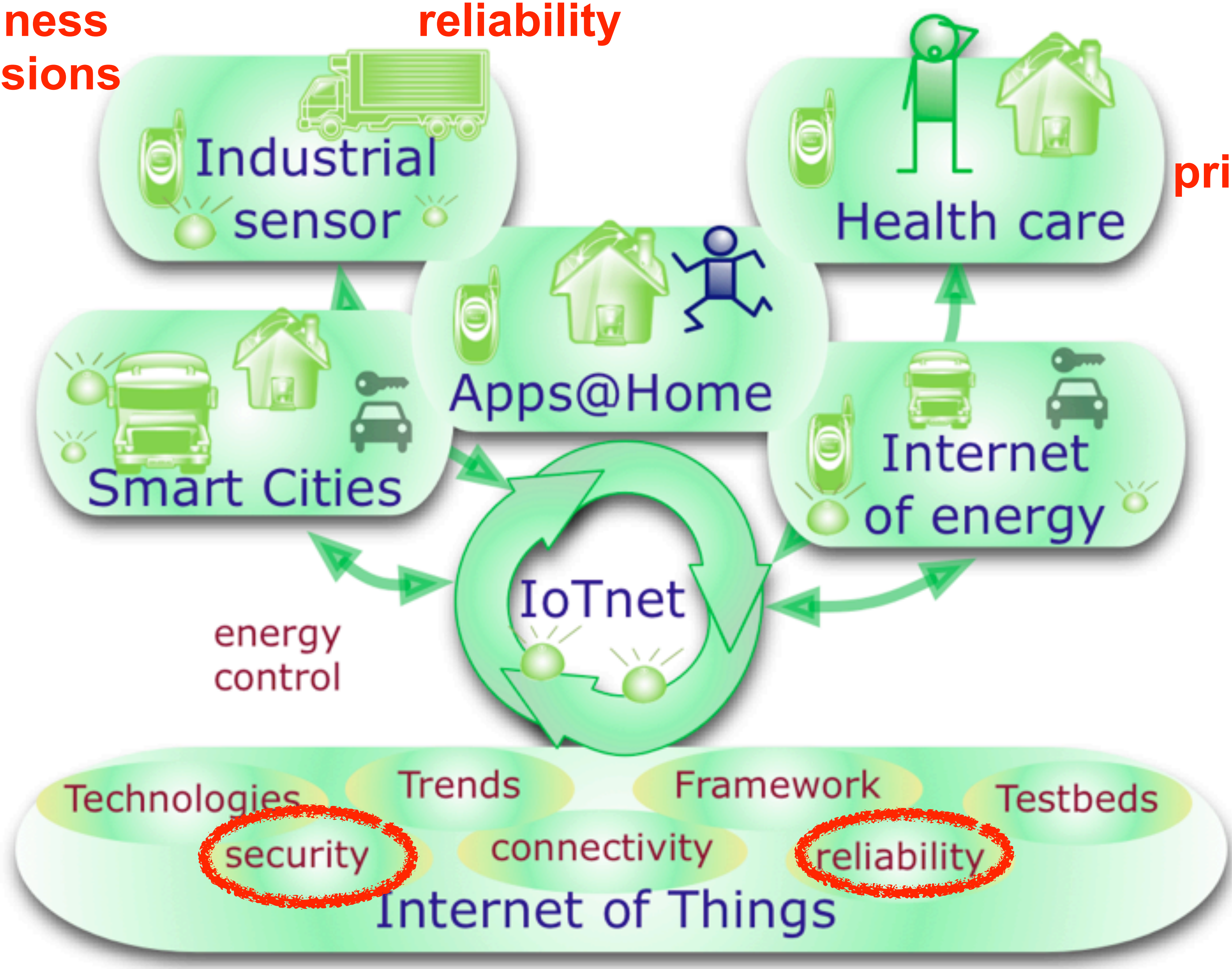
[Source: J. Schaper, FI PPP Constituency Event Nice, March 2010]

The IoT technology and application domain

business decisions

reliability

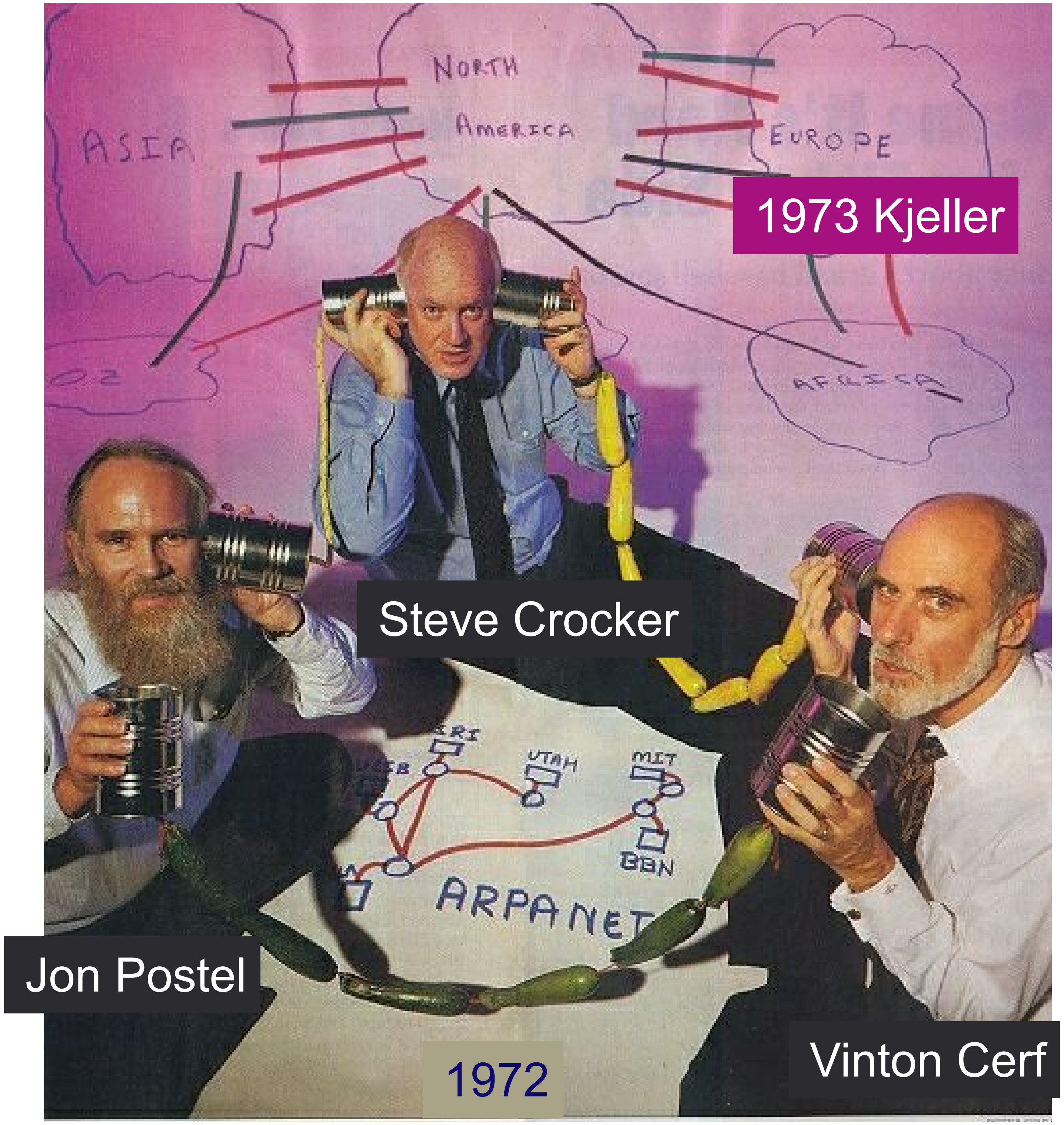
privacy



Outline

- About the author
- Security in Mobile Networks
  - Privacy
  - Dependability
- The way ahead: Internet of Things
  - connection of sensors to mobile
  - business decisions based on information
- Security Challenges
  - BYOD “bring your own device”
  - Be aware of the value of information
  - Measurable security
- Use case for
  - From Entertainment to Socialtainment
  - Sensor data fusion
- Conclusions

The security challenge of the Internet



1973 Kjeller

Steve Crocker

Jon Postel

1972

Vinton Cerf

"If we would have known how Internet developed, ..."

Source: http://www.michaelkaul.de/History/history.html

Security in the Internet of Things?

Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi: 10.1016/ j.comnet.2010.05.010

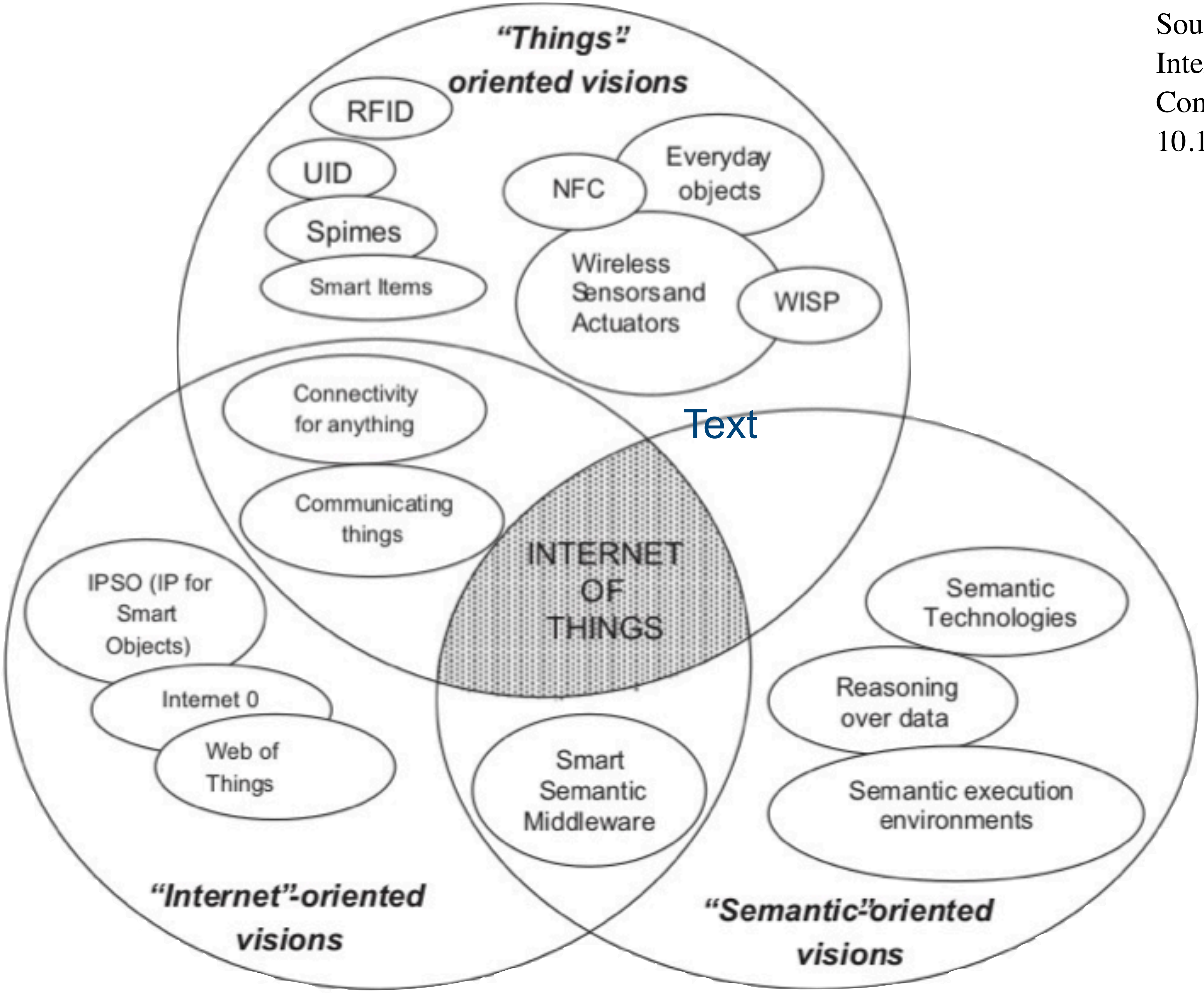
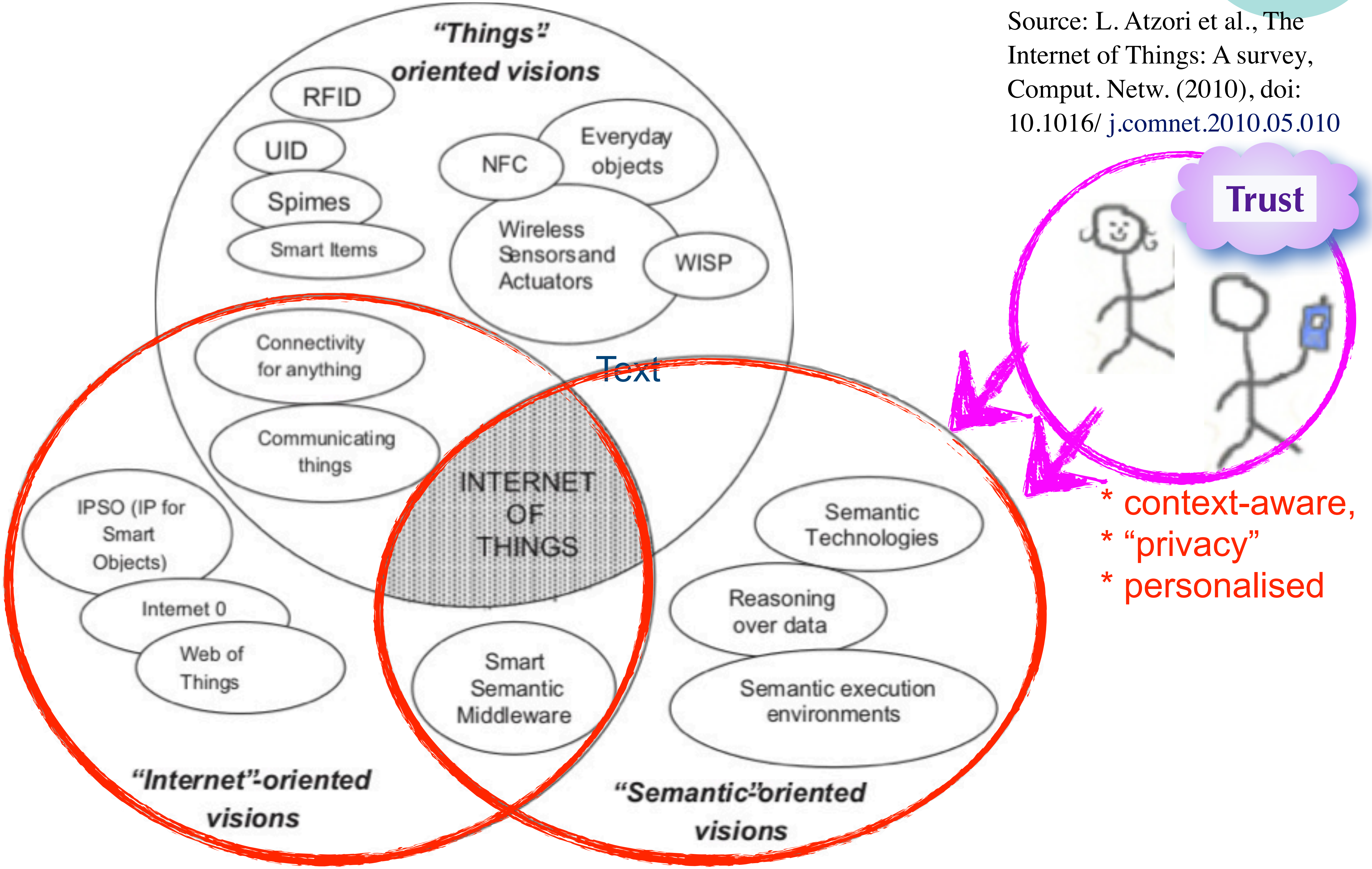

"Things" oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
Text
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

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

Security in the Internet of Things?


"Things" oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
Text
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions
Trust

Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi: 10.1016/ j.comnet.2010.05.010

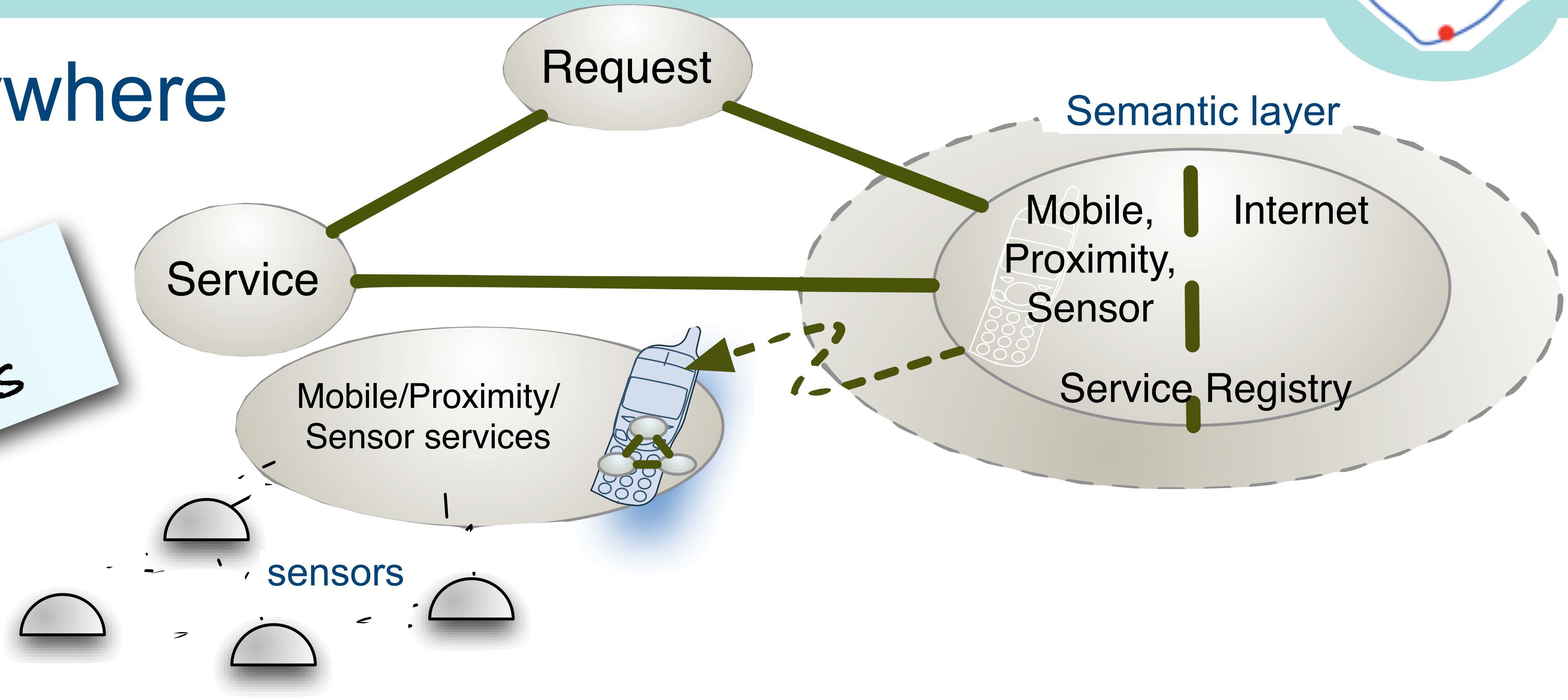
* context-aware,
* "privacy"
* personalised

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

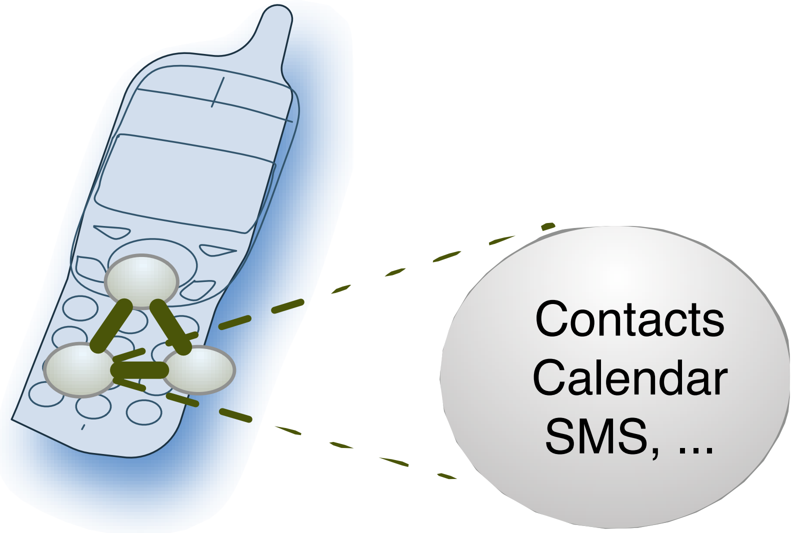
Security challenges

- Sensors everywhere
  - SOA based

medical, home,
industrial sensors



- Bring your own device (BYOD)
  - 30-100 devices/employee
  - "phone in the cloud"



PC, MAC, phone, tab,
pod, pad, embedded...

Measurable Security

- Value of information
  - Identify
  - Analyse
  - Evaluate Risk

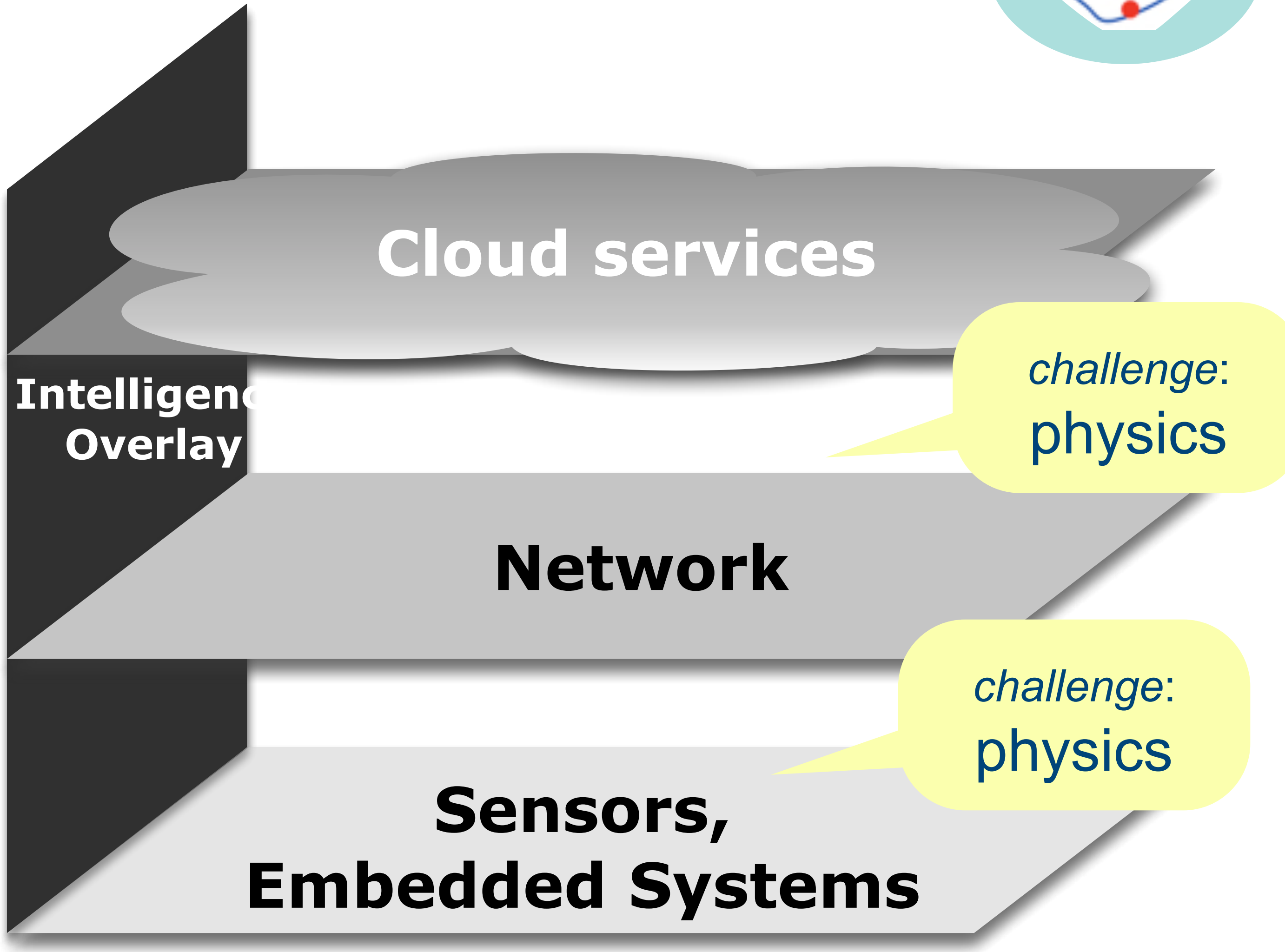
Risk Analysis & Assessment

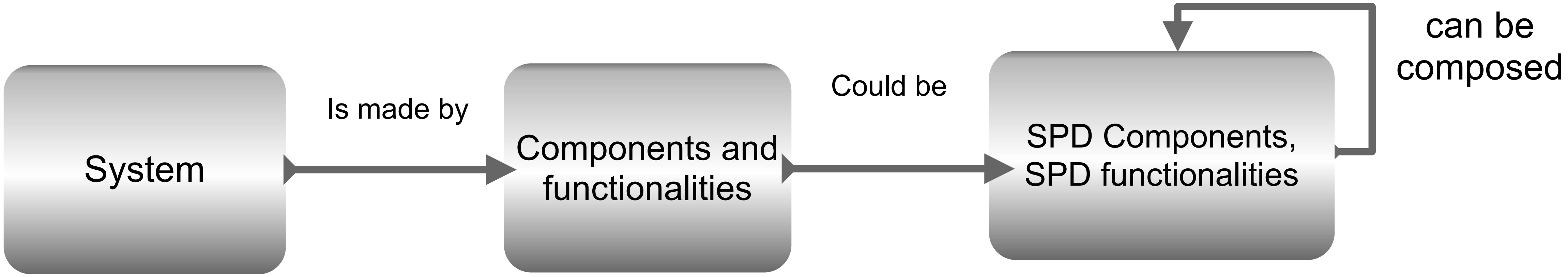
- Measurable security
  - “Banks are secure”
  - IETF working group: *Better than nothing security*
  - Cardinal numbers?

Cost - Benefit analysis

Security Challenges in sensor-enabled clouds

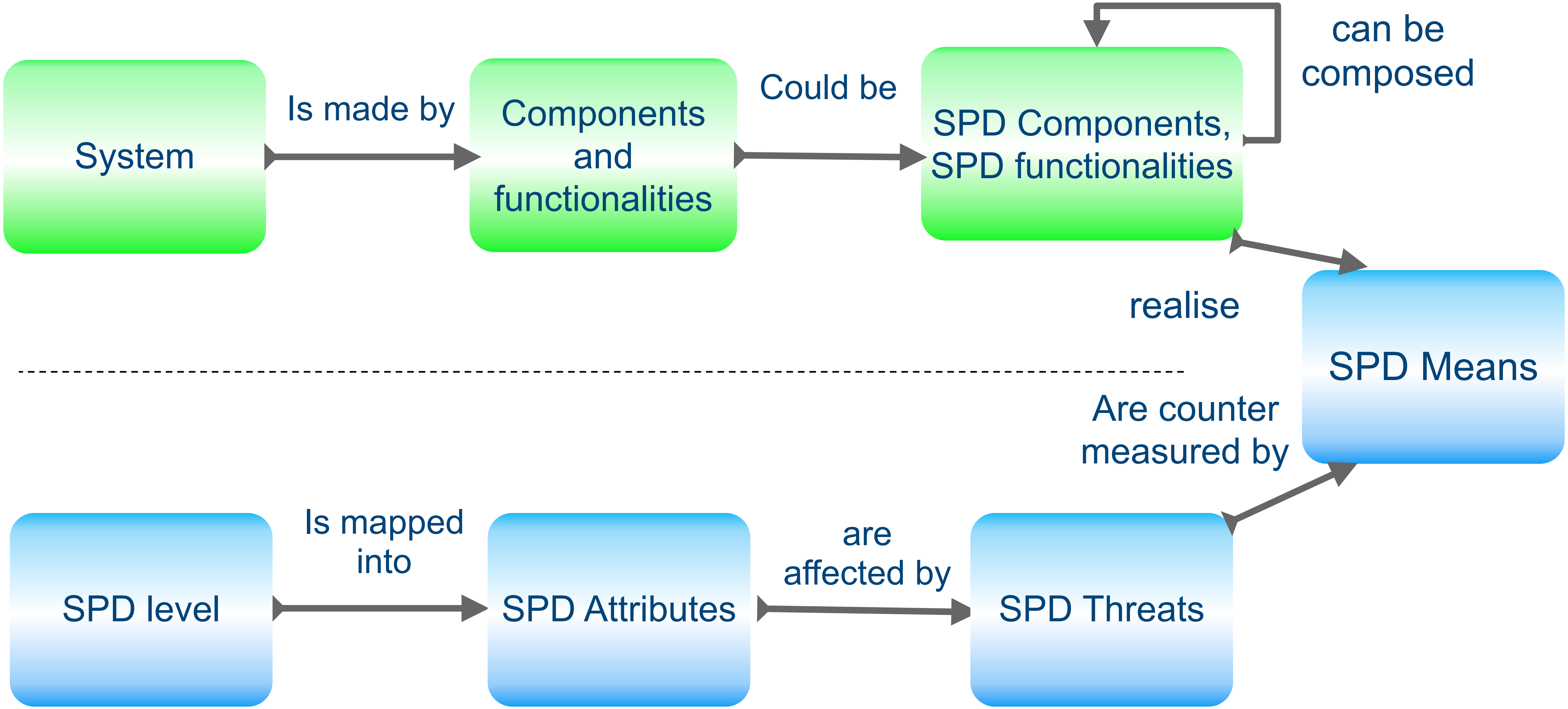
- Security, here
  - security (S)
  - privacy (P)
  - dependability (D)
- across the value chain
  - from sensors to services
- measurable security?




System
Is made by
Components and functionalities
Could be
SPD Components, SPD functionalities
can be composed

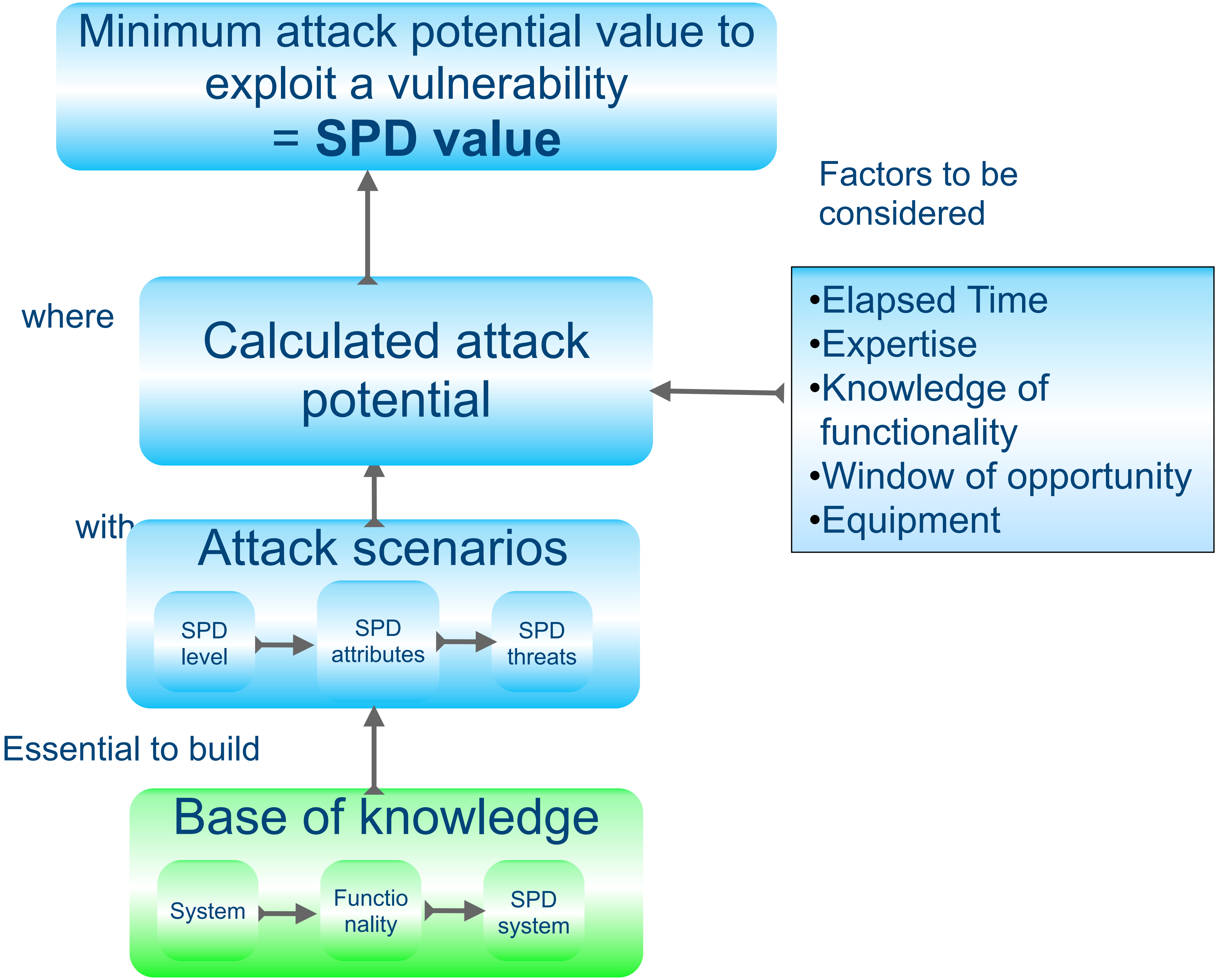
Measuring Security, Privacy and Dependability (SPD) in the IoT

Ontology logical representation: each concept is modelled and the relations are identified in order to have the logical chains that enables the SPD-aware composability



[source: Andrea Fiaschetti, pSHIELD project, Sep 2011]

SPD Metrics specification



Minimum attack potential value to exploit a vulnerability
= **SPD value**

where

Calculated attack potential

with

Attack scenarios

SPD level → SPD attributes → SPD threats

Essential to build

Base of knowledge

System → Functionality → SPD system

Factors to be considered

- Elapsed Time
- Expertise
- Knowledge of functionality
- Window of opportunity
- Equipment

Factor	**Value**
Elapsed Time	
<= one day	0
<= one week	1
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*[1]
Expert	6
Multiple experts	8
Knowledge of functionality	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
Unfeasible	25**[2]
Equipment	
Standard	0
Specialised	4[3]
Bespoke	7
Multiple bespoke	9

[source: Andrea Fiaschetti, pSHIELD project, Sep 2011]

Outline

- About the author
- Security in Mobile Networks
  - Privacy
  - Dependability
- The way ahead: Internet of Things
  - connection of sensors to mobile
  - business decisions based on information
- Security Challenges
  - BYOD “bring your own device”
  - Be aware of the value of information
  - Measurable security
- Use case for
  - From Entertainment to Socialtainment
  - Sensor data fusion
- Conclusions

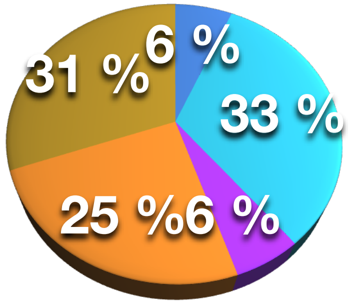
Use case: SPD in heterogeneous systems

- Nano-Micro-Personal-M2M Platform
  - identity, cryptography, dependability
- SPD levels through overlay functionality
  - answering threat level
  - composing services
- Policy-based management
  - composable security
- Integration into Telecom Platform
  - from information to business decisions

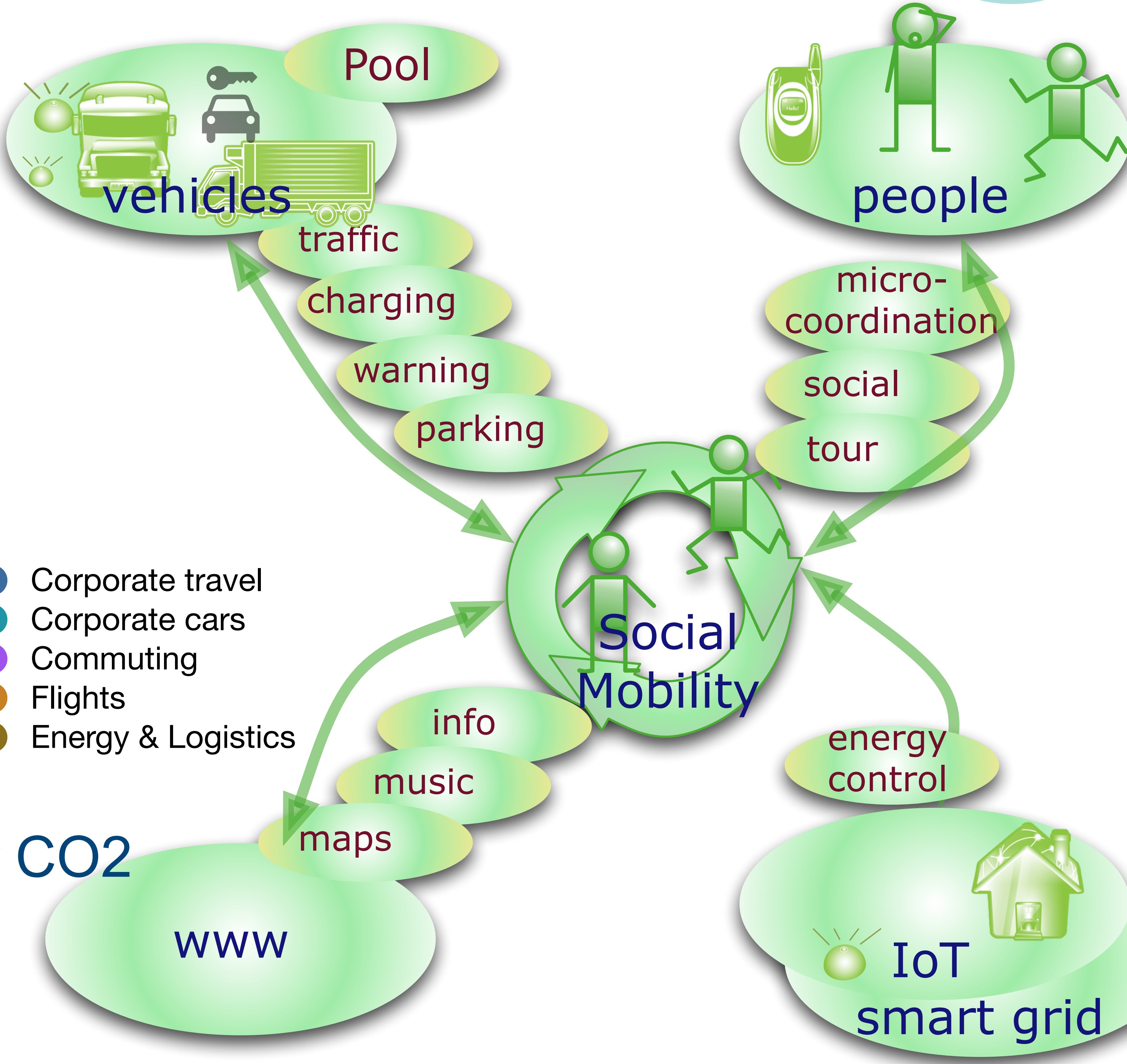
Application Example: Socialtainment (eMobility)

- From Entertainment to Socialtainment
- Social mobility through inclusion of social networks

CO2 consumption

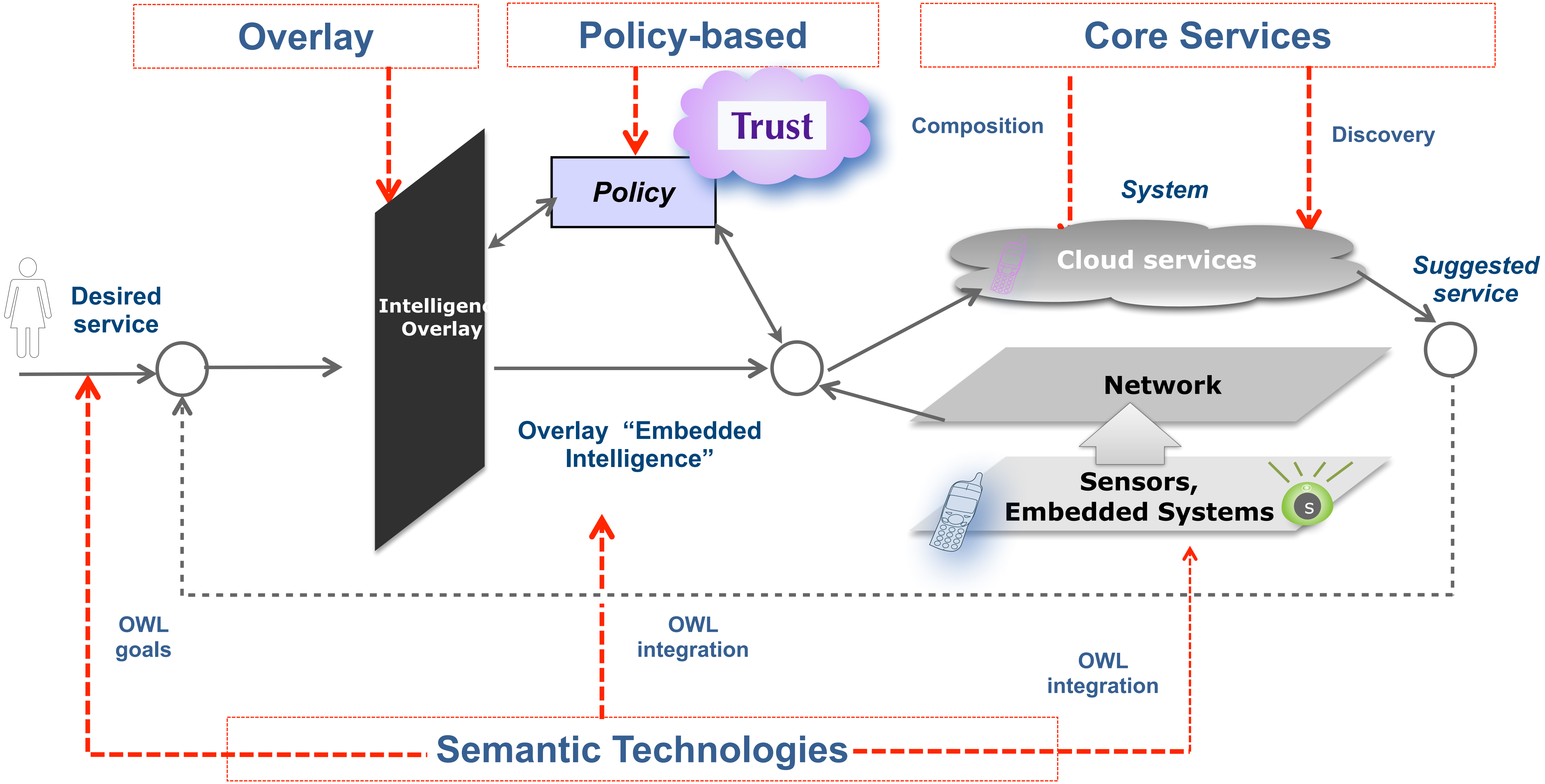


- answering the need for CO2 reduction in transport
  - SAP 45% (2009)



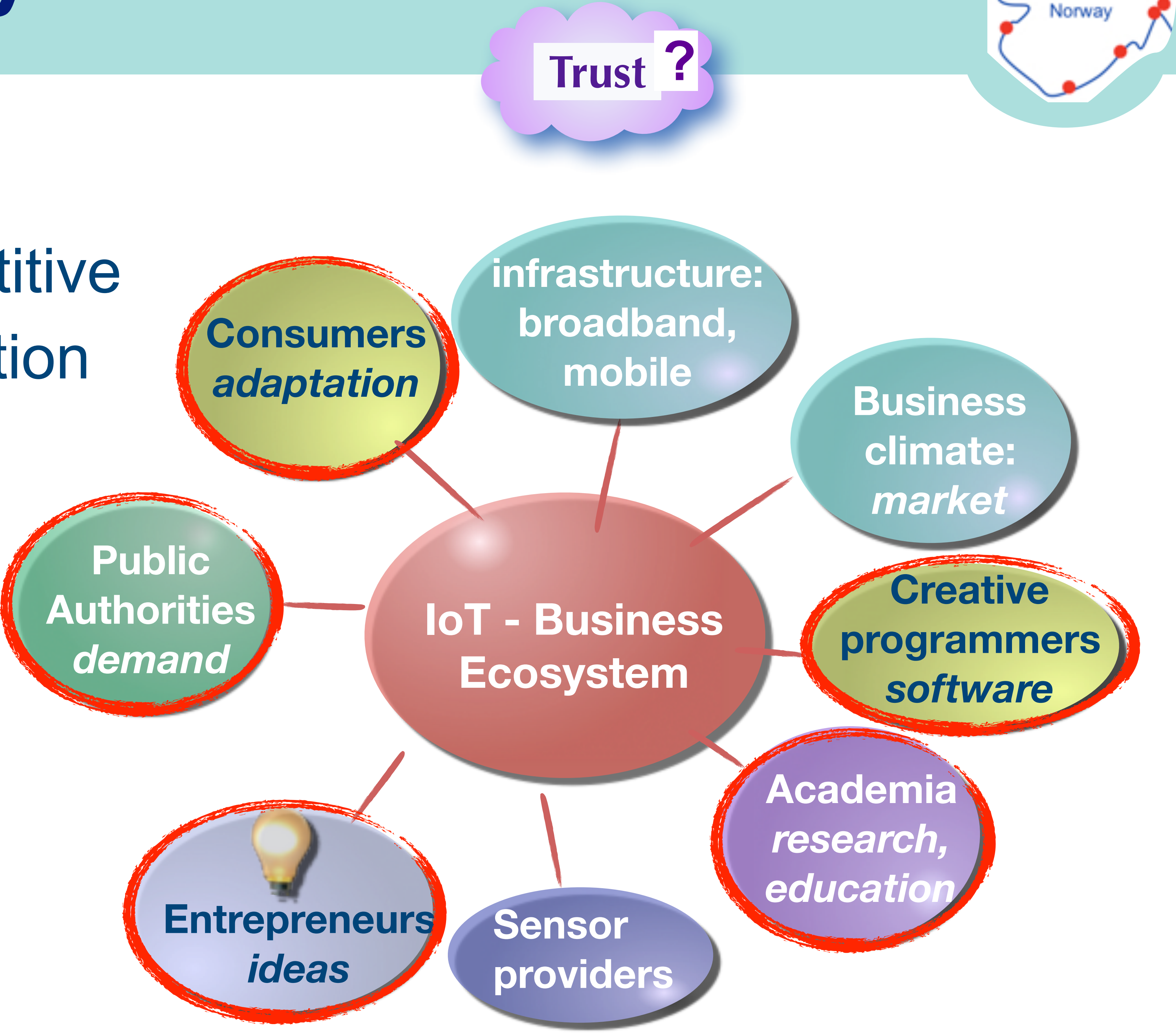
Semantic Representation

Cloud service representation through semantic integration



The IoT ecosystem

- Creating business
  - openness, competitive
  - climate for innovation
- Public authorities
  - trust, confidence
  - demand
- Consumers
  - (early) adapters
  - education
- Infrastructure
  - broadband, mobile
  - competition



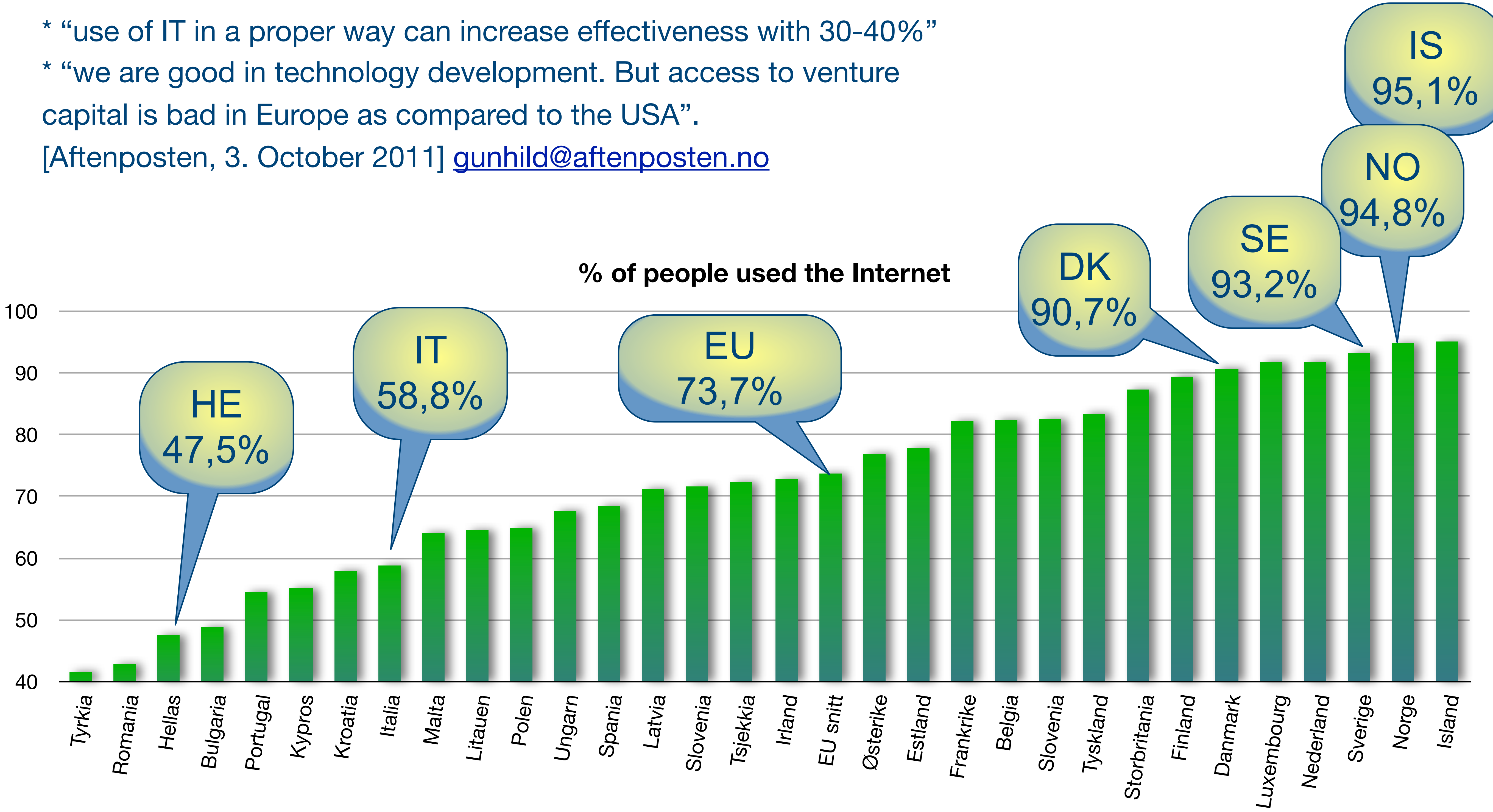
Trust ?
Consumers *adaptation*
infrastructure: broadband, mobile
Business climate: *market*
Public Authorities *demand*
IoT - Business Ecosystem
Creative programmers *software*
Academia *research, education*
Entrepreneurs *ideas*
Sensor providers

Internet usage across Europe

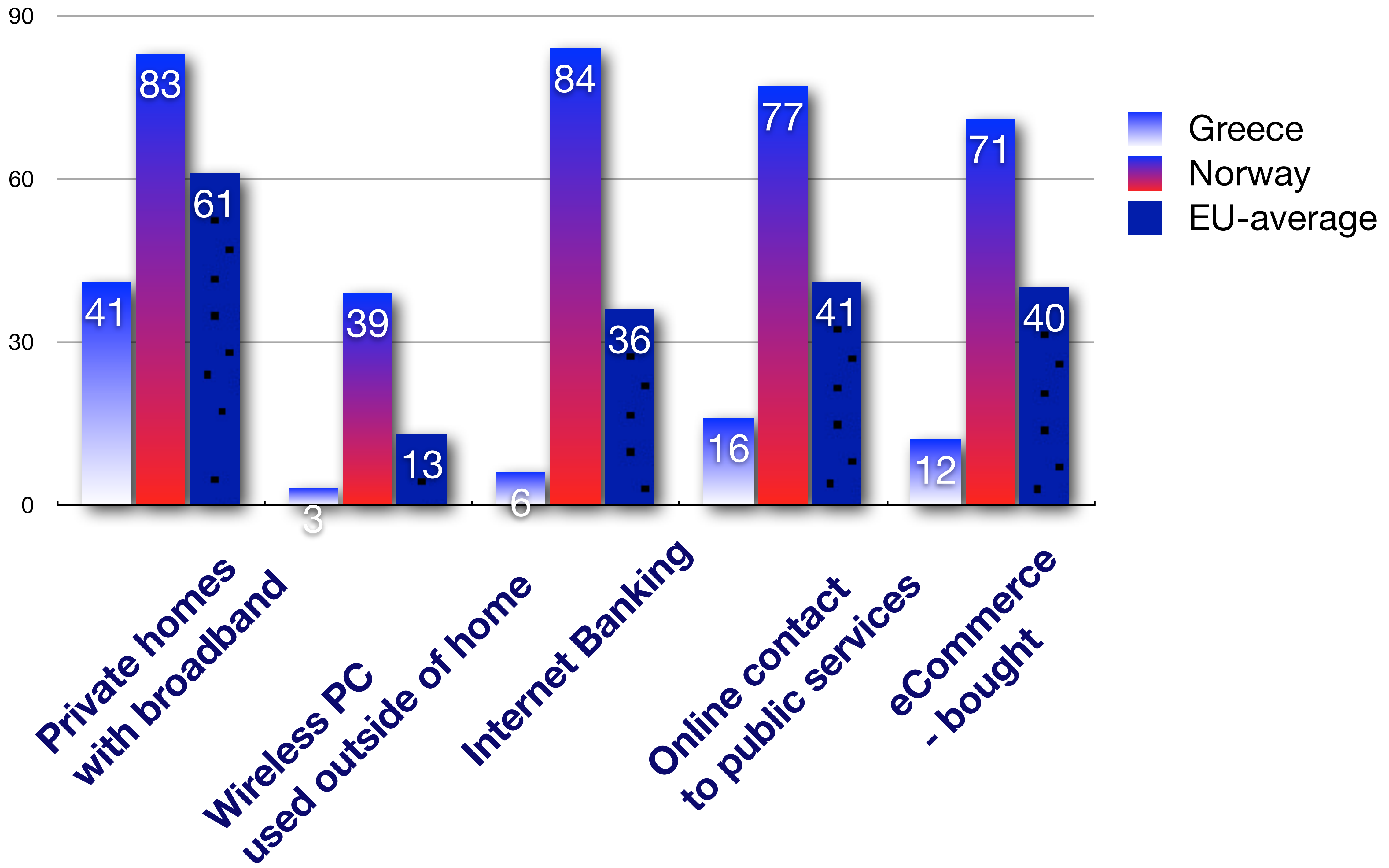
[Robert Madelin, Directorate-General for Information Society and Media, EU commission, Aug 2010]

* "use of IT in a proper way can increase effectiveness with 30-40%"
* "we are good in technology development. But access to venture capital is bad in Europe as compared to the USA".

[Aftenposten, 3. October 2011] gunhild@aftenposten.no



Internet service usage



Conclusions

- The mobile system is secure, but...
  - evolvement to provable security
  - bring your own devices, heterogeneity
  - from sensors to business decisions
- Building the IoT architecture
  - Cross-layer intelligence & knowledge
  - Accounting for security
- Measurable security
  - Metrics describing threats
  - Overlay description for system of systems
- Building the Ecosystem
  - Human perspective: trust, privacy, context
  - Security based on measures of components, attacks and human interaction

The world is wireless

My special thanks to

- JU Artemis and the Research Councils of the participating countries (IT, HE, PT, SL, **NO**, ES)
- Andrea Fiaschetti for the semantic middleware and ideas
- Inaki Eguia Elejabarrieta,Andrea Morgagni, Francesco Flammini, Renato Baldelli, Vincenzo Suraci for the Metrices
- Przemyslaw Osocha for running the pSHIELD project, Luigi Trono for running nSHIELD
- Sarfraz Alam (UNIK) and Geir Harald Ingvaldsen (JBV) for the train demo
- Zahid Iqbal and Mushfiq Chowdhury for the semantics
- Hans Christian Haugli and Juan Carlos Lopez Calvet for the Shepherd ® interfaces
- and all those I have forgotten to mention

Høgskolen i Telemark

NTNU

Universitetet i Agder

Universitetet i Oslo

Høgskolen i Bergen

UNIK Universitetsstudiene på Kjeller

Universitetet i Stavanger