From Use Cases to Show Cases
The SCOTT impact

the SCOTT-NO team, see: SCOTT.IoTSec.no/About

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

Secure **CO**nnected **T**rustable **T**hings key message

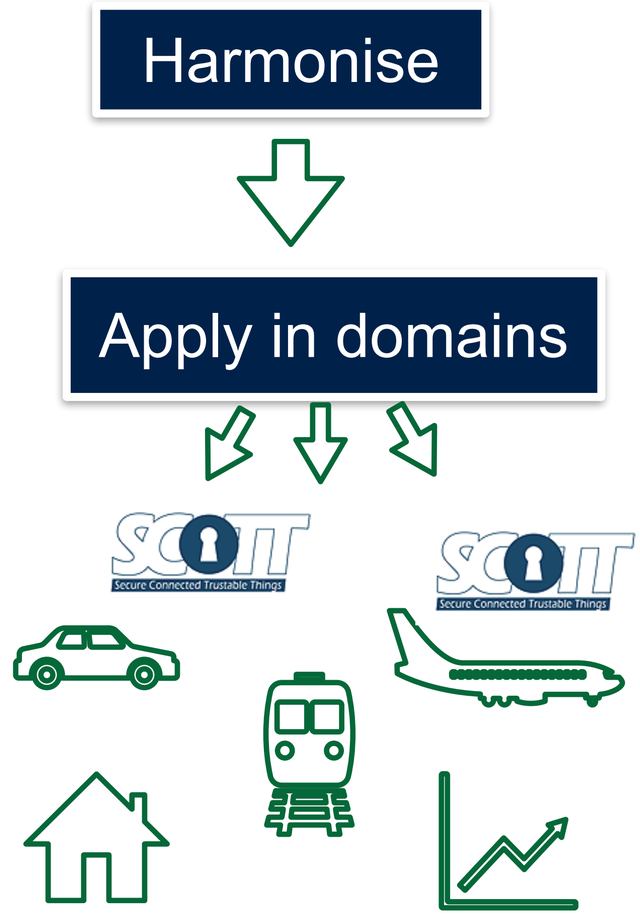
IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- **Answer the IoT need for a new and more advanced security paradigm through security classes**
- **Create a Convincing privacy assessment through privacy labelling**
- **Establish a clear link between security and safety**

Key IoT concerns (ongoing discussion)

Steps

- **Answer the IoT need for a new and more advanced security paradigm**
  - *How to measure security of (complex) IoT systems, how to incorporate security it into designs, how to have a clear (understandable to end-users) security level assessment*
  - *Address cybersecurity through proactive safeguard*
- **Create a Convincing privacy assessment (privacy labelling)**
  - *Privacy labelling – a market opportunity for companies and a response for the consumers need*
  - *What is acceptable to different end users and what is not, how to incorporate it into designs*
  - *Incorporate convenience, dependability and transparency*
  - *How to incorporate trustability in the design (how to increase trust in future IoT solutions)*
- **Establish a clear link between security and safety**
  - *How security influences safety: of people, systems, environment, … IoT needs advance in security (handling/addressing) security – by security classification (how to measure it)*
- **How the architecture enabling the above should look like**



Security in IoT
- postulation of Security Classes, based on “exposure” and “impact”

Security Classes and System design

- Security Classes in IoT
  - Consequence
  - Exposure
- Consequence
  - as in risk map
- Exposure
  - Physical exposure
    - people, building, physical ports,…
  - IT exposure
    - ports, firewall, connectivity
- Used to assess the security class of Syst
  systems and components

New postulate of security class

Consequence				
5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Cl…	…	Class 5
3	Class …	…	… 4	Class 4
2	Class …	…ass 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

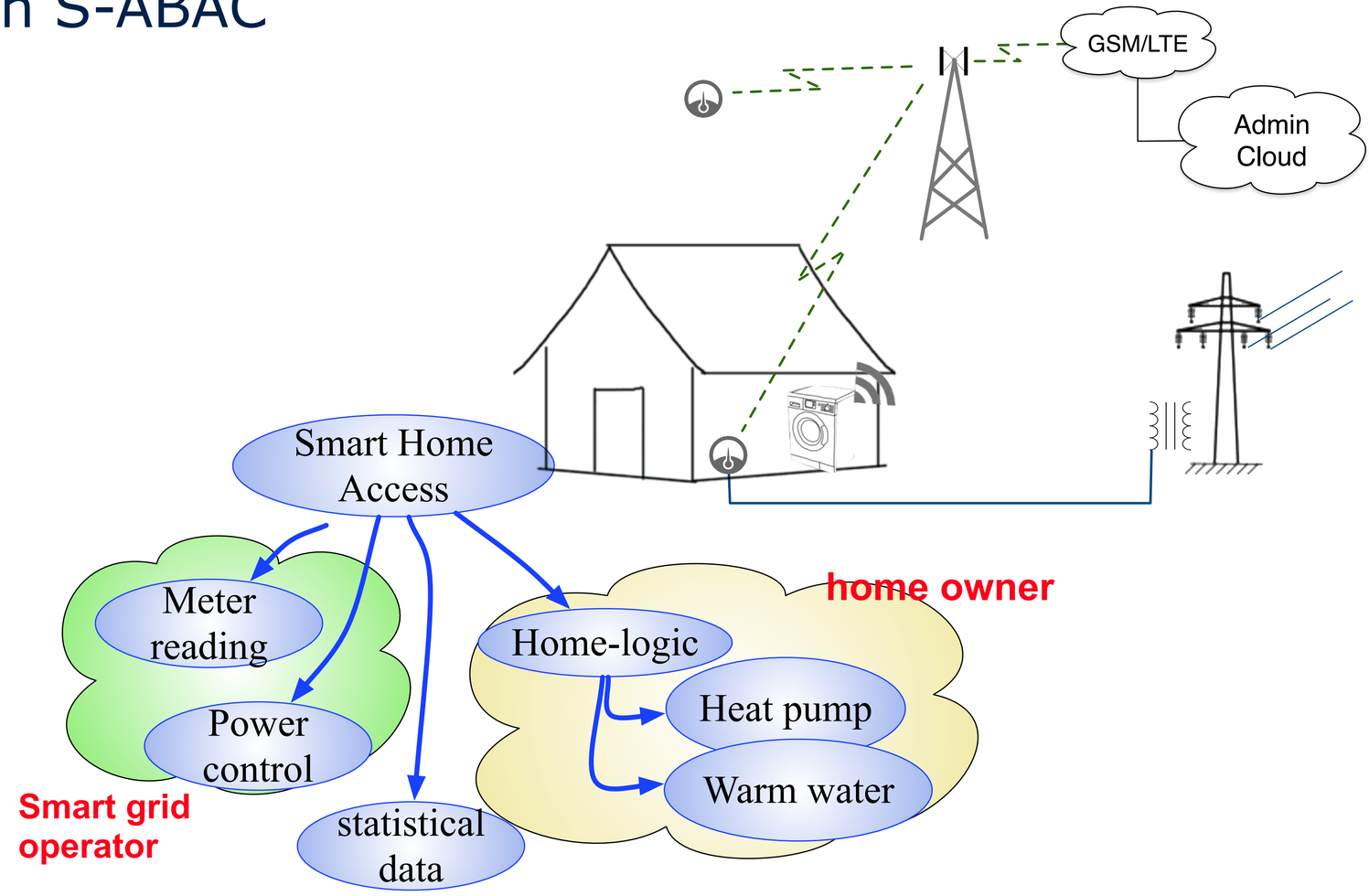
Security Class

Exposure

Increase weak security:
- watchdog
- Attribute based access control (S-ABAC)

Semantic attribute based access control (S-ABAC)

- Lifting the security class through S-ABAC
- Access to information
  - who (sensor, person, service)
  - what kind of information
  - from where
- Attribute-based access
  - role (in organisation, home)
  - device, network
  - security tokens
- Rules inferring access rights



Attributes: roles, access, device, reputation, behaviour, ...

SCOTT trust framework

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

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

Privacy labelling (A-F)
- declare the level of privacy of devices and services

The economic perspective

- The big 5 IT companies have a GDP as big as that of France
- Amazon largest sector in terms of revenue is selling of data
  - 20% of revenue

- How can SMEs compete?
  - Each service and device gets a privacy label

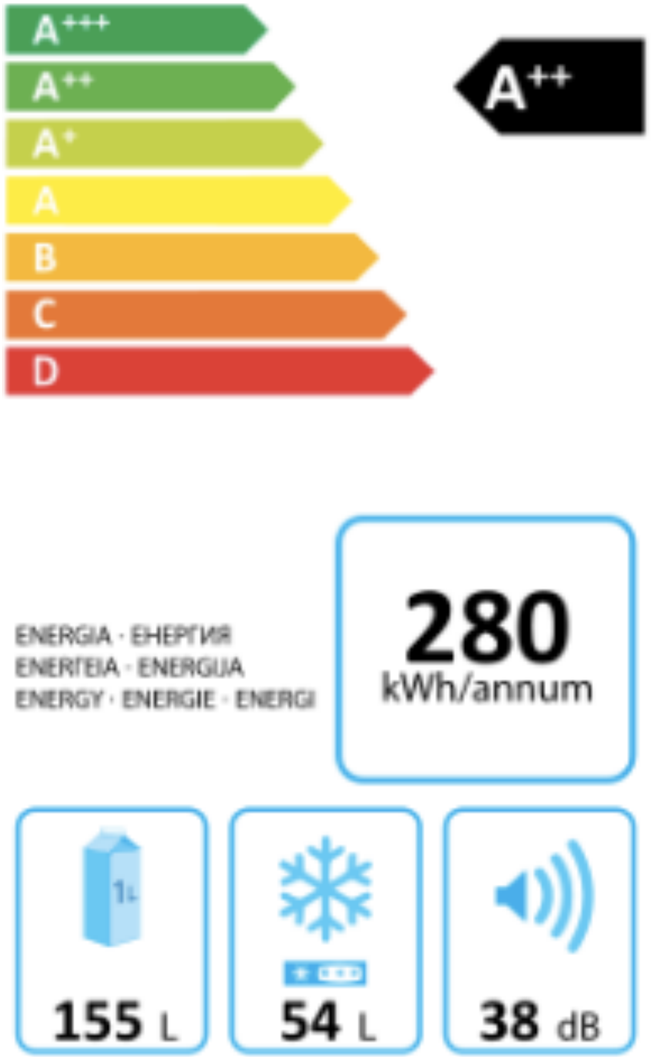
- Four areas for Privacy Label
  - ➡ which data are collected
  - ➡ sharing to my phone, my cloud, public cloud,...
  - ➡ data communication integrity and storage
  - ➡ further distribution of data, ownership of data, further processing

Privacy Label (A-F)

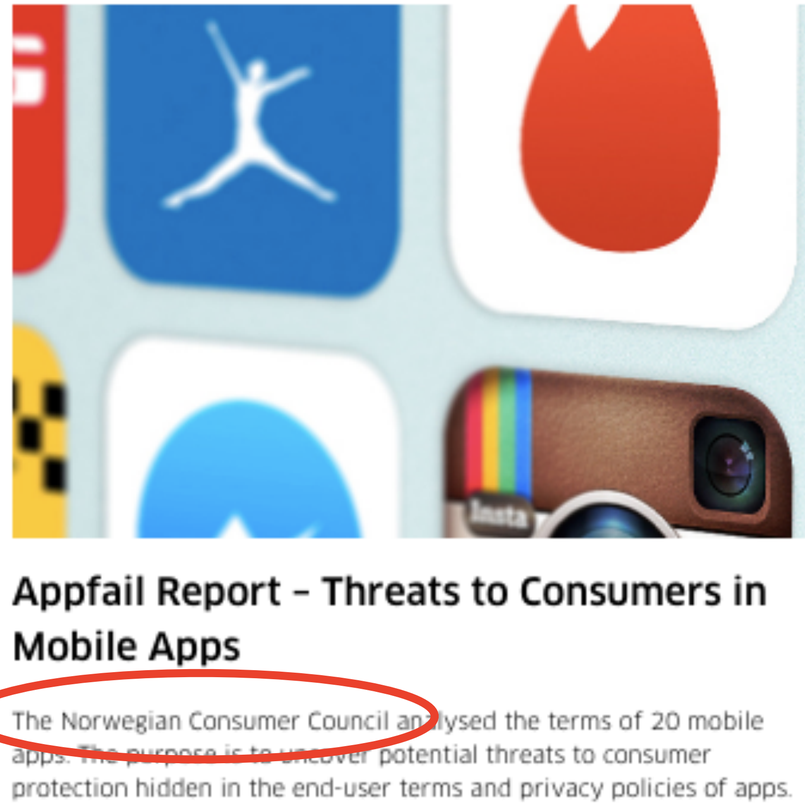
- easy visibility
- customer focus
- transparent

privacylabel.IoTSec.no

Privacy Labelling
http://PrivacyLabel.IoTSec.no



- "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.

Privacy Label (A-F) - *ongoing discussion*

Level A++

- no data are shared

Level A+

Level A - Very high

- restricted use of data to purpose only (particular service)
- supplier should bear the risk of incidents, e.g. they rather than I get penalised when things go wrong - equivalent to finansavtaleloven
- if device is stolen - nobody else

Level B

- specify the data to be collected, re-use for statistical data only, ensured integrity
- customizable access control, eg.. add stronger authentication or consent requirements
- must be able to trade off the various security requirements, e.g. confidentiality agains availability - i.e. I want flexibility
- compliance with other standards - and this be listed (information requirement) - clipper compatible
- anonymity of my interaction with the supplier
- customer can control with how the information is transferred and used by a third party

Level C

- data are collected without control (GPS+activity+heart rate), re-use only for statistical, encrypted storage
- must be possible to withdraw consent - and that this results in all relevant information being deleted - and proof of deletion

Level D

- data are collected, transparency of re-use
- Data is not sold without consent/knowledge
- transparency - I get told about the criteria that the supplier has used in their information classification
- Information is only used for its legitimate purpose

Level E

- collected data, no transparency of re-use
- in compliance with GDPR
- if data is stolen, I will get told
- notification if DSO is hacked

Level F - Failure

- no privacy, no control of data, everyone can see
- nothing , no expectations

Answer the Challenges addresse

DIGITALEUROPE

Our Work | Press Room | Services | Events | About Us | Why Join Us | A A

EUA European University Association | DIGITALEUROPE

DIGITALEUROPE Digital in Practice Programme workshop

The importance of openness
for sustainable knowledge societies

Wed, September 27, 2017
8:30 AM – 10:30 AM CEST

DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes

Brussels, 23 March 2017

RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security **certification framework for ICT products** and 2) a **"Trusted IoT label"** giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

2. Trusted IoT Label

In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.

SCOTT contribution: privacy label?

Organisational impact

Health, Security and Environment
Helse, Miljø og Sikkerhet

- Security affects safety
  - IoT attack -> car crashes
- Security affects core business
  - company confidential information
  - Customer information
    - Privacy regulative (GDPR May2018): 4% of revenue

➡IoT is corporate governance