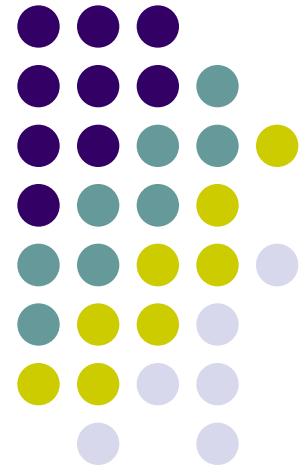


# Challenges from the Identities of Things

Internet of Things World Forum 2014

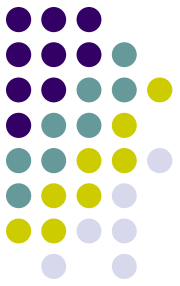
**Seoul, March 6<sup>th</sup> – 8<sup>th</sup>, 2014**

Ingo Friese,  
Telekom Innovation Laboratories,  
Berlin, Germany



# Challenges from the Identities of Things.

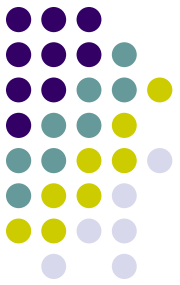
## Agenda.



- Exemplary IoT Scenario
- Object Identifier and Namespace
- Authentication and Authorization
- Ownership and Identity Relationships
- Governance of Data and Privacy

# Exemplary IoT Scenario

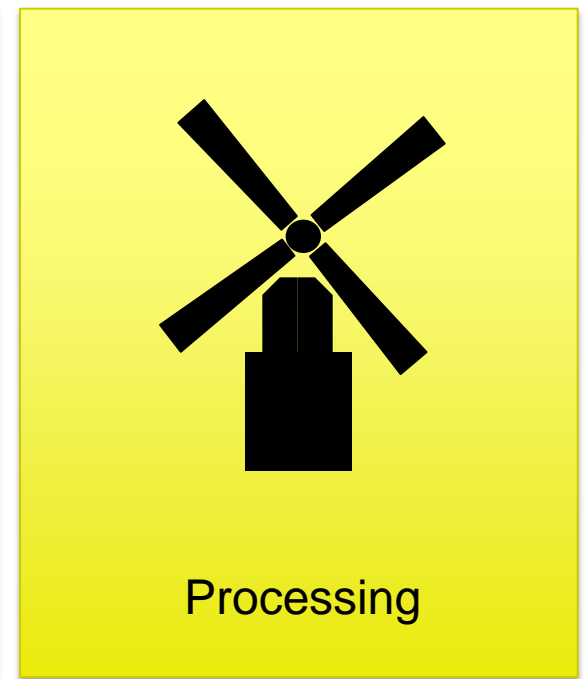
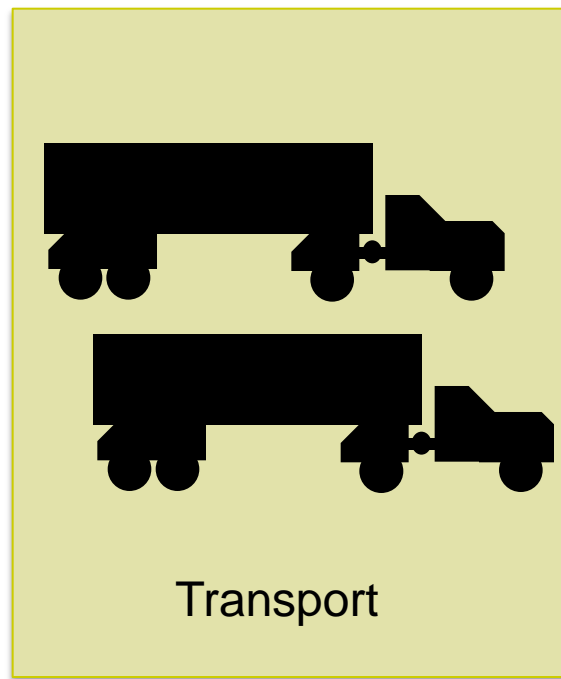
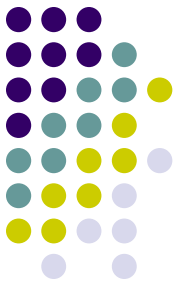
# Exemplary IoT Scenario: Fleet management in farming industry.



\*by courtesy of Claas

# Exemplary IoT Scenario:

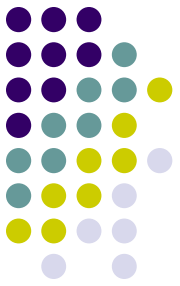
Support of farming production processes.



# Object Identifier and Namespace

# Object Identifier and Namespace

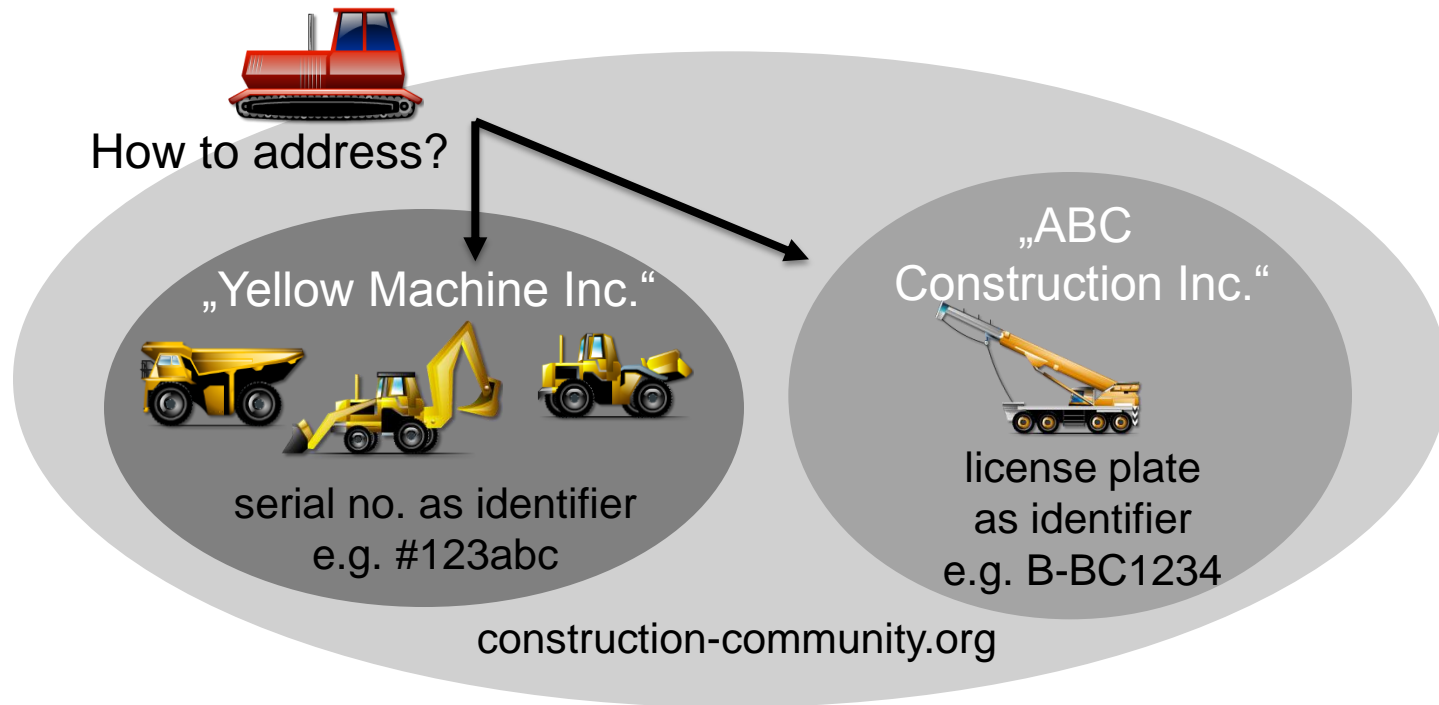
It needs new mechanisms to find identifier and addresses of communication partners in the IoT.



## Example XRI

`xri://construction-community.org/(urn:yellowMachine.serialNo:#123abc)`

`xri://construction-community.org/(urn:abcConst.license:#B-BC1234)`

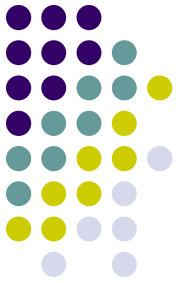


# **Authentication and Authorization**



# Authentication and Authorization

## Proper IdM mechanisms become paramount in the IoT.



**HOTforSecurity**

E-THREATS | INDUSTRY NEWS | MALWARECITY | TIPS AND TRICKS

You Are Here: Home » Industry News » Vulnerability in Vaillant Heating Systems Allows Unauthorized Access

### Vulnerability in [REDACTED] Heating Systems Allows Unauthorized Access

By Loredana Botzatu | comment: 0 | April 16, 2013 | Posted in: Industry News

A critical security vulnerability in the heating and power systems of German company [REDACTED] allows unauthorized people access the systems, turn them off and damage them at will.

[REDACTED] sent all its customers a warning, recommending they manually disconnect the vulnerable systems from the network and wait for one of their employees to fix the systems on site.

Image credit: Vaillant

The heat and power ecoPower 1.0 systems connect to the Internet so their owners can control their homes from afar via a web interface. It is apparently this web interface that has proven vulnerable to unauthorized access. [REDACTED] apparently enjoying great popularity: You switch and control in use worldwide than 200,000 of these controllers with network connection. How critical and H Security in May reported [3], such controls are, however, often carelessly connected directly to the Internet.

**highTech**

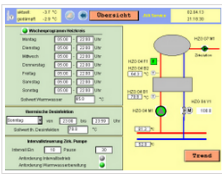
Home

Home » Unlabeled » Critical security update for 200,000 industrial control

### Critical security update for 200,000 industrial control

8:18 PM | Johnny Gagnon

The Swiss manufacturer [REDACTED] has a firmware update for published its industrial control [1], which of the documented by heise Security vulnerability [2] in the authentication remote maintenance access to fix finally – after we have informed the company about the problem for over half a year. However, even after installing the safe firmware version reckless to make these systems directly accessible via the Internet



. < RSPEAK\_STOP ->

The tracked by us control system of a Hessian prison could have control over the Internet.

Industrial control of [REDACTED] apparently enjoying great popularity: You switch and control in use worldwide than 200,000 of these controllers with network connection. How critical and H Security in May reported [3], such controls are, however, often carelessly connected directly to the Internet.

THE CYBERCRIME ECONOMY

### Hacker hits on U.S. power and nuclear targets spiked in 2012

By David Goldman @DavidGoldmanCNN January 9, 2013: 1:41 PM ET

Recommend 566



Department of Homeland Security released this map showing the locations of 7,200 key industrial control systems that appear to be directly linked to the Internet and vulnerable to attack.

31 TOTAL SHARES

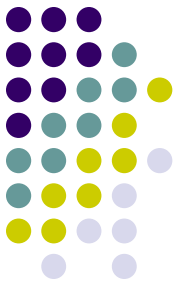
280 254 51 146

YORK (CNNMoney)

America's power, water, and nuclear systems are increasingly being targeted by cybercriminals seeking to gain access to some of the nation's most critical infrastructure.

# Strong Authentication 1/2

How to strengthen authentication means in the IoT?



## User Identities



Something you



know + have + are



## Identities of Things



Something you

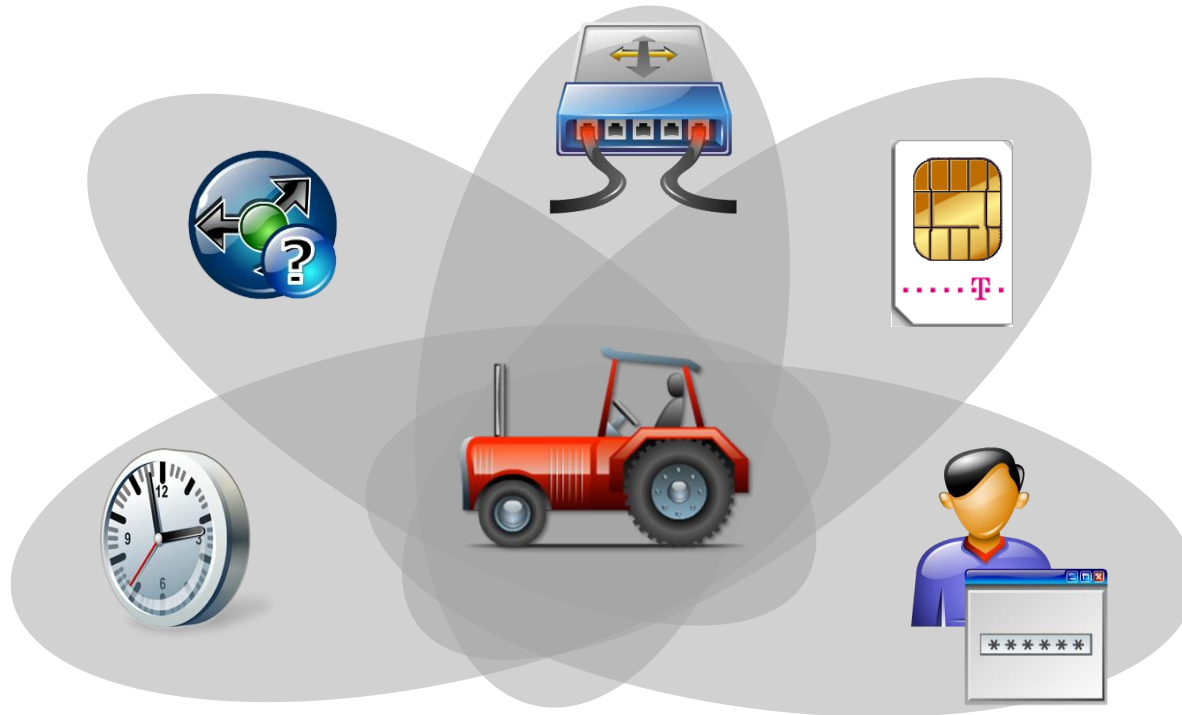
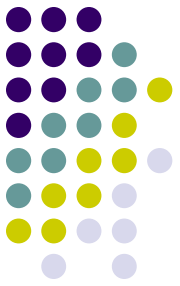


know + have + are



# Strong Authentication 2/2

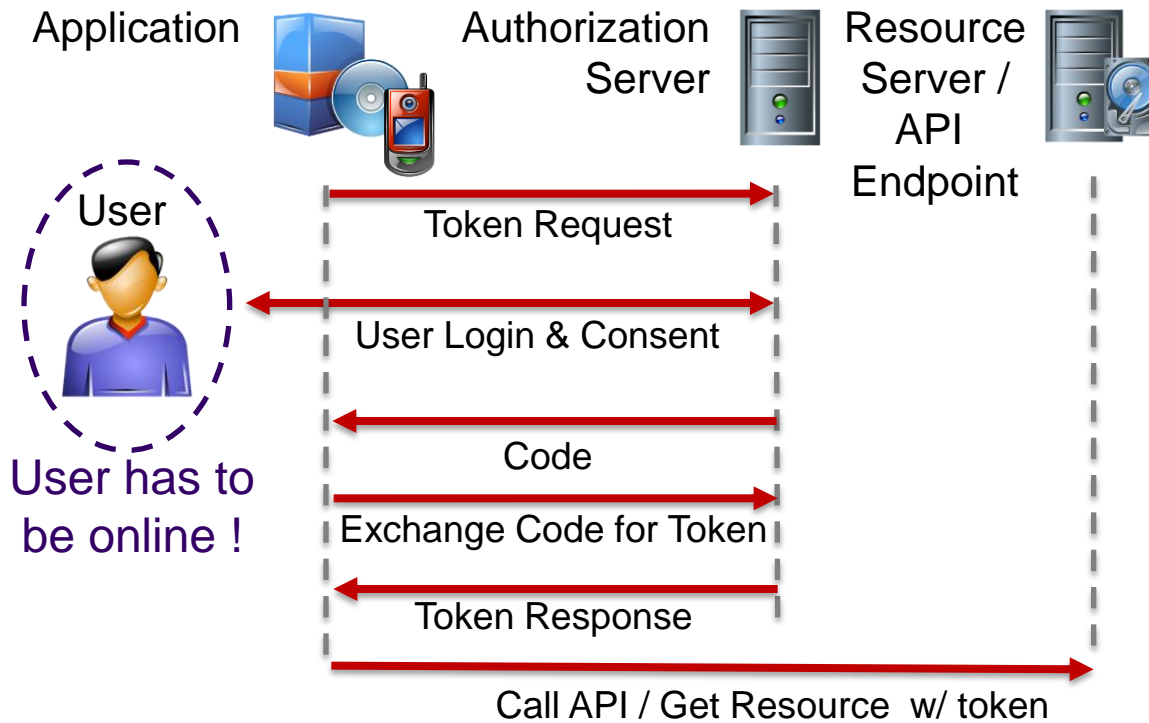
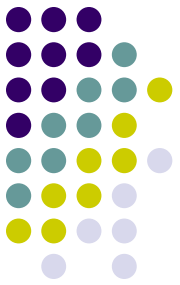
## Context-based authentication.



Additional information could be taken e.g. from the network layer, from geographical information or from other use case specific factors.

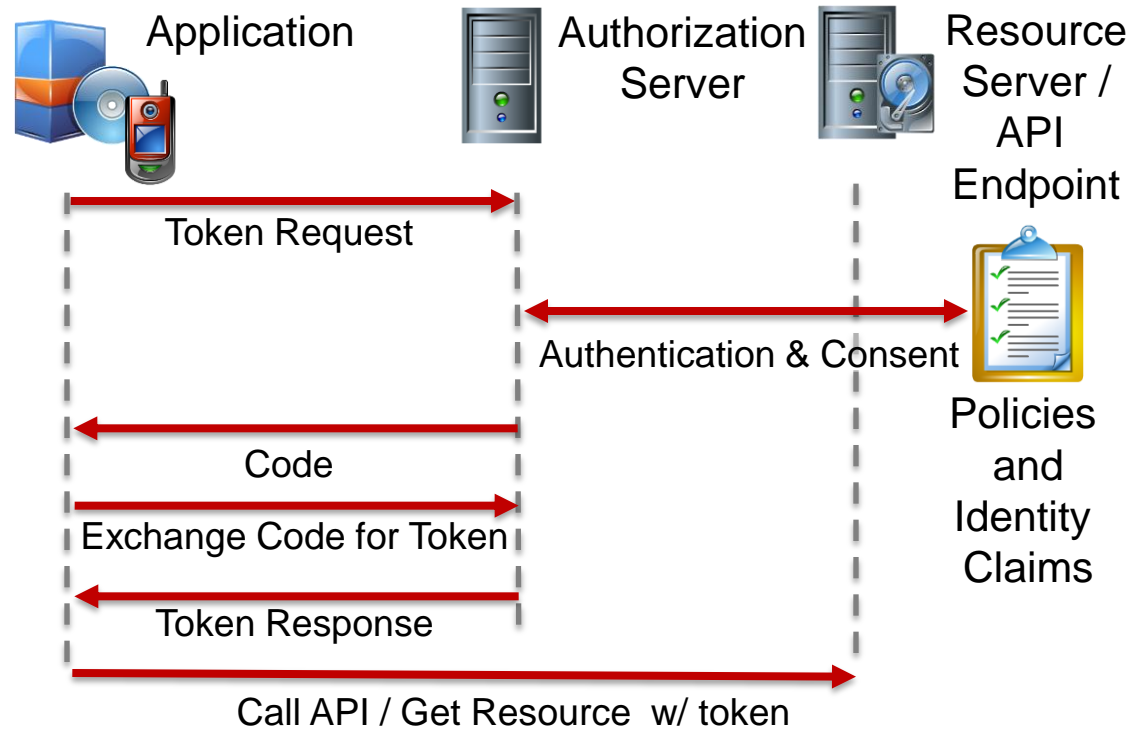
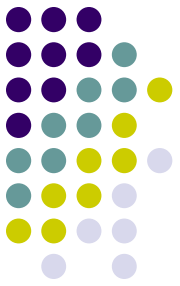
# Authorization 1/2

OAuth – Authorization for the “classic” Internet.



# Authorization 2/2

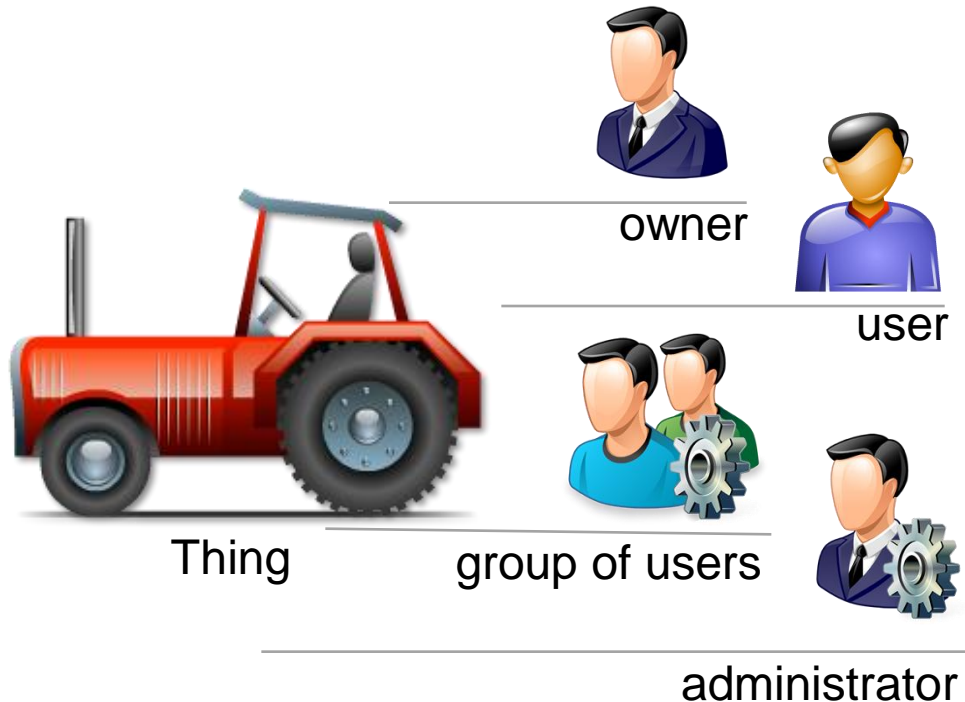
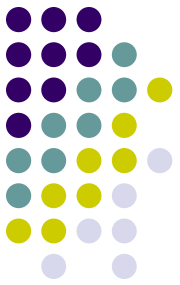
## User Managed Access - Authorization for the IoT(?)



# **Ownership and Identity Relationships**

# Ownership and Identity Relationships

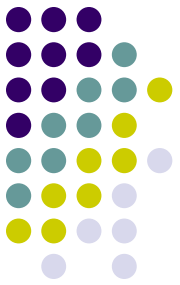
Things or objects in the IoT often have a relationship to real persons.



Identity relationships in the IoT have an impact on other identity related processes like e.g. authentication, authorization or governance of data.

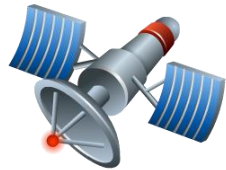
# **Governance of Data and Privacy**





# Governance of Data and Privacy

## The problem.



GPS



Data produced  
in a IoT device

Position

Velocity

Usage of Gas

Oil temperatur

Oil pressure

Engine status

...

Sensors

Persons having  
different claims  
to data



owner



user

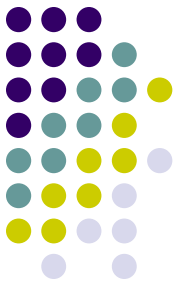
Claims  
to data

„I want to use the  
position data for  
statistics!“

„I don't want the  
position data to be  
used. They could be  
used to track my  
personal behavior“

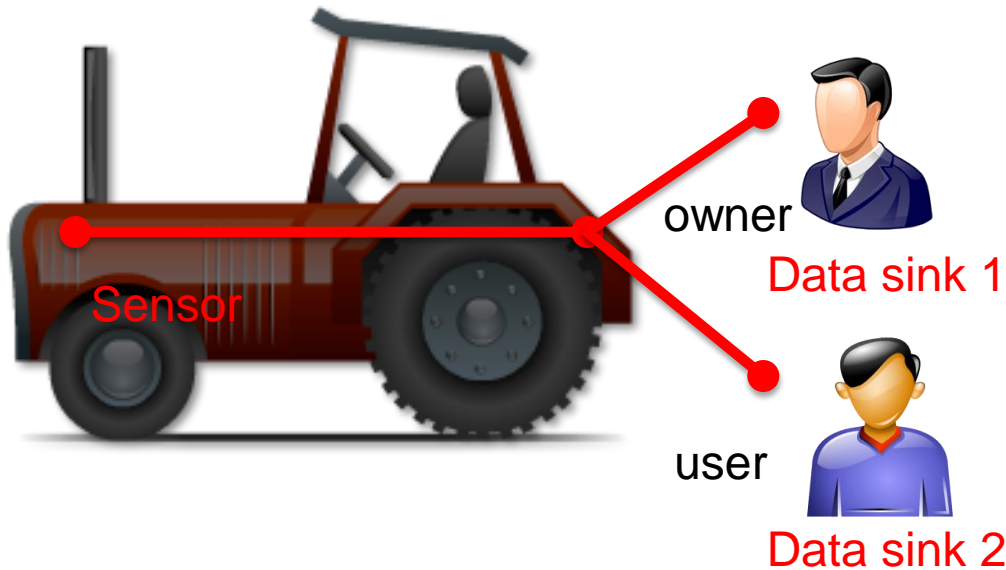
# Governance of Data and Privacy

Users have their claims-to data.



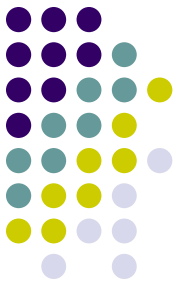
Persons having  
different claims  
to data

Appropriate methods  
to be applied to the data



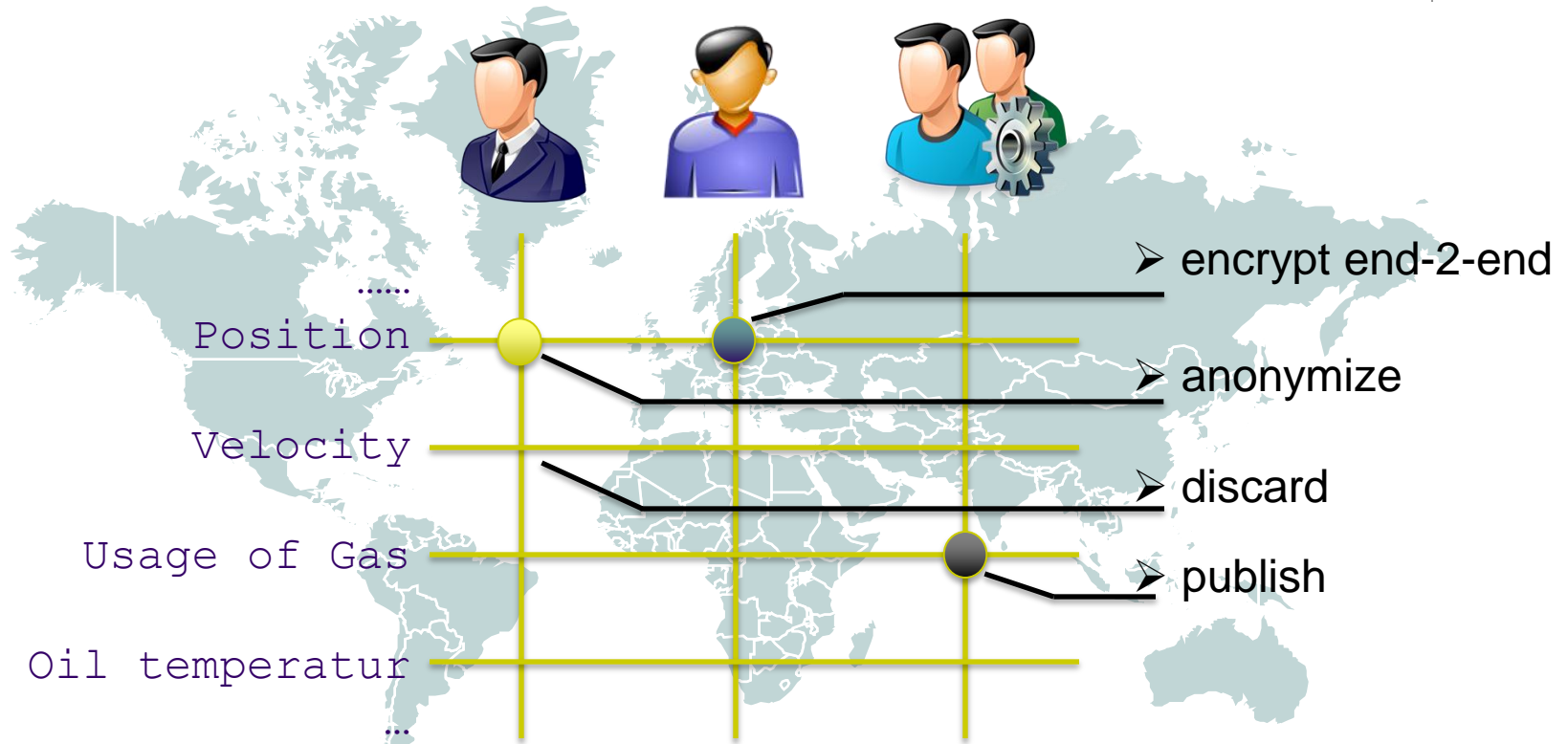
- publish
- anonymize

- discard
- encrypt end-2-end



# Governance of Data and Privacy

## The configurable “claims-to” approach.

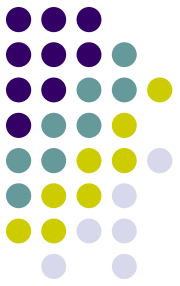


Different configurations in different domains, regions and countries.

**Identities of Things  
Discussion Group  
IDoT**

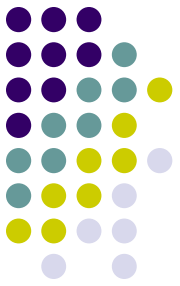
# Identities of Things Discussion Group

## Current Members.



# Identities of Things Discussion Group

## Become a member.



- No formal burdens in Kantara Initiative
- Rather hands on work
- No membership fees apply for working in a DG
- Just sign GPA:  
<http://signup.kantarainitiative.org/?selectedGroup=34>
- Agenda and more: <http://kantarainitiative.org/groups/idot/>

Let's work together on an interesting and most relevant topic.  
Join IDoT DG in Kantara Initiative!

**Questions?**