kantara INITIATIVE™

Authentication with the help of public keys in a Blockchain

EIC 2018

Ingo Friese, Deutsche Telekom AG
Identity of Things Discussion Group

Background: Smart City

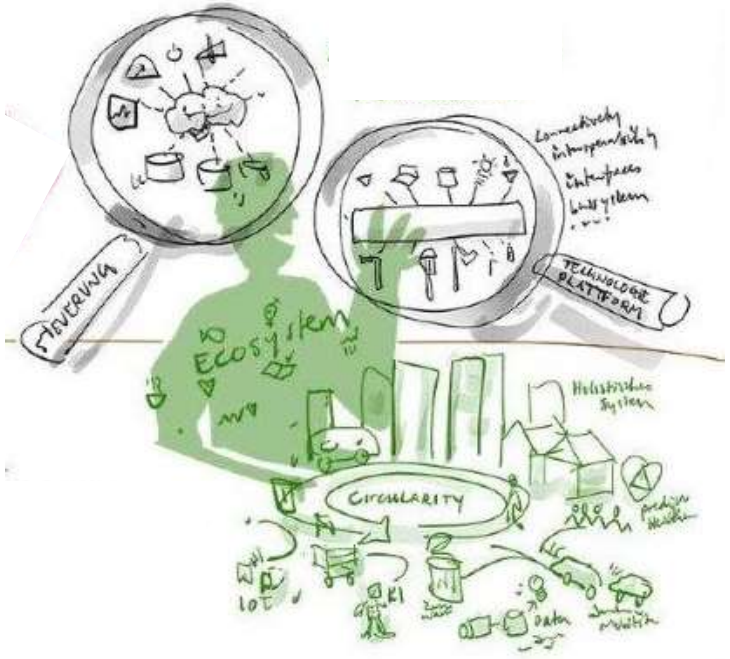
Source: Christian Ridder + Deutsche Telekom

Status today:

- industry started to digitalize assets
- few services like smart-parking, smart-energy, e-gov, e-health, traffic management etc. existing already
- some cities have first trails others are not prepared
- the business model works only for some verticals

Smart City services today are rather isolated silos; technically and businesswise

From “Smart City” to an “Urban Ecosystem"



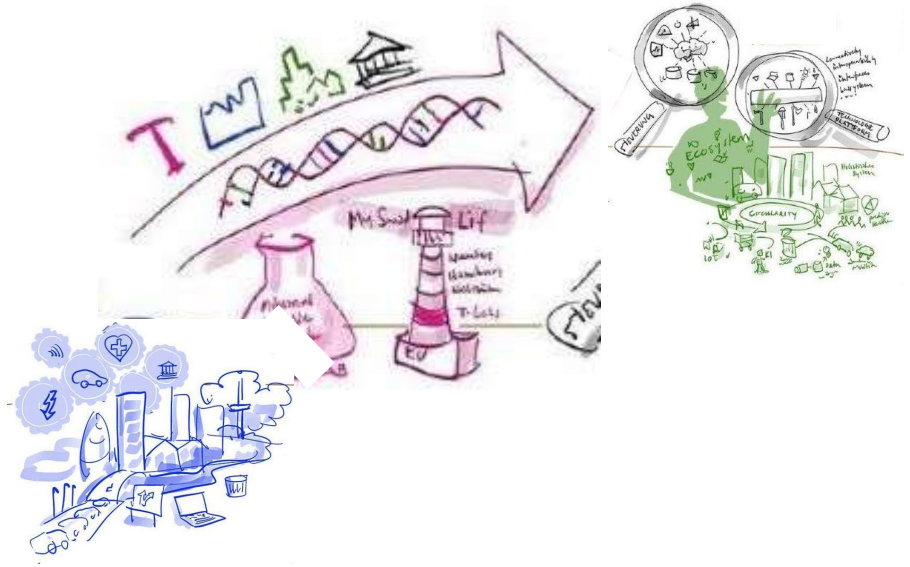
Source: Christian Ridder + Deutsche Telekom

Our vision of a Smart City of tomorrow:

- is an Eco-system with many players from various domains
- with close cooperation of services as a base
- for a circular econonmy
- provided by different partners (communities, authorities, companies, citizens,…..)
- participation of citizens as basic principle
- its about data ethics
- helping to achieve sustainable development goals

An Urban Ecosystem requires an holistic approach

“Urban Ecosystem“ How to get there?



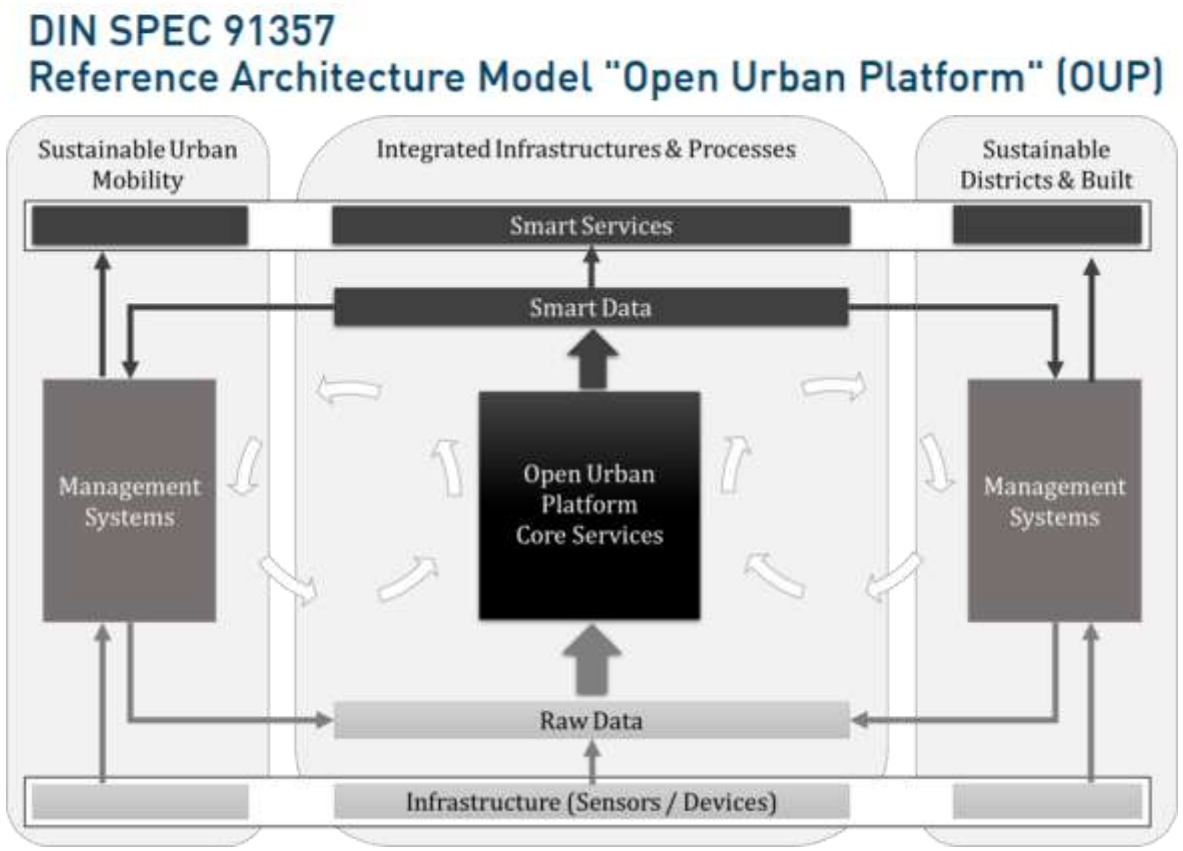
Source: Christian Ridder + Deutsche Telekom

An Urban Ecosystem needs a different thinking :

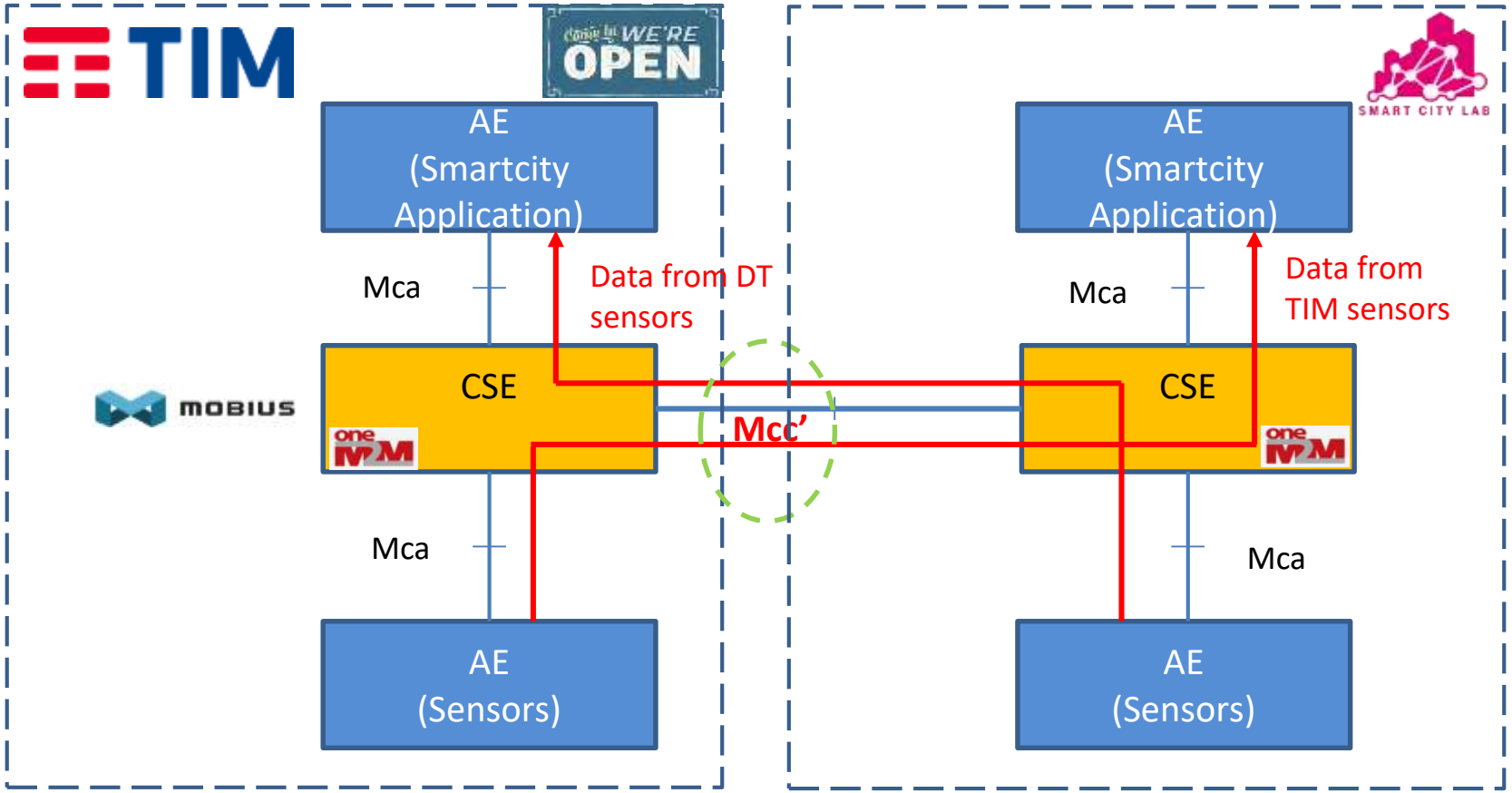
- needs alliances in industry, R&D, intra- and cross domain
- needs interdisciplinary thinking with engineers, sociologists, urban planners in order to define the “DNA” of future cities, villages, regions
- requires modular architectures based on open standards
- scalable and resilient
- needs political involvement and citizen participation
- build living Labs and conduct “Light House Projects”

Join us in building alliances and partnerships

System of Systems



we provided interoperability with OneM2M



Interoperability between oneM2M platforms (CSE):

- AE of TIM can access to data of CSE of DT via Mcc' reference point (and vice versa) using the RCSE
- We have defined data structure of sensors that are accessible via Mcc' reference point
- Only a subset of specific data stored on CSE are accessible from Mcc' reference point
- On Mcc' the protocol used is compliant with oneM2M standard on HTTP(S)

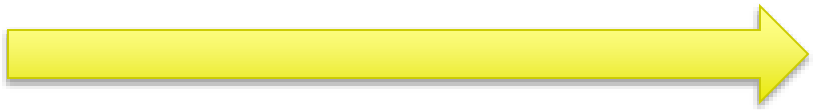
Validation Use Case

http://Provider_A

Service 1

PrKey1 PuKey1

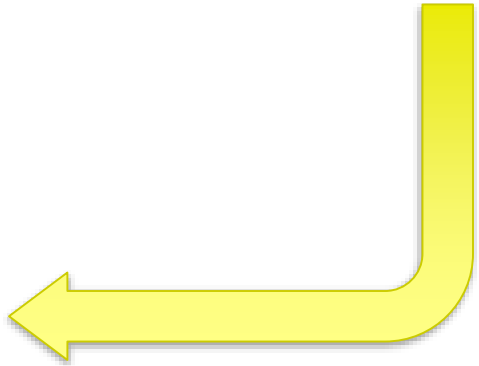
Encrypt
message with
private key (PrKey1)



Send
message along with
public key (PuKey1)
of Service 1

http://Provider_B

Service 2



Validate
belongs public key (PuKey1)
to Service 1
with ID http://Provider_A?

Decrypt
message using
public key (PuKey1)

But how to validate?

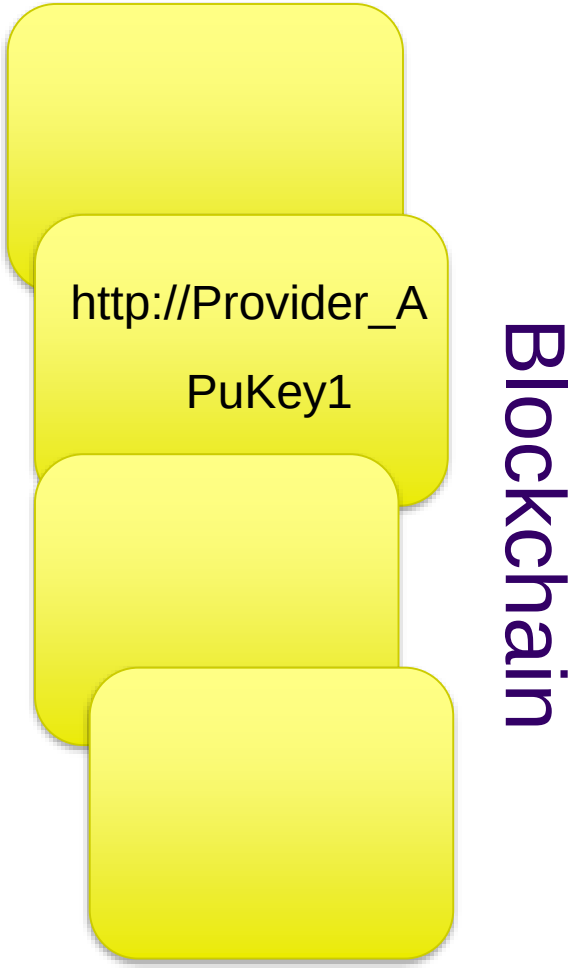
The basic idea

- Is based on public private / public key mechanism
- The private key needs to be as private as possible
- The public key needs to be as public as possible
- The public key combined with a URL is stored in a BC
- “Everyone” can validate / compare the public key by “asking” the BC

Why?

- authentication based on BC might be safer, cheaper, more efficient and easier to use than todays PKI

The BC is used as a “tamper proof” data base



Future Work

Open Questions we want to address in IDoT DG

- What kind of BC is needed? Public/Private
- How to transport the PuKey in a message? JWT/JOSE?
- Who is allowed to write key-URL pair to the BC? (Consensus-Mechanism)
- How to handle/mark outdated data?
- What BC Technology is the most suitable one?
- Implement a prototype?
- Many others…

Lets discuss, design and prototype a great way for authentication in the Internet of Things

JOIN ON:

HTTPS://KANTARAINITIATIVE.ORG/GPA-SIGNUP/?SELECTEDGROUP=34

OR CONTACT:

INGO.FRIESE@TELEKOM.DE