

# IMPULSE TALK #2: PROTECTION

## Next Generation Internet

Thomas Lorünser  
AIT Austrian Institute of Technology

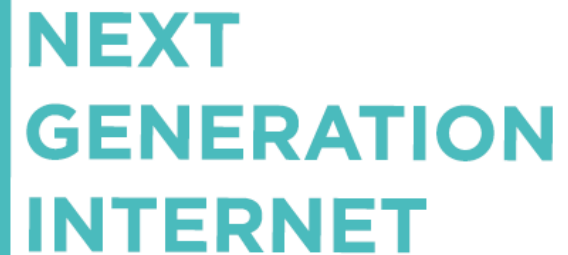


27.11.2018, 16:00 – 18:00 Uhr  
OVE, Eschenbachgasse 9, Wien, 1010 Austria



# NGI RESEARCH CHALLENGES

- Decentralisation
- Privacy
- Innovation Networks
- Multidisciplinarity & End-to-end Networks
- Legislation
- Responsible Machines
- Echo Chambers
- Economics & Wealth Distribution
- Trust and Security



**NEXT  
GENERATION  
INTERNET**

**AN INTERNET OF HUMAN VALUES**  
**Resilient. Trustworthy. Sustainable.**

# DECENTRALISATION

- Decentralisation of Power
- Decentralisation of Infrastructure

Technologies: edge computing, blockchain, IoT, end-to-end security

Research is needed to determine:

- The socioeconomic implications of a few large corporations holding monopolies.
- Options to address these implications, possibly learning from previous economic situations where monopolies needed to be controlled.
- How disruptive technologies and innovations from small players can be given space, freedom and exposure to demonstrate their potential.
- The chances for positive effect of any EC regulation / legislation offset against the cost of pursuing it.
- How any regulation can promote diversity, pluralism and freedom of choice without compromising the services the incumbents provide (which are popular with the general public).

# PRIVACY

Key recommendations are

Technologies: Privacy enhancing technologies, data minimization, privacy by design and default

- Enable transparency
- Raise awareness
- Develop easy to use mechanisms, protocols and legislation
- Towards a practical GDPR

How to enforce control over data for citizens and businesses?

# TRUST AND SECURITY

- Security threats:
  - Trinity of Trouble: Complexity, Connectedness and Dynamicity
  - From Cloud to IoT
- Trust
  - Transparency is enabler for privacy and trust
  - Concentration of power
- Key recommendations:
  - Research on the impact of IoT devices on security
  - Impact of cyber physical systems (networks, devices, resources and people)
  - AI transparency
  - Trust implications of power concentrated in large dominant cooperations

## A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### SECTION 1. SHORT TITLE.

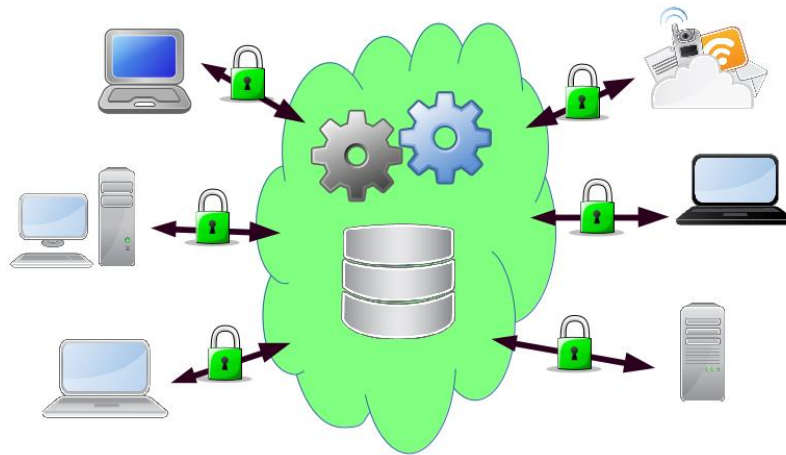
This Act may be cited as the “Internet of Things (IoT) Cybersecurity Improvement Act of 2017”.

# TECHNOLOGIES

Cryptography will be at the heart of a resilient society



# AGILE CRYPTOGRAPHIC SOLUTIONS FOR SECURITY AND PRIVACY

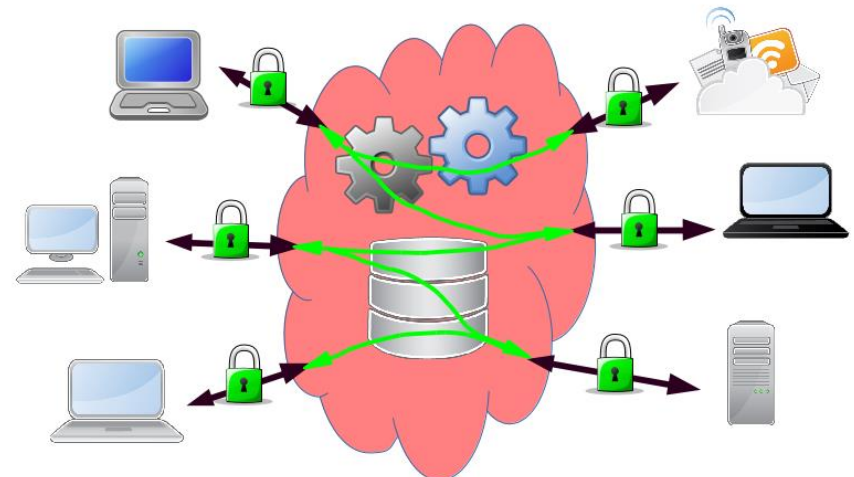


Crypto Agility

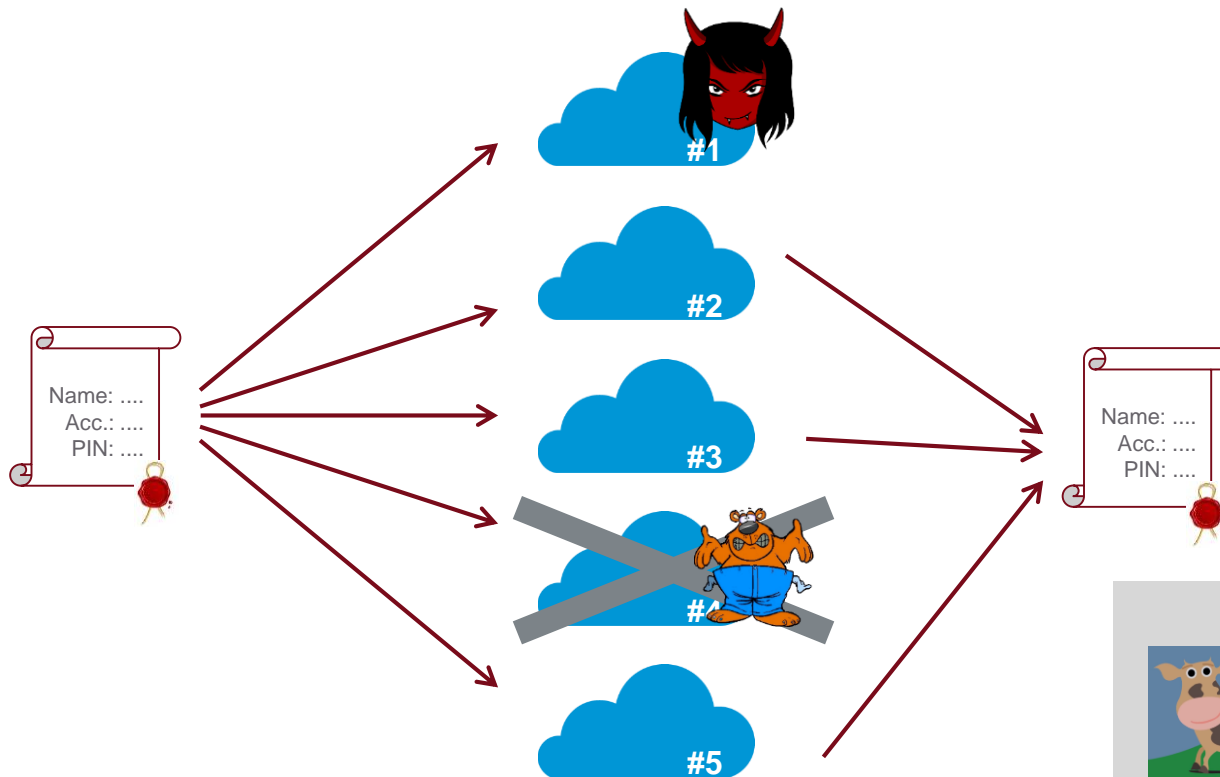
Privacy by  
Data Minimization

Data Agility

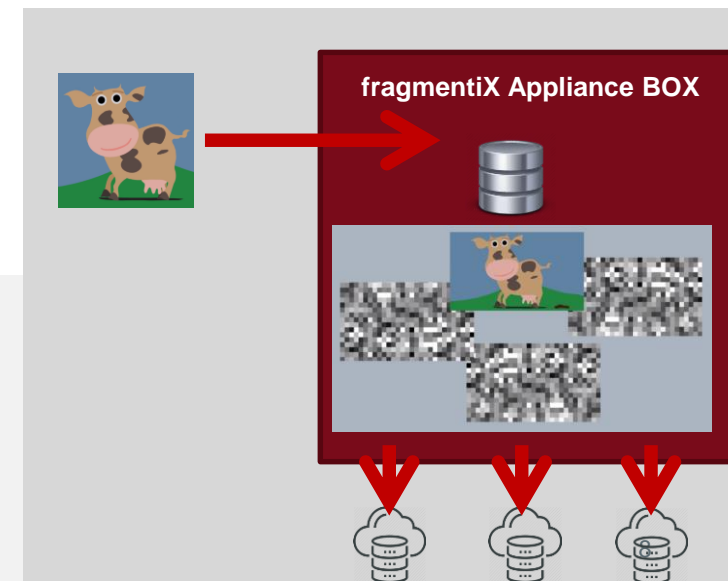
Preventive Protection  
End-to-End Security



# AVAILABLE: DISTRIBUTED STORAGE



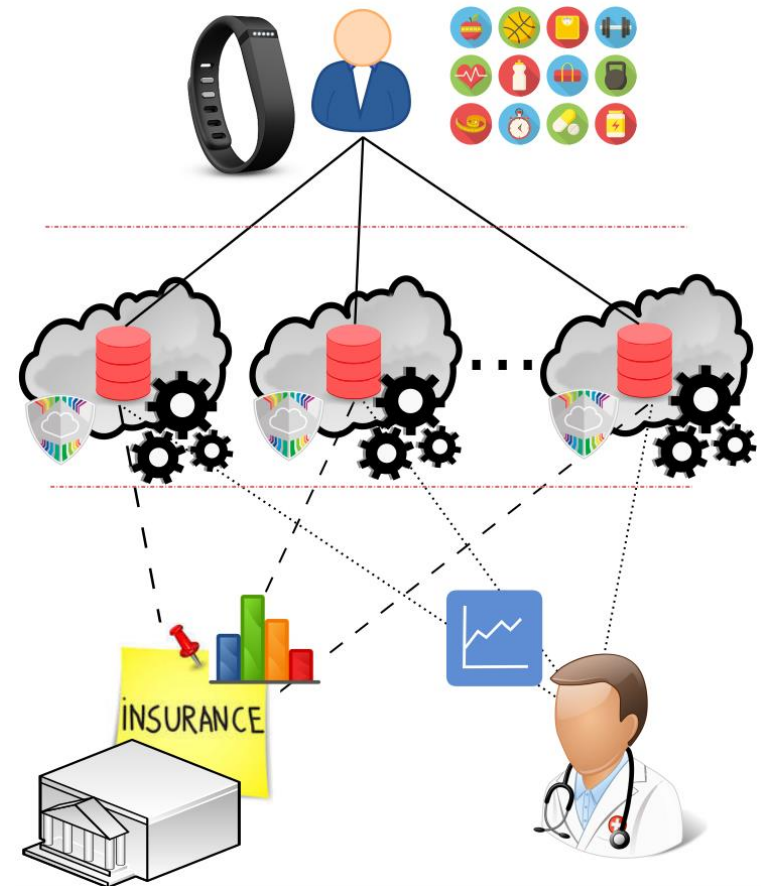
**LINBIT**





# TO COME: MULTI-PARTY COMPUTATION

- Computations on encrypted data
- Distributed system
- Security based on non-collusion
- First application was secure auction



# EXAMPLE: IPFS APPROACH

## Interplanetary File System

- Content addressed distributed storage (CADS)
- Files/content identified by hash of contents (CID)

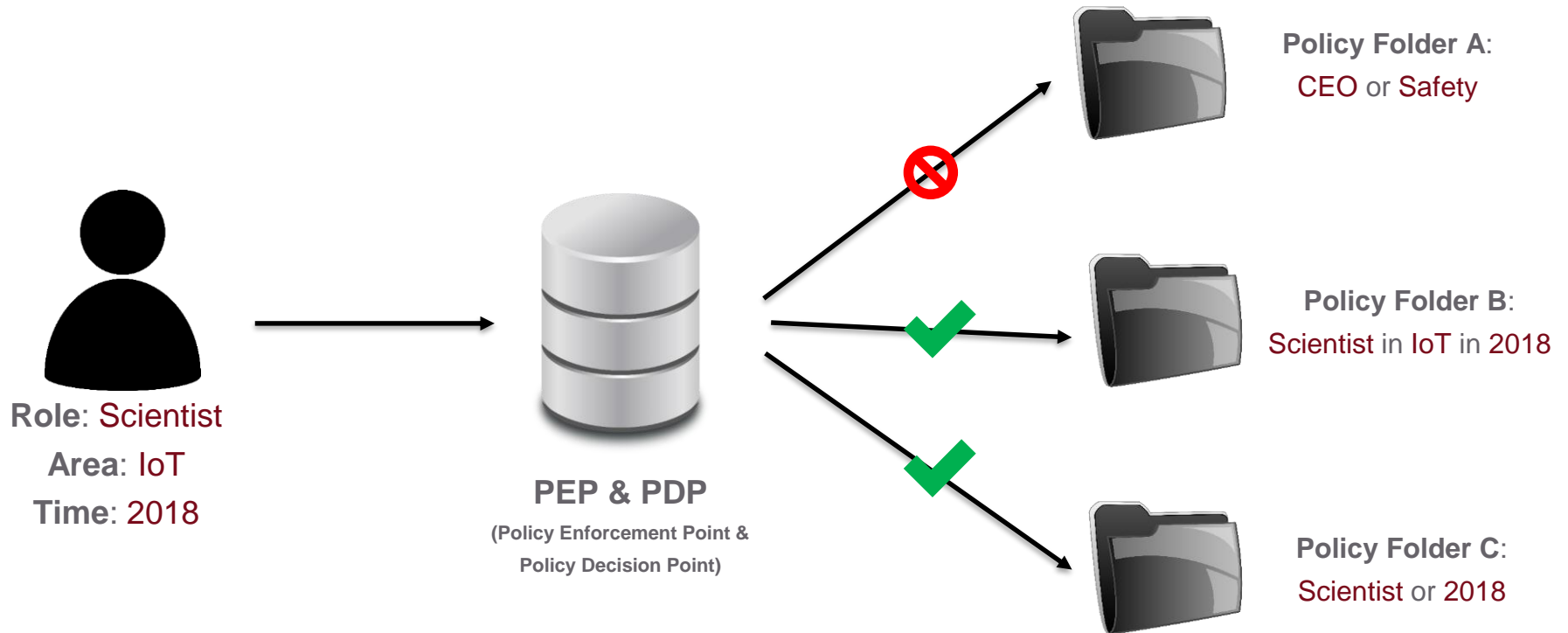
No Confidentiality  
and Authenticity!

=> IdM, Access Control,  
Encryption

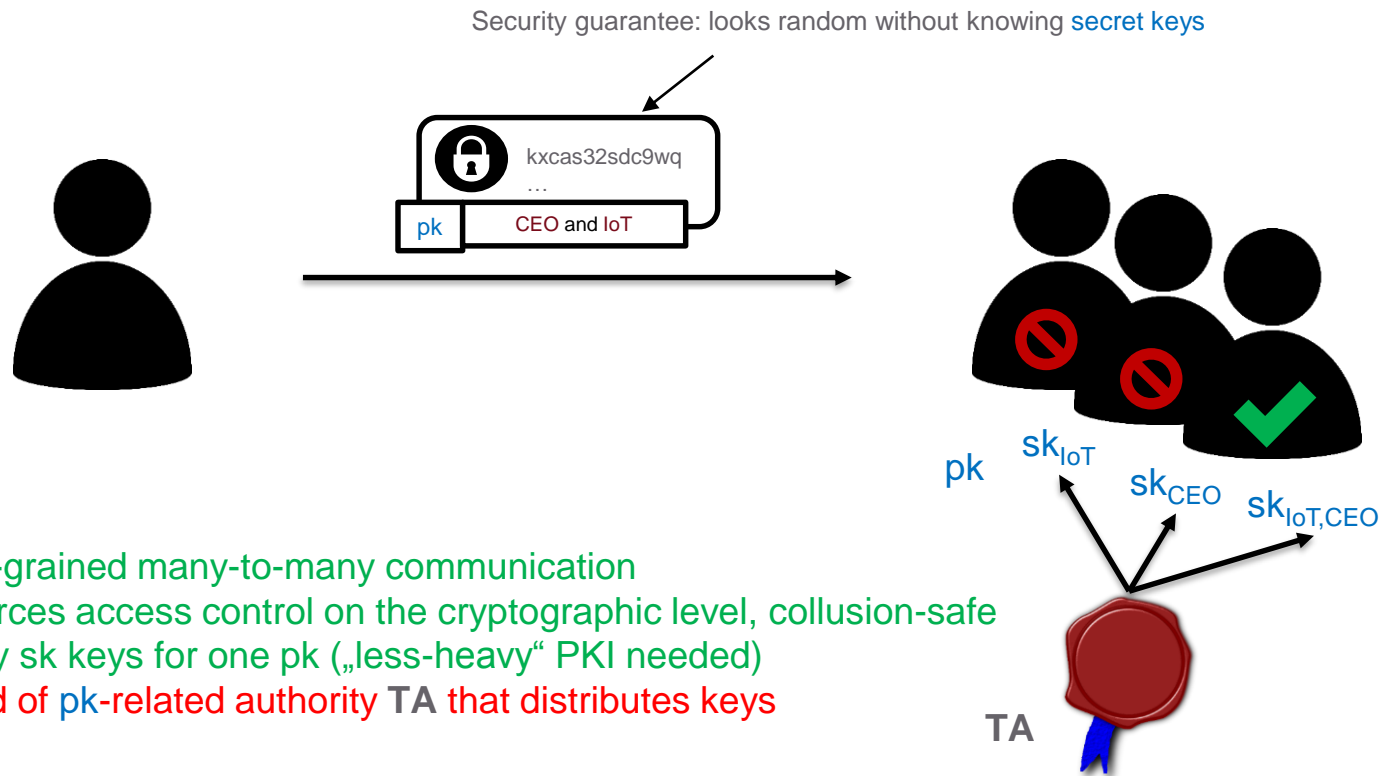
### Combination of different technologies:

- Distributed Hash Tables (DHT)
- Block Exchanges – Bittorrent
- Version Control Systems – Git
- Self-certifying File System (SFS)

# DATA SHARING SIMPLIFIED

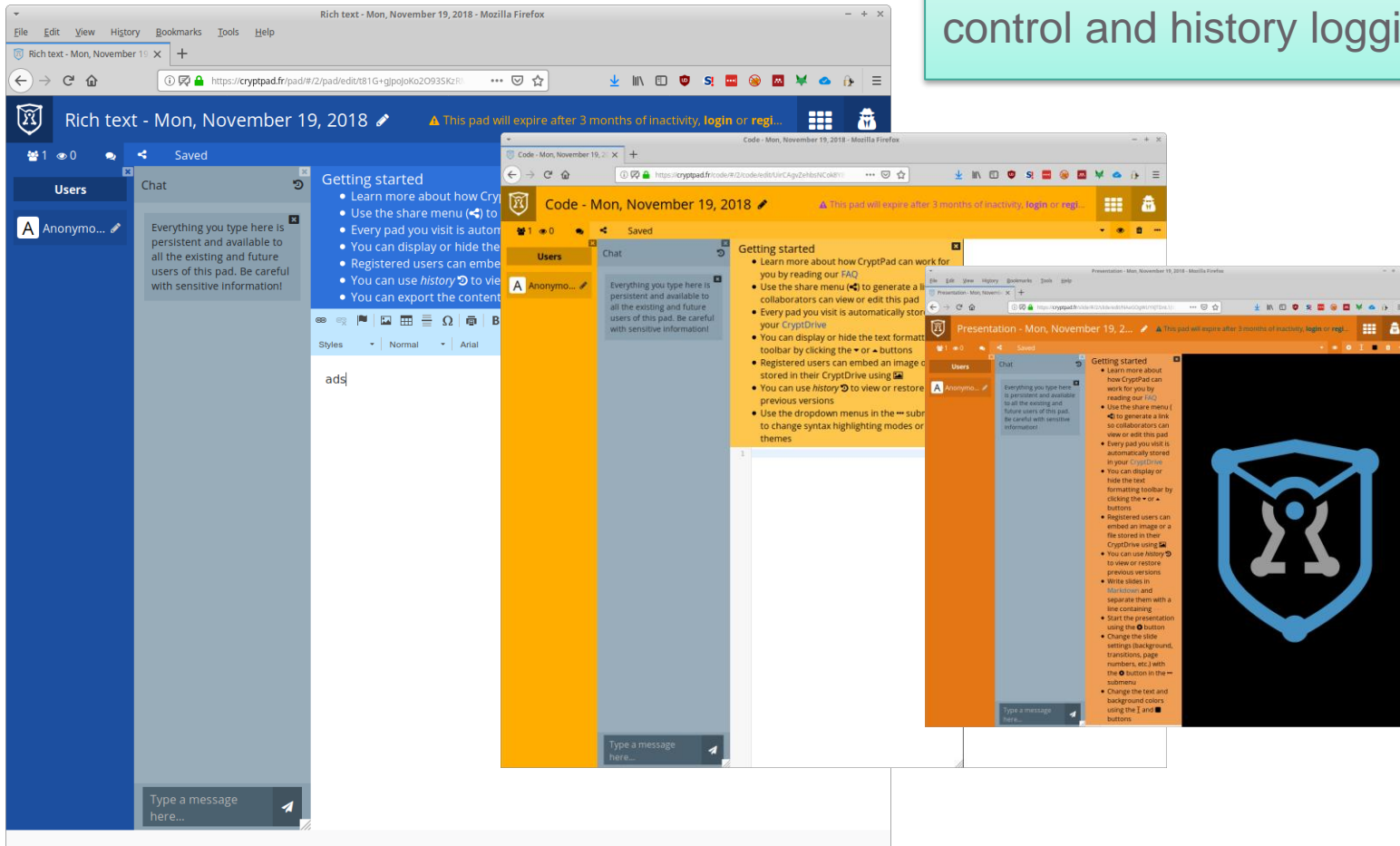


# IN STANDARDIZATION: ATTRIBUTE-BASED ENCRYPTION



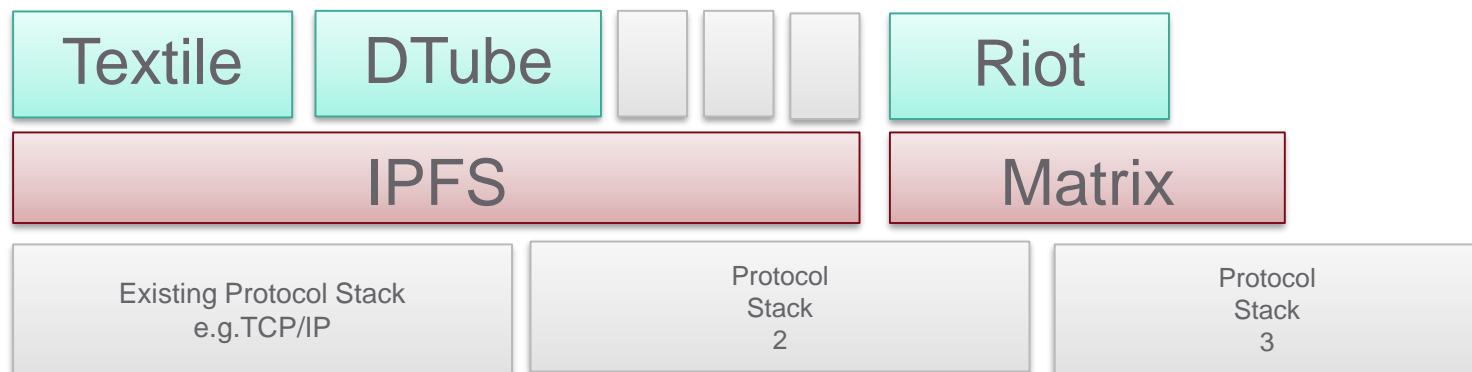
# EXAMPLE: CRYPTOPAD

Peer-to-peer operational transformation (OT) with version control and history logging

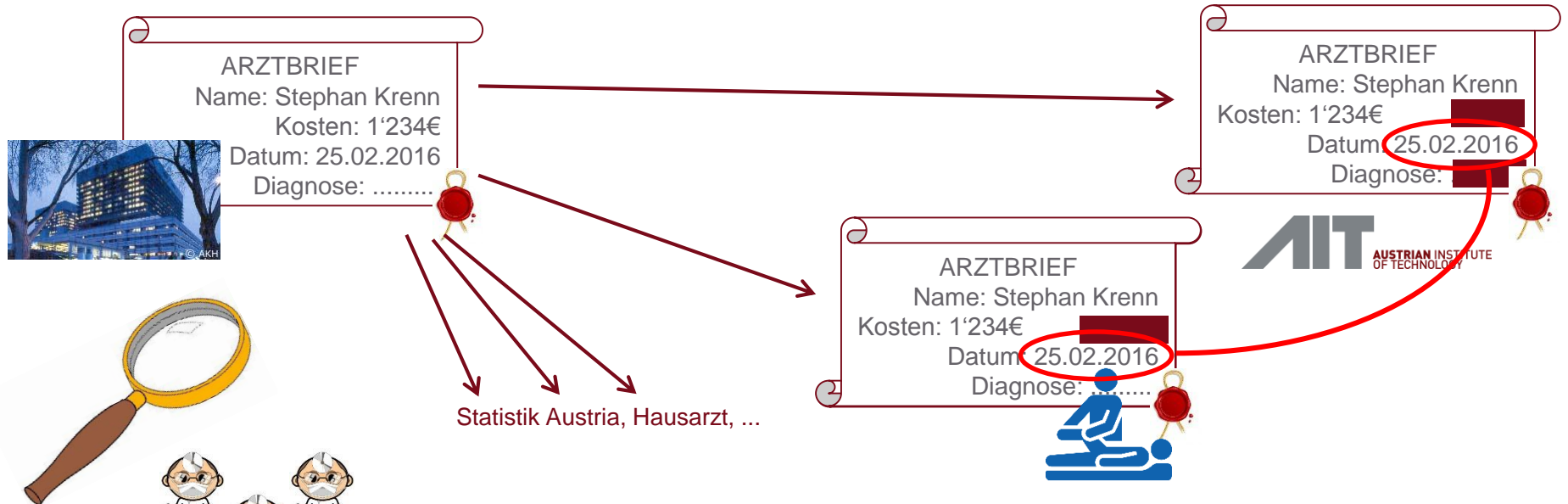


# DEZENTRALIZED WEB APPLICATIONS

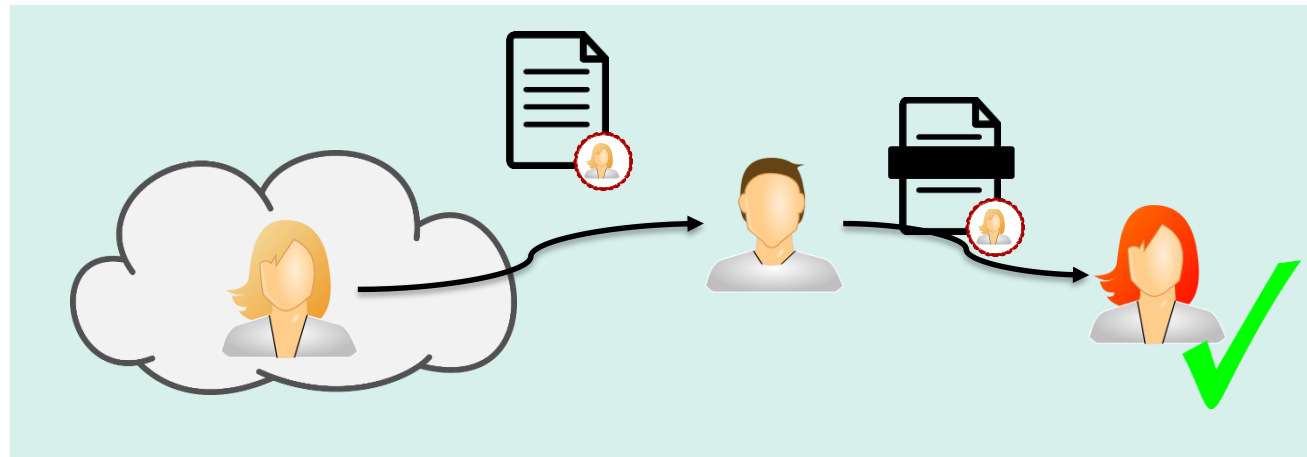
- OpenBazaar (a decentralised marketplace) <https://openbazaar.org/>
- Graphite Docs (a Google documents alternative) <https://www.graphitedocs.com/>
- CryptPad (Google docs alternative) <https://cryptpad.fr>
- Textile Photos (an Instagram-like alternative for storing, managing, and sharing photos on the DWeb) <https://www.textile.photos/>
- Matrix (which provides Slack and WhatsApp alternatives) <https://matrix.org>
- DTube (a YouTube alternative) <https://d.tube/>
- Social network alternatives include [Akasha](#) and [Diaspora](#)



# SANITIZABLE SIGNATURES FOR SELECTIVE DISCLOSURE

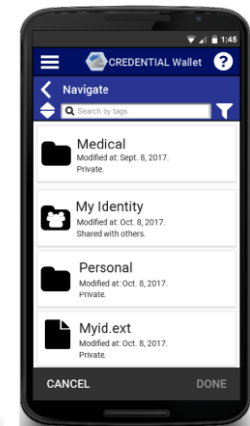
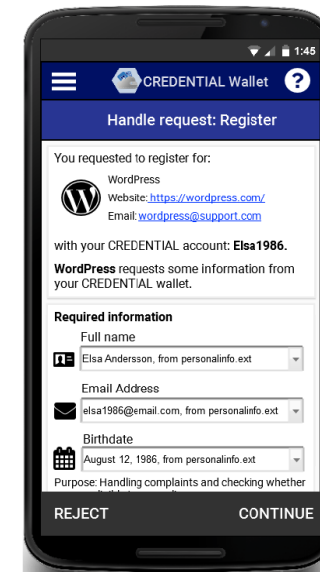
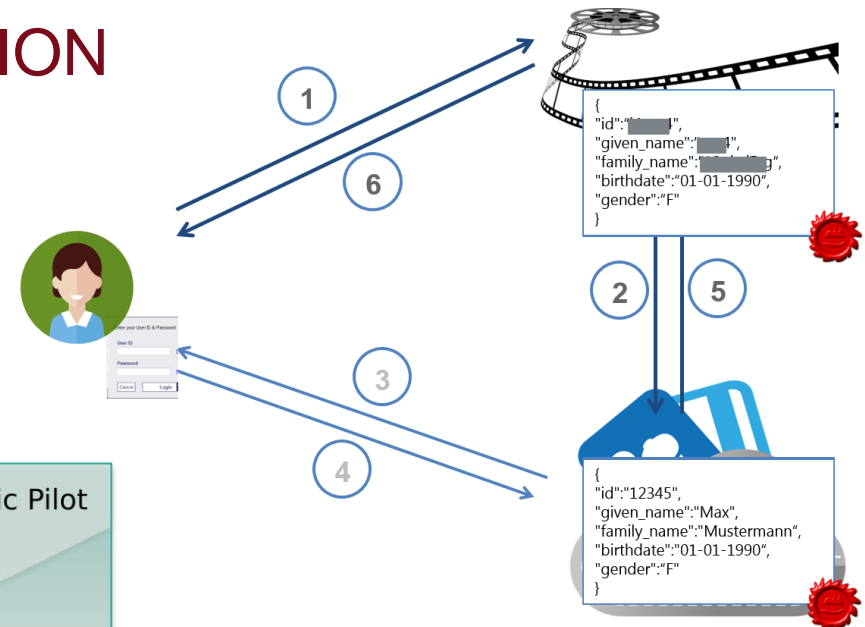
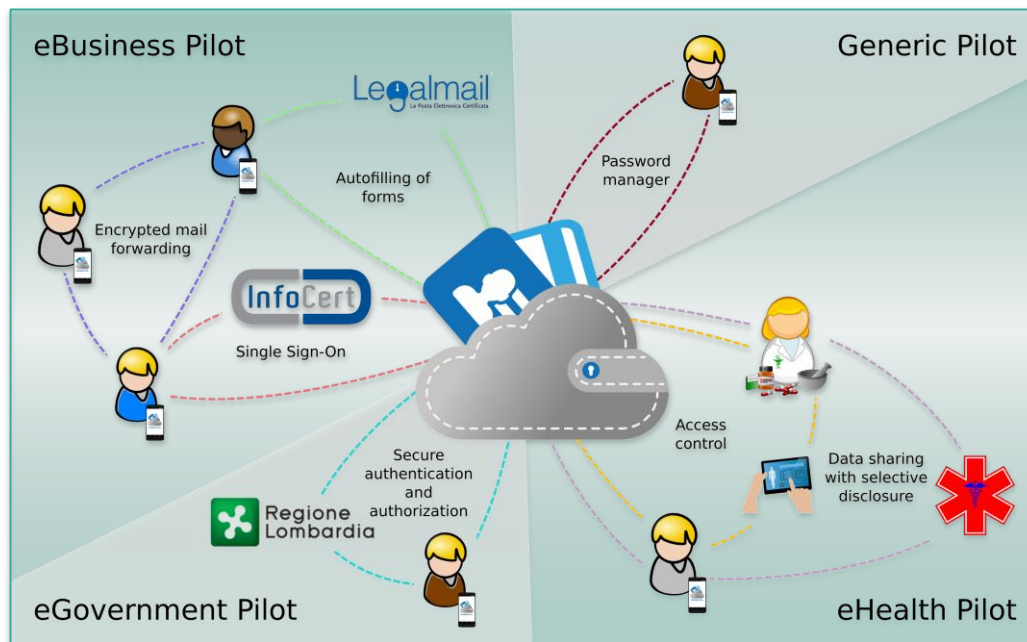


Darf Identität des Unters-  
schreibenden bekannt sein?



# ANONYMOUS AUTHENTICATION

- Strong authentication to the cloud
- Certain anonymity
- Unlinkability





# AND MANY MORE CRYPTOGRAPHICAL TOPICS FOR A BETTER NGI

- Ring-Signatures
- (Fully) homomorphic encryption
- Verifiable computing
- Functional encryption
- Lightweight encryption
- E-Voting
- Authenticated encryption
- Efficient implementations
- New stream and block ciphers

A large, light blue speech bubble containing the text "NEXT GENERATION INTERNET" in bold, dark blue capital letters.

**NEXT  
GENERATION  
INTERNET**

**Thank you!**