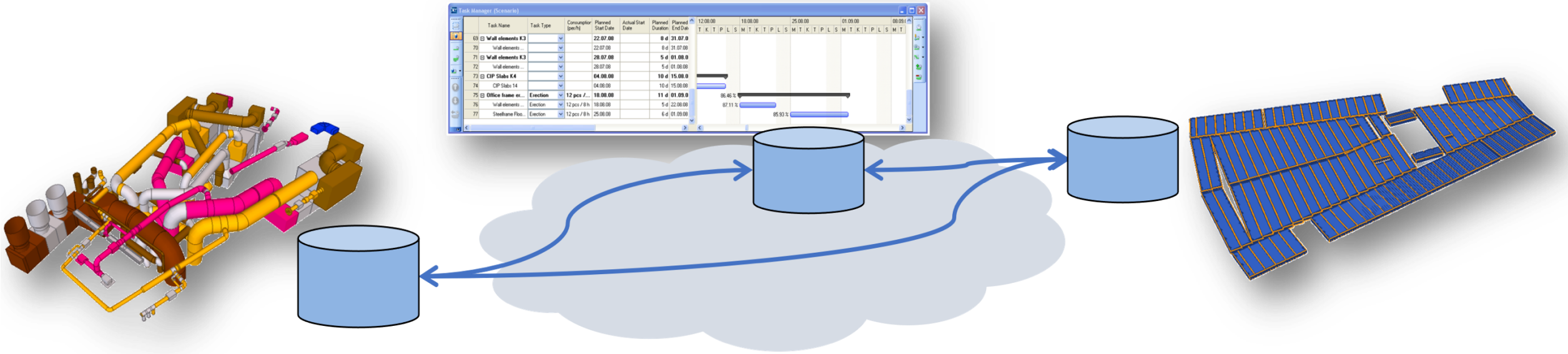


Decentralization and trust

Managing and Sharing of Construction Data

Computing in Construction

Metropolia

Metropolia

Collaboration and trust

Efficient collaboration and interoperability require trust among parties

In construction where consortiums change from project to project, new collaborating parties can often be encountered

In digitalized construction, especially in the design stage, the parties may even meet only in the digital realm

How can the necessary trust be established between parties?

Metropolia

Trust

- Definition [Oxford languages]
  - *trust is firm belief in the reliability, truth, or ability of someone or something*
- Establishing trust between parties unknown to each other is challenging
  - yet it is essential for cooperation, data sharing, and secure interactions
- Trust is complicated in digital systems in general
  - in decentralized systems it is even more difficult

Challenges: We may not know

- who the other party is
  - in the digital world
  - in the real world
- whether the other party
  - is reliable
  - is truthful in general
- what the other party
  - is able to do (competencies)

Solution approaches

- identity systems
  - centralized identity: government, bank, ...
  - self-sovereign identity: public/private cryptographic keys
- reputation systems
  - feedback from previous actions
  - social proof: linking to trusted third parties
- credentials
  - verifiable credentials

Centralized identity management

- National Digital ID – mobile certificate (personal id, id card)
  - single, secure identity for various official and private transactions
  - physical identification is required at some point to acquire the id
- Bank ID – online banking codes
  - customer relationship with a bank is required
  - bank must invest in resources to keep identification services up
- Directory-based identity management
  - common in corporate settings to manage employees' access to internal systems and resources
- Social login – Google, Facebook, Apple, ...
  - single sign-on: identity provider issues tokens that allow access to other connected services
- Others
  - biometric identification – recorded fingerprints, iris scans, facial images managed by authority
  - certificate-based identification – user has digital certificates issued by a certificate authority

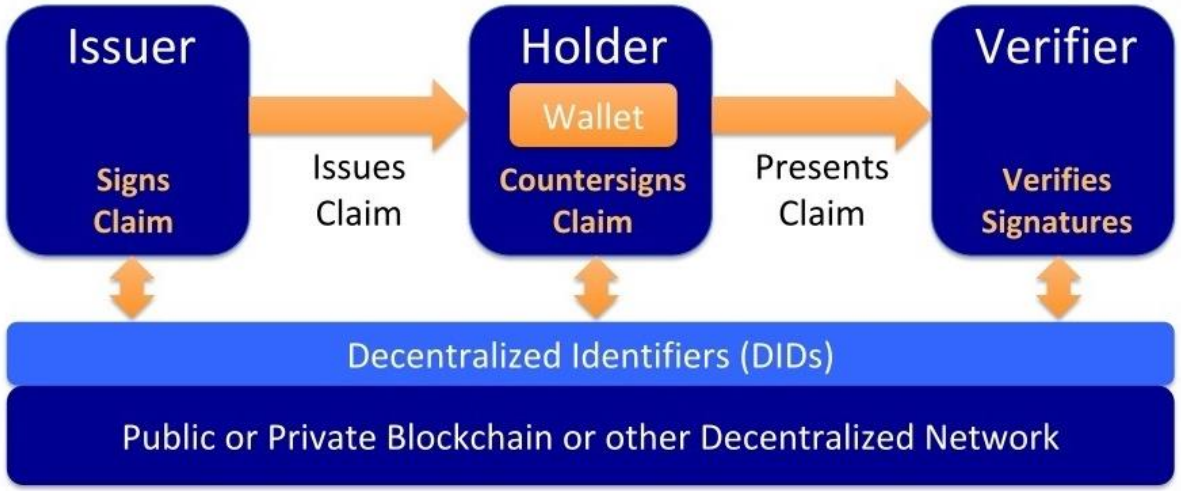
Centralized systems are relatively
- simple and
- easy to manage

However, they often come with trade-offs with
- data ownership
- user privacy
- security: vulnerability to cyberattacks
- bottleneck in verification process

Metropolia

Decentralized identity management

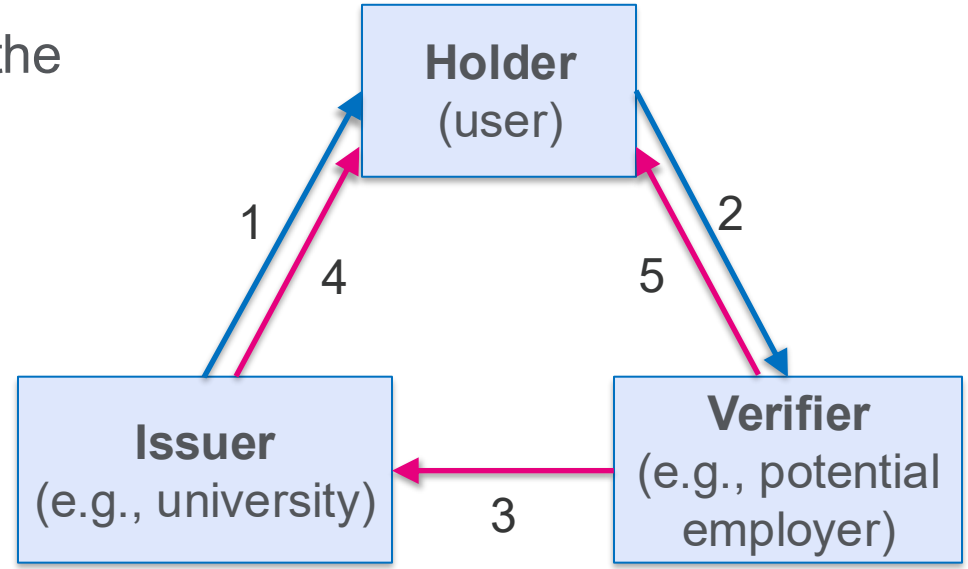
- Self-sovereign identity (SSI)
  - User creates and controls her digital identity using cryptographic keys
    - key are created and managed by the user
    - no central or external authority is involved
  - Public and private key (~ a digital ID card)
    - public key is shared openly
    - the private key is kept secret



- Verifiable credentials
  - User can have digital credentials (e.g., diploma) issued by some party (e.g., a university) in a form that can be digitally verified by a third party (e.g., a potential employer)
  - Process needs a decentralized registry (or blockchain)
    - issuers publish their public keys for verification purposes
    - can contain also a credential registry for information about revoked or expired credentials

Verifiable credentials

- User can have credentials (diploma) from a university that she needs to present to a potential new employer
- Verifiable credentials work as follows:
  1. The issuer trusts the holder (and gives the credentials signed with issuer's private key)
  2. The holder trusts the verifier (and presents credentials, optionally signed with private key to prove ownership)
  3. If the verifier trusts the issuer
  4. then he verifies the credentials given by the issuer to the holder (using the public key of the issuer), and optionally the holder's signature (with her public key), to ensure the rightful ownership of the credential
  5. as the result, the verifier also becomes to trust certificate of the holder



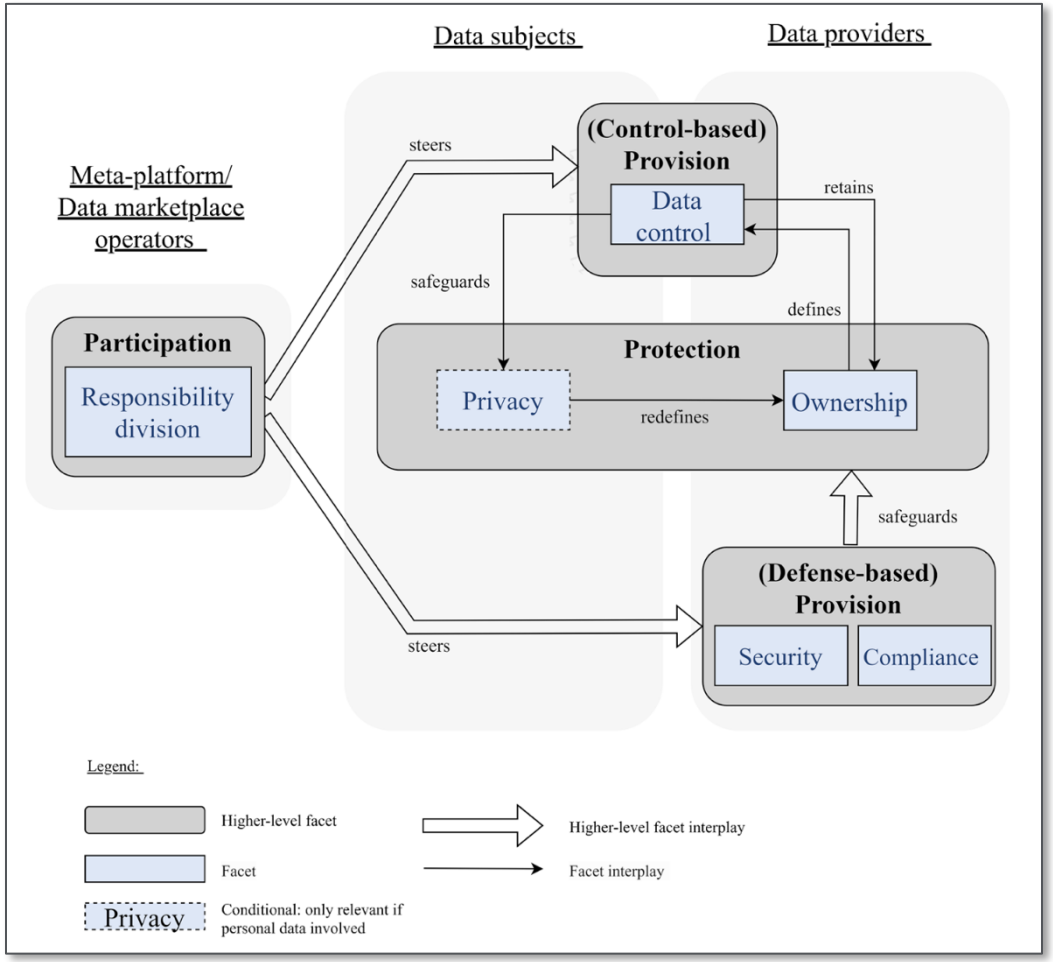
Tackling the challenges of trust

1. Identity and verification
   - self-sovereign identity and verifiable credentials
2. Reputation systems
   - feedback, social proof, reputation scores
3. Trust frameworks and governance models
   - trust achors (trusted organizations, e.g., government, banks, universities)
   - can play a regulatory role
4. Auditability and transparency
   - immutable ledgers (e.g., blockchain): information and transactions can be recorded in shared and unchangeable manner
5. Incentive and penalty mechanisms
   - incentives for honesty
   - escrow services: hold funds in a neutral account to ensure that both parties fulfill their commitements
6. Consensus Mechanisms
   - to reach consensus (make common decisions) even if all parties cannot be trusted
   - proof-of-work, proof-of-stake, byzantine fault tolerance algorithms

Metropolia

Control over the data

- Data sovereignty
  - the ability of individuals, organisations, and governments to have control over the data they hold and
  - exercise their rights on the data, including its collection, storage, sharing, and use by others
  - involves the establishment and enforcement of rules for data sharing and utilization, including data usage policies and contracts, with differing levels of control
- Facets
  - protection
    - data ownership
    - privacy (claims of data ownership by the subjects)
  - participation
    - responsibility divisions
  - provision
    - control, security, and compliance mechanisms
    - ensure that foundational rights are preserved during and after data sharing
- Contextual conditions affecting data sovereignty
  - data type
  - organizational size
  - business data sharing setting



Abbas, A.E., van Velzen, T., Ofe, H. *et al.* Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electron Markets* **34** (2024).

Thank you!

Metropolia