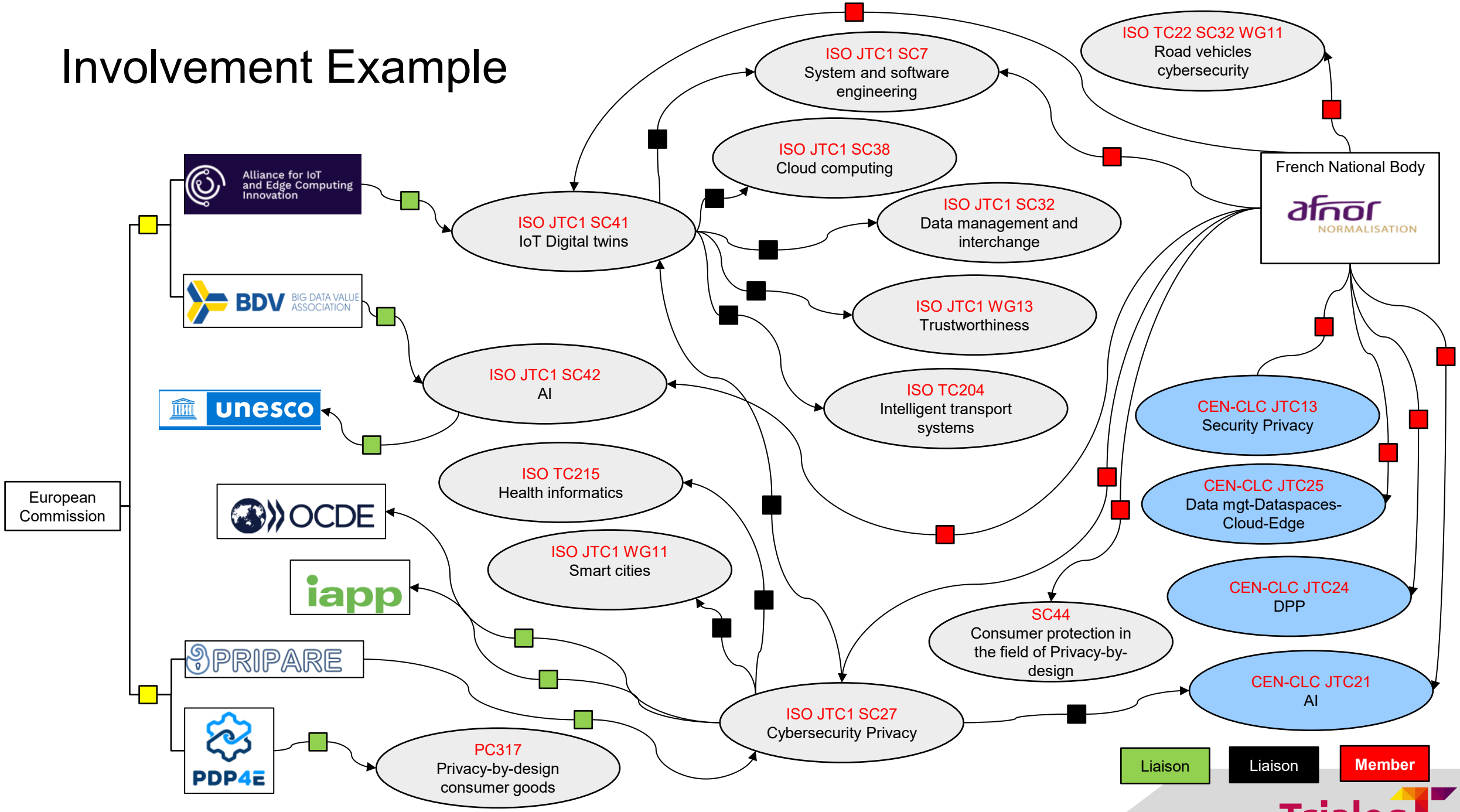
Security and privacy issues or challenges for Digital twins and Metaverse

Antonio Kung – Trialog

Speaker

- Co-founder - former CEO – Executive board
  - IoT systems
    - Smart meters, Vehicle charging, Connected vehicles
- AIOTI: Chair WG Standardisation
  - https://aioti.eu/
- BDVA: Lead TF Standards and Benchmarking
  - https://bdva.eu/
- Involved in ISO/IEC, ISO, ITU-T, CEN-CENELEC, ETSI
- Standardisation topics
  - Use cases, Architecture
  - IoT, Digital twin, AI, Metaverse
  - Security and Privacy, Interoperability, Trustworthiness
  - Smart cities, Automotive
  - Health, Energy, Vehicle charging

Involvement Example

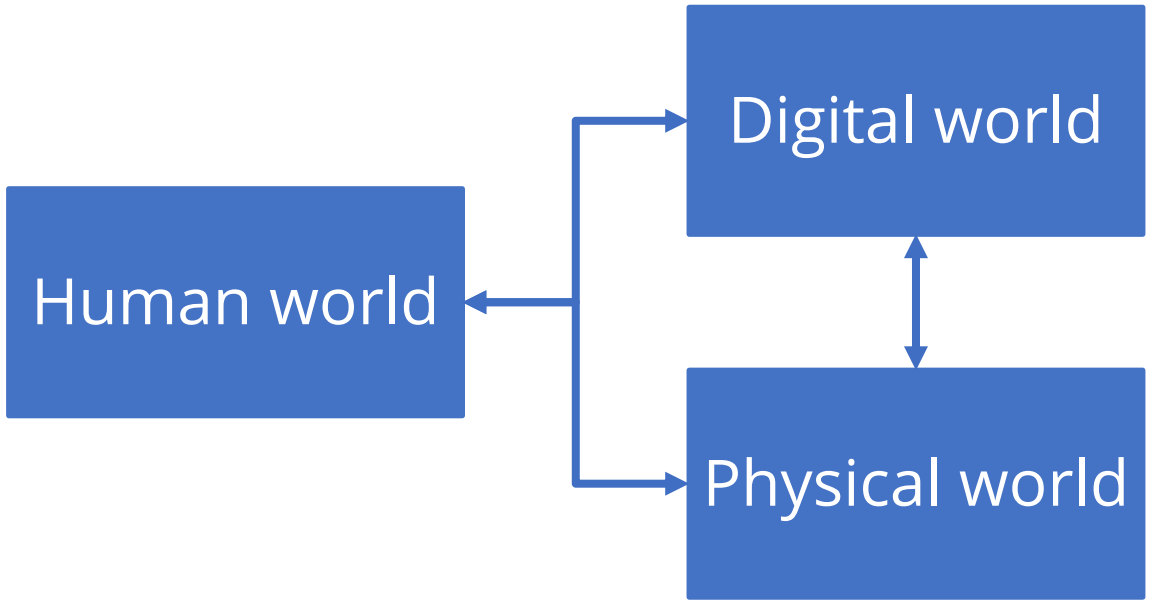


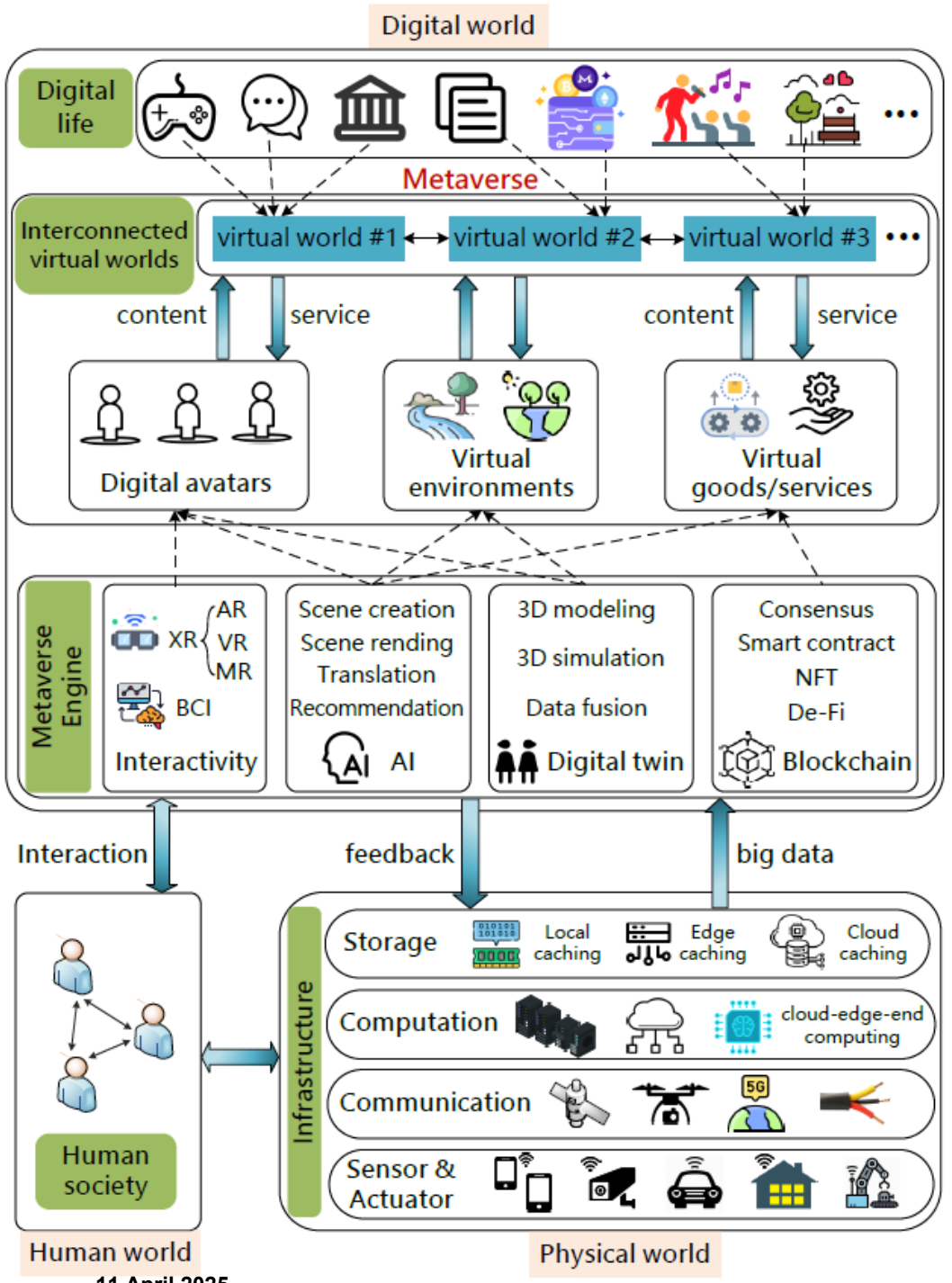
Challenges and issues

- Context
- Challenge: ecosystem domain integration
- Challenge: governance
- Hourglass model to describe ecosystem
- Hourglass model for security and privacy

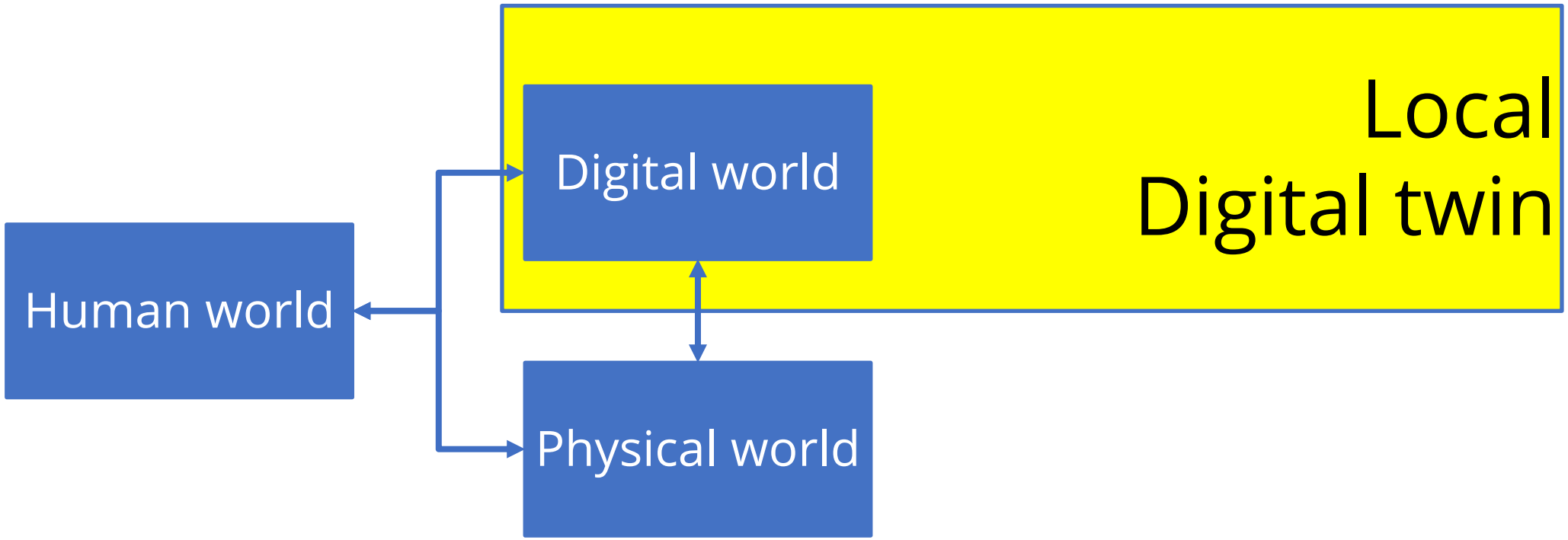
Conceptual view of virtual worlds

- A Survey on Metaverse: Fundamentals, Security, and Privacy
  - https://arxiv.org/abs/2203.02662



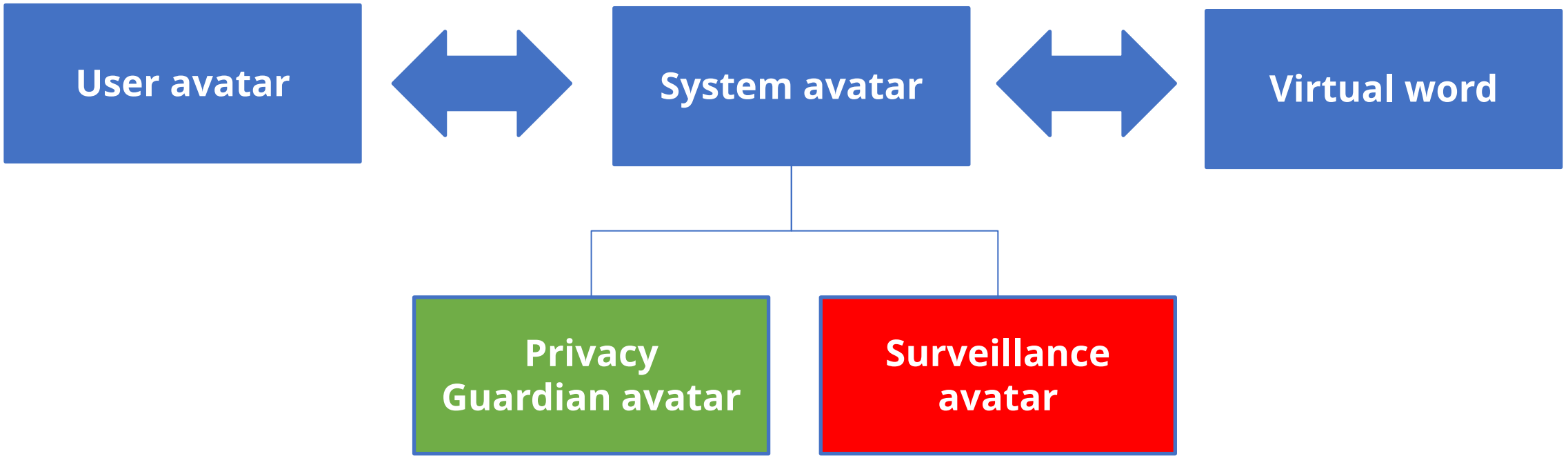


Digital twin for the virtual world



Privacy challenges for the virtual world

- Example of ISO/IEC 27573 Privacy protection of user avatar and system avatar interactions in metaverse



Challenges and issues

- Context
- Challenge: ecosystem domain integration
- Challenge: governance
- Hourglass model to describe ecosystem
- Hourglass model for security and privacy

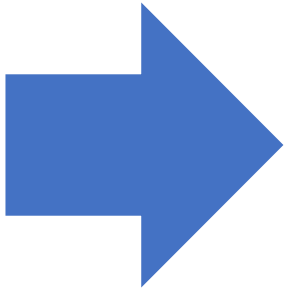
A Domain Approach

- Domain: field of special knowledge
  - Application domains - vertical domains: energy, health.
  - Technical domains - horizontal domains: AI, IoT, DLT, Data, Data space, Virtual World
  - Cross-cutting domains - security, privacy, safety, resilience.
- Ecosystem: deals with multiple domains.
  - The citiverse is a smart city ecosystem which integrates the virtual world
- Domains can include subdomains.
  - The energy domain includes the generation, transmission, or distribution subdomains.
  - The smart home domain includes the entertainment, home control, energy management subdomains.

The need for Interplay

Application domain A

- Domain information model
- Repository of practice
  - Interoperability models



Horizontal technology

- Artificial intelligence
- Virtual world
- IoT
- Digital twin
- DLT
- Quantum …

Cross-cutting characteristics

- Security
- Privacy
- Resilience
- Safety
- Sustainability
- …

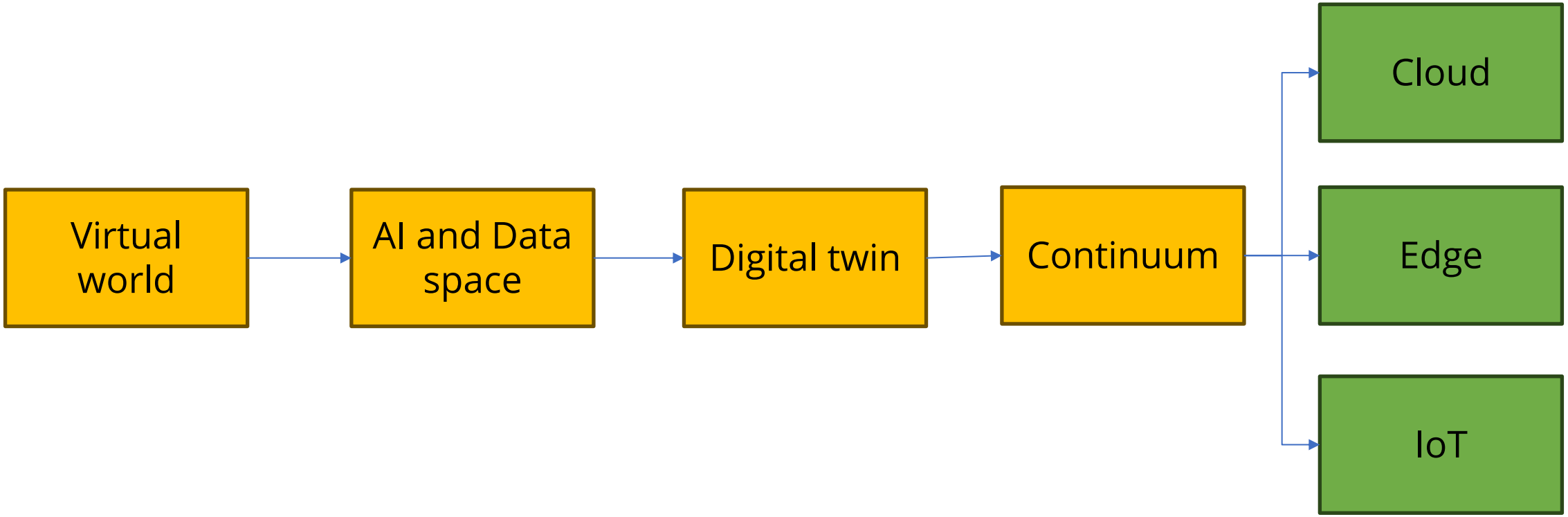
Application

- Health
- Energy
- Transport
- Manufacturing
- Finance
- …

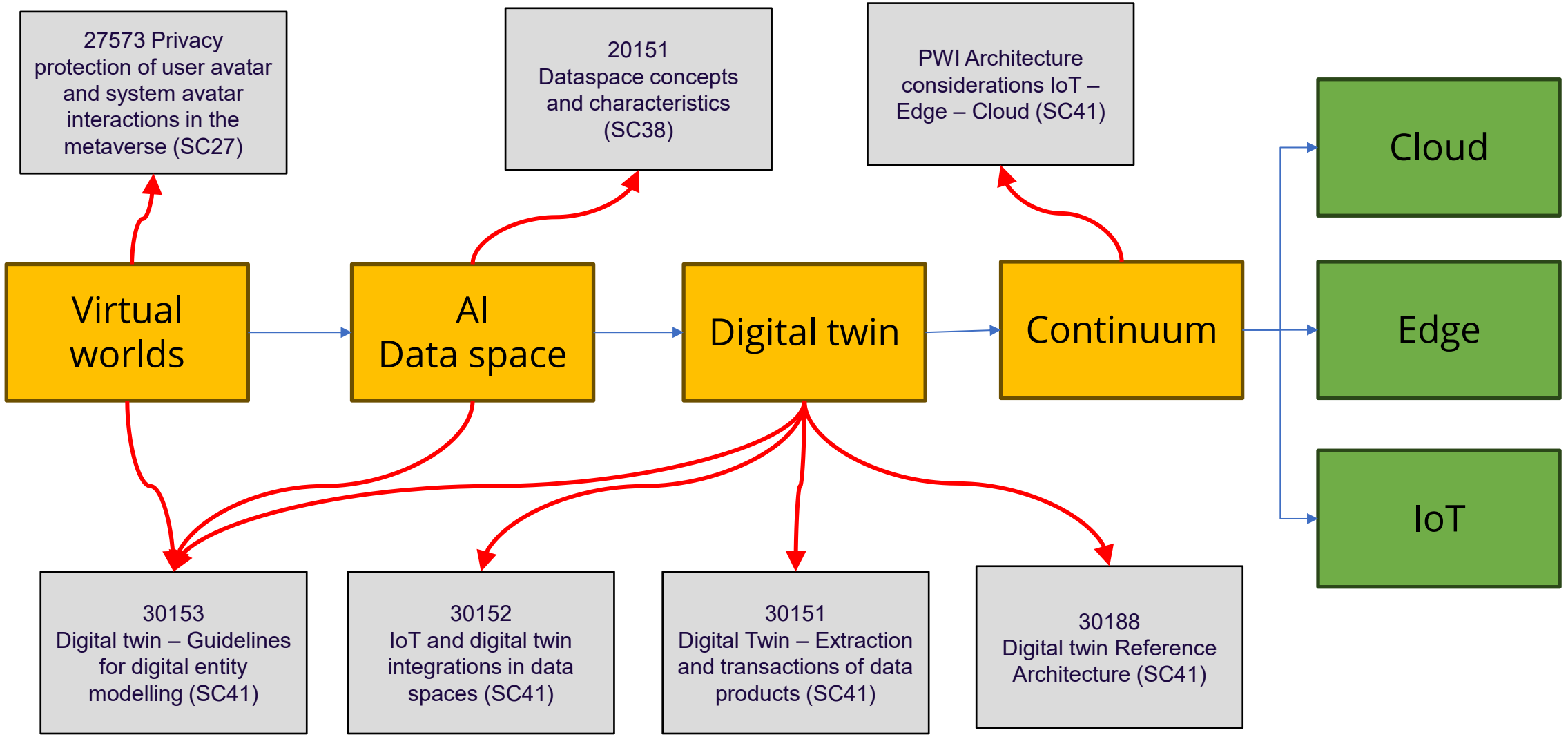
Ecosystem

- Smart cities
- Conformity
- Metaverse

An architecture and interoperability issue



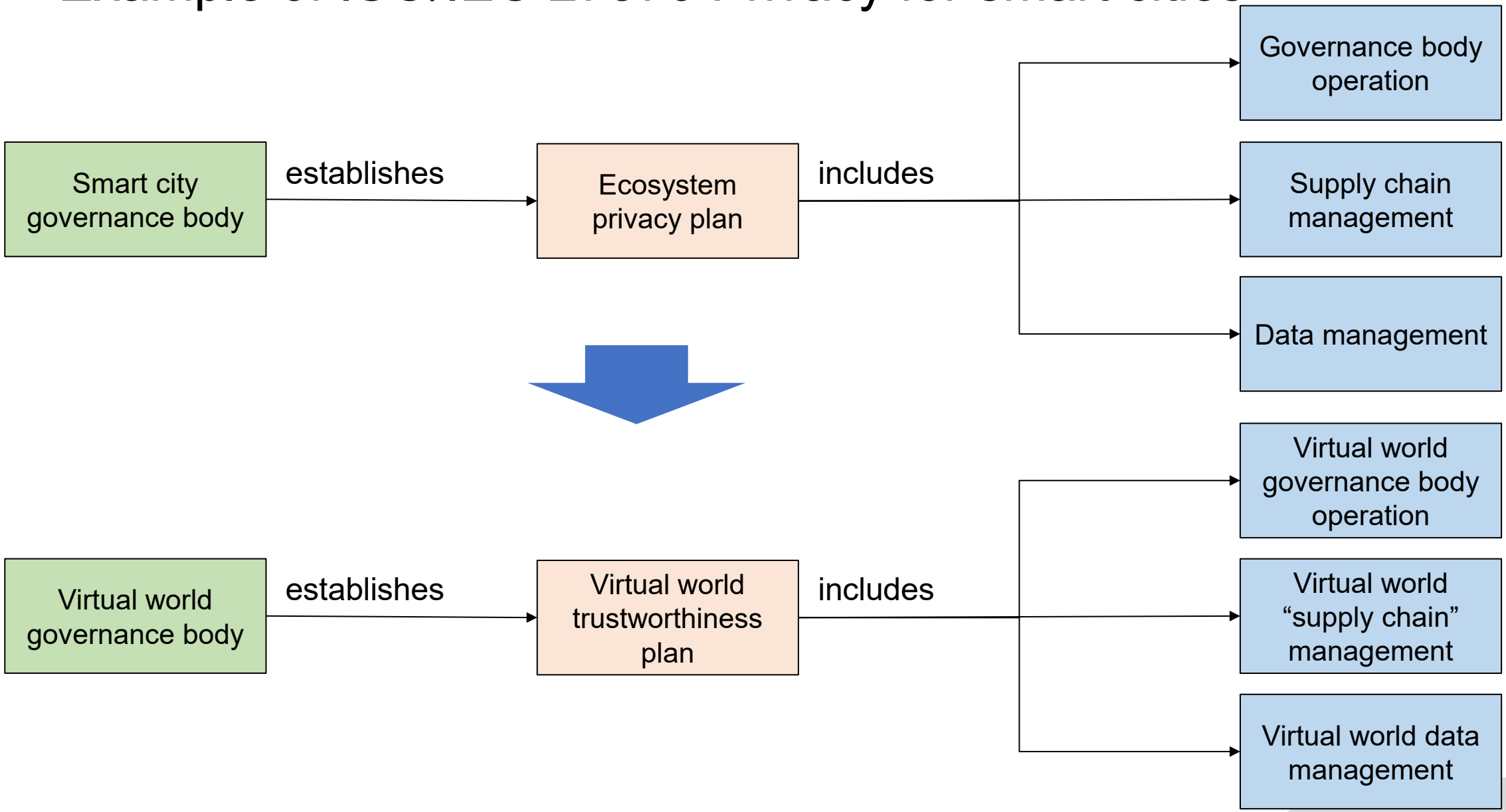
Example of related standards



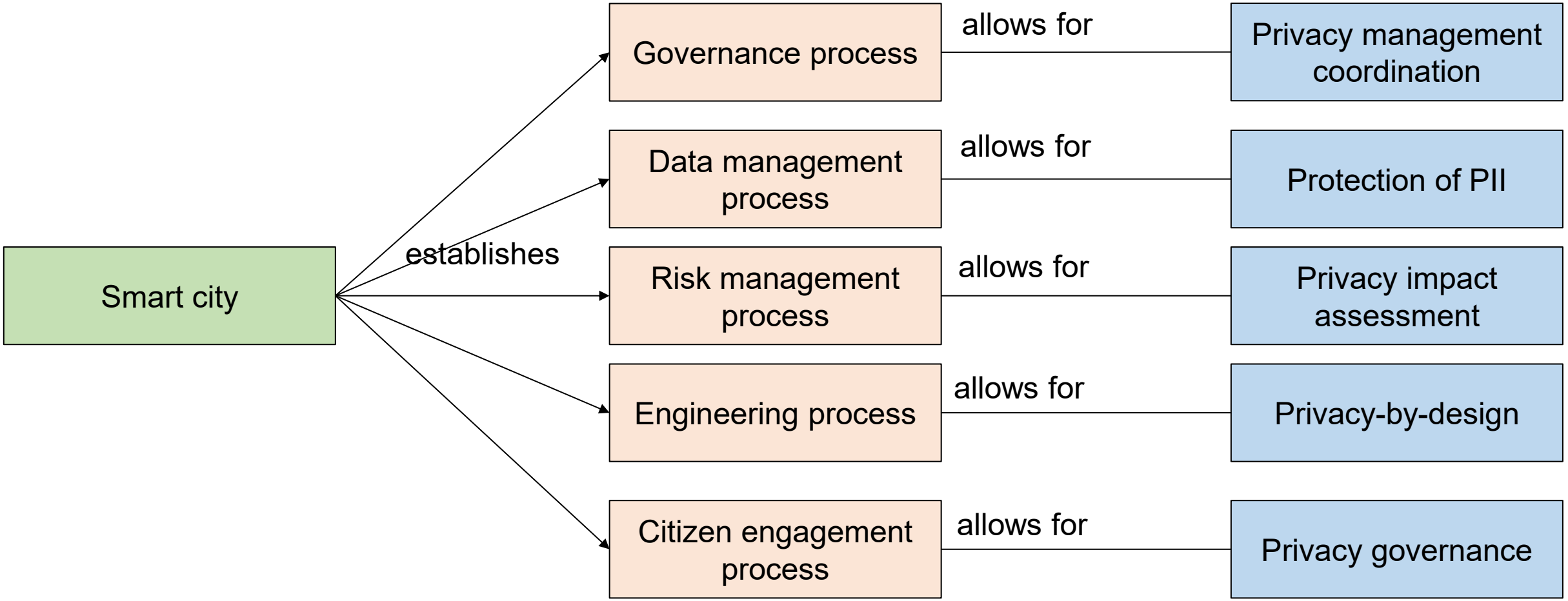
Challenges and issues

- Context
- Challenge: ecosystem domain integration
- Challenge: governance
- Hourglass model to describe ecosystem
- Hourglass model for security and privacy

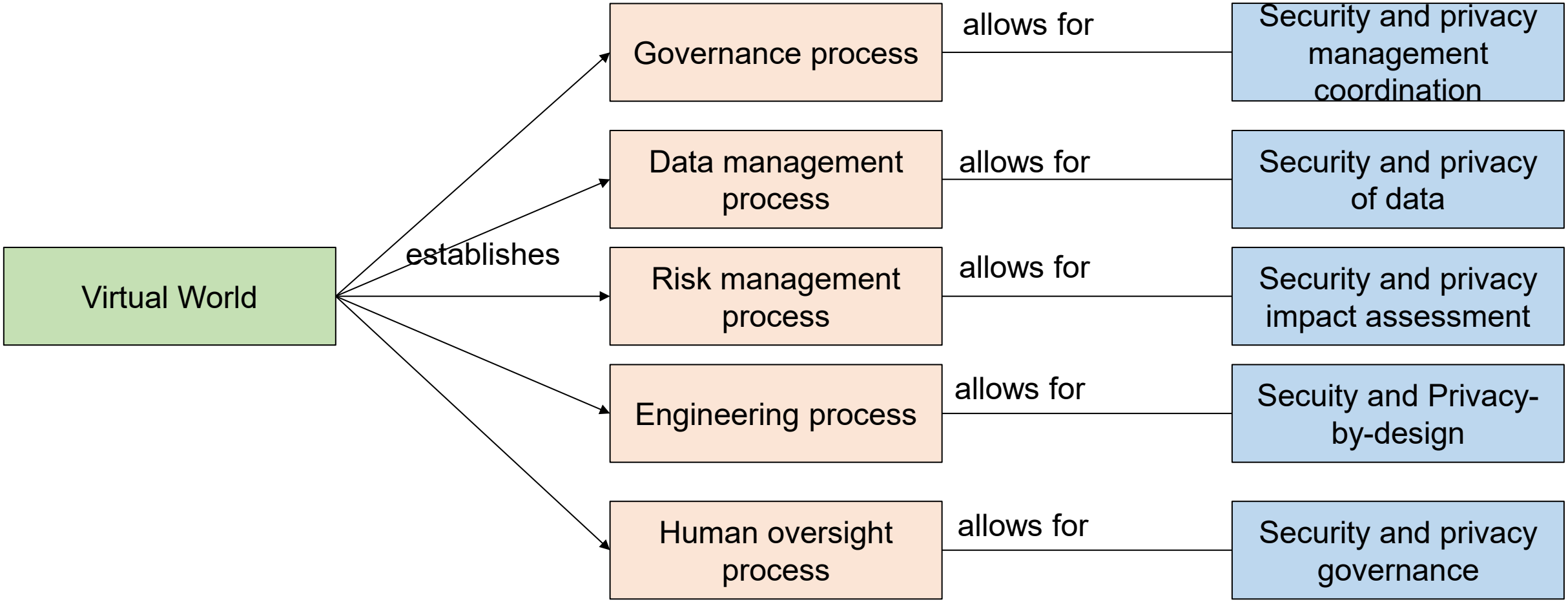
Example of ISO/IEC 27570 Privacy for smart cities



Example of ISO/IEC 27570 Privacy for smart cities



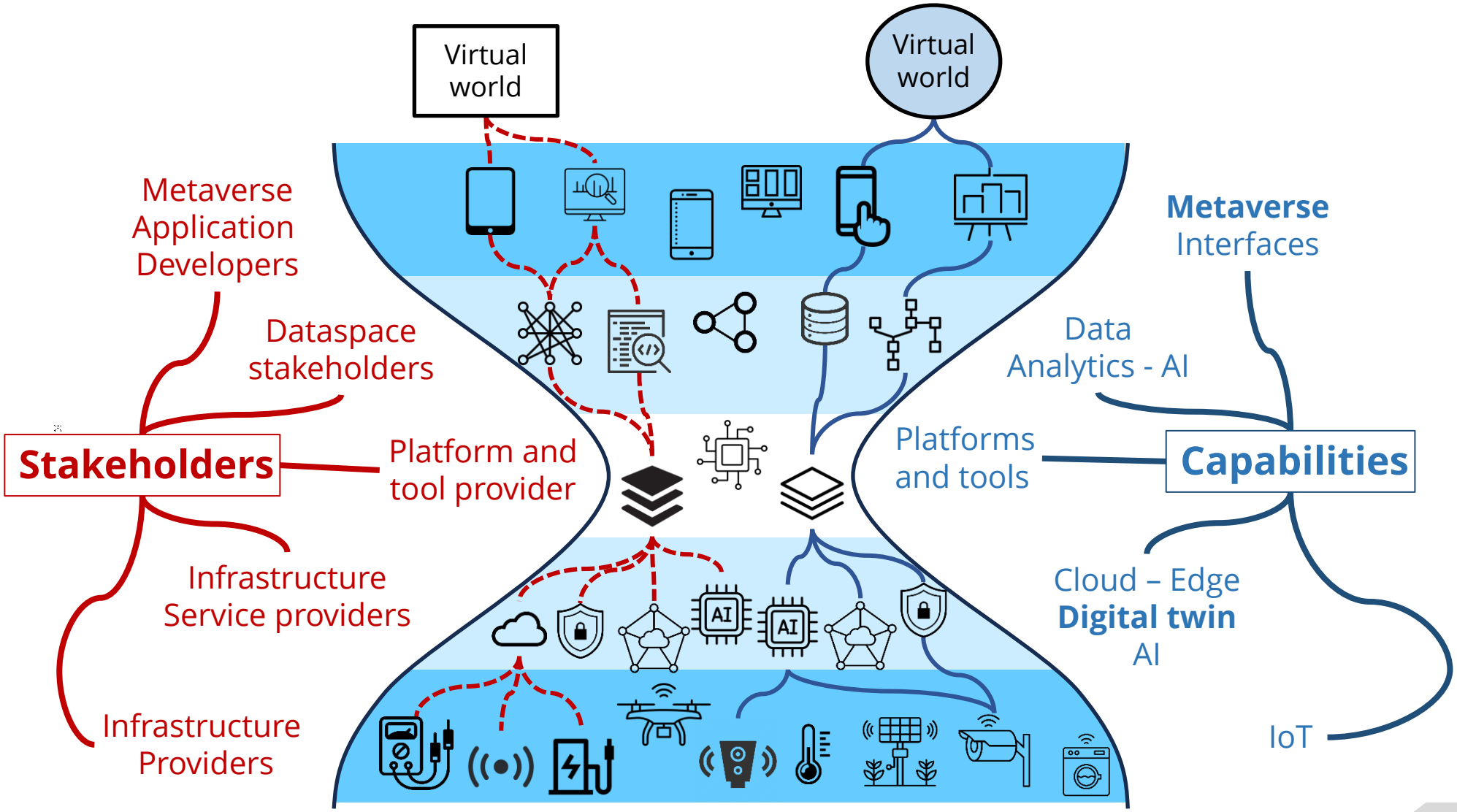
Equivalent for Metaverse



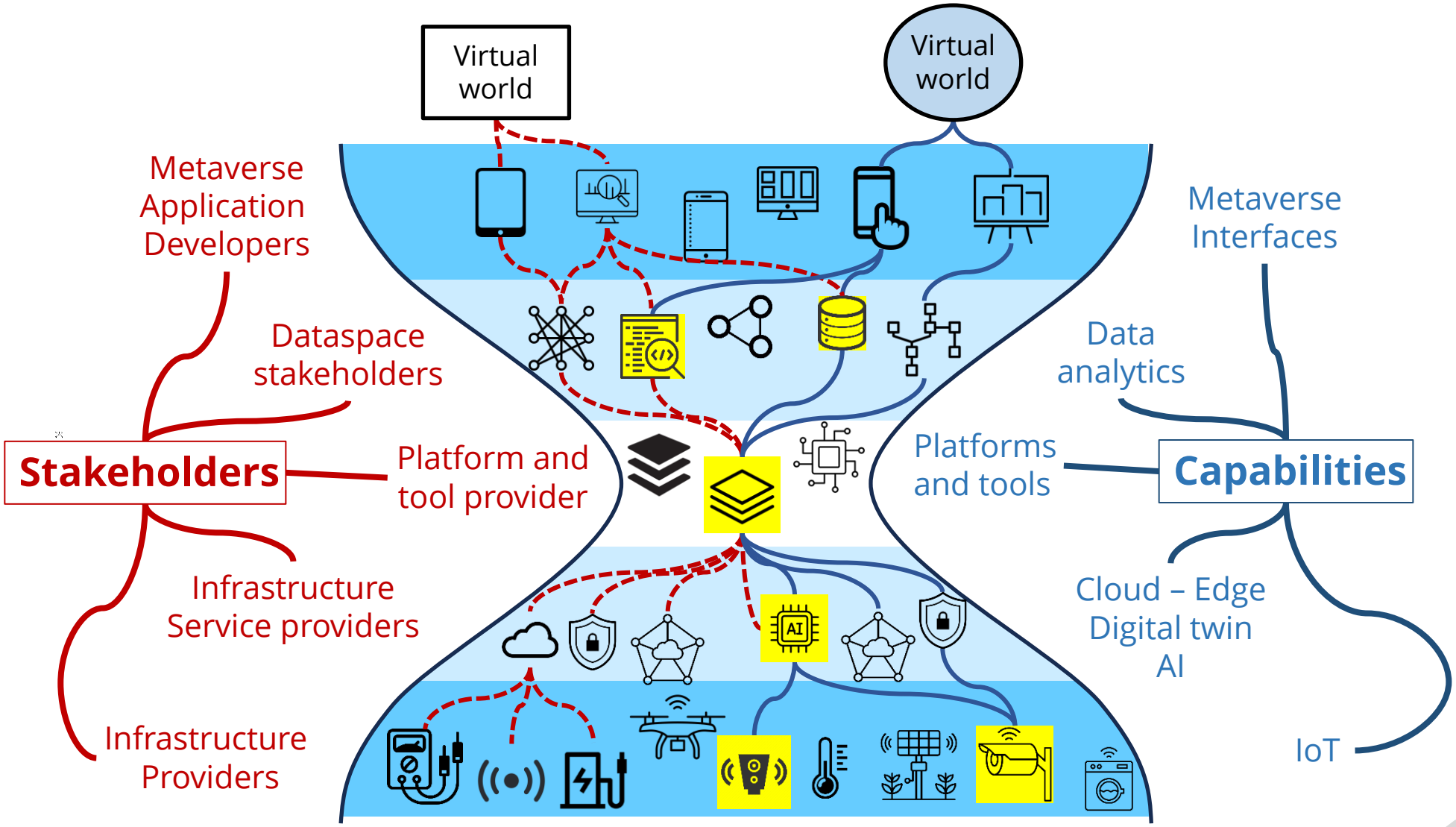
Challenges and issues

- Context
- Challenge: ecosystem domain integration
- Challenge: governance
- Hourglass model to describe ecosystem
- Hourglass model for security and privacy
- Using data and dataspace standards
- Using privacy standards

Hourglass Model of the Metaverse Ecosystem



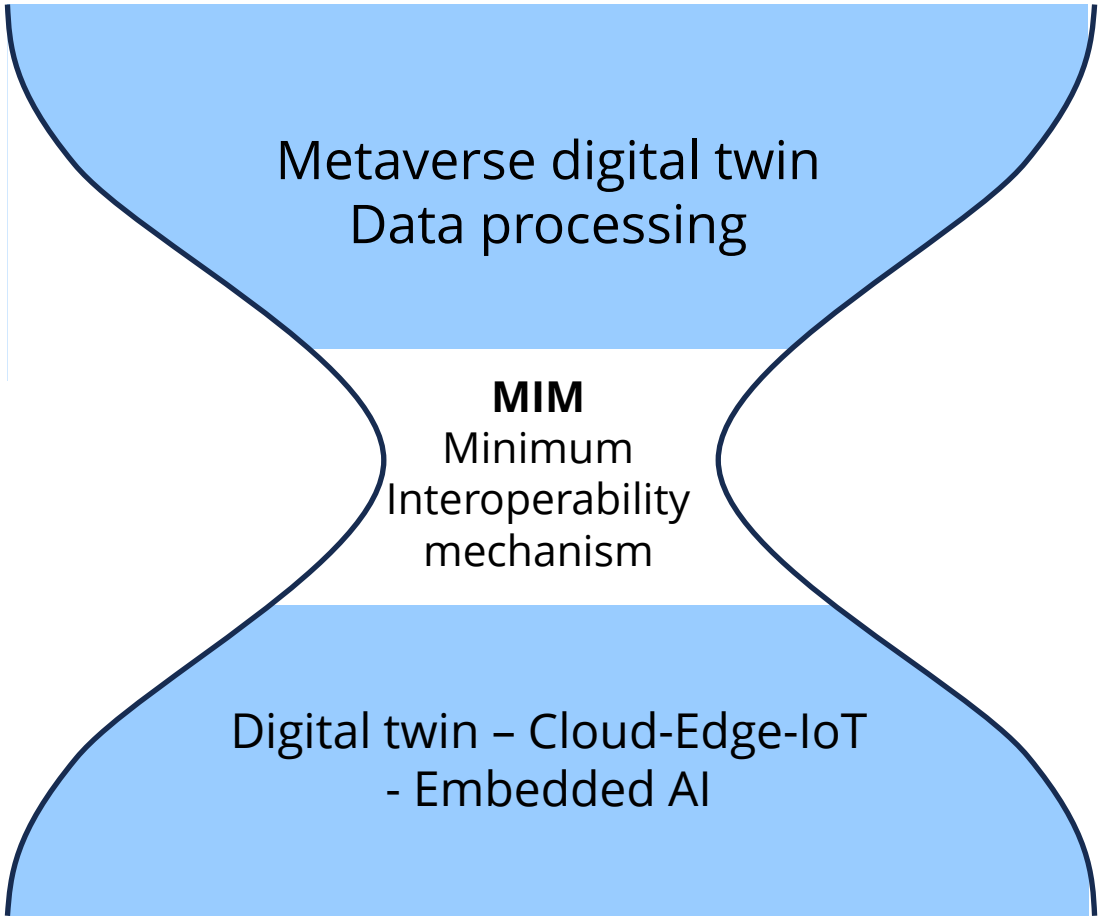
Fostering reuse



Hourglass Architecture Model: Two layers and one interface

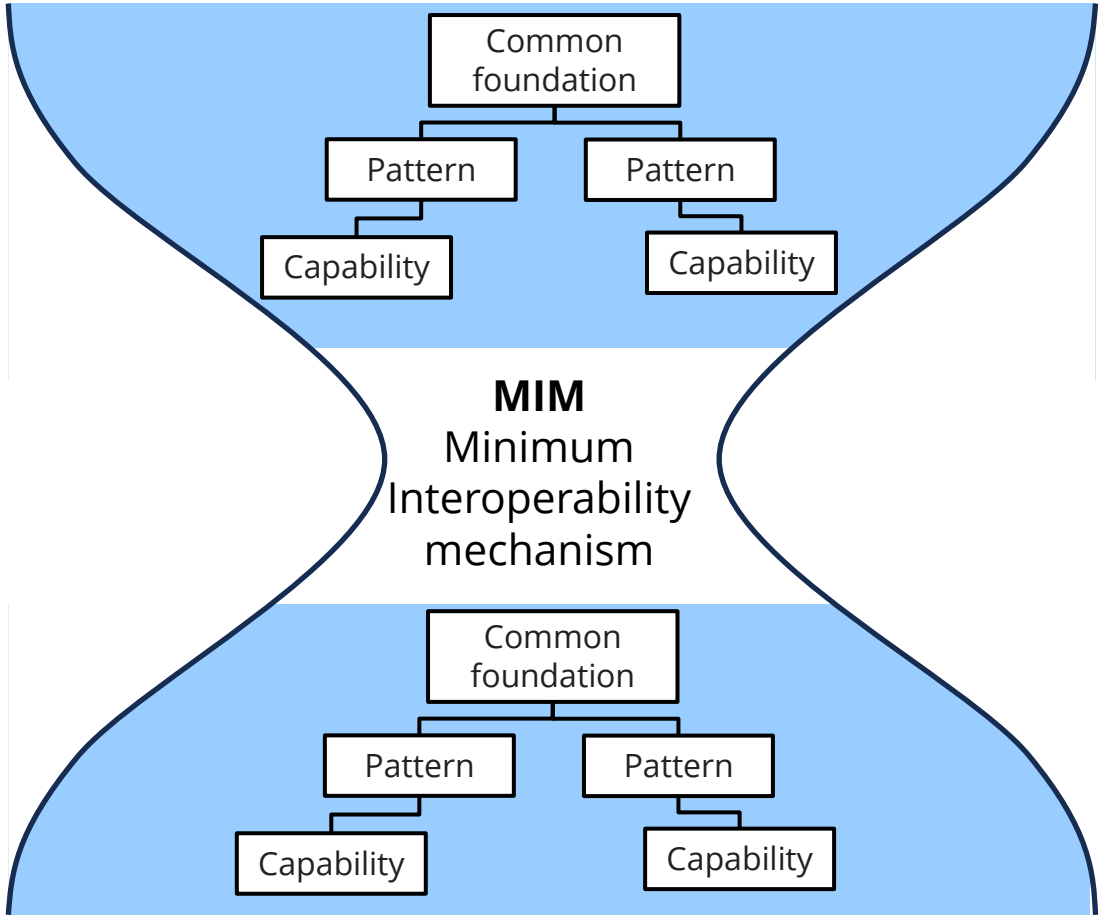
Metaverse applications and data processing concerns

Infrastructure concerns



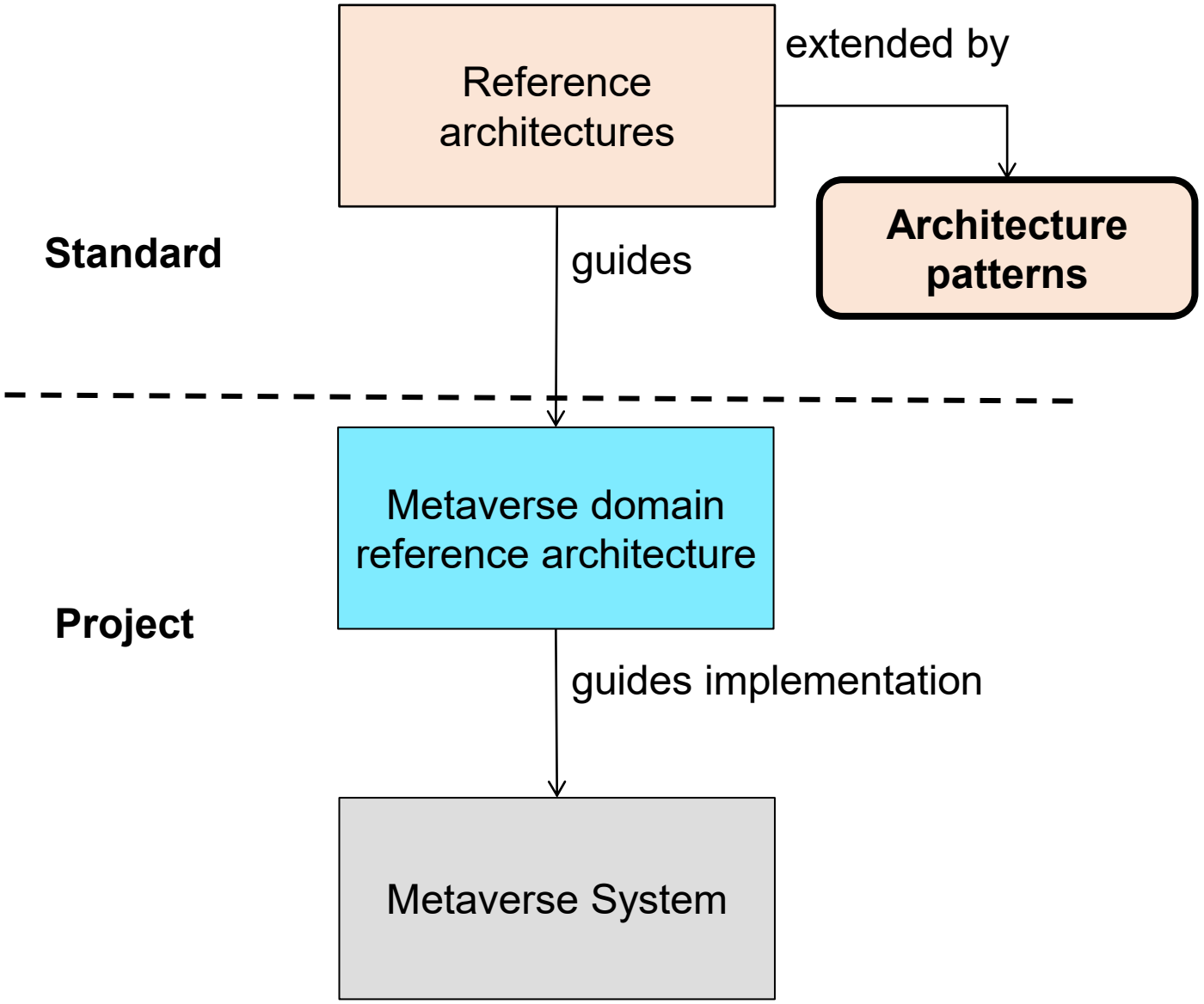
Hourglass Architecture Model: Architecture Patterns

Applications solutions
e.g. data analytics, metaverse digital twins

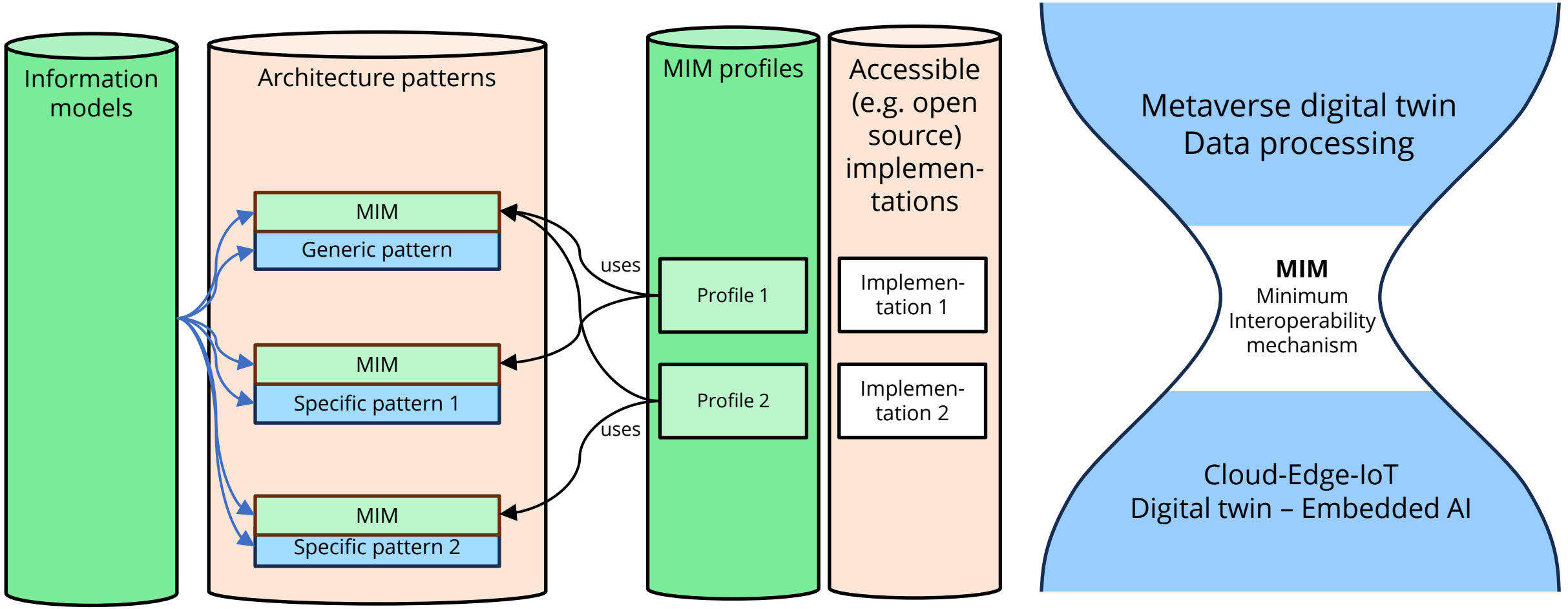


Infrastructure solutions
e.g. IoT, Infrastructure digital twins, AI

The Pattern Vision



Information models – Architecture patterns – Minimum Interoperability Mechanism profiles – Accessible Implementations

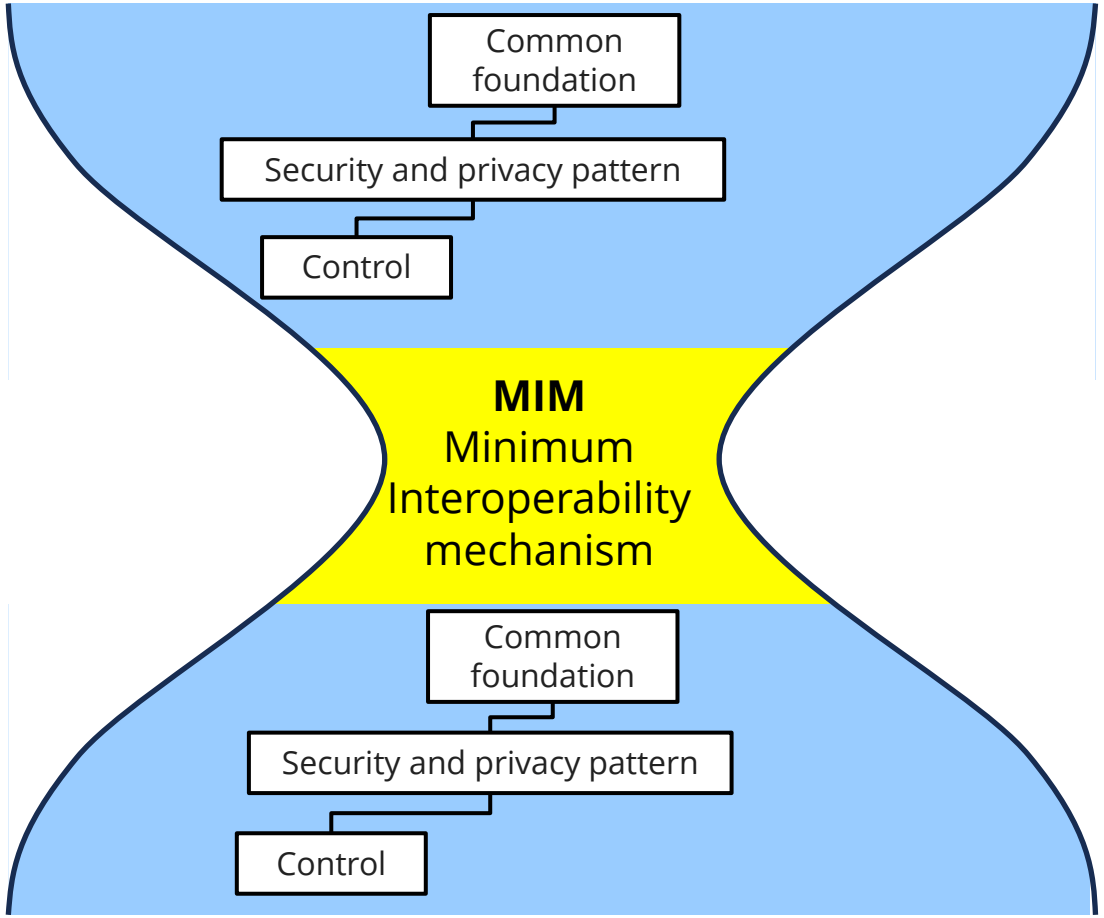


Challenges and issues

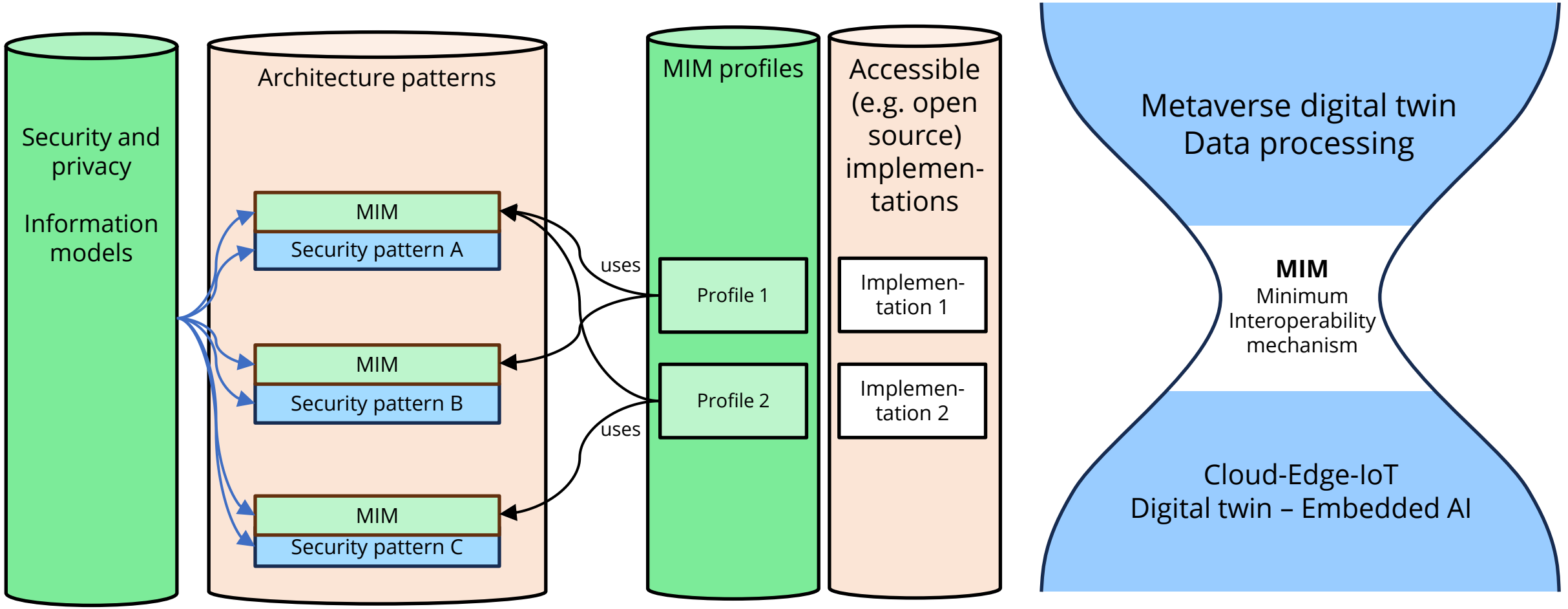
- Context
- Challenge: ecosystem domain integration
- Challenge: governance
- Hourglass model to describe ecosystem
- Hourglass model for security and privacy

Security and Privacy: Architecture Patterns - Controls

- ISO/IEC TS 27573 Privacy protection of user avatar and system avatar interactions in the metaverse (NP)
- ISO/IEC TS 27115 Cybersecurity evaluation of complex system (WD)
- ISO/IEC TS 27568 Security and privacy of digital Twins (NP)
- ISO/IEC 27090 Guidance for addressing security threats to artificial intelligence systems (DIS)
- ISO/IEC 27091 AI privacy protection (CD)



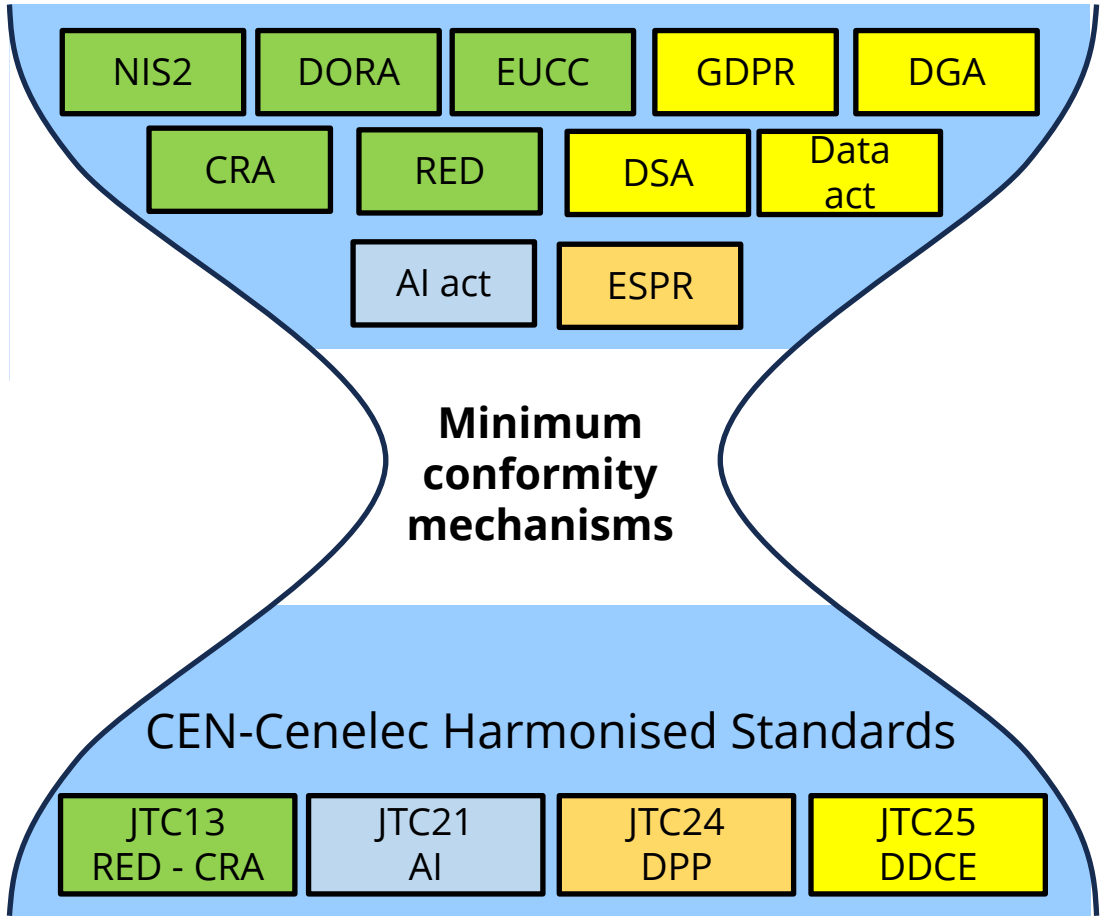
Information models – Architecture patterns – Minimum Interoperability Mechanism profiles – Accessible Implementations



What is at stake (Example of EU)

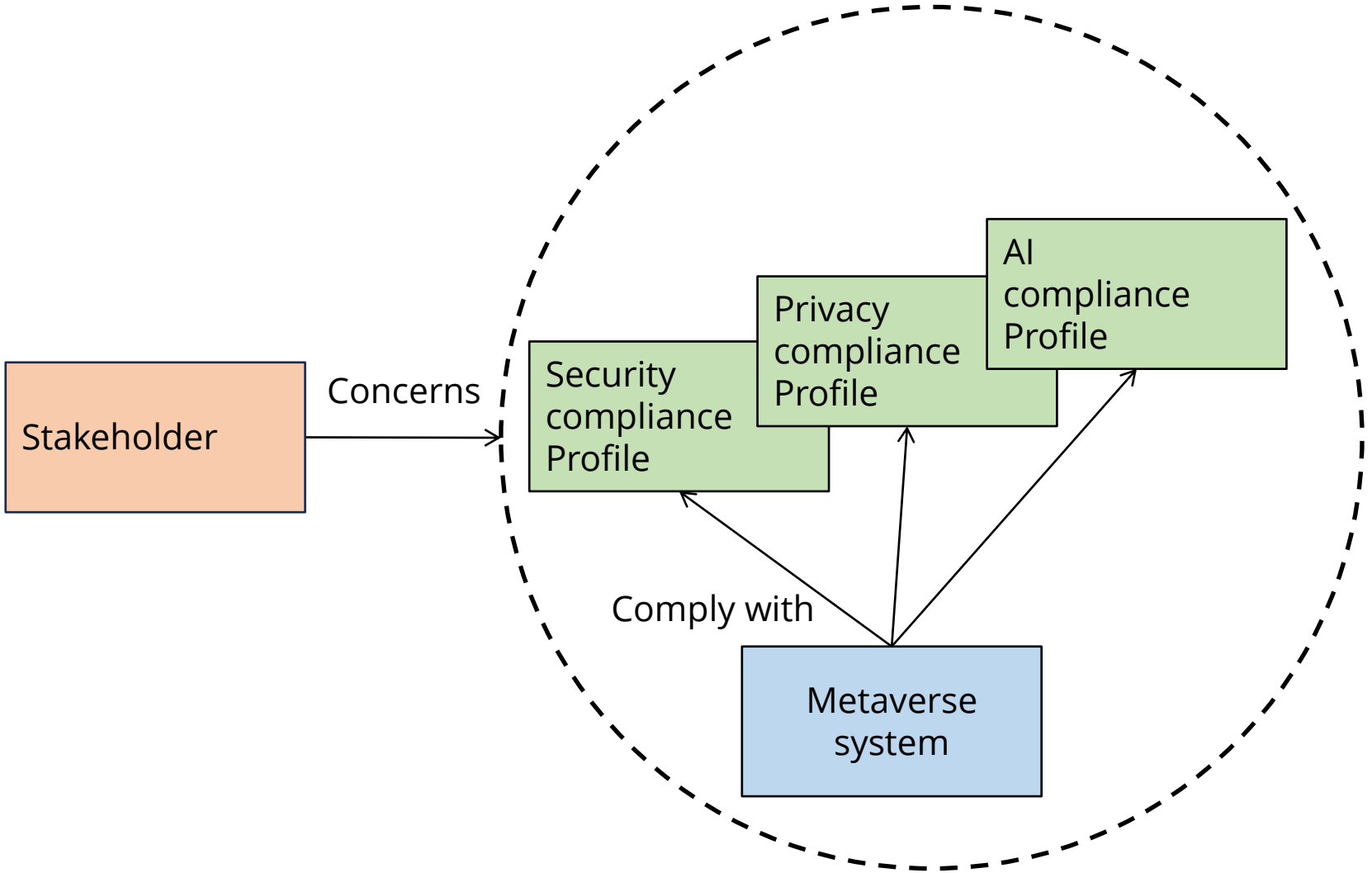
Regulations

ISO/IEC PWI 27116
Customised and multipurpose evaluation



ISO/IEC PWI 27116 - Support for customized or multipurpose evaluation

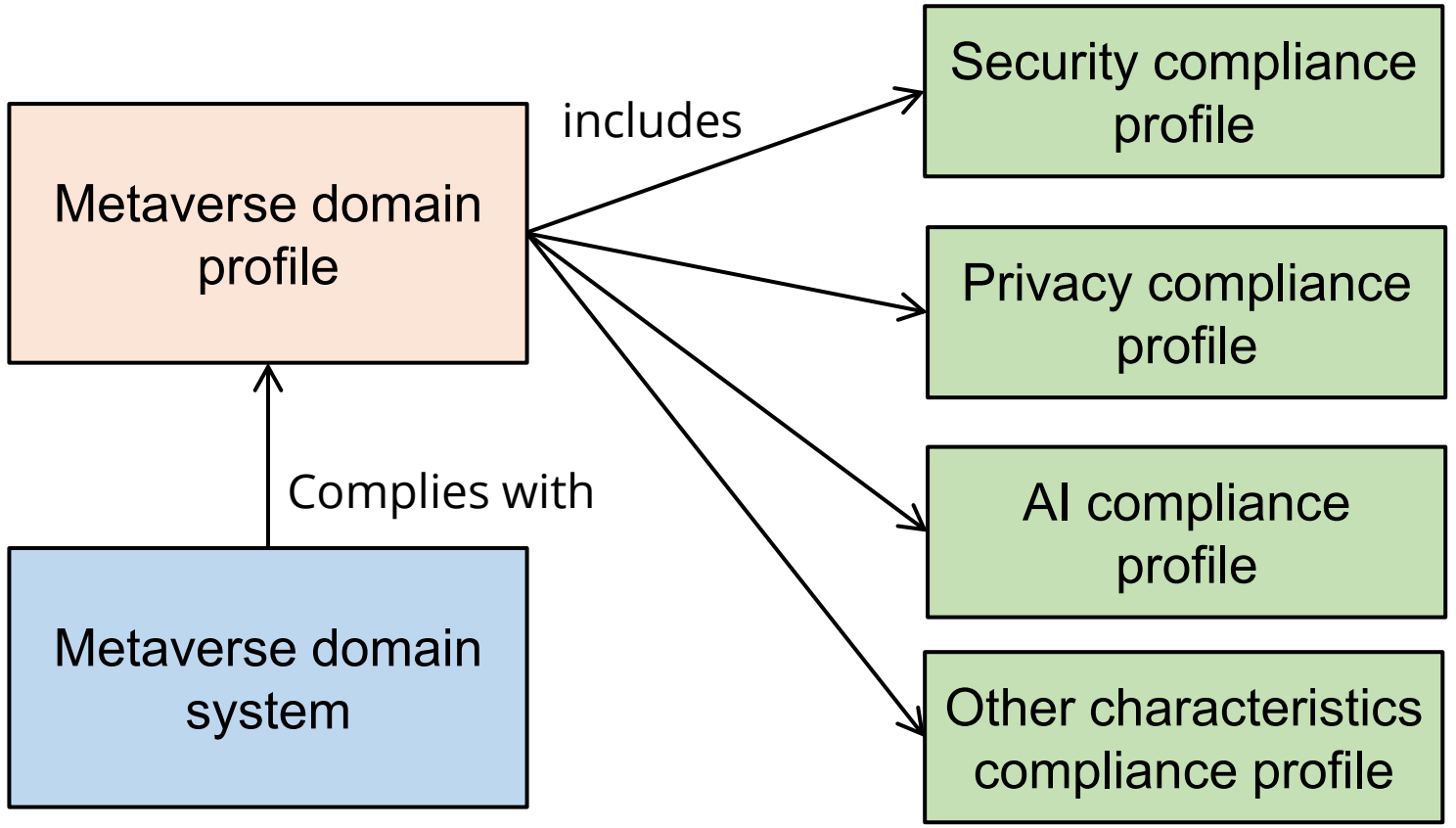
- Security evaluation
- Safety evaluation
- Privacy evaluation
- AI evaluation
- Other evaluation



ISO/IEC PWI 27116 – Metaverse domain profiles

Defined and validated By domain governance

Validated by domain conformity program application



Challenge: assurance