



omega-x



**Orchestrating an interoperable sovereign federated Multi-vector
Energy data space built on open standards and ready for GAia-X**

Interoperability in data spaces

Ecosystem standards

Antonio Kung

Ecosystem standards

4 April 2025

Slide 1

Speaker

- Standardisation in associations and liaison
 - AIOTI: Chair WG standardisation
 - ISO/IEC JTC1/SC41 IoT and digital twins
 - ITU-T SG20 IoT and SCC
 - BDVA: Leader TF benchmark and standards
 - ISO/IEC JTC1/SC42 Artificial intelligence
- Editors of related standards
 - Data spaces connected to IoT and digital twins
 - 30151 Extraction of data products - 30152 Integration of IoT and digital twin in data spaces
 - Interoperability
 - 21823-1 IoT interoperability framework - 21823-5 IoT behavioral and policy interoperability
 - Digital twins
 - 30188 Reference architecture - 27568 Security and privacy
 - Artificial intelligence
 - 27091 Privacy - CEN CLC JTC21 Trustworthiness framework

Hourglass model

CEI-Sphere
part of EU CloudEdgeIoT.eu

January 15th 2025

Alliance for AI, IoT and Edge Continuum Innovation

January 21st 2025

Network Europe and AIOTI workshop • 21 January 2025

Driving Standardisation for the Digital Society

Antonio Kung
Co-founder

Dialog - Chair AIOTI WG standardisation

Lunch Talk

The hourglass model and MIMs (interoperability mechanisms) for semantic interoperability

Date 2025-02-25

February 2nd 2025

Antonio Kung, Dialog

int:net
Interoperability Network for the Energy Transition

TwinEU

Developing a concept of Pan-European Digital Twin of the electricity system

March 6th 2025

Workshop on Trustworthy AI

March 26th 2025

CONNECT
ESAM TRUST & RESILIENCE



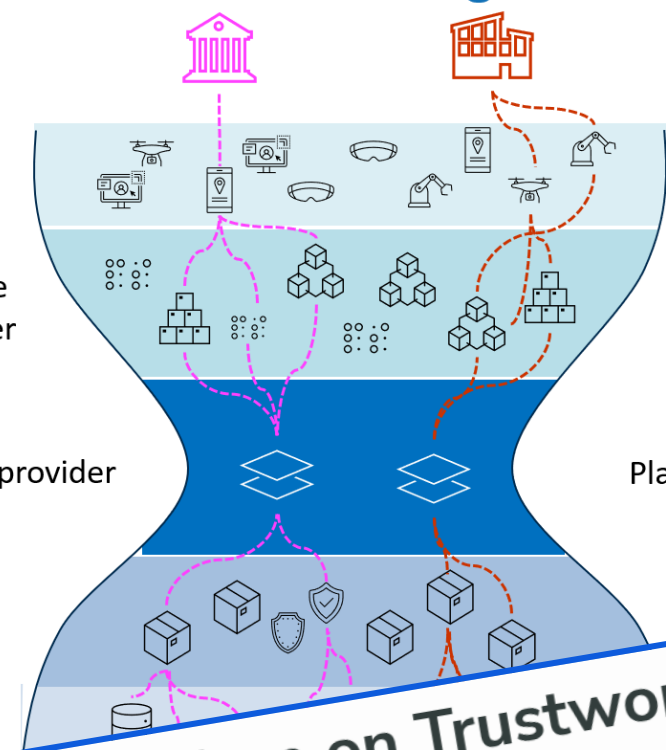
App Developers

Data Space stakeholder
AI Apps

Platform provider

Microservice Providers

Infrastructure Providers



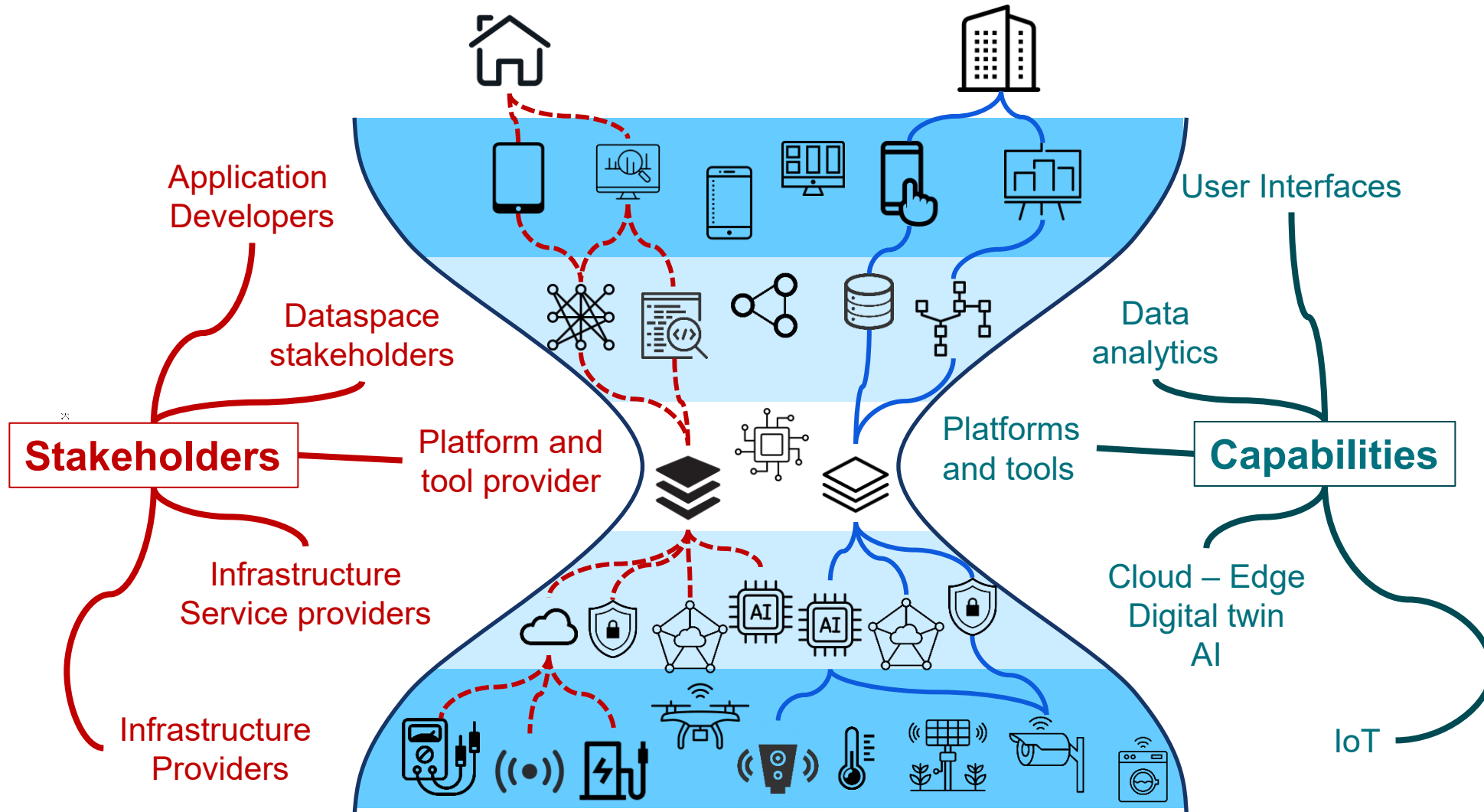
UI

SDKs
Data Spaces
AI Engines

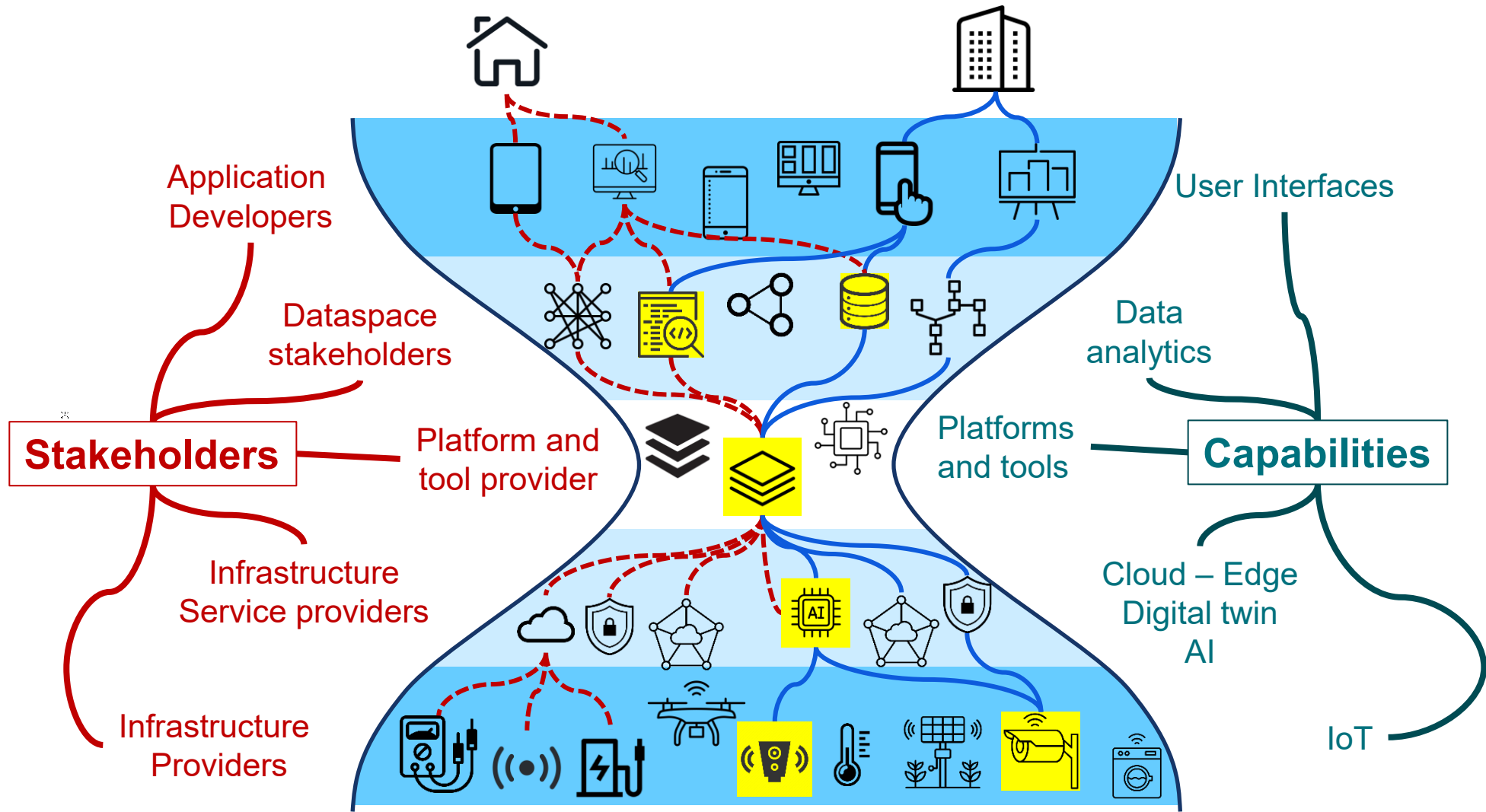
Platforms

VM/Containers

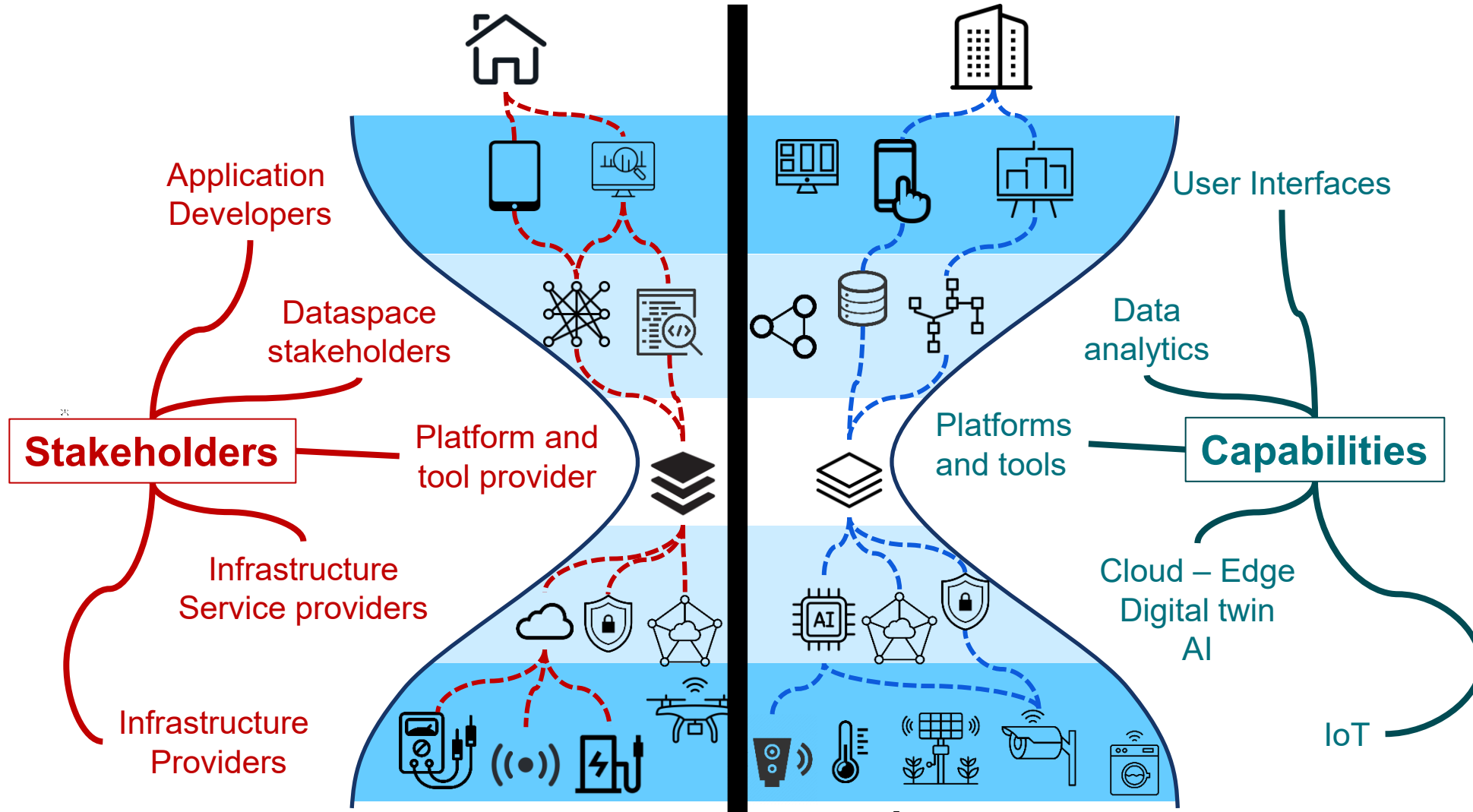
Hourglass Model of the Ecosystem



Objective – Fostering reuse



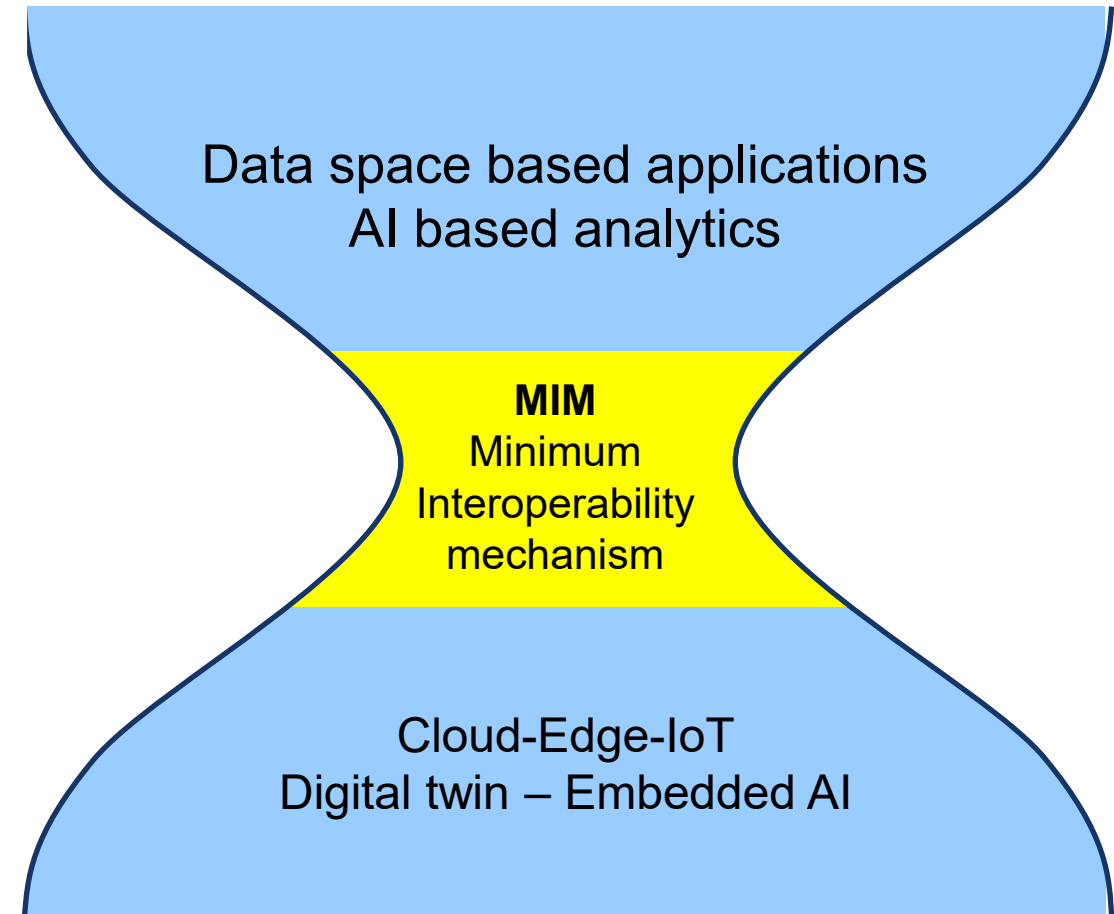
Challenge: Fragmentation



Hourglass Architecture Model: Two layers and one interface

Applications and data analytics concerns

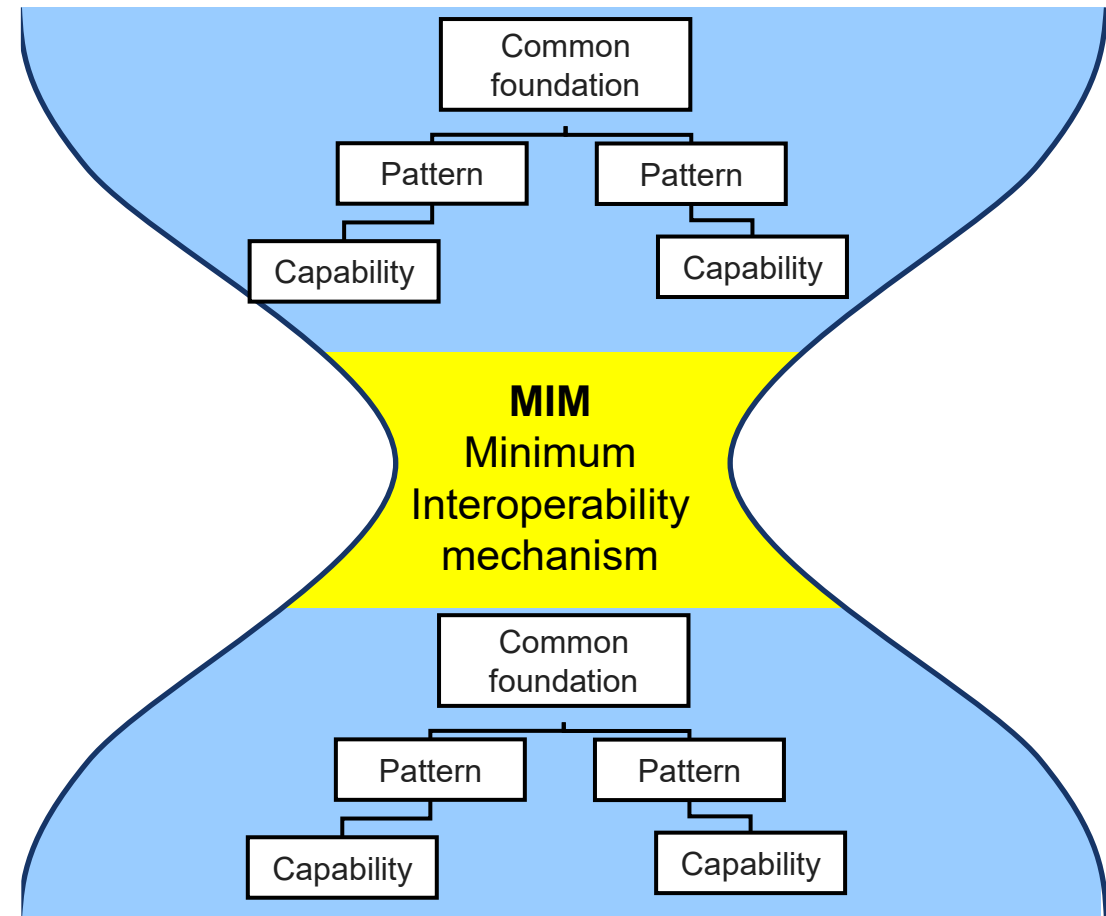
Infrastructure concerns



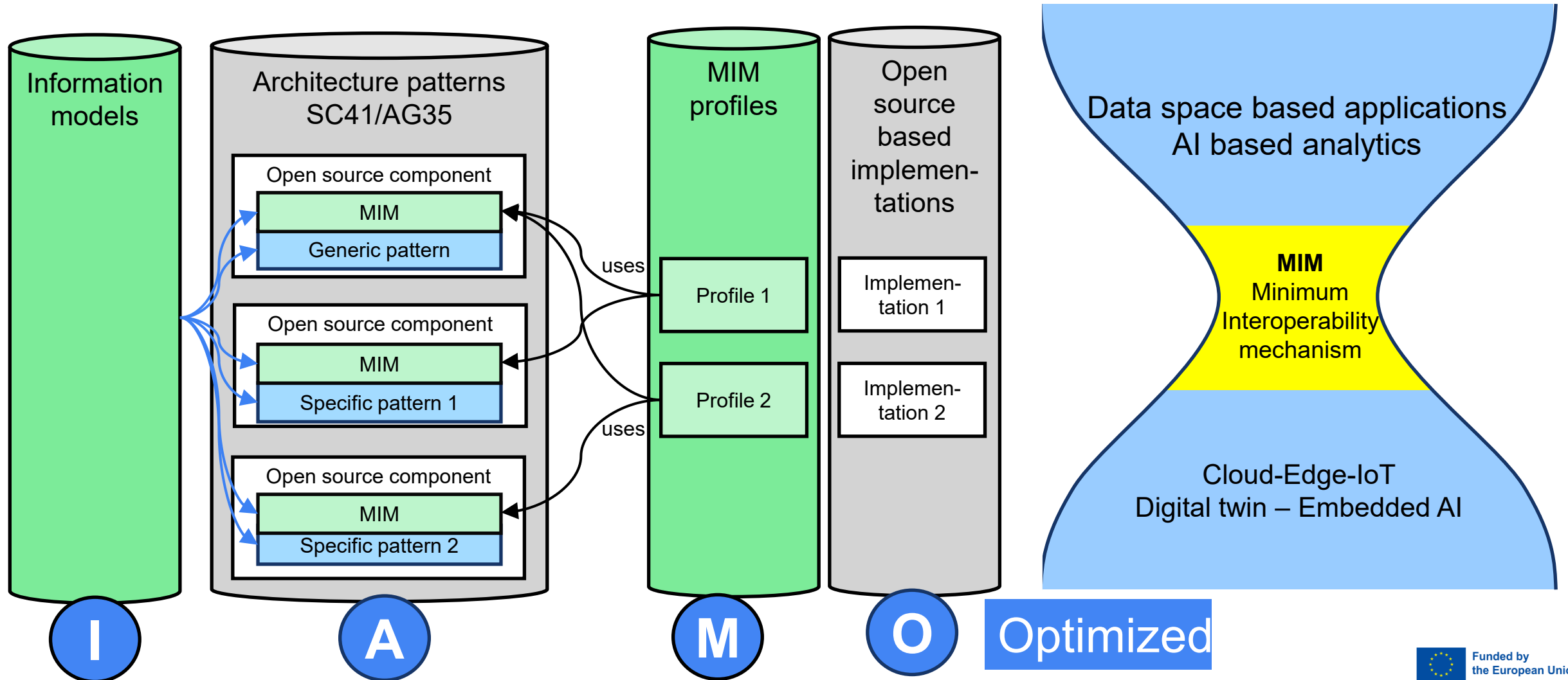
Hourglass Architecture Model: Architecture Patterns

Applications solutions
e.g. data analytics

Infrastructure solutions
e.g. MetaOS, embedded AI
Energy OS, ...



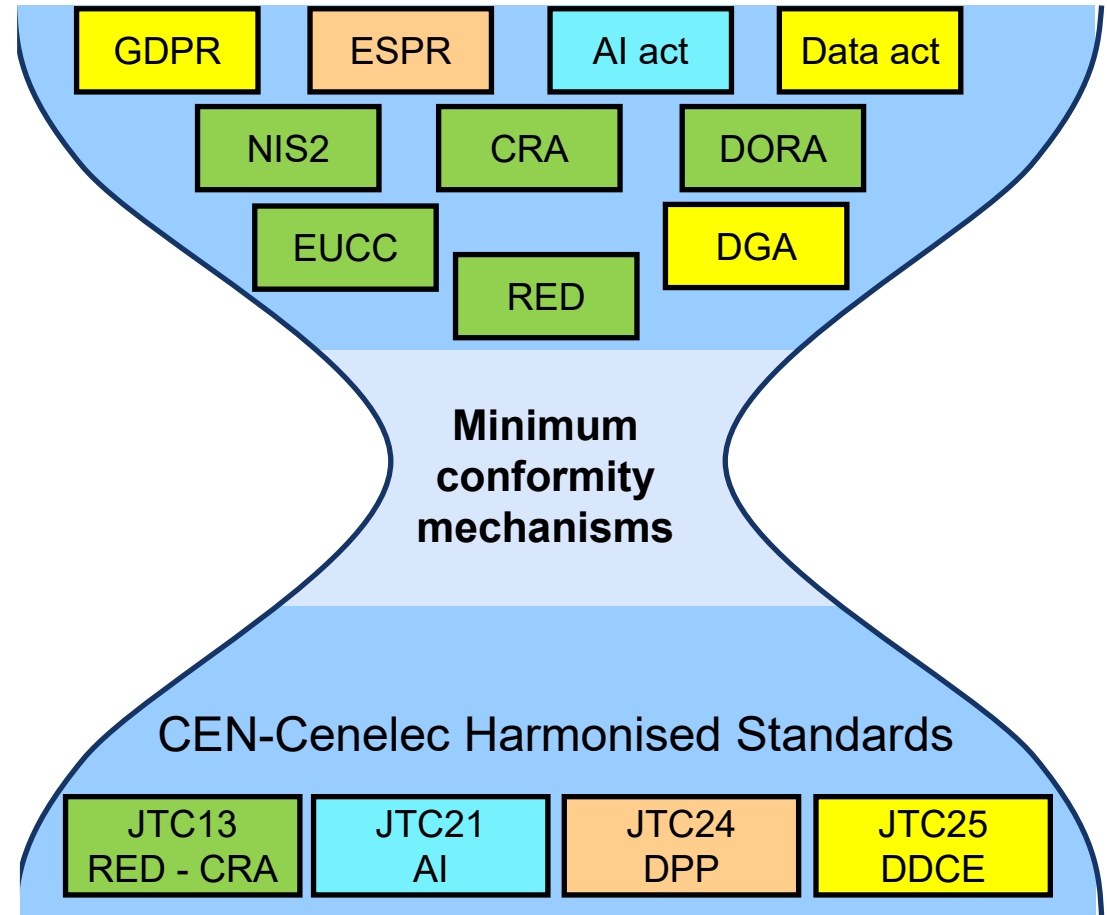
Information models – Architecture patterns – Minimum Interoperability Mechanism profiles – Open-source Based Implementations

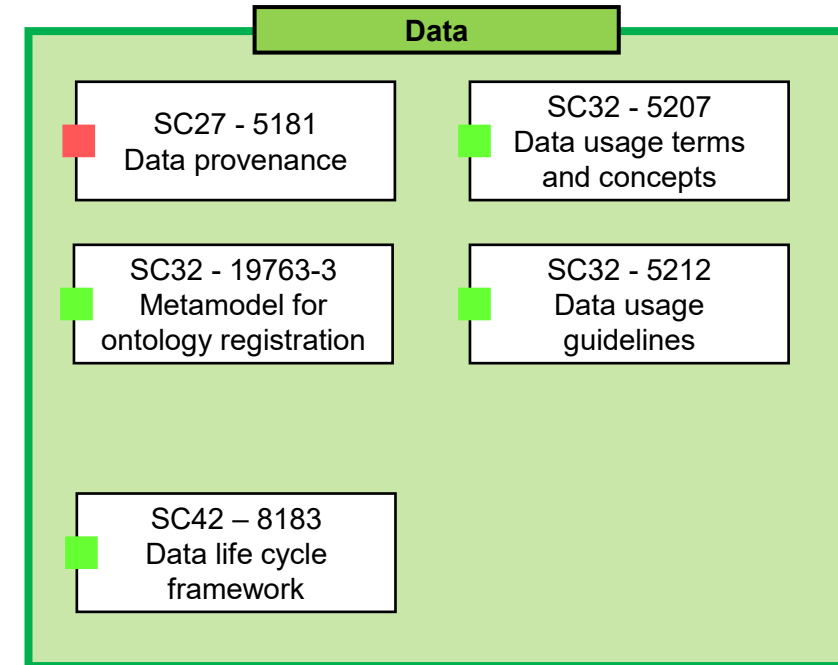


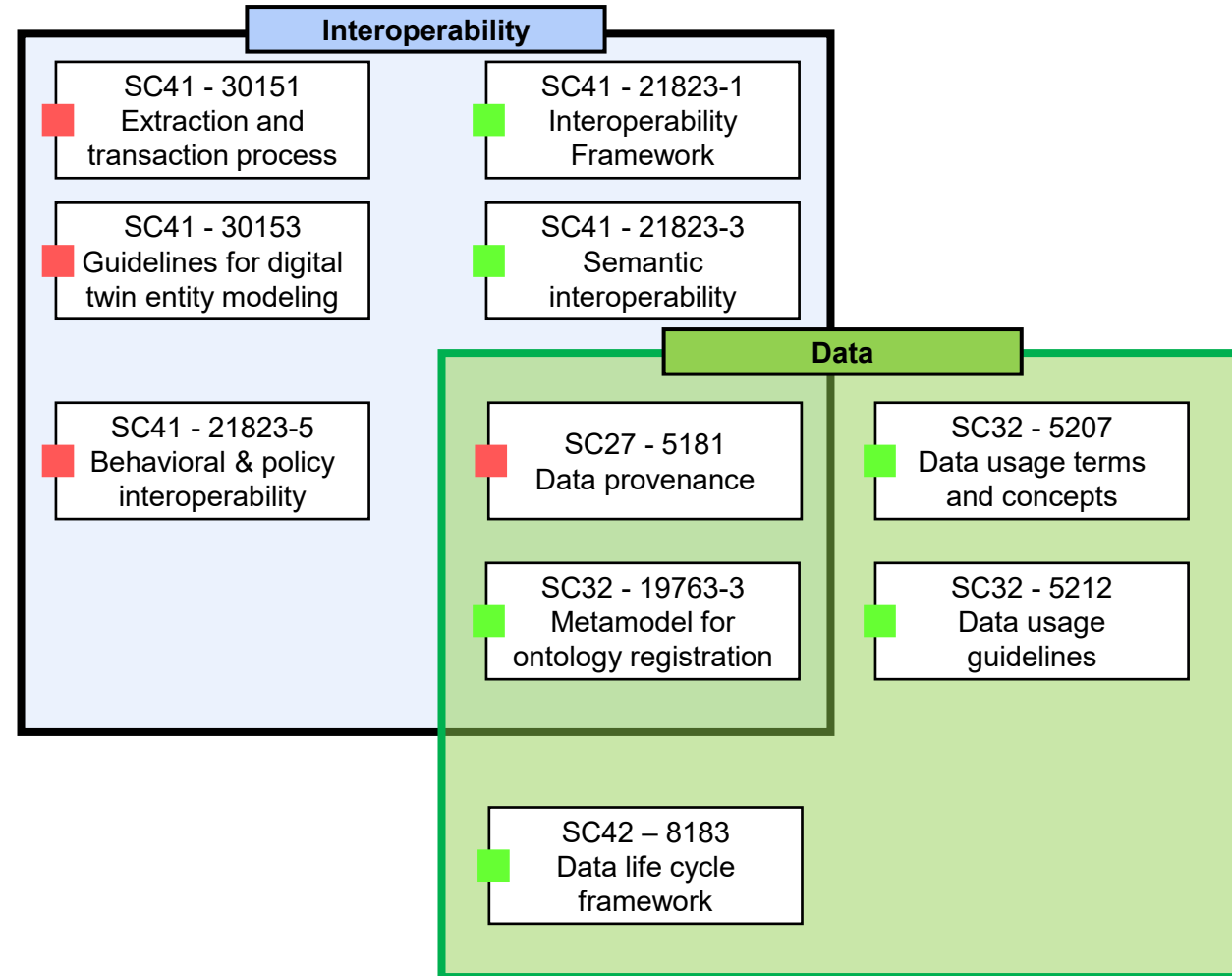
What is at stake

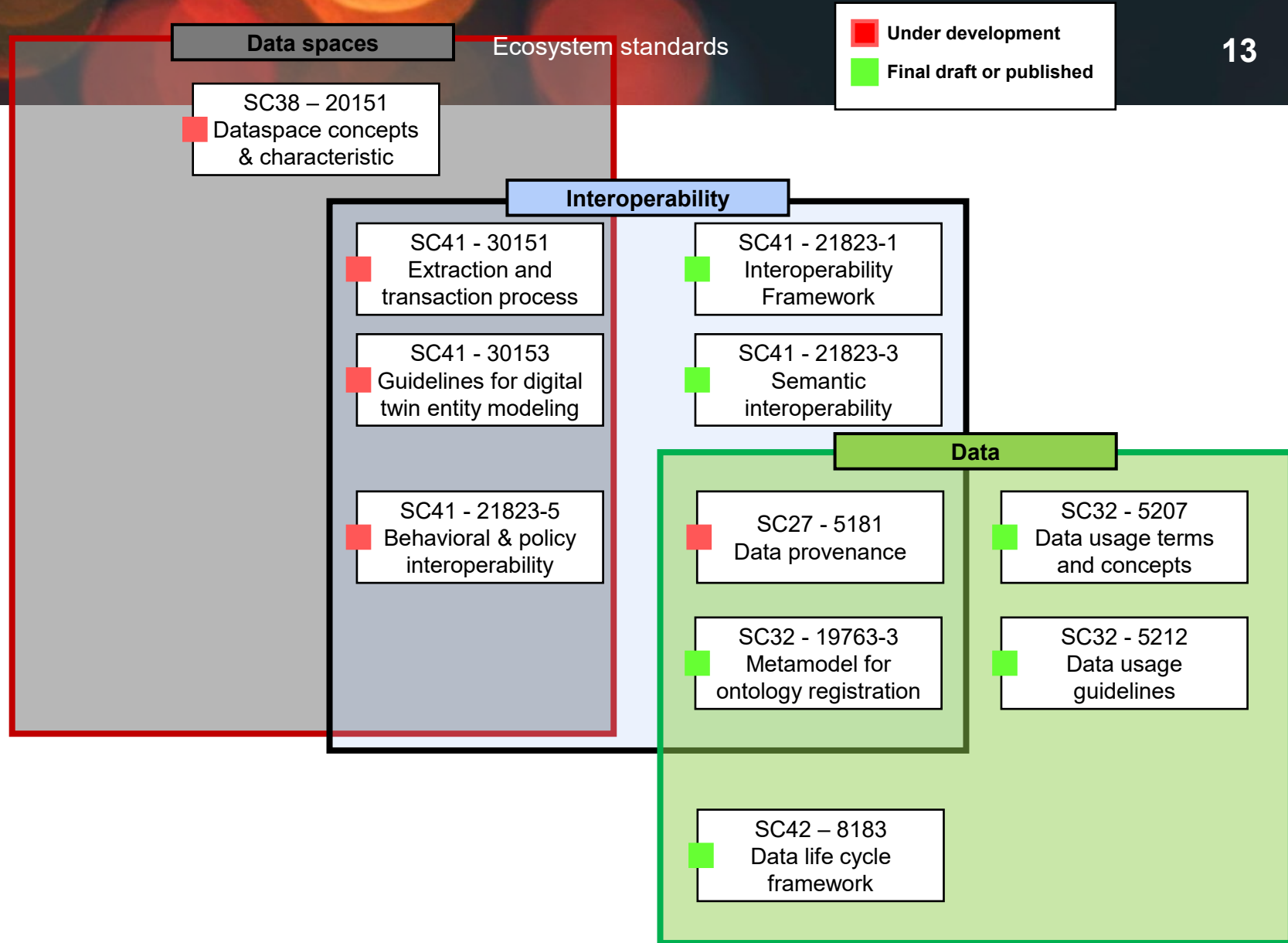
Regulations

Optimised infrastructure
Supporting harmonized
standards

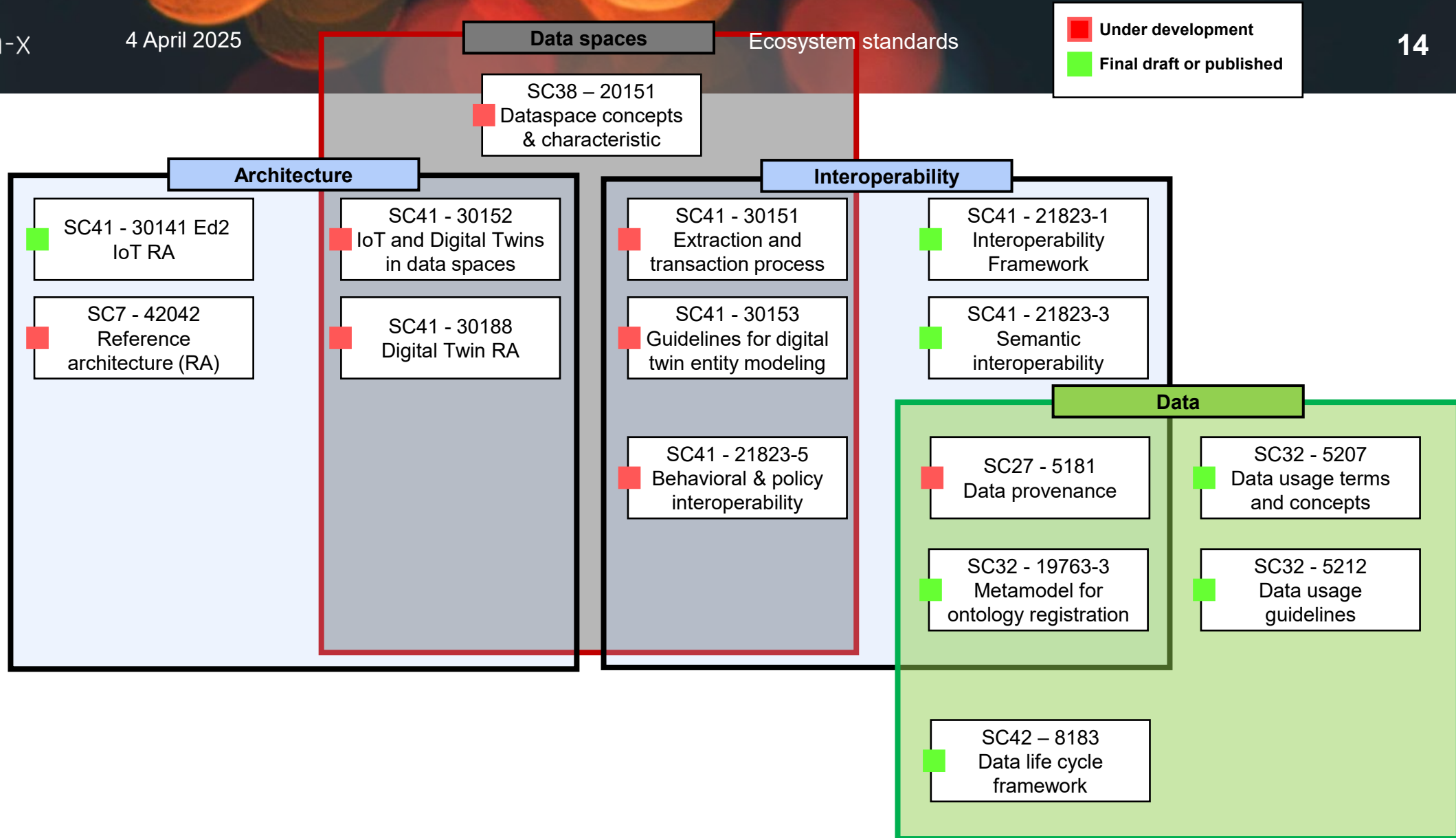




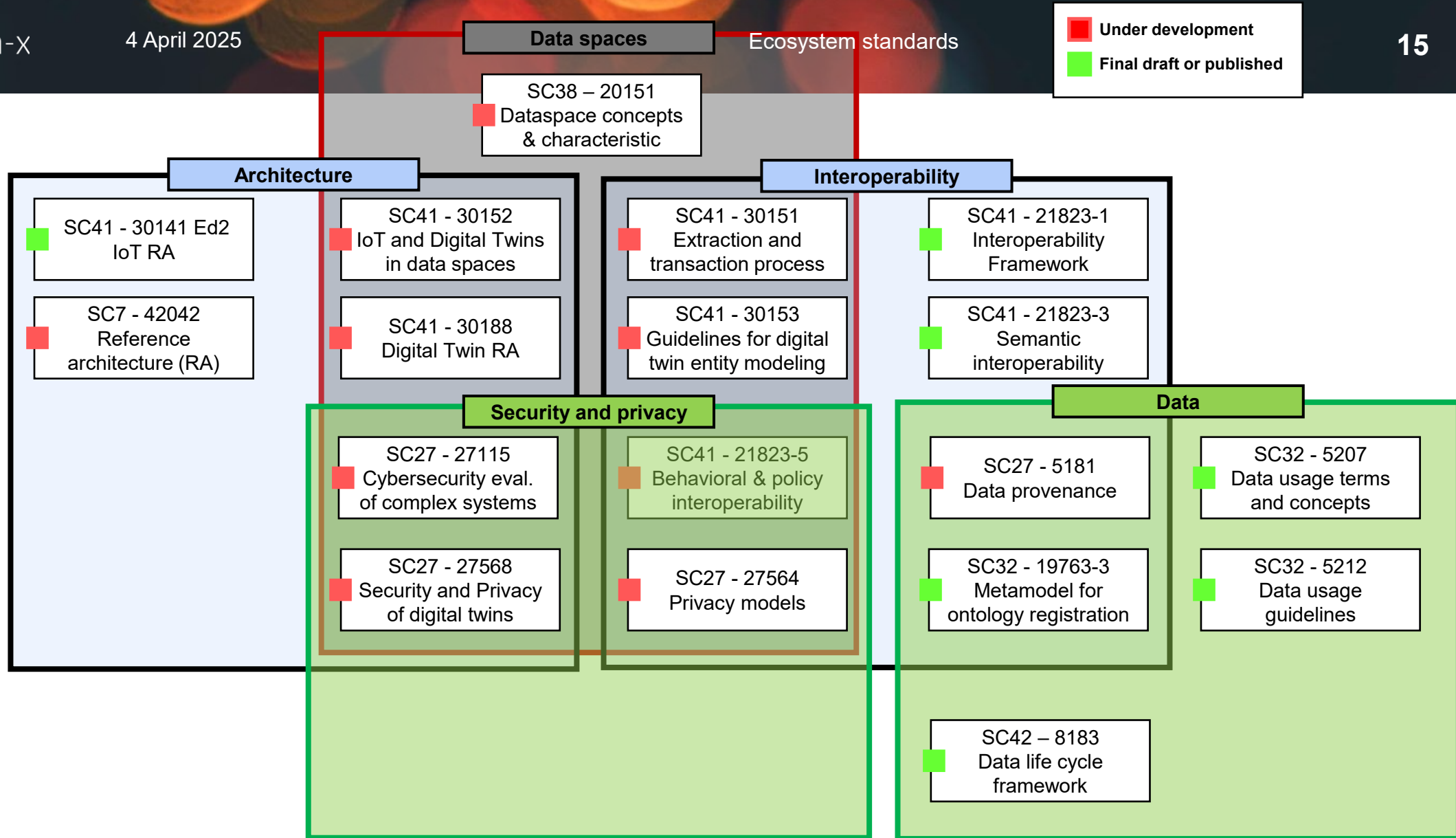




Standardization perspective **Data ecosystems**



Standardization perspective **Data ecosystems**



Standardization perspective **Data ecosystems**

■ Under development
■ Final draft or published

Data spaces

Ecosystem standards

SC38 – 20151
■ Dataspace concepts & characteristic

Architecture

■ SC41 - 30141 Ed2 IoT RA
■ SC7 - 42042 Reference architecture (RA)

Interoperability

■ SC41 - 30152 IoT and Digital Twins in data spaces
■ SC41 - 30188 Digital Twin RA
■ SC41 - 30151 Extraction and transaction process
■ SC41 - 30153 Guidelines for digital twin entity modeling
■ SC41 - 21823-1 Interoperability Framework
■ SC41 - 21823-3 Semantic interoperability

Trustworthiness

■ WG13 – 5723 Trustworthiness vocabulary
■ WG13 – 31303 Trustworthiness overview & concepts

■ SC41 – 30149 IoT Trustworthiness principles

Security and privacy

■ SC27 - 27115 Cybersecurity eval. of complex systems
■ SC27 - 27568 Security and Privacy of digital twins

■ SC41 - 21823-5 Behavioral & policy interoperability
■ SC27 - 27564 Privacy models

Data

■ SC27 - 5181 Data provenance
■ SC32 - 19763-3 Metamodel for ontology registration
■ SC42 – 8183 Data life cycle framework

■ SC32 - 5207 Data usage terms and concepts
■ SC32 - 5212 Data usage guidelines

Standardization perspective Data ecosystems

■ Under development
■ Final draft or published

Data spaces

Ecosystem standards

SC38 – 20151
■ Dataspace concepts & characteristic

Architecture

■ SC41 - 30141 Ed2 IoT RA
■ SC7 - 42042 Reference architecture (RA)

Interoperability

■ SC41 - 30152 IoT and Digital Twins in data spaces
■ SC41 - 30188 Digital Twin RA
■ SC41 - 30151 Extraction and transaction process
■ SC41 - 30153 Guidelines for digital twin entity modeling

■ SC41 - 21823-1 Interoperability Framework
■ SC41 - 21823-3 Semantic interoperability

Trustworthiness

■ WG13 – 5723 Trustworthiness vocabulary
■ WG13 – 31303 Trustworthiness overview & concepts

■ SC41 – 30149 IoT Trustworthiness principles

Security and privacy

■ SC27 - 27115 Cybersecurity eval. of complex systems
■ SC27 - 27568 Security and Privacy of digital twins

■ SC41 - 21823-5 Behavioral & policy interoperability
■ SC27 - 27564 Privacy models

Data

■ SC27 - 5181 Data provenance
■ SC32 - 19763-3 Metamodel for ontology registration

■ SC32 - 5207 Data usage terms and concepts
■ SC32 - 5212 Data usage guidelines

Artificial Intelligence

■ Cen-cenelec JTC21 AI Trustworthiness framework

■ SC27 - 27090 AI Security



■ SC27 - 27091 AI Privacy

■ SC42 – 8183 Data life cycle framework

Standardization perspective Data ecosystems

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact
assessment

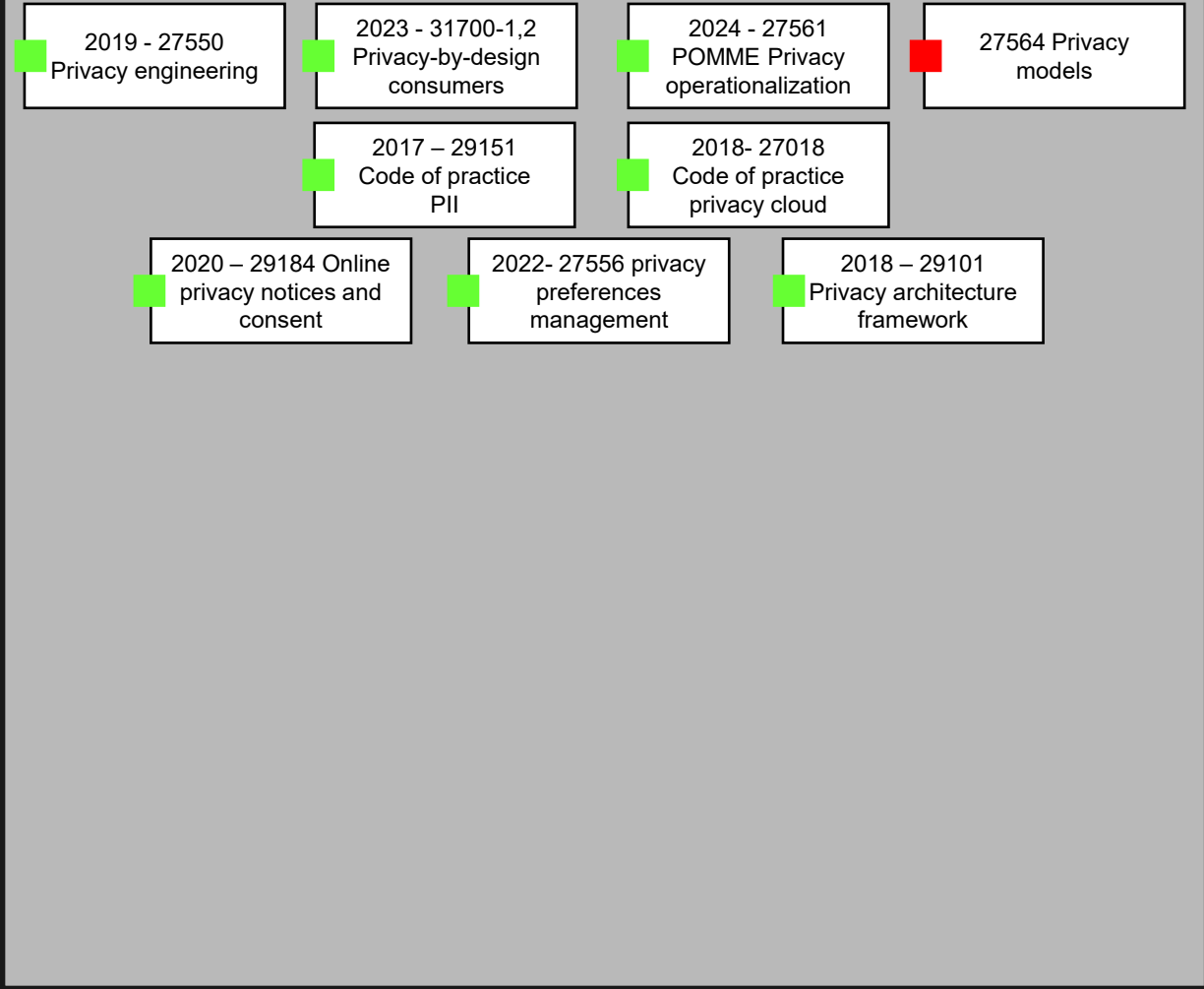
 Under development
 Final draft or published



Standardization perspective **Privacy**

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact
assessment

Practice – architecture - engineering



 Under development
 Final draft or published

Standardization perspective **Privacy**

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact
assessment

Organisation

Practice – architecture - engineering

2019 – 27701
Privacy information
mgt systems

27706 Requirements
for bodies providing
audit

2022 – 27557
Privacy
organisational risk

2019 - 27550
Privacy engineering

2023 - 31700-1,2
Privacy-by-design
consumers

2024 - 27561
POMME Privacy
operationalization

27564 Privacy
models

2017 – 29151
Code of practice
PII

2018- 27018
Code of practice
privacy cloud

2020 – 29184 Online
privacy notices and
consent

2022- 27556 privacy
preferences
management

2018 – 29101
Privacy architecture
framework

Under development

Final draft or published

Standardization perspective Privacy

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact
assessment

Organisation

Practice – architecture - engineering

De-identification

- 2019 – 27701 Privacy information mgt systems
- 27706 Requirements for bodies providing audit
- 2022 – 27557 Privacy organisational risk

- 2019 - 27550 Privacy engineering
- 2023 - 31700-1,2 Privacy-by-design consumers
- 2024 - 27561 POMME Privacy operationalization
- 27564 Privacy models
- 2017 – 29151 Code of practice PII
- 2018- 27018 Code of practice privacy cloud
- 2020 – 29184 Online privacy notices and consent
- 2022- 27556 privacy preferences management
- 2018 – 29101 Privacy architecture framework

- 2021 – 27551 Req attribute-based unlinkable authen.
- 2012 – 29191 Req partially unlikable authen.
- 2018 – 20889 De-identification classification
- 27565 privacy based on zero knowledge proofs
- 2023 – 27559 De-identification framework

■ Under development
■ Final draft or published

Standardization perspective Privacy

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact assessment

Organisation

Practice – architecture - engineering

De-identification

2019 – 27701 Privacy information mgt systems

27706 Requirements for bodies providing audit

2022 – 27557 Privacy organisational risk

2019 - 27550 Privacy engineering

2023 - 31700-1,2 Privacy-by-design consumers

2024 - 27561 POMME Privacy operationalization

27564 Privacy models

2017 – 29151 Code of practice PII

2018- 27018 Code of practice privacy cloud

2020 – 29184 Online privacy notices and consent

2022- 27556 privacy preferences management

2018 – 29101 Privacy architecture framework

2021 – 27551 Req attribute-based unlinkable authen.

2012 – 29191 Req partially unlinkable authen.

2018 – 20889 De-identification classification

27565 privacy based on zero knowledge proofs

2023 – 27559 De-identification framework

Data and AI

2023 – 42001 AI management system

42006 Requirements for bodies providing audit

2021 - 38505-2 Governance of data

42005 – AI system impact

2021 – 27555 Guide PII deletion

2020 - 20547-4 Big data security and privacy

27091 AI privacy protection

5181 Data provenance

25569 De-identification of training data for ML

Under development

Final draft or published

Standardization perspective Privacy

Organisation

Practice – architecture - engineering

De-identification

2019 – 27701 Privacy information mgt systems

27706 Requirements for bodies providing audit

2022 – 27557 Privacy organisational risk

2019 - 27550 Privacy engineering

2023 - 31700-1,2 Privacy-by-design consumers

2024 - 27561 POMME Privacy operationalization

27564 Privacy models

2017 – 29151 Code of practice PII

2018- 27018 Code of practice privacy cloud

2020 – 29184 Online privacy notices and consent

2022- 27556 privacy preferences management

2018 – 29101 Privacy architecture framework

2021 – 27551 Req attribute-based unlinkable authen.

2012 – 29191 Req partially unlinkable authen.

2018 – 20889 De-identification classification

27565 privacy based on zero knowledge proofs

2023 – 27559 De-identification framework

Data and AI

2023 – 42001 AI management system

42006 Requirements for bodies providing audit

2021 - 38505-2 Governance of data

42005 – AI system impact

2021 – 27555 Guide PII deletion

2020 - 20547-4 Big data security and privacy

27091 AI privacy protection

5181 Data provenance

25569 De-identification of training data for ML

IoT and digital twin

27404 Labelling framework for consumer IoT

2022 – 27400 IoT security and privacy

2023 – 27402 IoT devices req for security and privacy

30187 Evaluation indicators

2023 – 27403 IoT domotics security and privacy

27568 Digital twin security and privacy

Under development

Final draft or published

Standardization perspective Privacy

2011 - 29100
Privacy framework

2017 - 29134
Privacy impact assessment

Organisation

Practice – architecture - engineering

De-identification

2019 – 27701 Privacy information mgt systems
27706 Requirements for bodies providing audit
2022 – 27557 Privacy organisational risk

2019 - 27550 Privacy engineering
2023 - 31700-1,2 Privacy-by-design consumers
2024 - 27561 POMME Privacy operationalization
27564 Privacy models
2017 – 29151 Code of practice PII
2018- 27018 Code of practice privacy cloud
2020 – 29184 Online privacy notices and consent
2022- 27556 privacy preferences management
2018 – 29101 Privacy architecture framework

2021 – 27551 Req attribute-based unlinkable authen.
2012 – 29191 Req partially unlinkable authen.
2018 – 20889 De-identification classification
27565 privacy based on zero knowledge proofs
2023 – 27559 De-identification framework

Data and AI

2023 – 42001 AI management system
42006 Requirements for bodies providing audit
2021 - 38505-2 Governance of data

42005 – AI system impact
2021 – 27555 Guide PII deletion
2020 - 20547-4 Big data security and privacy
27091 AI privacy protection
5181 Data provenance

25569 De-identification of training data for ML

IoT and digital twin

27404 Labelling framework for consumer IoT
2022 – 27400 IoT security and privacy
2023 – 27402 IoT devices req for security and privacy
30187 Evaluation indicators
2023 – 27403 IoT domotics security and privacy
27568 Digital twin security and privacy

Applications

2021 – 27570 Privacy smart cities
27562 Privacy for fintech
27566-1,2,3 Age assurance
27573 Privacy of avatars

Under development
Final draft or published

Standardization perspective Privacy

Interest Group: Models for Privacy



Established early 2024

Purpose:

- practices for privacy engineering based on **models**
- create synergies to foster development of an **ecosystem of privacy models**
- promote the **creation, use and sharing of privacy models**

<https://models4privacy.org/>

- join as a member of the interest group
- join mail list
- stay updated on the interest group activities/events



Michelle Chibba - Antonio Kung - Ann Cavoukian

omega-x **standardization workshop**

Learnings and recommendations for [Energy] Data Spaces

Online | April 4th 9:00 to 11:00



Arturo Medela

Eviden

Omega-X coordinator



Sebastian Steinbuss

Chairman CEN/CLC JTC 25

Data management,
dataspaces, cloud and edge.



Martin Brynskov

Co-chair CEN/CLC JTC25

WG 2 Dataspaces



Antonio Kung

Trialog



Javier Valiño

Eclipse DSWG

