Security Challenges and Standardization Strategies for Metaverse Data Processing and Management

— A Pathway to a Safer and Scalable Metaverse

Xiongwei Jia
China Unicom

11 April 2025, Geneva, Switzerland

Metaverse, new experience, new life style

The Metaverse seamlessly converges virtual and physical realities, fostering innovative lifestyles that deliver transformative experiences. Empowered by AI integration, metaverse will permeate every aspect of daily life.

Metaverse hotel

Metaverse mall

Metaverse town

* Images were generated by using Qwen

The growing burden on metaverse platforms

The diverse applications within metaverse platforms—from graphic rendering and data processing to interactions among human avatars, digital humans and objects—significantly increase computational demands. This necessitates integrating external resources to enhance data processing and management (DPM) capabilities and others.

- Graphic rendering
- Data storage and exchanging
- Digital human controlling
- AI agents ...

Interaction between the physical and virtual scenarios

Interaction with external supporting functionalities

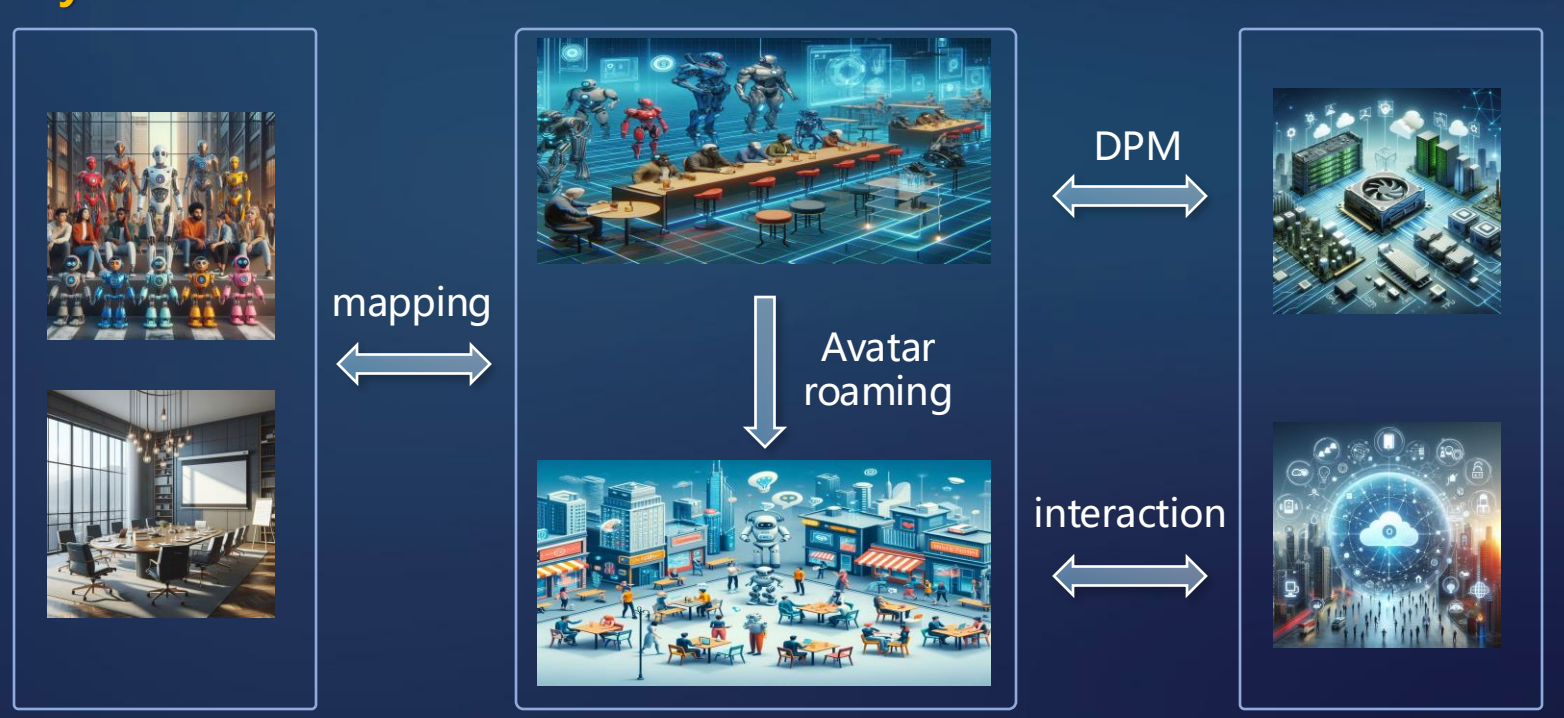
* Images were generated by using Qwen

Key security challenges in DPM for metaverse

Managing and processing data within and beyond metaverse platforms pose critical security challenges, including integration between physical and virtual worlds, interoperability across metaverses, and interactions with external resources—all demanding rigorous safeguards for data security and user privacy.

Dynamic interactions bridging physical and virtual platforms

Cross-metaverse interactions (e.g., Avatar roaming)



Dependency on external resources for DPM

Interactions with underlying infrastructures

Diverse operations across and within the metaverse, including mapping, interoperability, interactions, and more.

* Images were generated by using Copilot

Security risks and vulnerabilities

As metaverse applications grow, the closer integration of virtual and physical worlds, the fragility of communication between them, differences in protection mechanisms during cross-platform interactions, and reliance on external resources can all pose significant security risks to data security and user privacy.

Interactions between physical and virtual worlds

- Device and Hardware Vulnerabilities: The metaverse relies on devices like VR headsets, AR glasses, and other wearable technology. Weaknesses in these devices can be exploited by attackers, creating entry points into secure environments.
- Threats to virtual assets and financial transactions …

Interactions within and across metaverse platforms

Metaverse is working in decentralized environments, which faces typical and new security risks, such as,

- Data breaches and privacy concerns
- Weak identity verification and authentication
- Decentralization and lack of standardization
- Cyberattacks and system disruptions
- Social engineering, harassment, and psychological risks …

Interactions with external supporting entities

- Security risks when delivering data to/from the external supporting entities
- Security risks when using external supporting resources to process and manage data of metaverses
- Security risks when using external supporting resources in metaverse services like avatar rendering, status sensing, digital entity controlling, etc.

Standardization strategies to address security challenges

To overcome these security challenges and reduce security risks, industries need to work together. The focus should be on safeguarding data security and privacy across different domains, with particular attention to protecting individuals' safety and their sensitive information.

Physical-virtual interaction standards

- For metaverses, the interaction standards between the physical and virtual worlds are primarily designed to ensure secure, efficient, trustworthy, and reliable data exchange, while also safeguarding the safety of individuals and their properties in the physical world.

Inter-metaverse standards

- The security standards for cross-metaverse platforms are designed to regulate and protect the data and assets within the metaverse, ensuring secure, efficient, trustworthy, and reliable cross-platform circulation.

Intra-metaverse standards

- Metaverse platforms require extensive security standards to ensure safe, trustworthy, and reliable operations in a decentralized environment. This involves the protection of infrastructures, systems, data, assets, and more.

Collaboration with trusted external providers

- The security standards for interactions between metaverse platforms and external entities (such as infrastructure providers and DPM providers) are primarily designed to ensure that the metaverse's data and assets are effectively and reliably protected during circulation.

Standardization activities of FG-MV

The Focus Group on Metaverse (FG-MV) had produced 52 deliverables about the metaverse, and its WG6 focused on the studies on the security, data & PII protection of metaverse.

Nine deliverables related security, safety and trustworthiness of metaverse

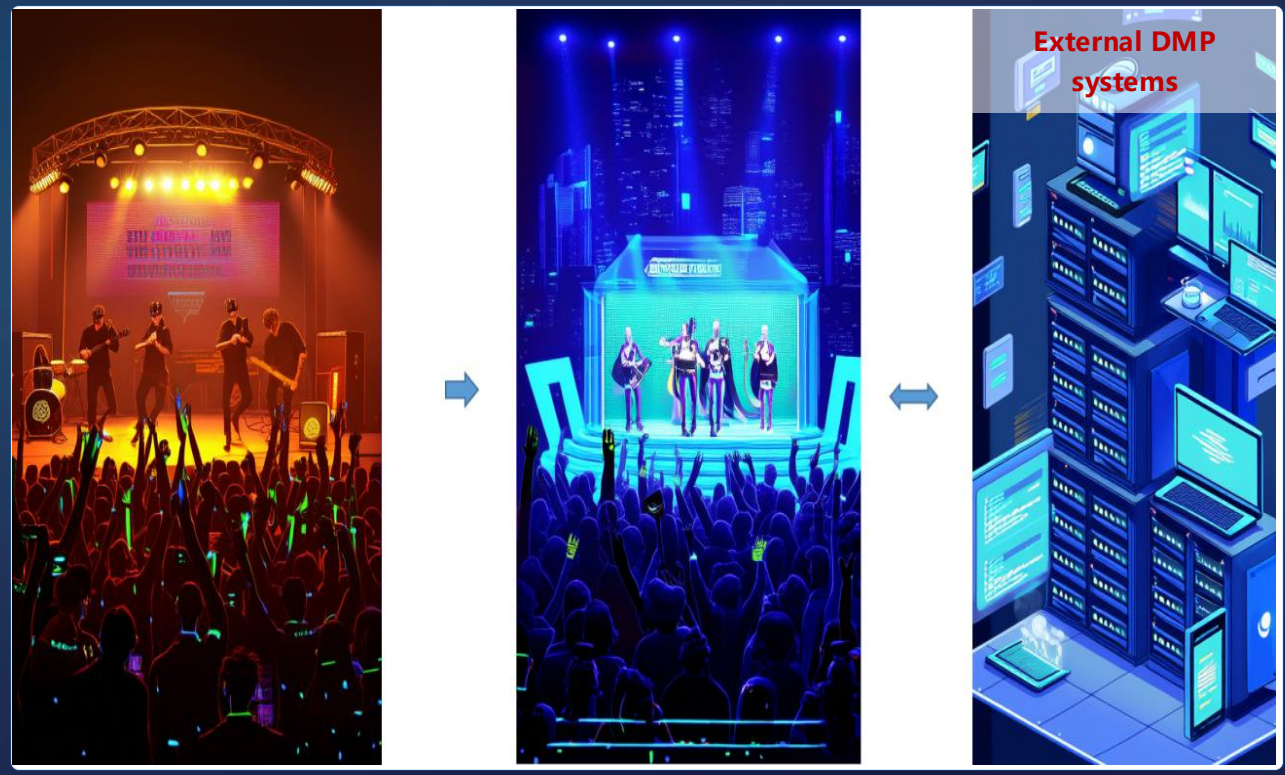
- FGMV-06, Guidelines for consideration of **ethical issues** in standards that build confidence and security in the metaverse
- FGMV-10, **Cyber** risks, threats, and harms in the metaverse → **SG17- C60**
- FGMV-11, **Embedding safety** standards and the user control of Personally Identifiable Information (PII) in the development of the metaverse
- FGMV-12, **Children**'s age verification in the metaverse
- FGMV-13, Responsible Use of AI for **Child** Protection in the metaverse
- FGMV-23, Considering online and offline implications in efforts to build **confidence** and security in the metaverse
- FGMV-44, Security for **things across metaverses** in aspects of data processing and management → **X.stm-dpm**
- FGMV-45, Challenges to achieving **trustworthy** metaverse → **SG17- C172**
- FGMV-46, The essential components of trusted data use in building a **trustworthy**

https://www.itu.int/en/ITU-T/focusgroups/mv/Pages/deliverables.aspx

Current activity: Draft Rec. X.stm-dpm

ITU-T **X.stm-dpm**: Security requirement and framework of metaverse platform for things across metaverses in relation to data processing and management

Use case: Meeting room mapping and operating in metaverse (physical/virtual)

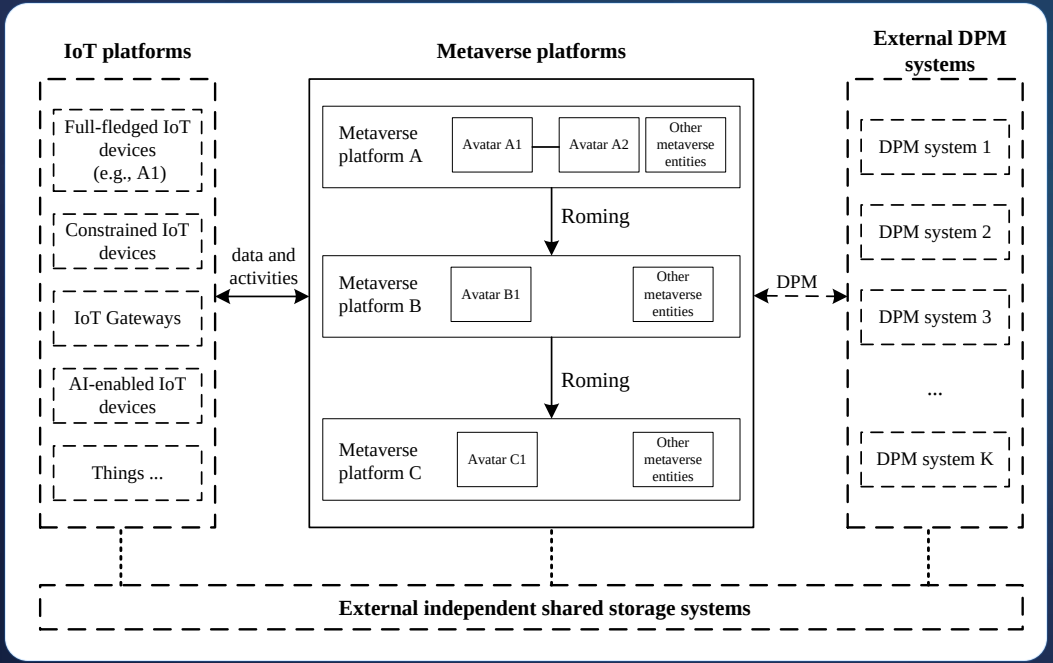


Use case: External DPM for operating the virtual concert in metaverse (physical/virtual)

* Images were generated by using Qwen

Current activity: Draft Rec. X.stm-dpm (cont.)

ITU-T **X.stm-dpm**: Security requirement and framework of metaverse platform for things across metaverses in relation to data processing and management



Virtual and physical things (e.g., sensors, IoT devices, IoT systems, IoT gateways) can be connected to or mapped into multiple metaverse platforms, and interact with ...

Study Scope

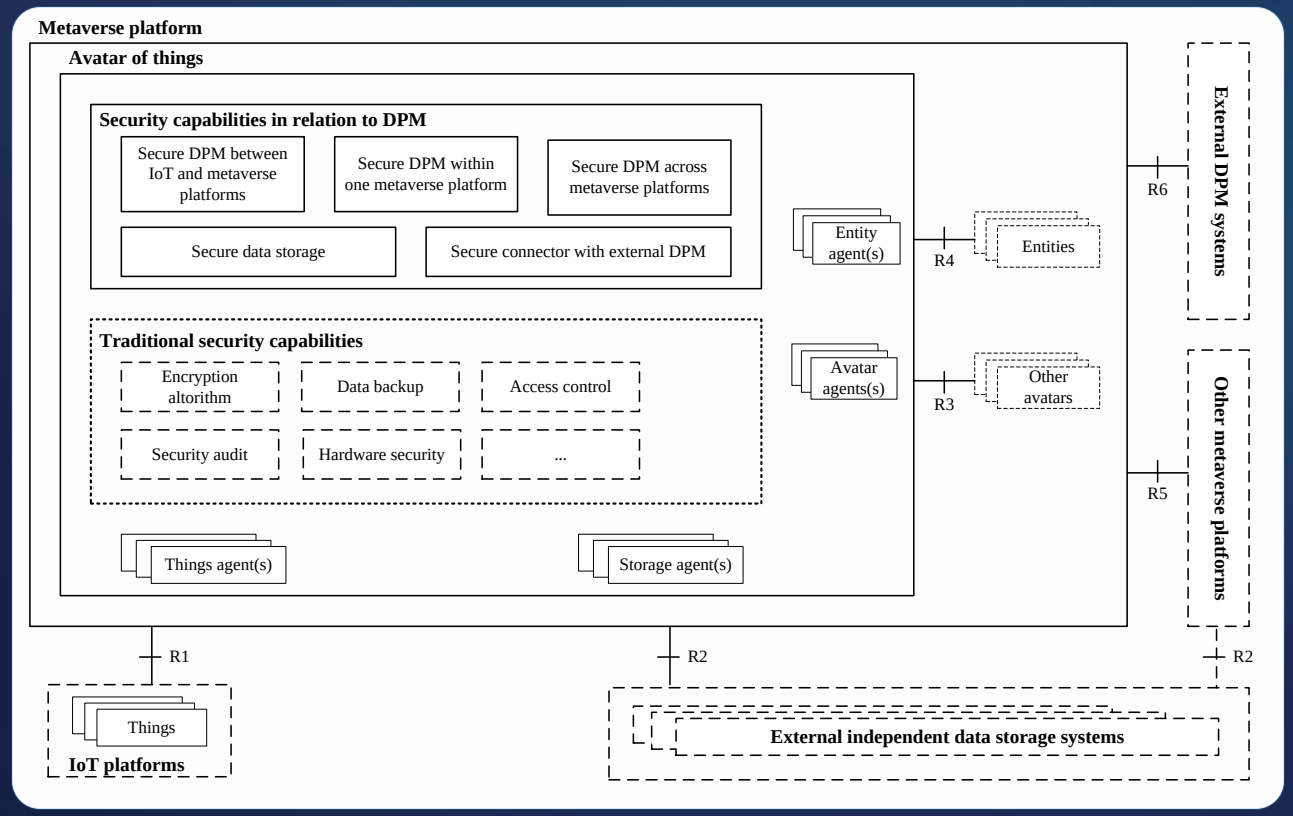
Analyse and provide solutions regarding the security for things across metaverses in relation to data processing and management, and includes relevant technical features, security risks and requirements, and reference security frameworks of security.

Security requirements

- for things across metaverses in relation to data processing
- for things across metaverses in relation to data lifecycle management
- for things across metaverses in relation to outside DPM resources
- for things across metaverses in relation to data encryption
- for things across metaverses in relation to access control

Current activity: Draft Rec. X.stm-dpm (cont.)

ITU-T **X.stm-dpm**: Security requirement and framework of metaverse platform for things across metaverses in relation to data processing and management



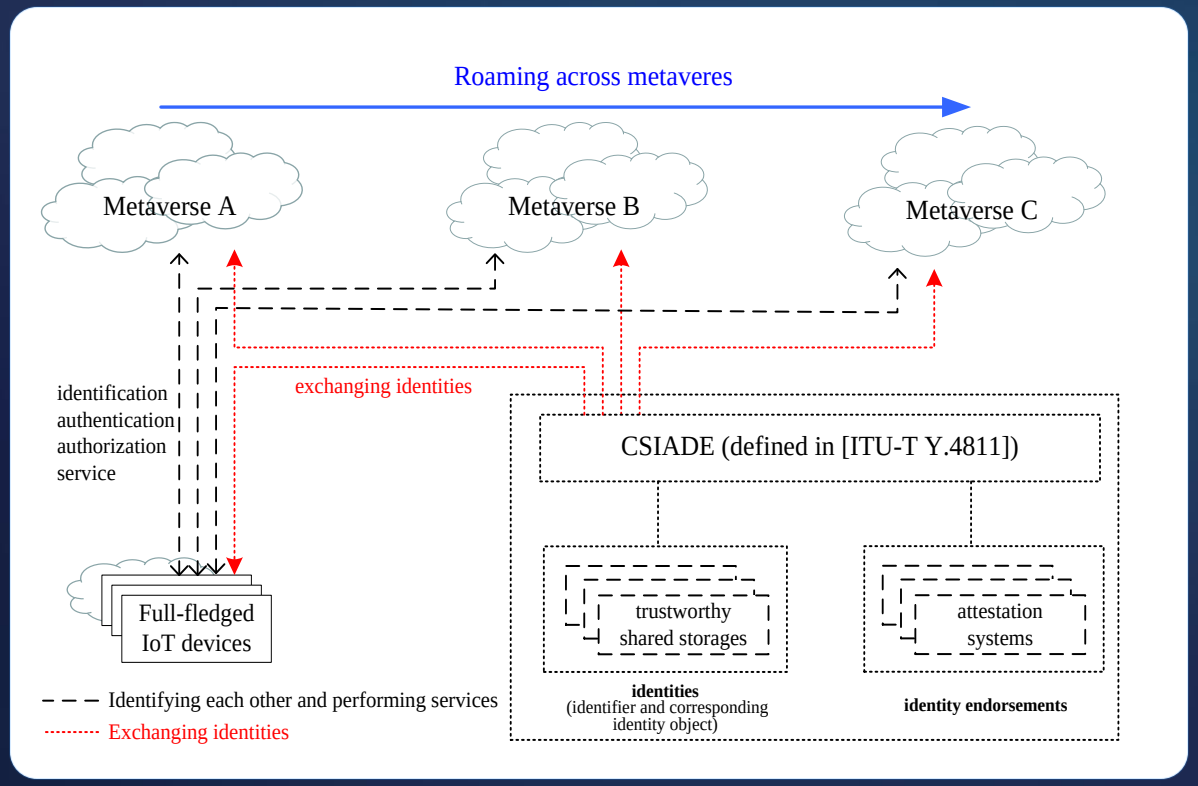
A security framework and relevant security capabilities

Key functional components

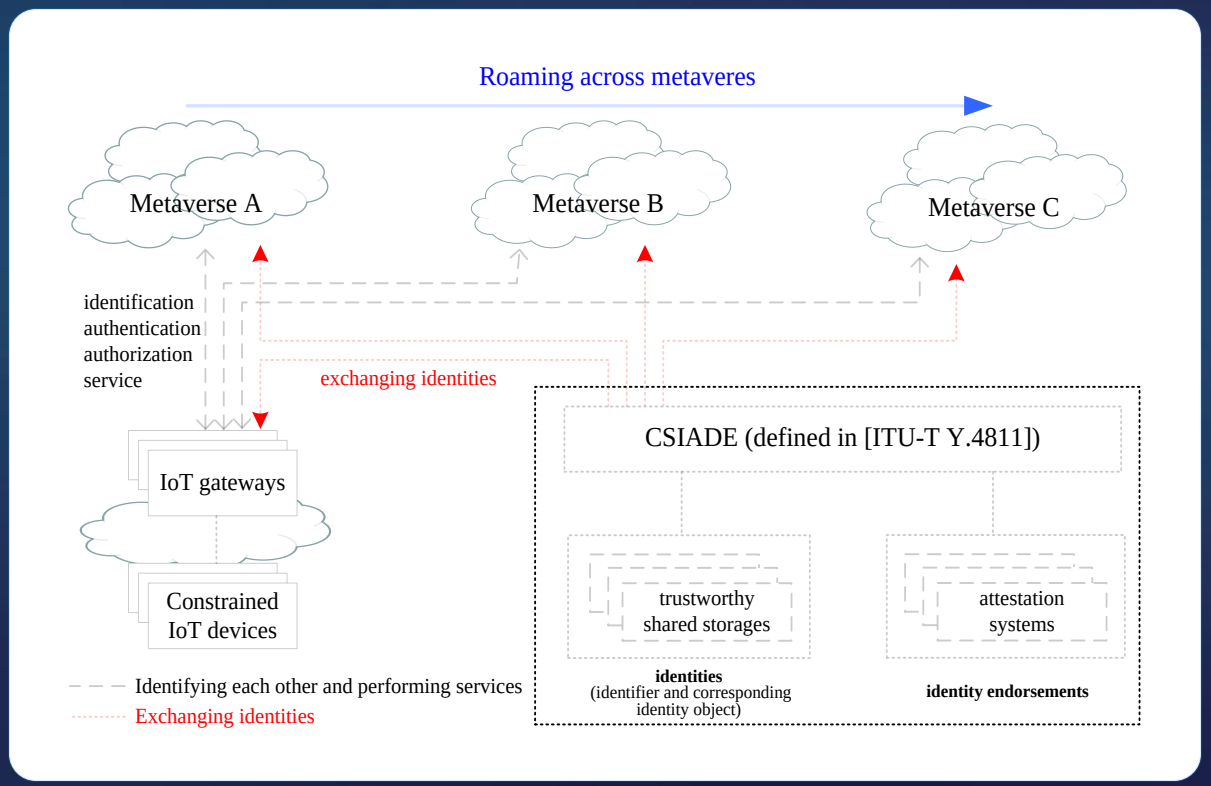
- Secure DPM between IoT platforms and metaverse platforms
- Secure DPM within one metaverse platform
- Secure DPM across metaverse platforms
- Secure data storage
- Secure connector with external DPM
- Things agents
- Storage agents
- Avatar agents
- Entity agents
- External entities (IoT platforms, external DPM systems, external independent data storage systems, etc.)
- Open reference points

Current activity: Rec. ITU-T Y.4812

ITU-T **Y.4812**, *Interoperability of IoT devices' identity across metaverse platforms*, describes **identity interoperability** for **IoT device across metaverse platforms**, and provides relevant technical features, functional requirements and reference frameworks.



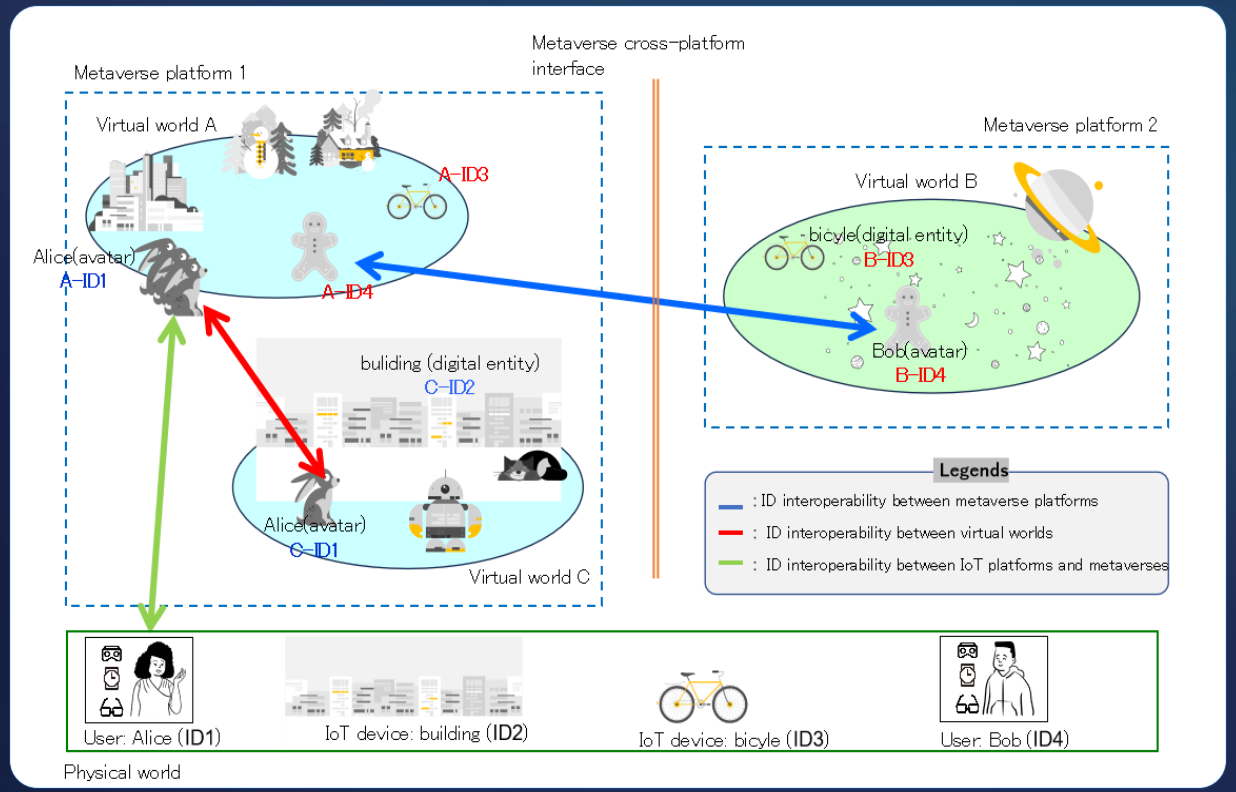
Use case: Full-fledged IoT devices to be across metaverse platforms



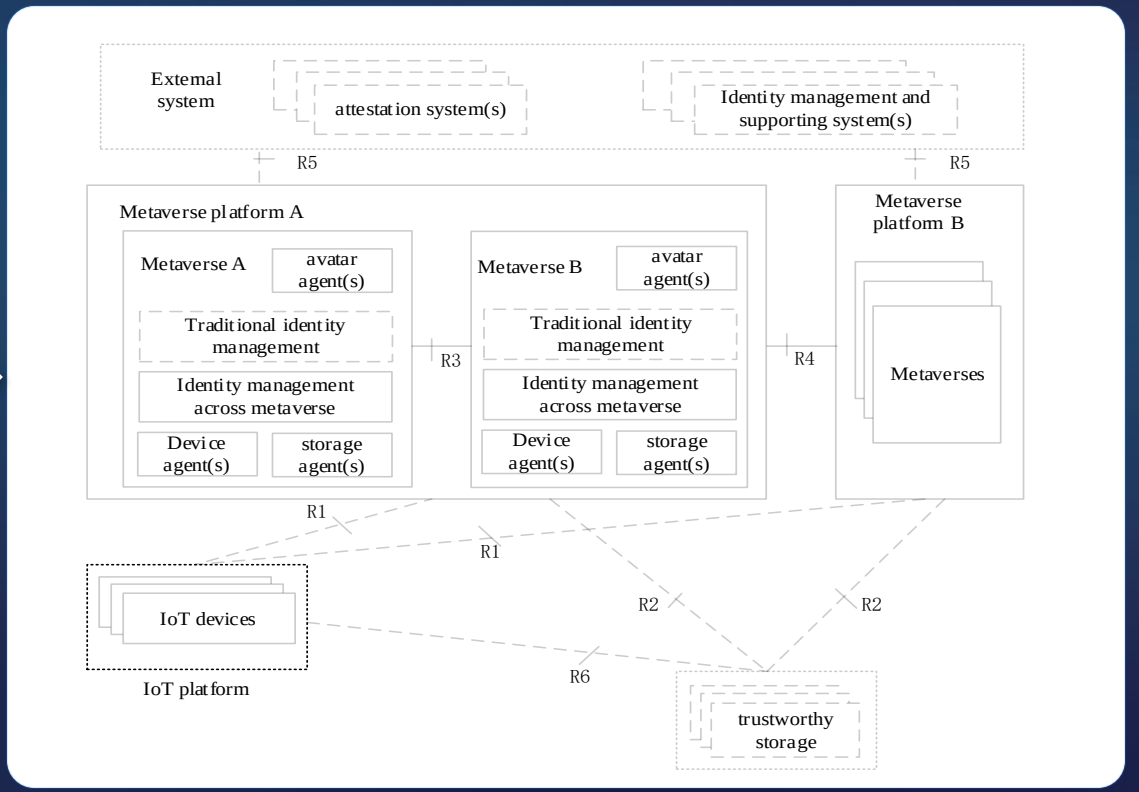
Use case: Constrained IoT devices to be across metaverse platforms

Current activity: Rec. ITU-T Y.4812 (cont.)

ITU-T **Y.4812**: Covering unique identity for IoT devices and corresponding digital entity, identification and authentication, data security and PII protection mechanisms, trustworthy storages for identity interoperability, and multiple identity management.



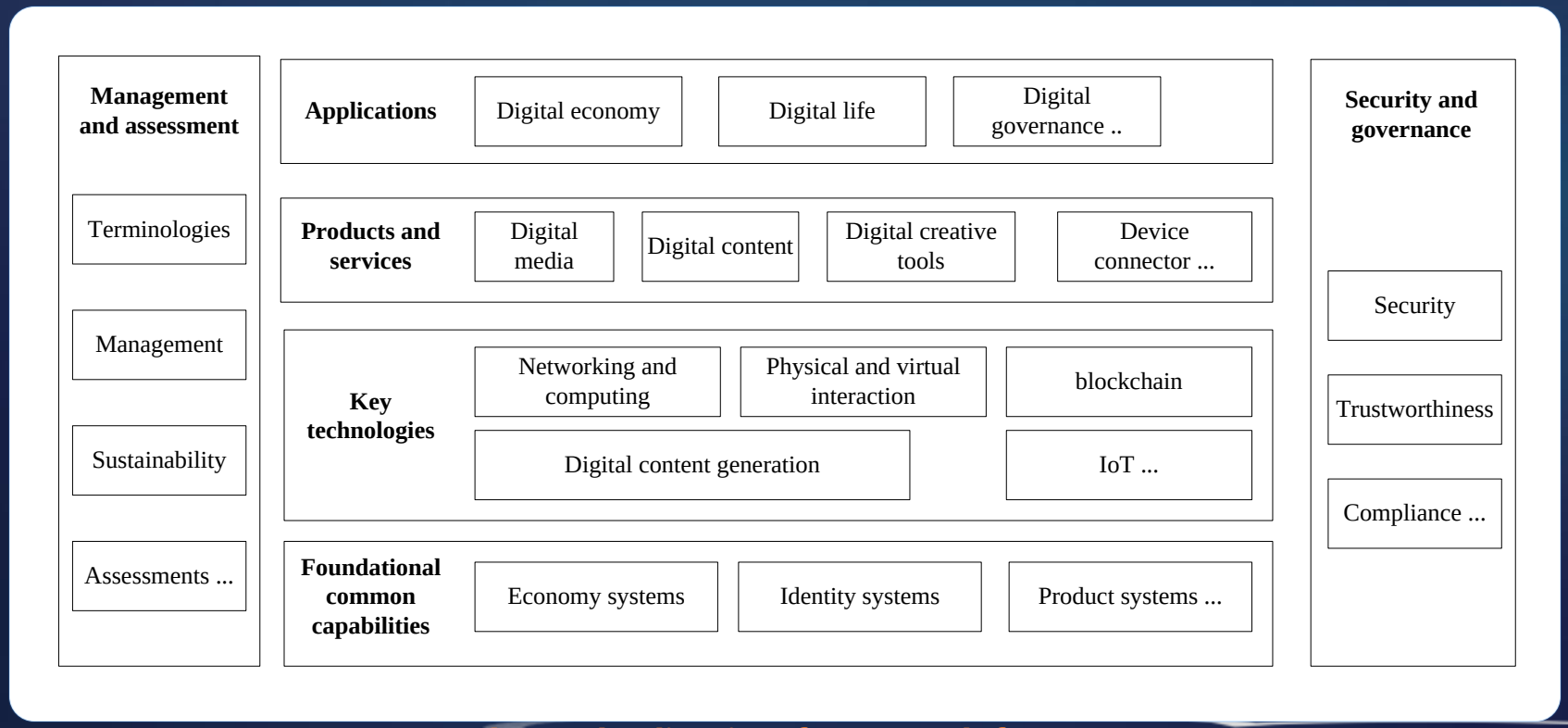
Three scenarios for identity interoperability [ITU-T Y.4812]



Reference framework for identity interoperability across metaverse platforms [ITU-T Y.4812]

More standards to foster a safer, credible, and reliable metaverse

The metaverse is set to transform the way we live and interact, opening up entirely new experiences. However, it also presents unprecedented challenges in terms of safety and ethics. To ensure we harness its full potential, it's critical to establish robust standards, with a primary focus on security.



Metaverse Security

- **Security and privacy protection (data, network, physical system, access system, environment, etc.)**
- **Ethical compliance (classification, ethical education, children protection, etc.)**
- **Regulation compliance ...**

A general standardization framework for metaverse

ITU Workshop on *Security and Privacy for Digital Twin and Metaverse*

Thanks

Xiongwei Jia, China Unicom, jiaxw9@chinaunicom.cn

* Images were generated by using Copilot