ITUPublications

International Telecommunication Union
Standardization Sector

# ITU Focus Group Technical Report

(06/2024)

ITU Focus Group on metaverse
(FG-MV)

# FGMV-42

# Interoperability of identity of things across metaverse platforms

*Working Group 5: Interoperability*

# Technical Report ITU FGMV-42

## Interoperability of identity of IoT device across metaverse platforms

### Summary

With regard to Internet of Things (IoT) [ITU-T Y.4000], each IoT device may have a single or multiple unique identities in multiple IoT systems. Similarly, each IoT device also may have a single or multiple identities in multiple metaverses. An identity of an IoT device usually includes a unique identifier and a corresponding identity object [ITU-T Y.4811].

Although, it may take advantage of one IoT device having one unique identity in multiple metaverses, there are challenges; how those metaverses identify, authenticate and authorize the IoT devices when they roaming across metaverse platforms, and how the trustworthy shared storages interact with each other to support identity interoperability across storages.

This Technical Report describes identity interoperability for IoT devices across metaverse platforms, and provides relevant technical features and reference framework.

### Keywords

IoT device; identity; interoperability; Internet of Things; metaverse; functional requirements

### Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

### Change Log

This document contains Version 1.0 of the ITU Technical Report on "*Interoperability of identity of IoT device across metaverse platforms*" approved at the 7th meeting of the ITU Focus Group on metaverse (FG-MV) held on 12-13 June 2024.

### Acknowledgements

This Technical Report was developed in WG5 of FG-MV, with inputs from NICT, ETRI, and China Unicom as a contribution to the ITU Focus Group on metaverse (FG-MV). The development of this document was coordinated by Hideo Imanaka (NICT) as FG-MV Working Group 5 (WG5) Chair, and Wook Hyun (ETRI) as WG5 Vice-Chair. In addition, special thanks go to Shin-Gak Kang (FG-MV Chair), the FG-MV management team, and the FG-MV Secretariat.

Additional information and materials relating to this Technical Report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact

Cristina Bueti at tsbfgmv@itu.int.

| | | |
|---|---|---|
| **WG5 Chair:** | Hideo Imanaka<br>NICT<br>Japan | E-mail: h.imanaka@nict.go.jp |
| **Editor:** | Xiongwei Jia<br>China Unicom<br>China | **E-mail:** jiaxw9@chinaunicom.cn |
| **Editor:** | Ziqin Sang<br>CICT<br>China | **E-mail:** zqsang@wri.com.cn |

| | | |
|---|---|---|
| **Editor:** | Keng Li<br>China Information Communication Technologies Group<br>China | **E-mail:** kli@fiberhome.com |
| **Editor:** | Xiaojun Mu<br>China Unicom<br>China | **E-mail:** muxj@chinaunicom.cn |
| **Editor:** | MiYoung Huh<br>ETRI<br>Korea (Republic of) | **E-mail:** myhuh@etri.re.kr |

## Table of contents

# Technical Report ITU FGMV-42

## Interoperability of identity of IoT device across metaverse platforms

## 1 Scope

This Technical Report describes identity interoperability for IoT device across metaverse platforms, and provides relevant technical features, functional requirements and reference frameworks.

The scope of this Technical Report includes:

- Overview of interoperability of identity of IoT device across metaverse platforms.
- Technical features, requirements of identity interoperability for IoT device across metaverse platforms.
- Reference framework of identity interoperability for IoT device across metaverse platforms.

Use cases and analysis on the identity solutions for IoT device across metaverses are provided in the appendix.

NOTE – The Technical Report will not bring new underlying identity standards for IoT devices, and blockchain itself is outside the scope.

## 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[ITU-T Y.4464] Recommendation ITU-T Y.4464 (2020), *Framework of blockchain of things as decentralized service platform.*

[ITU-T Y.4811] Recommendation ITU-T Y.4811, *Reference framework of converged service for identification and authentication for IoT devices in decentralized environment*

[ITU FGMV-19] Technical Specification ITU FGMV-19 (2023), Service scenarios and high-level requirements for metaverse cross-platform interoperability

[ITU FGMV-20] Technical Specification ITU FGMV-20 (2023), Definition of metaverse.

[ITU FGMV-31] Technical Specification ITU FGMV-31 (2024), Requirements, functional framework and capability of IoT for metaverse

## 3 Definitions

### 3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

**3.1.1 application** [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

**3.1.2 blockchain** [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

**3.1.3 decentralized system** [b-ITU-T X.1400]: Distributed system wherein control is distributed among the persons or organizations participating in the operation of system.

**3.1.4 device** [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, date capture, data storage and data processing.

**3.1.5 distributed ledger technology** (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

**3.1.6 identity** [b-ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

**3.1.7 Internet of things (IoT)** [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

**3.1.8 metaverse** [ITU FGMV-20]: An integrative ecosystem of virtual worlds offering immersive experiences to users, that modify pre-existing and create new value from economic, environmental, social and cultural perspectives.

**3.1.9 personally identifiable information (PII)** [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

**3.1.10 thing** [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

### 3.2 Terms defined in this Technical Report

None.

## 4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

| | |
|---|---|
| ID | Identity |
| IoT | Internet of things |
| PII | Personally Identifiable Information |

## 5 Conventions

None.

## 6 Overview of interoperability of identity of IoT devices across metaverses

With regard to Internet of things (IoT), each thing, called an IoT device in this document, is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing [ITU-T Y.4000]. In the metaverse, IoT devices could obtain the real-world environmental data and realize virtual and real interaction. IoT devices can transmit data to the virtual world and interact between the virtual world and the physical world [FGMV-31]. Each IoT device has a single or multiple unique identities in multiple IoT systems. An identity usually includes a unique identifier and a corresponding identity object [ITU-T Y.4811]. The unique identifier identifies corresponding IoT device, and the corresponding identity object usually includes information to resolve the identity of the IoT device, and to authenticate the IoT device.

The figure below explains the overview of identity interoperability.

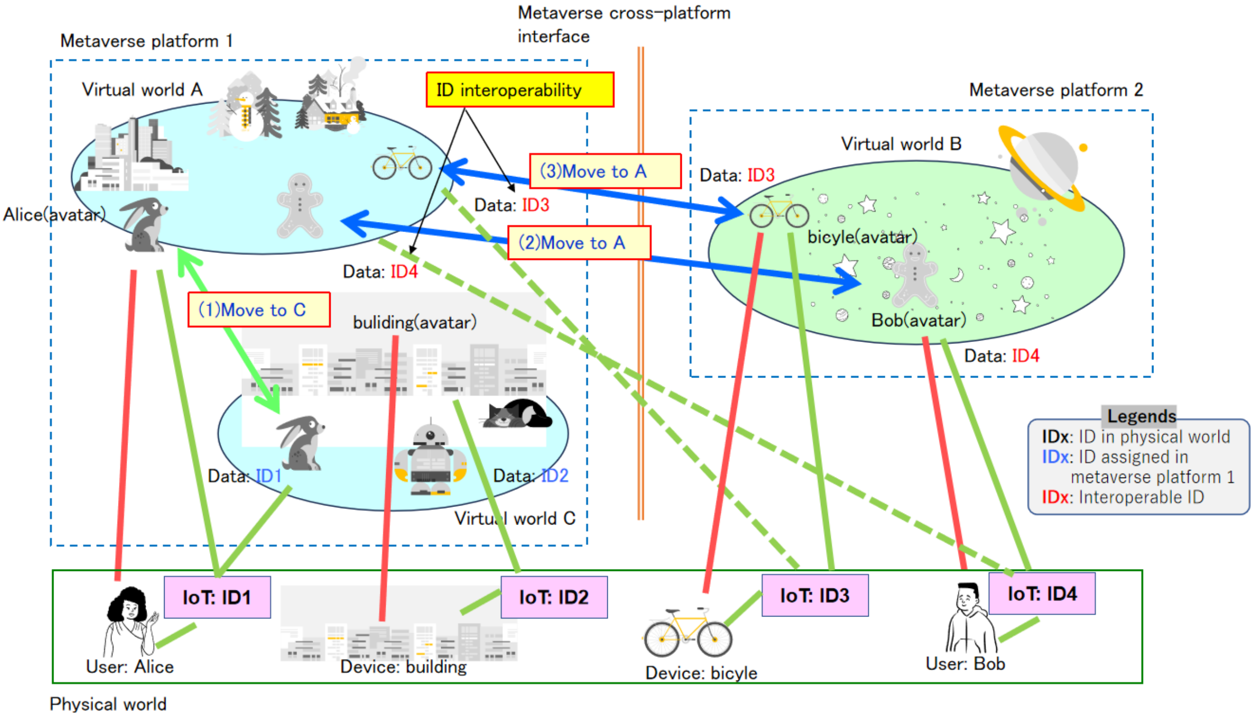


**Figure 6-1: Overview of identity interoperability**

In the figure 6-1, there are two metaverse platforms, 1 and 2, and one real world, and there are two virtual worlds (metaverses), A and C, in metaverse platform 1, and there is also one metaverse B in metaverse platform 2.

User Alice is connected to metaverse A (shown by the red line) with her environmental information, for example her body temperature, head movement and eye tracking information (shown by the green line), which was sensed by IoT devices with ID1. When Alice’s avatar moves to metaverse C in the same platform, as shown in (1) with the green arrow of the figure, the environmental information can be transferred from the same IoT device by using the same ID, i.e., ID1. Such ID can be used same manor within the same metaverse platform.

User Bob is connected to metaverse B (shown by the red line) and his environmental information (shown by the green line), which was sensed by IoT devices with ID4. When Bob’s avatar moves to metaverse A in the different platform, as shown in (2) with the blue arrow in the figure, the environmental information needs to be transferred from the same IoT device (show as the dotted green line). In this case, metaverse A needs to recognize ID4, in order to utilize the IoT device with ID4 from metaverse A. To do this, IDs of IoT devices need to be interoperable.

As the same manor, assets (bicycle) with ID3 in the figure, as shown in (3) with the blue arrow in the figure, and buildings with ID2 can be used in other metaverses of different platforms by ID interoperability, when these move to the other metaverses (shown as a dotted green line).

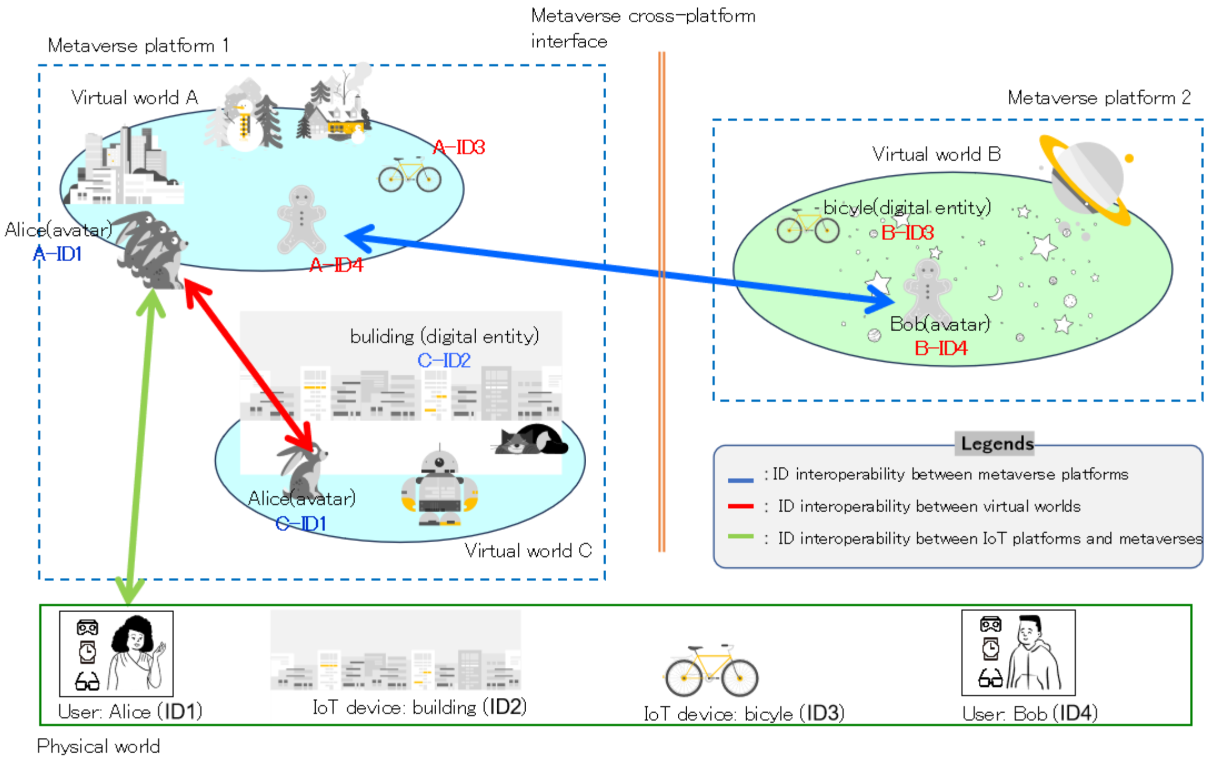
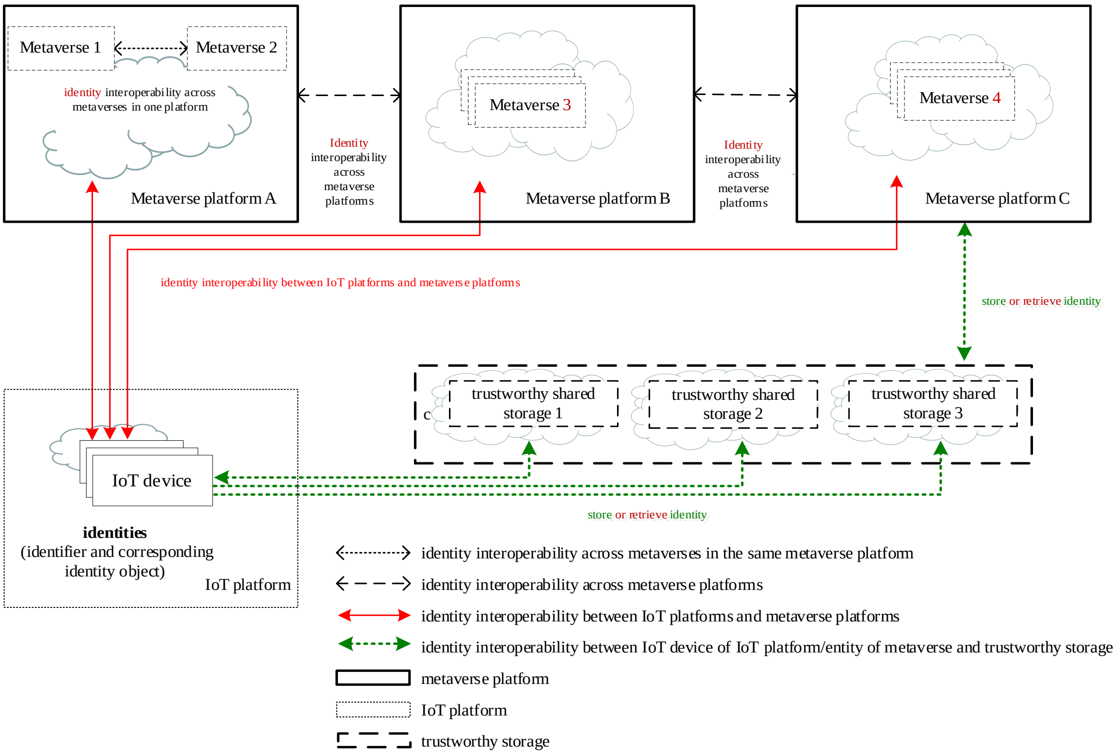


**Figure 6-2: Three scenarios for identity interoperability**

As figure 6-2 shows, the ID of Alice's avatar ID1 in the metaverse A can be named A-ID1; similarly, Alice's avatar in the metaverse C can be named C-ID1, and Bob's avatar in the metaverse B can be named B-ID4. There are three scenarios for identity interoperability. The IDs in the physical world interoperate with the IDs in the metaverse, e.g., ID1 and A-ID1 (shown in green arrow), the interoperability between different virtual worlds in one metaverse platform, e.g., A-ID1 and C-ID1 (shown in red arrow), and interoperability across metaverse platforms, e.g., A-ID4 and B-ID4 (shown in blue arrow). This deliverable focuses only on the interoperability across metaverse platforms.

# 7 Technical features of identity interoperability for IoT devices across metaverse platforms

Identity (ID) interoperability refers to the transfer of the entities' IDs between different metaverse platforms. Although, it may take advantage of entities to maintain unified IDs across multiple metaverse platforms [ITU FGMV-19], there are challenges; how the metaverses identify, authenticate and authorize the IoT devices when the digital entity of IoT devices are roaming across metaverse platforms (see figure 7-1), and how the trustworthy shared storages interact with each other to support ID interoperability across storage.



Metaverse 1
Metaverse 2
identity interoperability across metaverses in one platform
Metaverse platform A
Identity interoperability across metaverse platforms
Metaverse 3
Metaverse platform B
Identity interoperability across metaverse platforms
Metaverse 4
Metaverse platform C
identity interoperability between IoT platforms and metaverse platforms
store or retrieve identity
c
trustworthy shared storage 1
trustworthy shared storage 2
trustworthy shared storage 3
IoT device
identities
(identifier and corresponding identity object)
IoT platform
store or retrieve identity
identity interoperability across metaverses in the same metaverse platform
identity interoperability across metaverse platforms
identity interoperability between IoT platforms and metaverse platforms
identity interoperability between IoT device of IoT platform/entity of metaverse and trustworthy storage
metaverse platform
IoT platform
trustworthy storage

**Figure 7-1: Technical feature of identity interoperability across metaverse platforms**

Figure 7-1 shows the ID interoperability of IoT devices across metaverses mainly includes three cases:

- ID interoperability between IoT platforms and metaverse platforms,
- ID interoperability across different metaverses in the same metaverse platform,
- ID interoperability across metaverse platforms.

The ID of IoT device is usually stored in trustworthy shared storages (such as DLT systems) [ITU-T Y.4811]. Metaverses may also entrust their identity-related data to trustworthy shared storages. If a metaverse supports ID interoperability for IoT devices, it should exchange identity-related data with external IoT devices through independent trustworthy shared storages.

In the case of sharing IDs, if a given IoT device is roaming across metaverses, the IoT devices and the metaverses should exchange the shared identity-related data in order to identify and authenticate with each other, through the trustworthy shared storages.

## 7.1 ID interoperability between IoT platform and metaverse platforms

Users and IoT devices generate corresponding digital entities in the metaverses. The ID in the IoT platform and the ID in the metaverse platform are managed independently. ID interoperability between IoT platform and metaverse platforms can be realized through external services such as third-party platforms (e.g., blockchain platforms).

An IoT device can be connected to multiple metaverses to generate multiple different digital entities like avatars. IoT devices and their corresponding digital entities in the metaverse are independent with one another. If the IoT device is an access device sensing user's behaviour, the IoT device can share the same digital entity and ID with the user. If the IoT device and user are independent of each other, the IoT device can generate its own digital entity in the metaverse platform. In order to guarantee a trustworthy exchange of ID data, ID of IoT device may be stored in trustworthy shared storages, not in metaverses.

### 7.2 ID interoperability across metaverses in the same metaverse platforms

In the same metaverse platform, the IoT device information can be transferred from the same IoT device by using the same ID. Independent end-to-end identification and authentication can be supported between digital entities in the same metaverse.

Different digital entities of the same IoT device can be directly identified and authenticated through signatures. Correspondingly, the digital entities of different IoT devices will be assisted by external authentication systems to identify and authenticate. The data generated during ID interoperability across digital entities can be stored on the metaverse or on external trustworthy storage as required.

### 7.3 ID interoperability across metaverse platforms

The ID interoperability of the cross metaverse platforms requires ID identification and authentication across platforms. Multiple digital entities of one IoT device on different metaverse platforms are independent from one another. The operation of one digital entity in one metaverse platform does not affect other digital entities in the same metaverse or in other metaverses. ID interoperability across metaverse platform provides a variety of ID identification and authentication mechanisms, and can also invoke external ID identification and authentication systems for ID resolution. The mechanisms and policies for identification and authentication are jointly determined by the participants in metaverse platforms. The identity object [ITU-T Y.4811] contains the information required for identification and authentication. The data generated by the ID interoperability will be stored on multiple metaverse platforms, and can also be stored on external trustworthy storage. The identity object contains information about the data storage.

## 8 Functional requirements of ID interoperability for IoT devices across metaverse platforms

### 8.1 Unique identity for IoT devices and corresponding digital entity

All digital entities have a distinguishable identifier to ensure uniqueness within the home metaverse platform. This identifier needs to be globally unique when combined with a metaverse identifier for digital entities across metaverse platforms. One IoT device can have multiple digital entities, and the IoT device may be able to select a digital entity or multiple digital entities for moving to the other metaverse depending on the policy of the metaverse platform.

- It is recommended to generate a corresponding digital entity in metaverse of the IoT device, which have separate IDs if the IoT device is independent from the user. [IDIHR-101 of FGMV-19]
- It is recommended that the assignment of the unique identifier is carried out using cryptographic techniques to ensure security and prevent tampering. [GENHR-003 of FGMV-19]
- It is recommended to use traditional IoT device identification methods such as OID, Handle, and ECode, or use new decentralized IoT device identification methods such as DID for ID interoperability across metaverses.
- When IoT device have one unique identifier, it is required to provide globally unique identifiers for consistent identification as the digital entity moves to different metaverse platforms.

  NOTE: The examples of the unique ID are MAC address and Digital Object Identifier (DOI).
- It is recommended that the unique identifier embeds metadata related to the digital entity for creation date, originating platform, version information, and other information.

### 8.2 Identity identification and authentication

Identification and authentication of IoT devices in metaverse platforms are necessary to ensure securely and transparently record creation, authentication, validation and updating. The candidate technology includes blockchain technology, the unique identifier linked to a user's decentralized digital identity, and centralized registry or database storing unique identifiers.

For different cross-platform situations, the ID identification and authentication processes for IoT device and corresponding avatar are also different.

- It is recommended to enable digital entities of IoT devices in a metaverse platform to perform end-to-end identification and authentication with other digital entities in one or other metaverse platform directly. For ID interoperability between the IoT platform and the metaverse platform, it is recommended to introduce external systems platform to assist trustworthy identification and authentication between IoT devices and digital entities
- For different virtual worlds in the same metaverse platform, it is recommended that end-to-end identification and authentication can be carried out directly between digital entities.
- For different metaverse platforms, ID identification and authentication between digital entities are required to meet the requirements of ID management of different platforms.
- It is required for users to be able to link or unlink their ID to other platforms.

NOTE: If a user is linked to a metaverse platform, the platform can access the profile consented by the user.

### 8.3 Data security and PII protection mechanisms

In the process of ID interoperability, there may be threats such as data leakage and identity theft. PII protection mechanisms should be provided to improve ID security.

- It is recommended to provide security mechanisms for ID data processing (e.g., storage, transmission, validation) across metaverse platforms.

  NOTE: Blockchain technology might be used for securely and transparently record creation, authentication, validation and updating.
- It is recommended to ensure the security of ID storage, including the encryption, access control and security audit of identity information.

### 8.4 Trustworthy storages for identity interoperability

Trustworthy storage is used to store the ID of IoT devices and digital entities, ID authentication information, identity interoperability information, and so on.

- It is recommended to have a capability for connecting external storage to accommodate data volume growth in metaverses.
- It is recommended to ensure maintainable storage for identity, which means the system can be easily upgraded, backed up, and restored to ensure metaverse stability and availability.
- It is recommended to support a single sign-on (SSO) across platforms.

### 8.5 Multiple identity management policies

ID management policy refers to a comprehensive strategy for creating, authenticating, authorizing, monitoring and revoking the IDs of users, devices, applications, and other entities in an effective, secure, and compliant digital environment. For different countries and/or enterprises, the ID management policy might be different. For the metaverse platform, the ID management policy may be jointly decided by the metaverse company, the government and the regulatory authorities.

IoT platforms and metaverses have different ID management policies. ID interoperability follows different management policies, especially for cross-metaverse platforms.

IoT devices in IoT platform and digital entities in metaverses use the same or different ID management policies. The type of interoperability policy to be used depends on the specific scenario.

- It is recommended to evaluate the reputation of IoT devices which move from other platforms to determine whether to allow the move.
- It is recommended to be able to determine the eligibility for moving based on the criteria of the target metaverse such as the age and appearance of users intending to transfer from other platforms.
- It can optionally check the reputation of the user belonging to another platform through the agreement between platforms. [IDIHR-104]
- It is required that the reputation data is written in a standardized way for the compatibility of reputation evaluation between platforms. [IDIHR-104]
- It is required for metaverse platforms to manage digital entities access from other platforms based on the identity.
  NOTE: This identity can be received from other metaverse platforms or obtained in a variety of ways, such as DID and blockchain.
- It is required to support ID policies of each platform for ID interoperability. ID management policies may be set by governments or by companies.

## 9 Reference framework for identity interoperability for IoT devices across metaverse platforms

Figure 9-1 is a schematic diagram of the reference framework for ID interoperability across metaverses. ID interoperability across the metaverses includes ID interoperability between IoT platforms and metaverse platforms (R1); ID interoperability between IoT platforms, metaverse platforms, and trustworthy storage (R2); ID interoperability for different avatars in the same metaverse platform (R3); ID interoperability between different avatars across multiple metaverse platforms (R4); ID interoperability between metaverse platforms and external authentication systems (R5); ID interoperability between IoT device and trustworthy storage (R6).

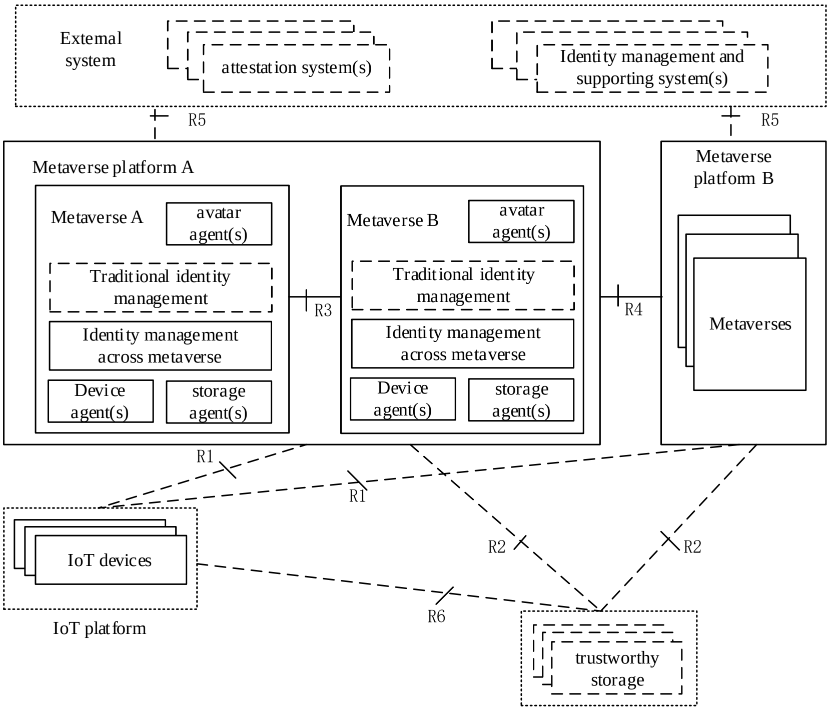


**Figure 8-1: Reference framework for identity interoperability across metaverse platforms**

## 9.1 Traditional ID management

Traditional ID management provides management services for the whole management process of ID generation, transmission, storage and resolution, as follows:

- generating unique IDs and corresponding ID objects, which can have aliases but all refer to unique entities;
- providing ID data transmission services, supporting identification and authentication services on different platforms; and
- providing ID endorsement management services; Different platforms have different ID management strategies and policies, traditional management function can coordinate and match ID resolution requirements for ID interoperability.

NOTE: The traditional ID management function provides some basic abilities of ID management across metaverses, which is out of the scope of this report.

## 9.2 ID management across metaverses

Compared with the traditional ID management module, the ID management across metaverses adds capabilities as follows:

- providing ID management policies for digital entities in metaverses, such as ID generation, identification, transmission, backup;
- providing ID authentication and resolution across metaverses. The metaverse platform may have multiple ID authentication policies, and ID management across metaverses can manage different policies for ID interoperability; and
- providing data management across metaverses. The upload and download of data need to be encrypted or packaged according to the relevant policies, and the data across metaverses will be stored on the metaverse platform or external trustworthy storage according to the policy.

### 9.3 IoT devices agent(s)

IoT devices agents interact with IoT devices, which provide capabilities as follows:

- interacting with IoT devices. One IoT devices agent can serve one or more IoT devices;
- supporting IoT devices to identify and authenticate digital entity of IoT devices mutually, end-to-end; and
- supporting IoT devices to manage policy related to their identities such as where to store, how to resolve ID and how to interact with digital entities.

### 9.4 Avatar agent(s)

Avatar agents interact with digital entity of IoT devices in the same or other metaverse platforms, which provide capabilities as follows:

- interacting with digital entity of IoT devices. One avatar agent can serve one or more IoT devices;
- supporting digital entity of IoT devices to identify and authenticate digital entity of IoT devices mutually, end-to-end; and
- supporting digital entity of IoT devices to manage policies related to their IDs such as where to store, how to resolve ID and how to interact with other avatars.

### 9.5 Storage agent(s)

Storage agents interact with decentralized systems and clouds, which provide capabilities as follows:

- connecting trustworthy storage to store and retrieve identity information of digital entities and IoT devices; and
- connecting trustworthy storage to store and retrieve modules for identifying and authenticating identities.

### 9.6 Reference points

There are a group of reference points for interoperability across metaverses, including:

- R1: for IoT devices to interact with digital entities and to identify and authenticate avatar IDs;
- R2: for trustworthy storage to store the ID and ID object information of avatars;
- R3: for ID interoperability between digital entities in the same metaverse platform;
- R4: for ID interoperability across multiple metaverse platforms;
- R5: for digital entities to interact with external authentication systems for identity endorsement and authentication.
- R6: for trustworthy storage to store the ID and ID object information of digital entities.

### 9.7 External systems

#### 9.7.1 Attestation system

There may be one or multiple attestation systems deployed by the same or different operators. An attestation system provides capabilities related to ID endorsement, as follows:

- receiving and endorsing IDs of digital entities if requested; and
- creating and endorsing IDs for digital entities if requested, optionally.

#### 9.7.2 ID management and supporting system

In addition to the metaverse platforms, external platforms also provide ID management capabilities, as follows:

- supporting to identify and authenticate ID of digital entities;

- supporting to manage ID of digital entities of  IoT devices;
- supporting to manage the policies related to ID of digital entities of  IoT devices; and
- works on the CSIADE specified in [ITU-T Y.4811].

# Appendix I

## Use cases of IoT devices to be across metaverse platforms

(This appendix does not form an integral part of these Technical Report.)

The appendix provides representative use cases of IoT devices to be across metaverses in aspects of interoperability of identity.

NOTE: [ITU-T Y.4811] provides a converged service for identification and authentication for IoT devices in decentralized environment (CSIADE), which can facilitate IoT devices and metaverses to identify and authenticate each other in IoT decentralized environments.

### I.1 Use case: Full-fledged IoT devices to be across metaverse platforms

This use case shows full-fledged IoT devices are roaming across multiple metaverses.

### I.1.1. Description

With supports of CSIADE, the full-fledged IoT devices and metaverses can generate and store their identities in trustworthy shared storages (see Figure I-1).

When full-fledged IoT devices are roaming across metaverses, the metaverses and the full-fledged IoT devices can retrieve and verify the IDs of their counterparts through the CSIADE. After that, they can identify and authenticate each other, and then the metaverses can authorize and perform services to the full-fledged IoT device.

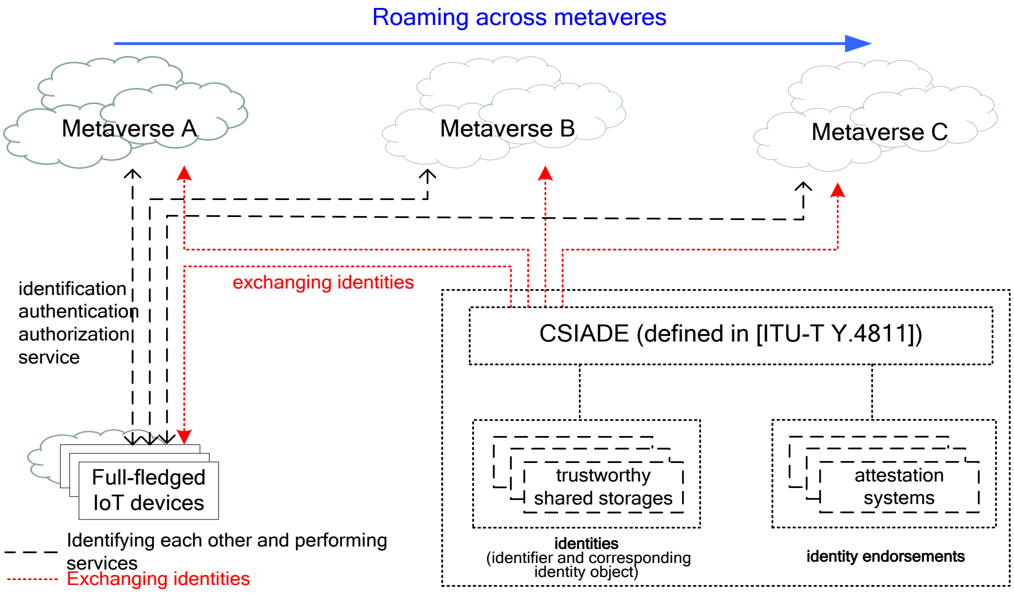


**Figure I-1: Full-fledged IoT devices to be across metaverse platforms**

### I.1.2. Assumptions

The assumptions related to this scenario include the following:

- It is assumed that metaverse platforms are independent from one another.
- It is assumed that I/O devices are independent of metaverse platforms.
- It is assumed that trustworthy shared storages and attestation systems are provided.

### I.2 Use case: Constrained IoT devices to be across metaverse platforms

This use case shows constrained IoT devices roaming across multiple metaverses.

### I.2.1. Description

Constrained IoT devices usually connect to metaverses via IoT gateways. With the support of CSIADE and IoT gateways, the constrained IoT devices and metaverses can generate and store their IDs in trustworthy shared storages (see Figure I-2).

When a constrained IoT device is roaming across metaverses, the metaverses and the IoT gateways (on behalf of the constrained IoT device) can retrieve and verify the IDs of their counterparts through the CSIADE. After that, they can identify and authenticate each other, and then the metaverses can authorize and perform services to the constrained IoT device.

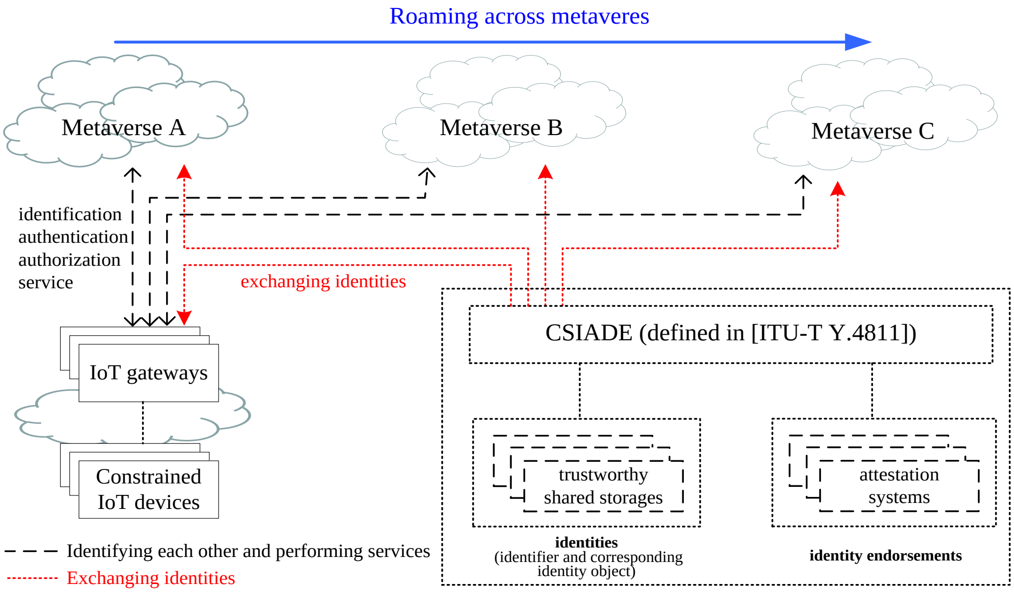


**Figure I-2: Constrained IoT devices to be across metaverse platforms**

### I.2.2. Assumptions

The assumptions related to this scenario include the following:

- It is assumed that metaverse platforms are independent from one another.
- It is assumed that IoT devices are independent of metaverse platforms.
- It is assumed that trustworthy shared storages and attestation systems are provided.

## Bibliography

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.