ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Specification

(06/2024)

ITU Focus Group on metaverse
(FG-MV)

FGMV-43

High-level interoperability architecture for cross-platform metaverse

Working Group 5: Interoperability

Technical Specification ITU FGMV-43

High-level interoperability architecture for cross-platform metaverse

Summary

This deliverable specifies the high-level interoperability architecture for cross-platform metaverse, highlighted for seamless integration and collaboration across different metaverse platforms. It provides a high-level functional architecture, outlining the key components and their interactions. Additionally, this identifies the reference points and information flows that enable interoperability between platforms.

Keywords

Metaverse; interoperability; high-level functional architecture

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 Specification on "*High-level interoperability architecture for cross-platform metaverse*" approved at the 7th meeting of the ITU Focus Group on metaverse (FG-MV) held on 12-13 June 2024.

Acknowledgements

This Technical Specification was developed in WG5 of FG-MV, with inputs from NICT, ETRI, China Unicom, and KDDI 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 and Editor. 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 Specification 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 NICT Japan	E-mail: h.imanaka@nict.go.jp
Editor and WG5 Vice-Chair:	Wook Hyun ETRI Korea(Republic of)	Tel: +82-42-860-1565 E-mail: whyun@etri.re.kr
Editor:	Xiongwei Jia China Unicom China	Tel: +86 15611092296 E-mail: jiaxw9@chinaunicom.cn
Editor:	Hideki YAMAMOTO OKI Japan	E-mail:yamamoto436@oki.com

Table of Contents

Page

Technical Specification ITU FGMV-43

High-level interoperability architecture for cross-platform metaverse

1 Scope

This technical specification describes the high-level interoperability architecture for cross-platform metaverse as follows:

- overview of interoperability architecture for cross-platform metaverse;
- high-level interoperability functional architecture;
- reference points for cross-platform metaverse; and
- information flows.

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

[ITU FGMV-10] Technical Report ITU FGMV-10 (2023), *Cyber risks, threats, and harms in the metaverse*

[ITU FGMV-28] Technical Specification ITU FGMV-28 (2024), *Requirements for the metaverse based on digital twins enabling integration of virtual and physical worlds*

[ITU FGMV-29] Technical Specification ITU FGMV-29 (2024), *Reference model for the metaverse based on a digital twin enabling integration of virtual and physical worlds*

[ITU FGMV-40] Technical Specification ITU FGMV-40 (2024), *Multimedia aspect of metaverse architecture*

[ITU FGMV-42] Technical Specification ITU FGMV-42 (2024), *Interoperability of identity of things across metaverse platforms*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Avatar [b-ITU FGMV-33]: Digital entity that can be used as a (visual) representation of the user inside the virtual environments.

3.1.2 home avatar [ITU FGMV-19]: the avatar which exists within original metaverse platform, remaining customizable for its corresponding entity. This primary version of an avatar ’in the metaverse resides exclusively within a specific metaverse platform or avatar service.

NOTE – The entity includes users, IoT devices, robots, digital humans, AI, system components, etc.

3.1.3 roaming avatar [ITU FGMV-19]: the avatar transitioning across various metaverse platforms from original metaverse platform, potentially undergoing alterations or transformations aligned with the destination platform's compatibility and features.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

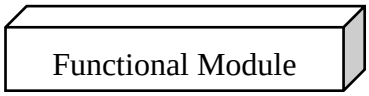
This Recommendation uses the following abbreviations and acronyms:

MP	Metaverse Platform
MIFM	Metaverse Interoperability Functional Module
AVIFC	Avatar Interoperability Functional Component
COIFC	Content Interoperability Functional Component
IDIFC	Identity Interoperability Functional Component
ASIFC	Asset Interoperability Functional Component
IMFC	Interoperability Management Functional Component
DTIFC	Digital Twin Interoperability Functional Component
AVTF	Avatar Transfer Functions
AVCF	Avatar Convert Functions
AVSF	Avatar Synchronize Functions
ASTF	Asset Transfer Functions
ASEF	Asset Exchange Functions
ASTKF	Asset Tokenize Functions
COTF	Content Transfer Functions
COCF	Content Convert Functions
COSF	Content Synchronize Functions
IDMF	Identity Migrate Functions
IDVF	Identity Verify Functions
IDSF	Identity Synchronize Functions
MPMF	Metaverse Platform Management Functions
MBMF	Metaverse Bridge Management Functions
LAF	Log and Audit Functions
DTFF	Digital Twin Federation Functions
DTTF	Digital Twin Translation Functions
DTBF	Digital Twin Brokering Functions
DTSF	Digital Twin Synchronization Functions

5 Conventions

In this Recommendation:

– The keyword “Functional Module” is defined as a collection of Functional components and represented by the following symbol:



– The keyword “Functional Component” is defined as a collection of Functions and represented by the following symbol:

– The keyword "Functions" is defined as a collection of functionalities and represented by the following symbol:

6 Overview

Currently, there are many metaverse platforms in the world, but they do not have interoperability capabilities in terms of avatar, asset, content, and identity interoperability as specified in [FGMV-19]. In order to provide such interoperability between metaverse cross-platforms, interoperability architecture for metaverse cross-platforms might be needed for common understandings among stakeholders.

6.1 Stakeholders of metaverse cross-platform interoperability

Stakeholders providing metaverse services were clarified in metaverse architecture document specified in [FGMV-40]. For providing interoperability between metaverse platforms, metaverse platform providers are included as one of the stakeholders, as shown in Figure 6-1. Other stakeholders such as network providers and metaverse component providers might be the same as stakeholders providing metaverse services, as shown in the architecture document.

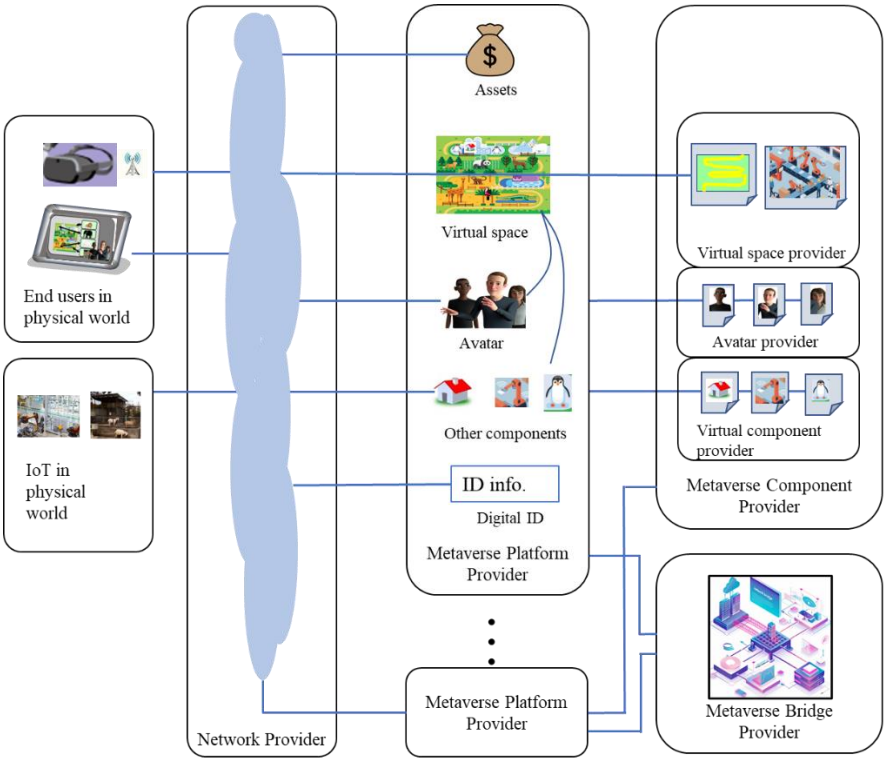


Figure 6-1 – Stakeholders for metaverse cross-platform interoperability

6.2 Frameworks of metaverse cross-platform interoperability

Based on the metaverse architecture framework described in the architecture document [FGMV-40], the interoperability framework is considered as a pair of architecture frameworks, as shown in Figure 6-2. In this figure, two metaverse platforms are connected by interface, and metaverse component providers are connected by application program interface (API) from both metaverse platforms.

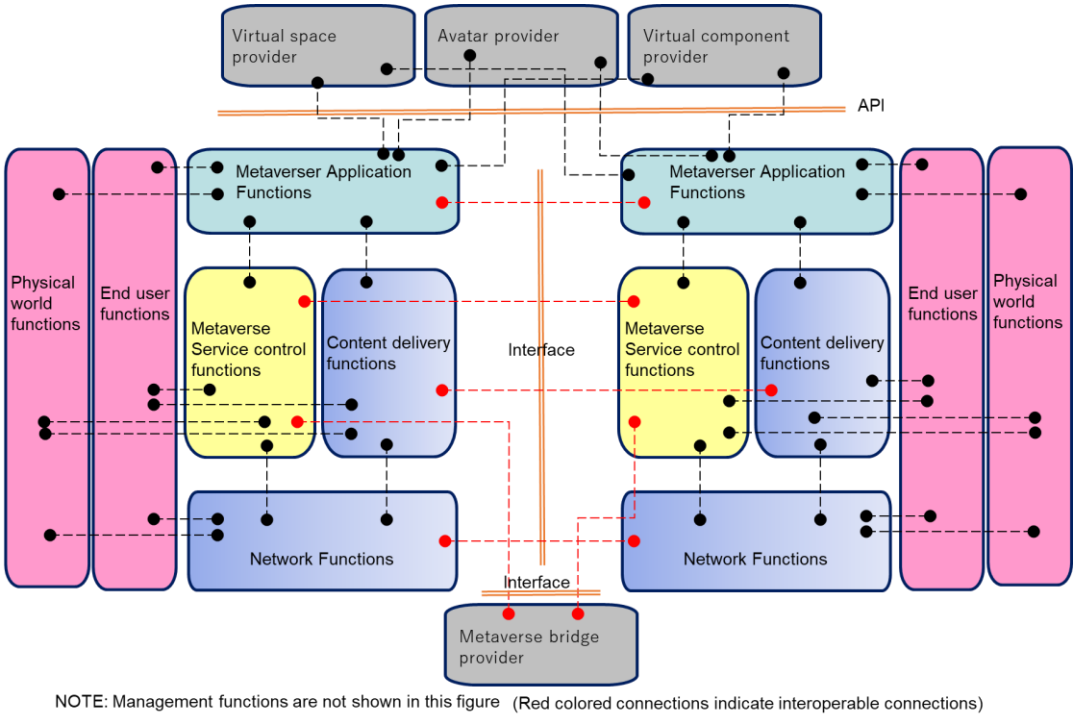


Figure 6-2 – Framework of metaverse cross-platform interoperability

In Figure 6-2, black links indicate connections between functions in a single metaverse platform, and red links indicate connections of functions between cross-platforms. The red-coloured links are

considered interoperability interfaces. It is noted that management functions are not indicated in the figure, and management functions exist in both metaverse platforms. Management function for managing interoperability might be required, so it is for further consideration.

6.3 Types of cross-platforms metaverse interoperability

(a) Metaverses without IoT or digital twins

Basically, metaverse consists of virtual assets, content, and digital entities such as avatars representing users or machines. Figure 6-3 shows the basic metaverse. Virtual assets and content are constructed virtually and do not depend on the real world. Users can operate virtual assets and content, but the results are not reflected in the real world.

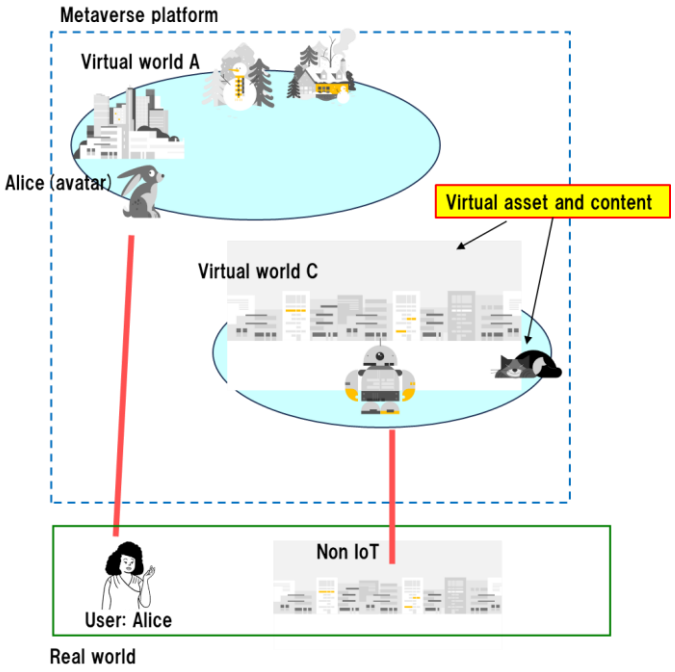


Figure 6-3 – Metaverses without IoT or digital twins

(b) Metaverses with IoT devices

On the other hand, IoT devices such as sensors and actuators can be utilized by metaverses [FGMV-WG40]. Sensed data from IoT devices such as temperature and factory data can be reflected to virtual assets in metaverse, and in addition, operation results in metaverse can be sent to the real IoT devices in the real world. Figure 6-4 shows metaverses with IoT devices. The IoT management functionality might be a part of metaverse platform, so some metaverses (virtual world C in the figure) can use the IoT.

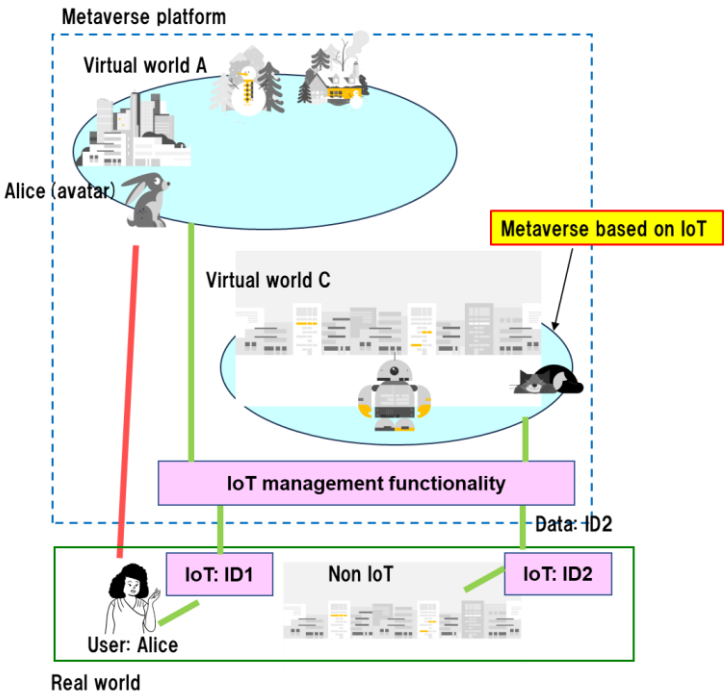


Figure 6-4 – Metaverses with IoT devices

(c) Metaverses with digital twins

Metaverses can utilize digital twin features to manage real-time synchronizing parameters between physical and virtual worlds [FGMV-28, FGMV-29]. In this type, called metaverse with digital twins, users may operate real world through virtual assets synchronized by digital twins. Figure 6-5 shows the metaverse with digital twins. In general, the digital twins feature is a part of metaverse platform. Some metaverses (virtual world A in Figure 6-5 may not use digital twin capabilities, and some metaverses (virtual world C in Figure 6-5) may use these capabilities.

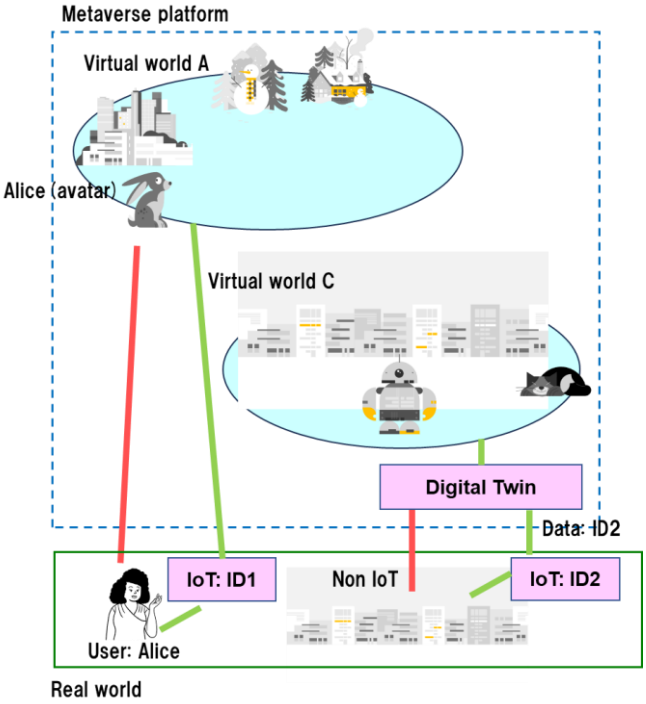


Figure 6-5 – Metaverses with digital twins

(d) Integrated metaverses with both digital twins and IoT devices

In general, digital twins utilize the sensed data from IoT devices, so IoT devices and digital twins can be used for metaverses. This type of metaverse platform utilizes IoT device management functionality included in the digital twin, so this type is covered by metaverses with digital twins.

Considering metaverse cross-platform interoperability, there are several types of interoperability, as shown in the table 6-1. In the table, the parts highlighted in grey are the same as the other parts.

Table 6-1: Types of interoperability between different types of metaverses

Type of metaverse	(a) without DT or IoT	(b) with IoT	(c) with DT
(a) without DT or IoT	Case A	Same as A	Same as A
(b) with IoT	-	Case B	Same as C
(c) with DT	-	-	Case C

Interoperability between (a) and (b), (c) or (d) are the same as case A because there are neither digital twin nor IoT capabilities in metaverse type (a). Interoperability between (b) and (c) is covered by case C. Case C covers all types of interoperability, so this document considers case C only. Figure 6-6 shows the interoperability of metaverses with both digital twins and IoT devices. Dashed lines between IoT management functionalities and between digital twins indicate necessary connections if these functions exist in the metaverse platforms.

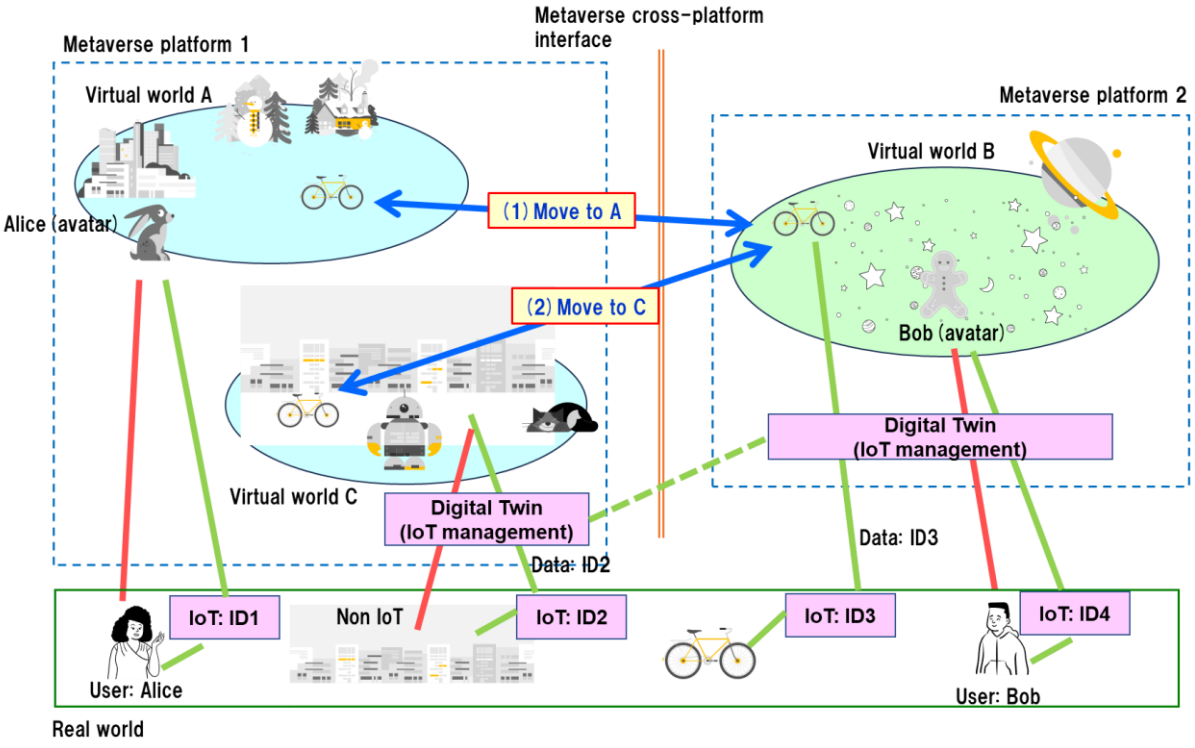


Figure 6-6 – Interoperability of metaverses with both digital twins and IoT devices

Arrow (1) in this figure shows that an asset with ID3 moves from virtual world B to virtual world A. In this case, there is no interoperability information on IoT devices and digital twins. Arrow (2) shows that an asset with ID3 moves from virtual world B to virtual world C, which uses IoT devices and digital twins. In this case, interoperability between digital twins in metaverse platforms 1 and 2 needs to be considered, and also between IoT management functionalities in metaverse platforms 1 and 2.

6.4 Architectural overview of cross-platform metaverse interoperability

The interoperability architecture for cross-platform metaverse is designed to address seamless integration and collaboration across different metaverse environments. This architecture enables users to navigate and interact seamlessly between various virtual worlds, promoting a unified and interconnected metaverse experience. This clause provides a high-level perspective on the interoperability architecture, outlining its key components and functionalities. The architecture facilitates the transfer of avatars, assets and user data across metaverse platforms, enabling users to maintain a consistent identity and experience. It encompasses aspects such as avatar interoperability, asset transfer mechanisms, content sharing, and identity management. There are many ways for metaverse platforms to interoperate with other platforms, but they can be generalized into two models:

- **Interoperation between metaverse platforms**: A metaverse platform can interact with other platforms using standardized protocols, as shown in Figure 6-7. As shown in the figure, since the interoperable metaverse platform bears Metaverse Platform (MP) and Metaverse Interoperability Functional Module (MIFM), there is no need for reference points.

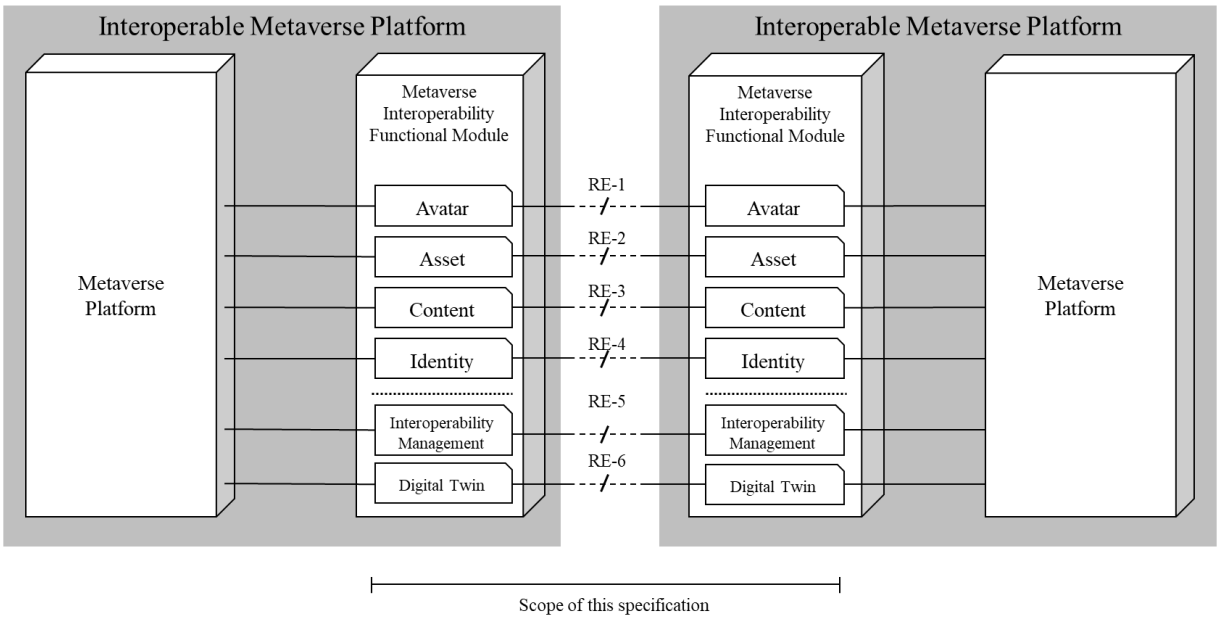


Figure 6-7 – Architectural overview of interoperation between metaverse platforms

NOTE—The dotted lines in MIFM (Metaverse Interoperability Functional Module) distinguish between the four interoperability functional components and the platform-related functional components.

- **Interoperation using metaverse bridge**: A metaverse platform uses a metaverse bridge to interact with other platforms. The metaverse bridge enables connectivity and interoperability between different metaverse platforms. It provides a virtual bridge which allows users, assets, identities and content to traverse and seamlessly interact between distinct metaverse platforms. This bridge does not need to be a part of a specific metaverse platform and can work independently as a third party service provider, as shown in Figure 6-8. Since this bridge is independent of metaverse platforms, it is easy for each bridge service provider to develop new features and various additional services quickly on a competitive basis.

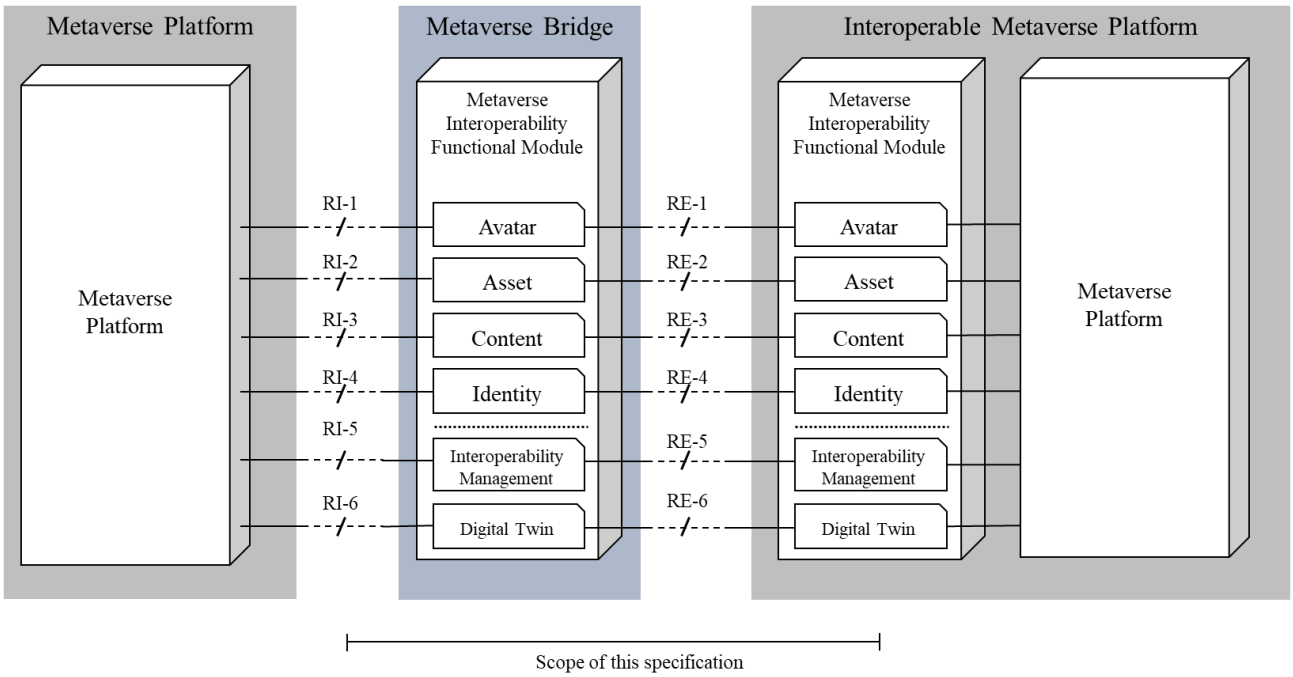


Figure 6-8 – Architectural overview on interoperation using metaverse bridges

NOTE—The dotted lines in MIFM (Metaverse Interoperability Functional Module) distinguish between the four interoperability functional components and the platform-related functional components.

7 High-level interoperability functional architecture for the cross-platform metaverse

This clause specifies the high-level interoperability functional architecture for cross-platform metaverse and describes relevant components to ensure interoperability with heterogeneous metaverse platforms. This architecture covers the metaverse bridge and interoperable metaverse platform models. However, depending on the interoperation model, each component of MIFM may interwork with other metaverse platforms through either an RI reference point or an RE reference point.

The metaverse interoperability functional module consists of AVIFC, IDIFC, ASIFC, COIFC, DTIFC, and IMFC. A metaverse service provider can selectively choose the component for their needs on interoperability for their metaverse platform.

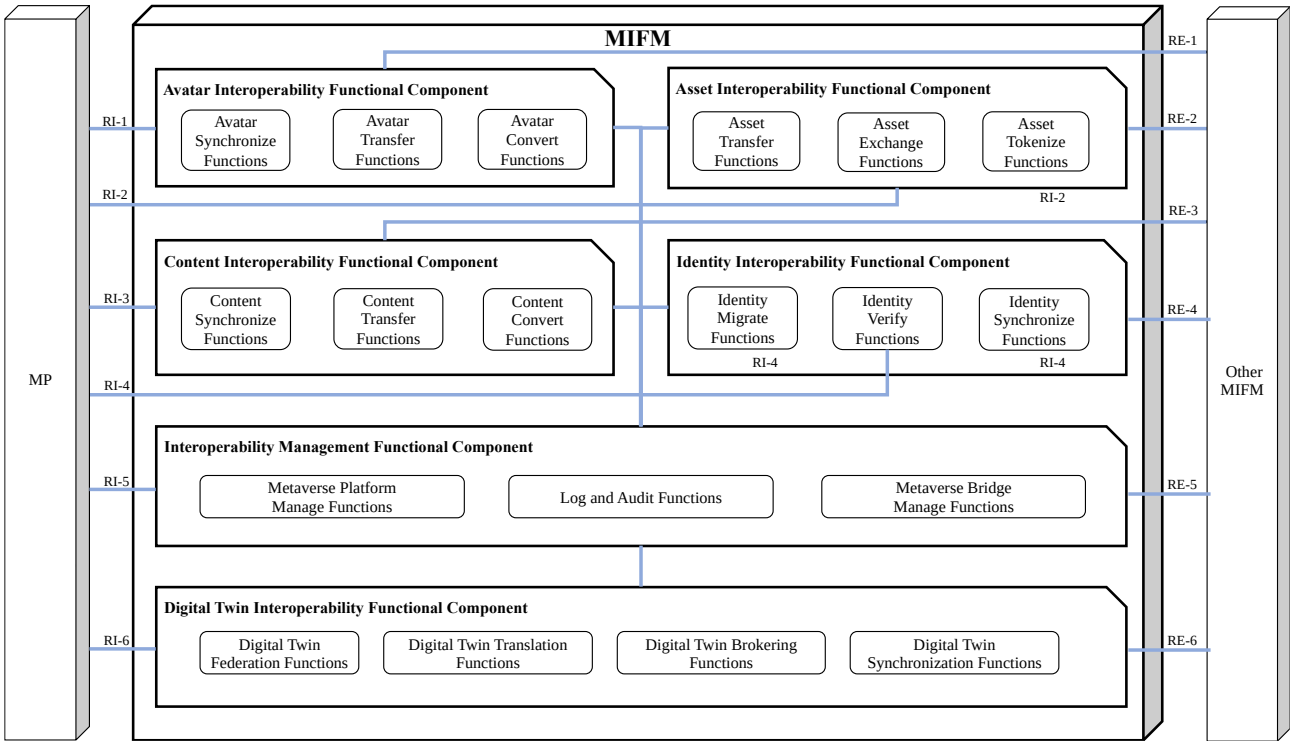


Figure 7-1 – High-level metaverse interoperability functional architecture

NOTE 1 – Users interact with MP using end-user devices, and this is beyond the scope of this document.

NOTE 2 – RI interfaces are used only when MIFM is not integrated with the interoperable metaverse platform.

7.1 Avatar Interoperability Functional Component (AVIFC)

The AVFIC is responsible for achieving avatar interoperability across different metaverse platforms. It enables seamless movement and utilization of avatars while preserving their appearance, identity and functionality. This component encompasses functionalities such as avatar transfer and synchronization to ensure compatibility and consistency of avatars across platforms.

7.1.1 Avatar Transfer Functions (AVTF)

AVTF enables avatars to migrate across different metaverse platforms while retaining their original characteristics. It manages the transfer of avatar data between platforms. This supports the transfer of, for example, state data, the profile of the avatar, accessories, control, rig and skeleton, across platforms.

When an avatar goes to another metaverse platform, each metaverse platform exchanges the constraints during the migration procedures for compliance and performance.

This interacts with the originating and destination metaverse platform for importing and exporting the avatar data through the reference point *RI-1* specified in clause 8.1.1 and interacts with Avatar Transfer Functions through the reference point *RE-1* specified in clause 8.2.1.

7.1.2 Avatar Convert Functions (AVCF)

If a roaming avatar does not satisfy the constraints of the destination metaverse platform that is exchanged through the interactions of AVTF of each platform, AVCF converts the data of the roaming avatar. This conversion also includes the appearance, accessories, and state data.

This interacts with the destination metaverse platform for getting the policy, such as the avatar appearance guidance, through the reference point *RI-1*. This converts the avatar received from Avatar Transfer Functions for the destination metaverse platform, and hands over to the destination metaverse platform through the *RI-1* reference point.

7.1.3 Avatar Synchronize Functions (AVSF)

AVSF facilitates seamless movement and activity of avatars across different metaverse platforms. Users can bring their created avatars to different platforms, and their actions and activities within each environment are recorded. These records are synchronized back to the avatar's original platform, allowing users to manage all activities in one place.

After an avatar has roamed across metaverse platforms, this synchronizes its attributes to ensure consistency. It synchronizes attributes of the avatar after experiencing by roaming the avatar across metaverse platforms to ensure the avatar’s consistent representation across metaverse platforms.

This interacts with the roaming metaverse platform, which retrieves the latest information on the roaming avatar through the reference point RI-1, and with the home metaverse platform, which synchronizes the information through the reference point *RE-1*.

7.2 Asset Interoperability Functional Component (ASIFC)

The ASIFC facilitates the transfer of digital assets, including tokenized items like NFTs, virtual real estate, and digital currencies, between metaverse platforms. It enables users to move and transact their assets seamlessly across different platforms, promoting cross-platform commerce. This is possible by leveraging technologies such as blockchain, which ensures secure and transparent asset transfers.

7.2.1 Asset Transfer Functions (ASTF)

ASTF enables the seamless transfer of tokenized assets between different metaverse platforms. It ensures that the necessary information, including ownership records, provenance, and metadata, is transferred accurately to maintain asset integrity during the process.

This interacts with the originating and destination metaverse platform for importing and exporting the asset data through the reference point *RI-2* specified in clause 8.1.2 and interacts with Asset Transfer Functions through the reference point *RE-2* specified in clause 8.2.2.

7.2.2 Asset Exchange Functions (ASEF)

ASEF allows users to exchange or convert their assets between different formats or currencies. It supports the seamless conversion of digital currencies, valuation mechanisms, and liquidity options, enabling users to transact and utilize their assets in diverse metaverse ecosystems.

If the asset is a blockchain-based cryptocurrency, the exchanged asset will reside in a crypto wallet of a specific blockchain supported by the destination metaverse platform. If the asset is a digital currency valid only for a particular metaverse platform, the exchanged asset will be kept in a user’s digital wallet of the destination platform.

This uses the reference point RE-2 to get the policy such as the exchange ratio, validation mechanism or blockchain, and performs actual asset exchanges. It also interacts with the metaverse platform through the reference point RI-2 to retrieve the asset of a specific user.

7.2.3 Asset Tokenize Functions (ASTKF)

ASTKF involves the conversion of digital assets, such as virtual real estate or collectibles, into tokenized forms using blockchain technology. It assigns unique identifiers and metadata to these assets, making them transferable and interoperable across metaverse platforms.

This interacts with MP to tokenize assets of MP, if it needs to make an NFT for use in other metaverse that supports a specific blockchain through the reference point RI-2. This does not interact with other MIFM directly but uses the indirect interoperability approach which is specified in [ITU FGMV-19].

7.3 Content Interoperability Functional Component (COIFC)

COIFC enables different metaverse platforms to share and exchange various contents of diverse media formats such as 3D models, animation, sound and text across platforms. This component also focuses on facilitating creators and developers in creating, sharing, and distributing content easily across different platforms. Additionally, considerations for content storage, retrieval, archiving, and meeting legal and regulatory requirements are addressed within this component.

7.3.1 Content Transfer Functions (COTF)

COTF is responsible for the transfer of content data between metaverse platforms to enhance efficiency securely. It facilitates the seamless transfer of metaverse content between metaverse platforms by exchanging content data including information for management, searchability, and interoperability, to be able to transfer between metaverse platforms. This facilitates the secure sharing of user content across metaverse platforms by encryption, access control, and authentication mechanisms to protect the data.

NOTE – The management of the content is up to the metaverse platform, not the scope of the MIFM.

This interacts with MP through the reference point *RI-4* to get/receive the content from the platform and interacts with the COTF of the corresponding CIFC through *RE-4*. The corresponding COTF hands over the received content to the COCF for converting or to MIFM directly through *RI-4*.

7.3.2 Content Convert Functions (COCF)

COCF ensures the compatibility of metaverse content, including user-created content, across different metaverse platforms by converting it into the target platform's supported format. It supports the maintenance of the quality and fidelity of the content during conversion, optimizes it for efficient rendering and performance, and adapts it to the specific requirements and limitations of the target platform. This enhances the portability of content data across platforms.

This converts the content received from COTF and hands over the result to COTF, which then hands over the converted content to MP through the reference point *RI-4*.

7.3.3 Content Synchronize Functions (COSF)

COSF synchronizes changes made to specific content across different platforms, ensuring that users always have the most up-to-date version. It detects and resolves conflicts that may arise when multiple users make changes simultaneously maintains the integrity and consistency of the content across platforms, and provides users with tools to manage and resolve conflicts. It also tracks and manages different versions of the content, allowing users to revert to previous versions and providing a history of changes.

This interacts with the COSF of the corresponding MIFM to synchronize specific content through the reference point RE-3, and it also interacts with MP to synchronize content across multiple metaverses through the reference point *RI-3*.

7.4 Identity Interoperability Functional Component (IDIFC)

IDIFC enables the transfer of user identities and associated data between different metaverse platforms, ensuring a unified identity experience across virtual worlds. It eliminates the need for users to create new accounts when transitioning between platforms. The identity interoperability component encompasses not just user identities, but also the identities of various objects within the metaverse that require recognition and identification.

7.4.1 Identity Migrate Functions (IDMF)

IDMF securely and efficiently transfers identities and associated information related to the user, avatars, virtual assets, permissions, preferences, and so on, between platforms. This supports a smooth transition and identity integrity across platforms while offering users control over the scope and granularity of data migration related to the identity.

This interacts with the MP and IDMF of the corresponding MIFM through the reference points RI-3 and RE-3, respectively. If the identity itself is managed by the MP, it hands over the migrated identity information to the MP directly. If the identity is platform-independent, it hands over the information to IDVF for verification.

7.4.2 Identity Verify Functions (IDVF)

IDVF ensures the authenticity and legitimacy of transferred identities. It can utilize various protocols and technologies such as cryptographic signatures, decentralized identifiers (DIDs) and zero-knowledge proofs to prevent unauthorized access and impersonation across platforms. This may also integrate with existing platform-specific authentication mechanisms for a seamless user experience.

This interacts with MP through *RI-3* to verify the validity of the migrated identity. In some cases, the identity is valid but not acceptable to a specific metaverse platform according to policy or administrative reasons. Hence, it is needed to interact with MP for the verification procedures.

7.4.3 Identity Synchronize Functions (IDSF)

IDSF enables real-time or periodic updates of migrated identities across platforms. This keeps user profiles, avatars, assets, and permissions consistent across different metaverse, addressing conflicts that may arise due to simultaneous updates on different platforms. This can provide users with a method to manage synchronized data across platforms.

This interacts with the IDSF of the corresponding MIFM through *RE-4* and also interacts with MP through *RI-4* for the synchronization of a specific identity. If the origin of the identity resides in a home metaverse platform, the changes made during roaming need to be synchronized in the home metaverse. However, it is also possible to keep the information in third-party service providers, such as cloud storage and blockchain. However, this Function takes care of the synchronization regardless of how it is managed.

7.5 Interoperability Management Functional Component (IMFC)

IMFC manages and facilitates seamless interactions between different metaverse platforms and the metaverse bridges. This management includes overseeing agreements and policies that govern the relationships between these platforms.

7.5.1 Metaverse Platform Management Functions (MPMF)

MPMF is responsible for managing the agreements between metaverse platforms. It keeps track of the specifics of these agreements, ensuring that all parties adhere to the established terms. This includes the exchanging and managing of manifesto that contains the details of bilateral agreements, which are direct agreements between two platforms regarding their interaction and data exchange protocols. It also oversees the policies, codes of conduct, and any regulatory guidelines that each platform must follow to maintain compatibility and ethical standards across the metaverse.

Each metaverse platform manages its manifesto and uses it for negotiating with other metaverse platforms. Through these negotiations, it is possible to figure out any functionalities that are interoperable or not. If it needs functionalities that are not compatible directly, it can ask Metaverse Bridge Management Functions to solve the situation. This involves ensuring that all platforms comply with agreed-upon norms and practices, promoting a safe and respectful environment for users.

This interacts with MP to get its manifesto information through the reference point *RI-5* and provides information or a guide for the decision-making process for each of the Functions in MIFM. It interacts with the MPMF of the corresponding MIFM to make an interoperable channel between them through the reference point *RE-5*. This also interacts with the MBFA of a metaverse bridge to make a detour channel between metaverse platforms through *RE-5*.

7.5.2 Metaverse Bridge Management Functions (MBMF)

MBMF manages information of metaverse bridges, which act as converters, allowing for seamless interaction between platforms by adapting information and content to be compatible across various metaverse platforms. By interacting with this, metaverse bridges can register their information with bilateral agreements or negotiations. The metaverse bridges support interoperability between metaverses on heterogeneous platforms. MBMF manages the virtual bridges of MIFM that it resides in. That is, MBMF in a metaverse bridge will manage all virtual bridges for multiple MIFMs, and MBMF in a MIFM manages only its virtual bridges.

MPMF interacts with this MBMF to manage a virtual bridge that connects heterogeneous metaverse platforms through the reference point *RE-5*.

7.5.3 Log and Audit Functions (LAF)

LAF performs logging and auditing, which are crucial for maintaining transparency and accountability. Logging refers to the systematic recording of events, transactions, and interactions that occur between the platforms. Auditing involves the review and examination of these logs to ensure compliance with the interoperability agreements and to identify any issues or discrepancies that may arise. However, this does not store all information related to logging and auditing functionalities directly. Instead, it provides an interface that facilitates the retrieval of this information from the metaverse platforms themselves. This provides up-to-date logging and auditing data without the need to maintain a separate, comprehensive database of such information. By offering an interface for this purpose, the component streamlines the process of monitoring compliance with interoperability agreements and policies, as well as conducting reviews and analyses of interactions between different platforms. This method supports a dynamic and efficient oversight mechanism, allowing for real-time access to relevant data directly from the source – the metaverse platforms.

This interacts with all Functions to log operational information for further auditing or inspection. However, it does not interact directly with the MP or the corresponding MIFM. The log or any record would be accessible through the MPMF or MBMF.

7.6 Digital Twin Interoperability Functional Component (DTIFC)

As stated in the use cases and requirements for the metaverse based on digital twins enabling integration of virtual and physical worlds [FGMV-28], digital twin serves as an interaction interface for integrating the virtual and physical worlds, allowing users to extend their experience beyond the confines of the virtual environment. As digital representations of physical objects, digital twins comprise the virtual worlds. For the integration of virtual and physical worlds, the digital twin is an interface between them.

Each digital twin consists of data and functions specific to domain-specific objectives and requirements. Through DTIFC, the data and functions of each digital twin can be linked to provide services that cannot be provided by individual digital twins alone.

7.6.1 Digital Twin Federation Function (DTFF)

The protection of private data and personally identifiable information held by individual digital twins is a critical issue. By making it possible to form a federation of digital twins that update a common virtual world model while maintaining the confidential data generated by entities in the real world, complex analysis, and simulation across different domains can be performed securely and in a scalable manner.

This function allows the formation of a federation of digital twins that update a common model while maintaining private data generated within each digital twin. It provides the following functionalities: aggregation that distributes and aggregates the common model; a model updating that updates the model using individual data; and a configuration that constitutes the federation.

7.6.2 Digital Twin Translation Function (DTTF)

Communication between digital twins in different metaverse platforms requires a wide range of transformations, from data format to units, languages, and semantics. Different levels of transformation are based on various approaches such as rules, ontologies, and AI needs to be provided for the purpose of digital twin collaboration.

This function realizes formal and semantic transformations of communication between digital twins of different metaverse platforms. Based on an abstract translation that defines an interface, it realizes a variety of transformations by embodying translators by rules, ontologies, AI, and so on, and combining them.

7.6.3 Digital Twin Brokering Function (DTBF)

If information is mistakenly shared among multiple digital twins, accurate analysis and simulation cannot be performed, and there is a risk of incorrect feedback to the real world, so an information exchange mechanism with high reliability and fault tolerance is necessary. There, it is required to identify and authenticate the digital twin, relay data transmission and reception, and perform data filtering, real-time delivery and guaranteed delivery.

This function uses brokering to mediate the exchange of information between the digital twin of the sender and receiver to identify and authenticate the digital twin, relay data transmission and reception, and perform data filtering, real-time delivery and delivery assurance.

7.6.4 Digital Twin Synchronization Function (DTSF)

To achieve interaction between entities in the real world and digital twin models in the virtual world, it is necessary to establish data flow between them and guarantee synchronization. It is necessary to perform many-to-many synchronization between different digital twin models and entities. In addition, it is necessary to take measures to prevent conflicting information from different digital twin models from being sent to the same entity.

This function performs the mapping between real-world entities and virtual world models between different digital twins, and synchronization and mediation of many-to-many information exchange between them between the different digital twins.

8 Reference points for cross-platform metaverse

This clause specifies the reference points of interoperability architecture for the cross-platform metaverse. It consists of two categories of reference points; MP -MIFM and MIFM-MIFM.

8.1 Reference points with metaverse architecture (MP-MIFM)

This clause specifies the reference points between MP and MIFM.

NOTE – This specification does not specify the details of the internal functional entities of MP.

8.1.1 Reference points RI-1 (MP –AVIFC)

This reference point is used for interactions between MP and AVIFC of MIFM. It encompasses the import and export of avatar data among metaverse platforms. Additional functionalities facilitated through this reference point include:

- **Importing Avatar Data**: Facilitates the process by which avatars entering a platform are integrated, ensuring that their appearance, identity, and associated data (e.g., state data, profile, accessories, control, rig, skeleton) are preserved.
- **Exporting Avatar Data**: Manages the preparation and transmission of avatar data when leaving a platform, ensuring all relevant characteristics are maintained for use on another platform.
- **Avatar Data Conversion**: In cases where an avatar does not meet the destination platform's constraints, RI-1 enables the conversion of avatar data (including appearance, accessories, and state data) to meet these requirements.
- **Policy Acquisition for Avatar Conversion**: Supports the retrieval of policies from the destination platform necessary for the conversion process, such as avatar appearance guidelines.
- **Retrieval of Latest Avatar Information**: For avatars that have migrated across platforms, RI-1 supports the retrieval of updated information to ensure the avatar's consistent representation.

8.1.2 Reference points RI-2 (MP – ASIFC)

This reference point is used for interactions between MP and ASIFC of MIFM, including the following functionalities;

- **Importing and Exporting of Asset Data**: Facilitates the secure transfer of digital assets, including ownership records, provenance, and metadata, between a platform and the interoperability framework, ensuring asset integrity is maintained.
- **Asset Tokenization**: Enables the conversion of digital assets like virtual real estate or collectibles into tokenized forms, assigning unique identifiers and metadata for interoperability across platforms, facilitated through direct interaction between MP and MIFM.
- **Asset Exchanges**: Conversion or exchange of assets between different formats or currencies within the ecosystem of metaverse platforms. It includes the seamless conversion of digital currencies, the valuation of different assets, and providing liquidity options for users to transact and utilize their assets across diverse environments.

8.1.3 Reference points RI-3 (MP – COIFC)

This reference point is used for interactions between MP and COIFC of MIFM for the following functionalities;

- **Importing and Exporting of Content and Meta-data**: Facilitates the secure transfer of content data, including 3D models, animations, sound and text, between a specific MP and MIFM. This includes mechanisms for encryption, access control, and authentication to protect the data.
- **Content Synchronization**: Enables the updating and synchronization of content across a specific MP and MIFM to ensure users have access to the latest content versions. This involves managing conflicts and providing version control.

8.1.4 Reference points RI-4 (MP – IDIFC)

This reference point is used for interactions between MP and IDIFC of MIFM for the following functionalities;

- **Secure Transfer of Identity Data**: Facilitates the secure and efficient movement of user identity information and associated data (e.g., avatars, virtual assets, permissions, preferences) between MP and MIFM, ensuring a smooth transition across platforms.
- **Verification of Transferred Identities**: Supports the verification of the authenticity and legitimacy of identities transferred to or from a platform, utilizing various protocols and technologies (cryptographic signatures, DIDs, zero-knowledge proofs) to prevent unauthorized access and impersonation.
- **Synchronization of Identity Information**: Enables the updating and synchronization of identity information within a specific platform and between the platform and the interoperability framework, maintaining consistency of user profiles, avatars, assets and permissions.
- **Conflict Resolution and Management**: Assists in detecting and resolving conflicts that may arise from simultaneous identity updates on the platform, ensuring the integrity of identity data is maintained.
- **User Control Over Identity Data Migration**: Empowers users with control over the migration of their identity data between platforms, allowing individuals to manage what parts of their identity are shared or transferred.

8.1.5 Reference points RI-5 (MP– IMFC)

This reference point is used for interactions between MP and IMFC of MIFM for the following functionalities;

- **Manifesto Information Retrieval and Sharing**: Facilitates the exchange of manifesto information, including the specifics of bilateral agreements, policies, codes of conduct, and regulatory guidelines between MP and MIFM, ensuring all parties adhere to established terms.
- **Logging and Auditing Interface Provision**: Offers an interface for the retrieval of operational information for logging and auditing purposes from the metaverse platform to support transparency and accountability.

8.1.6 Reference points RI-6 (MP – DTIFC)

This reference point is used for interactions between MP and DTIFC of MIFM for the following functionalities;

This reference point is used for interactions between MP and DTIFC of MIFM for the following functionalities. Here, “models” correspond to the virtual world model, common model, and digital twin model of DTIFC.

- **Analysis and simulation management**: Accesses to the models and functions of analysis and simulation in the digital twin of MP.
- **Object management**: Access to the models and functions of digital object management in the digital twin of MP.

- **Data management**: Access to the models and functions of stored and stream data management in the digital twin of MP.
- **IoT gateway**: Access to the MP functions for management and I/O of IoT devices in the digital twin of MP.

8.2 Reference points with other MIFM (MIFM-MIFM)

This clause specifies the four reference points with other MIFMs.

8.2.1 Reference points RE-1 (AVIFC – AVIFC)

This clause describes the reference points between AVIFMs to make an avatar interoperable including the following functionalities:

- **Synchronization of Avatar Attributes**: This ensures that any changes or activities undertaken by an avatar across different platforms are recorded and synchronized back to the avatar's home platform, allowing for unified management of the avatar's experiences.
- **Exchange of Constraints and Policies**: Facilitates the exchange of information regarding constraints and policies between originating and destination platforms to ensure compliance and optimal performance during avatar migration.
- **Avatar Transfer Coordination**: Coordinates the transfer of avatar data between platforms, ensuring seamless migration without loss of characteristics or functionality.
- **Cross-Platform Compatibility Checks**: This process checks to ensure avatars are compatible with the technical and operational standards of the destination platform and addresses any interoperability issues that may arise.
- **Conflict Resolution in Avatar Synchronization**: Manages the resolution of conflicts that may occur due to simultaneous updates to an avatar's state on different platforms, ensuring data integrity and consistency.

8.2.2 Reference points RE-2 (ASIFC – ASIFC)

This clause describes the reference points between ASIFCs to support asset interoperability, including the following functionalities:

- **Cross-Platform Asset Transfer Coordination**: Coordinates the seamless transfer of tokenized assets between different metaverse platforms through direct interactions between interoperability frameworks, ensuring the preservation of asset information across transfers.
- **Policy Exchange for Asset Exchange**: Facilitates the exchange of policies related to asset exchange between platforms, such as exchange ratios, validation mechanisms, and supported blockchains, ensuring that asset exchanges adhere to agreed-upon standards.
- **Interoperability Checks for Asset Tokenization**: Supports the process of ensuring that tokenized assets conform to the interoperability standards of participating platforms, allowing assets to be recognized and utilized across different metaverse environments.

8.2.3 Reference points RE-3 (COIFC – COIFC)

This clause describes the reference points between COIFCs to support content interoperability, including the following functionalities:

- **Cross-Platform Content Exchange**: Coordinates the exchange of content between different metaverse platforms through direct interactions between MIFMs, ensuring seamless content sharing and distribution.
- **Content Compatibility and Conversion Coordination**: Facilitates discussions and agreements on content conversion standards and practices between platforms to ensure content remains compatible and maintains its integrity across diverse environments.
- **Synchronization of Content Updates**: Manages the synchronization of content changes across platforms, ensuring that all users have access to the most current version of content,

regardless of the platform. This includes the resolution of conflicts that may arise from simultaneous updates and the management of content versions for historical tracking.
- **Cross-Platform Content Management and Archiving**: Supports the establishment of shared guidelines for content storage, retrieval, archiving and compliance with legal and regulatory requirements, facilitating a unified approach to content management across the metaverse.

8.2.4 Reference points RE-4 (IDIFC – IDIFC)

This clause describes the reference points between IDIFCs to support identity interoperability, including the following functionalities:
- **Cross-Platform Identity Synchronization**: Coordinates the real-time or periodic updates of migrated identities across different platforms through direct interactions between MIFMs, ensuring user identities are consistent and up-to-date across the metaverse.
- **Inter-MIFM Identity Verification Coordination**: Facilitates the exchange of verification outcomes and policies between different platforms to recognize and validate transferred identities across the ecosystem, ensuring seamless user access and interaction.
- **Management of Identity Synchronization Policies**: Oversees the establishment of common policies and protocols for identity synchronization across platforms, including guidelines for conflict resolution, data privacy, and user consent.
- **Cross-Platform Identity Conflict Resolution**: Supports mechanisms for resolving identity conflicts that arise from simultaneous updates across platforms, ensuring a coherent identity experience for users navigating multiple metaverse environments.

8.2.5 Reference points RE-5 (IMFC – IMFC)

This clause describes the reference points between IMFCs to support interoperability management, including the following functionalities:
- **Interoperable Channel Establishment**: Coordinates the creation of interoperable channels between different MIFMs to support seamless interactions and data exchange protocols between metaverse platforms, enhancing cross-platform compatibility and cooperation.
- **Negotiation and Agreement Management**: Facilitates the negotiation and management of agreements between different metaverse platforms, including the exchange and update of manifesto contents to reflect current and mutually agreed-upon terms for interaction and data exchange.
- **Metaverse Bridge Coordination**: Manages the information and operation of metaverse bridges that serve as converters to ensure seamless interaction between platforms, allowing for adaptation of information and content to be compatible across various environments.

8.2.6 Reference points RE-6 (DTIFC – DTIFC)

This clause describes the reference points between DTIFCs to support interoperability management, including the following functionalities:
- **Federation of digital twins**: Configures and manages federation tasks and conducts distribution, execution, aggregation, and optimization of common models between DTIFCs.
- **Translation between digital twins**: Facilitates conversion with translation of data through rules, schema matching, ontology inference and/or machine learning between DTIFCs.
- **Brokering information exchange between digital twins**: Transmits data and commands with their routing and filtering based on application context between DTIFCs.
- **Synchronization of access to IoT l entity between digital twins**: Coordinates I/O of IoT devices between DTIFCs.

9 High-level Information flows

This clause describes high-level information flows with functional components to support interoperability of avatar, asset, content, and identity, as well as the registration of the corresponding metaverse, with examples.

NOTE – In the future, other groups or other Recommendations may possibly further subdivide or merge these information flows.

9.1 Avatar migration

This clause describes high-level information flows to explain how each of the Functions interacts on an avatar migration. It is assumed that both platforms have established channels through the procedures described in clause 9.5.

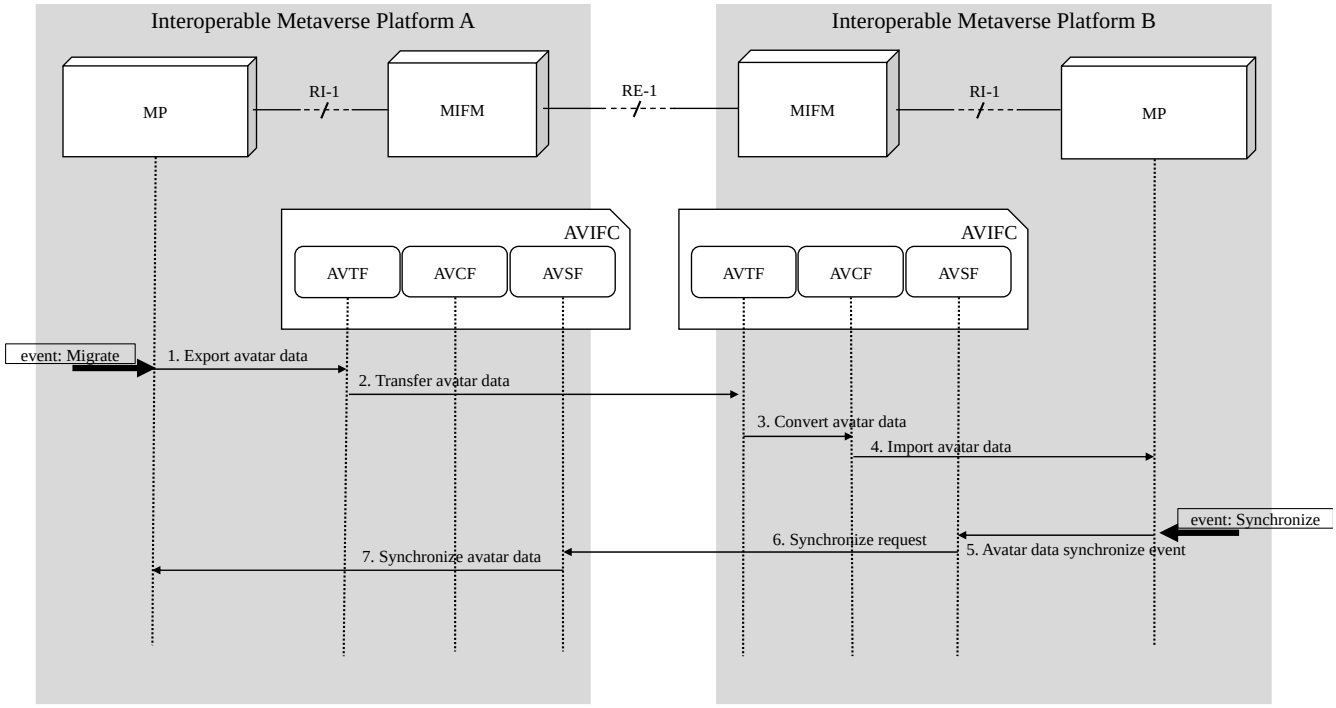


Figure 9-1 – High-level information flows for avatar migration

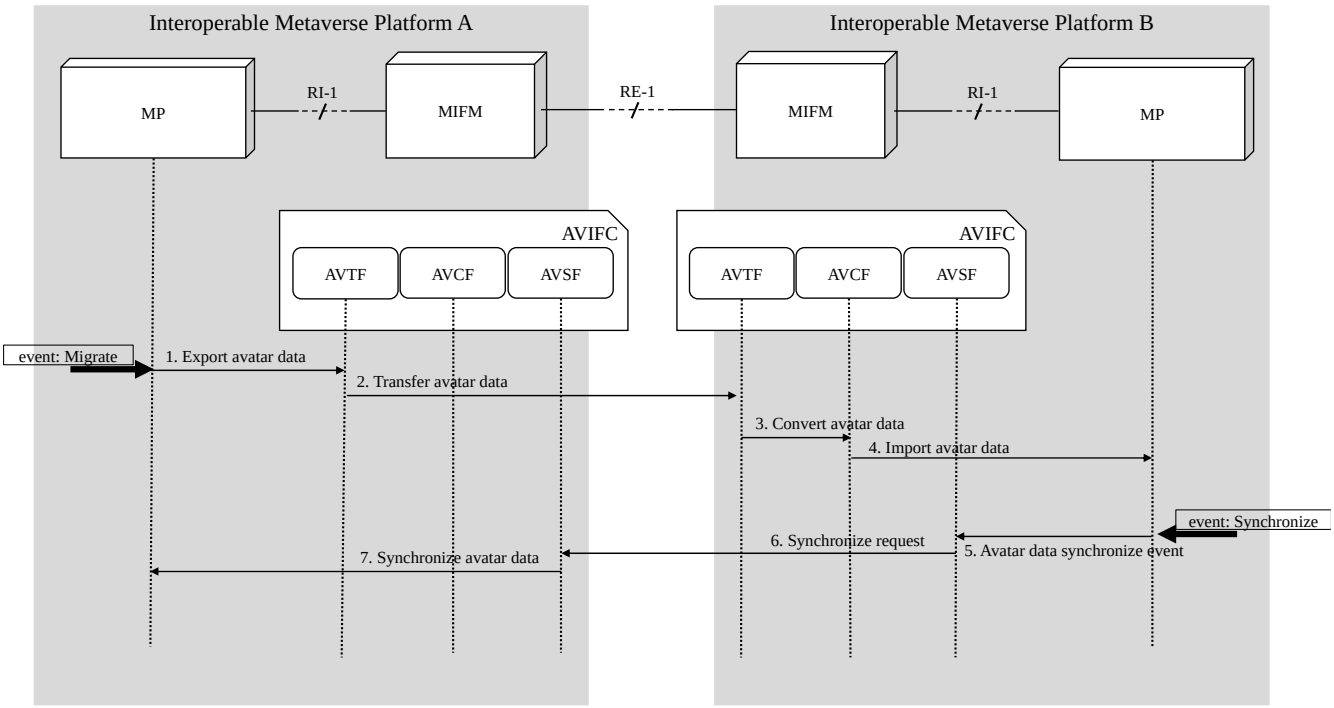


Figure 9-1 shows the information flows for the migration of an avatar across the metaverse platforms.

1. When an avatar goes to another metaverse platform B, the MP of platform A exports avatar data to the AVTF of MIFM.
2. AVTF interacts with AVTF of the corresponding MIFM of platform B.
3. AVCF converts the avatar data received from the AVTF of platform A if it needs to convert it to align the policy of the MP of platform B stored in the MPMF of IMFC.
4. MP of the platform B imports the avatar data from AVCF.
5. When it needs to synchronize the avatar data during the activities in the visiting metaverse platform B, MP of the visiting metaverse platform B requests to AVSF of MIFM to the originating metaverse platform A.
6. AVSF interacts with the AVSF of MIFM in the home metaverse platform A.
7. AVSF of MIFM in platform A sends a synchronization request to MP of the home metaverse platform A.

9.2 Asset migration

This clause describes high-level information flows to explain how each of the Functions interacts on the asset migration. It is assumed that both platforms have established channels through the procedures described in clause 9.5, and each MIFM is aware of the policy or digital currency of its relevant MP.

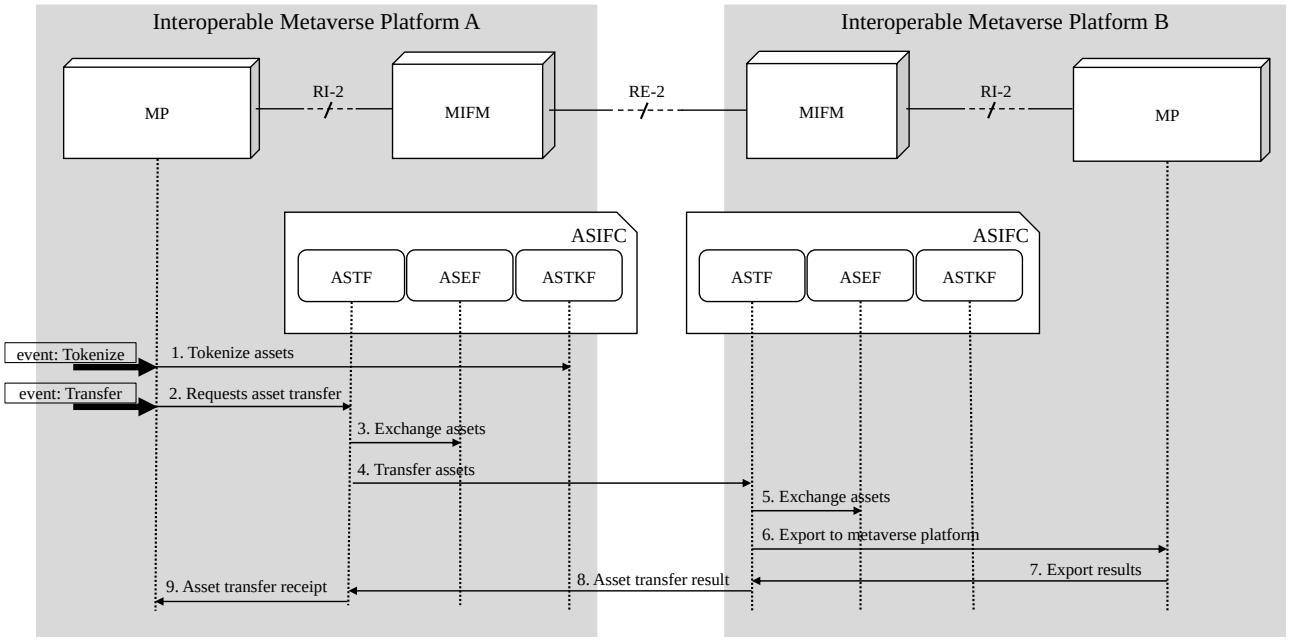


Figure 9-2 – High-level information flows for asset migration

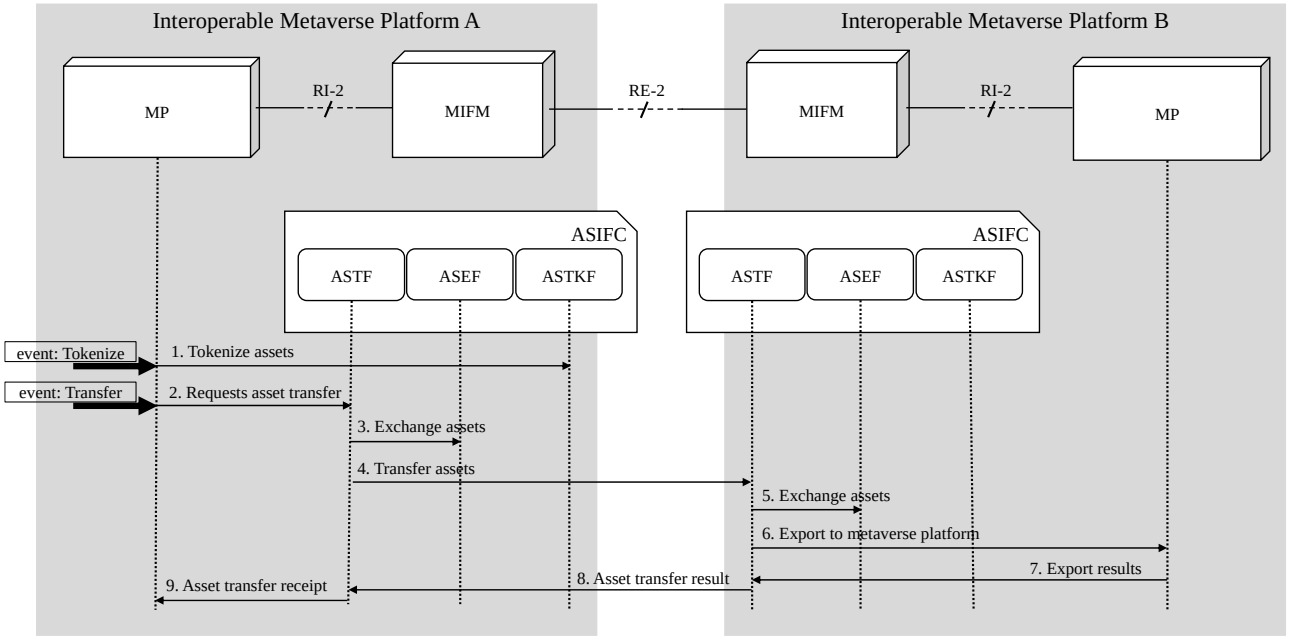


Figure **9-2** shows the information flows for the migration of an avatar across the metaverse platforms.

1. When MP wants to tokenize specific contents or assets to be accessible and usable across the multiple metaverse platform, it requests ASTKF to tokenize it.
2. When a user in platform A wants to transfer his/her own assets, such as NTF and digital currency, to another user in platform B, MP requests the ASTF to transfer it.
3. When transferring platform-dependent digital currency, the ASTF interacts with the ASEF to exchange the currency for global currency or currency of metaverse platform B.
4. The ASTF of platform A interacts with the ASTF of platform B to notify the transfer of the digital assets. The ASTF may use a blockchain to transfer the asset.
5. In the case of receiving global digital currency, the ASTF requests the ASEF to exchange it for the digital currency of the metaverse platform B if platform B uses its own platform-dependent currency. If platform A sends it with the currency of platform B, this step is omitted.
6. ASTF hands over the digital assets to MP of platform B.

7. MP of platform B responds to ASTF of MIFM in platform A with the result of export of the asset to the platform.
8. MIFM of platform B sends the result of the asset transfer to MIFM of platform A.
9. MIFM of platform A sends the receipt or result of the asset transfer to MP, and the MP will notify the result to the user.

NOTE 1 - Assetization turns items into digital assets for trade or investment, while tokenization specifically converts these assets into DLT tokens, offering secure and easily transferable ownership.

NOTE 2 - The timing for removal of transferred asset in the originating platform depends on the implementations and/or the attributes of the assets. It needs further study in other Recommendations in the future.

9.3 Content Migration

This clause describes high-level information flows to explain how each of the Functions interacts with each other for the content migration. It is assumed that both platforms have established channels through the procedures described in clause 9.5.

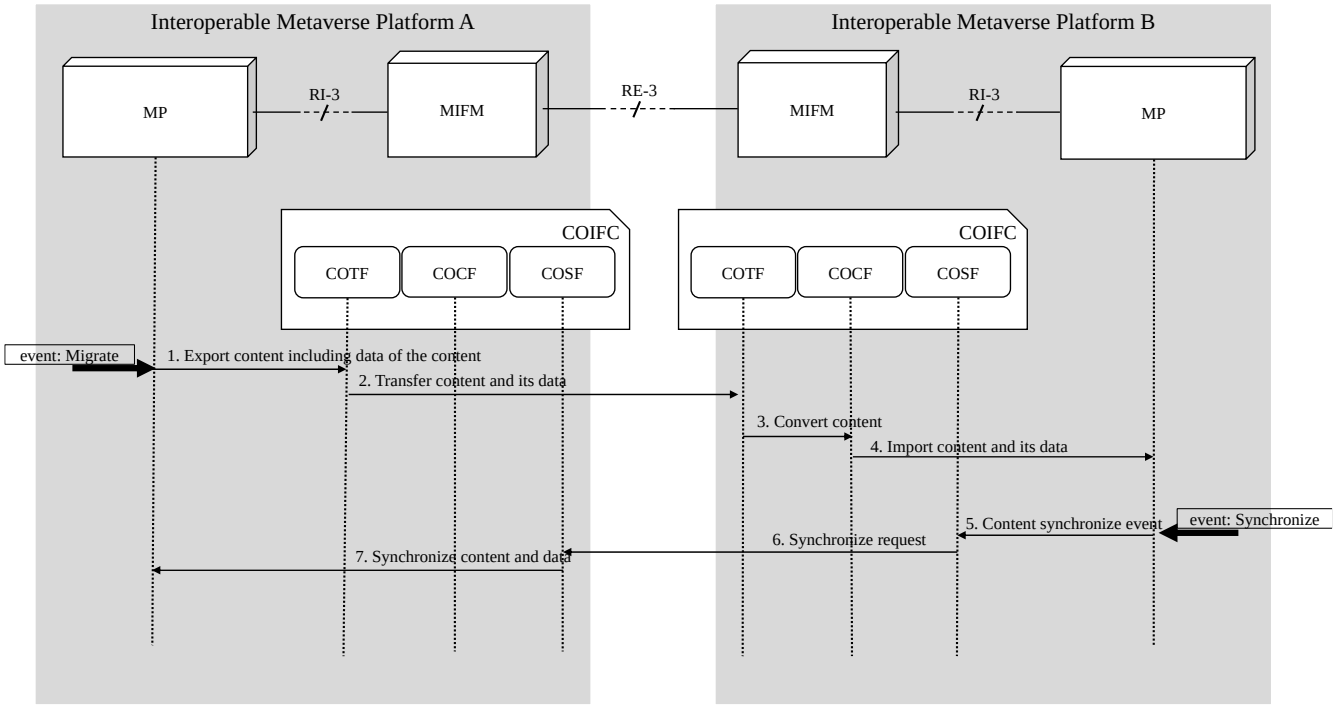


Figure 9-3 – High-level information flows for content migration

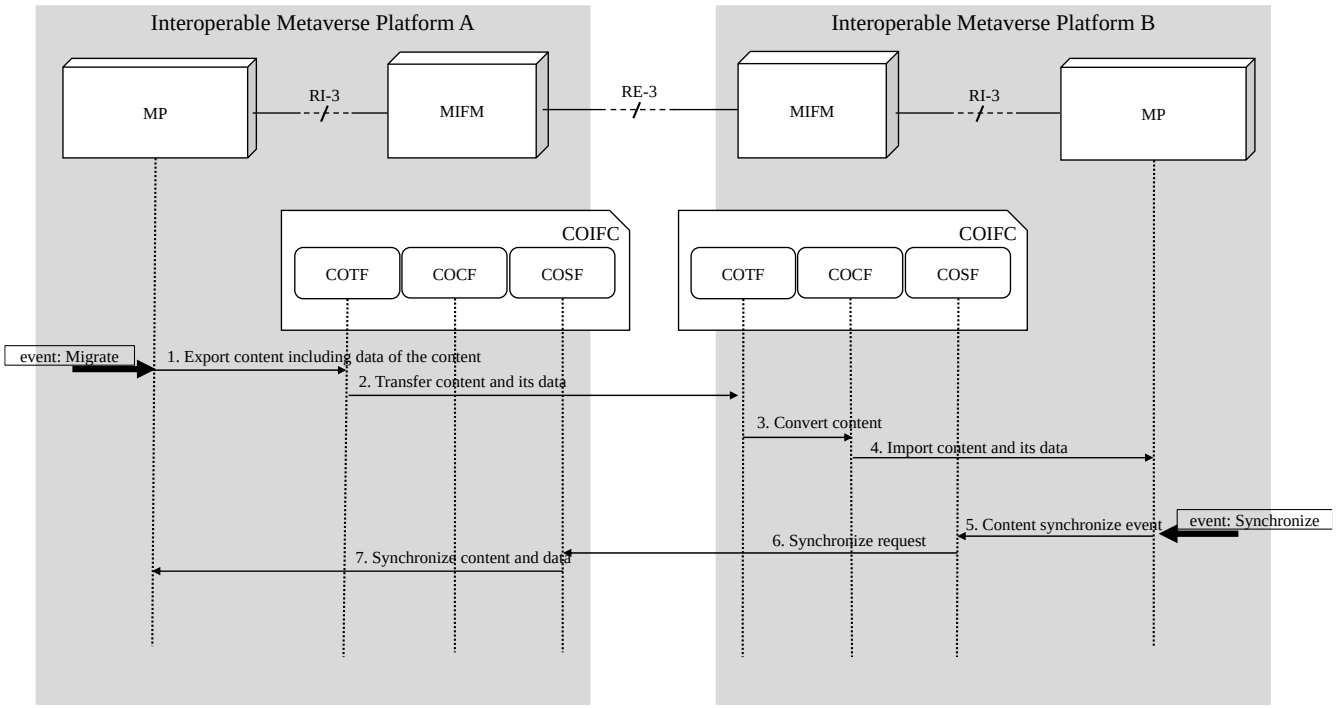


Figure **9-3** shows the information flows for the migration of content across the metaverse platforms.

1. When it needs to move specific contents to another metaverse platform B, MP of platform A exports the contents and relevant metadata to the COTF of MIFM.
2. The COTF interacts with the COTF of the corresponding MIFM of platform B to transfer the content.
3. The COTF of platform B requests the COCF to convert the content and its data received from the COTF of platform A if it needs to convert it to align with the policy of the MP of platform B. If there is no need to convert, the content will be passed to the MP directly.
4. MP of platform B imports the content and the data from the COCF or the COTF.
5. When it needs to synchronize the content and its data during the use in metaverse platform B, the MP of metaverse platform B requests the COSF of MIFM in metaverse platform A.
6. The COSF interacts with the ASF of MIFM in the home metaverse platform A.
7. The COSF of MIFM in platform B sends a synchronization request to MP in the metaverse platform A.

9.4 Identity Migration

This clause describes high-level information flows to explain how each of the Functions interacts with each other for identity migration. It is assumed that both platforms have established channels through the procedures described in clause 9.5.

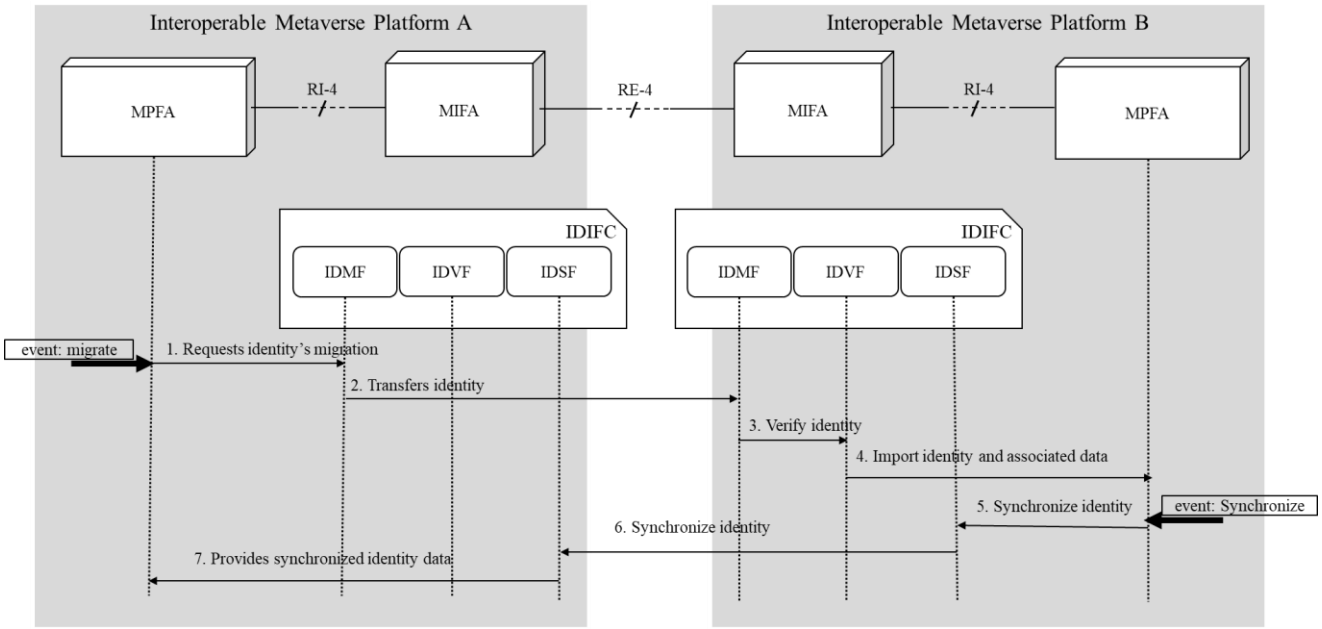


Figure 9-4 – High-level information flows for identity migration

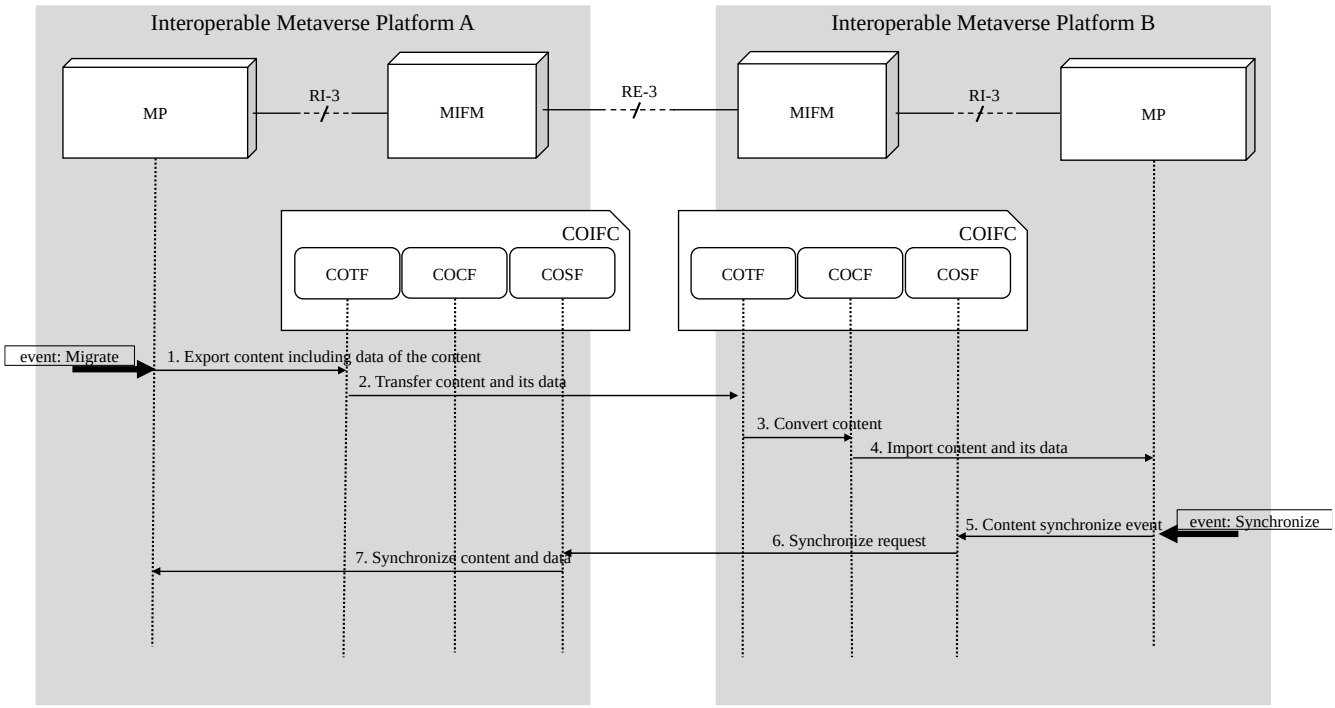


Figure **9-3** shows the information flows for the migration of an identity across the metaverse platforms.

1. When an identity is migrated from one metaverse platform A to another metaverse platform B, the MP on metaverse platform A sends the identity and associated data (e.g., users, avatars, crypto assets, permissions) to the IDMF in MIFM.
2. IDMF interacts with the IDMF of the corresponding MIFM of metaverse platform B. IDMF of the metaverse platform B forwards the identity data received from the IDMF of the metaverse platform A to the IDVF for verification.
3. IDVF verifies the identity data forwarded by the IDMF of IDIFC, utilizing various protocols and technologies such as cryptographic signatures, DIDs, and zero-knowledge proofs. Identity data is typically stored in a trustworthy shared storage (e.g., DLT system), which enables the exchange of identity data between metaverse platforms. See [FG-MV-42] for interactions to identify, authenticate, and authorize roamed entities between metaverse platforms.

4. MP of the platform B imports the identity data from IDVF.
5. When it needs to synchronize the identity data during the activities in the visiting metaverse platform B, MP of the visiting metaverse platform B requests to IDSF of MIFM to maintain consistency of user profiles, avatars, assets and permissions. IDSF also processes the detecting and resolving conflicts that may arise from simultaneous identity updates on the platform, ensuring the integrity of identity data is maintained.
6. IDSF interacts with the IDSF of MIFM in the home metaverse platform A.
7. IDSF of MIFM in platform A updates and synchronizes identity data. IDSF sends synchronized data to the MP of the home metaverse platform A to provide users with control over the migration of their identity data between platforms.

9.5 Metaverse platform registration for establishing an interoperable communication channel

This clause describes high-level information flows to explain how each of the relevant Functions interacts with the metaverse platforms to establish interoperable communication channels. Even though both interoperable metaverse platforms use the same protocol for interoperability, their capabilities may differ due to the extreme heterogeneity of metaverse implementations. For example, some platforms have enough computing power to convert various types of content, but others may not. Furthermore, the supported format of content will also differ depending on the platform's engine. This architecture provides a way to enhance the interoperability of the heterogeneous metaverse platforms. In the ideal case, it is possible to interoperate without any conversion if the whole metaverse uses one universal type of format, digital currency, and so on. For the time being, the metaverse bridge is the most predictable case of metaverse cross-platform interoperability

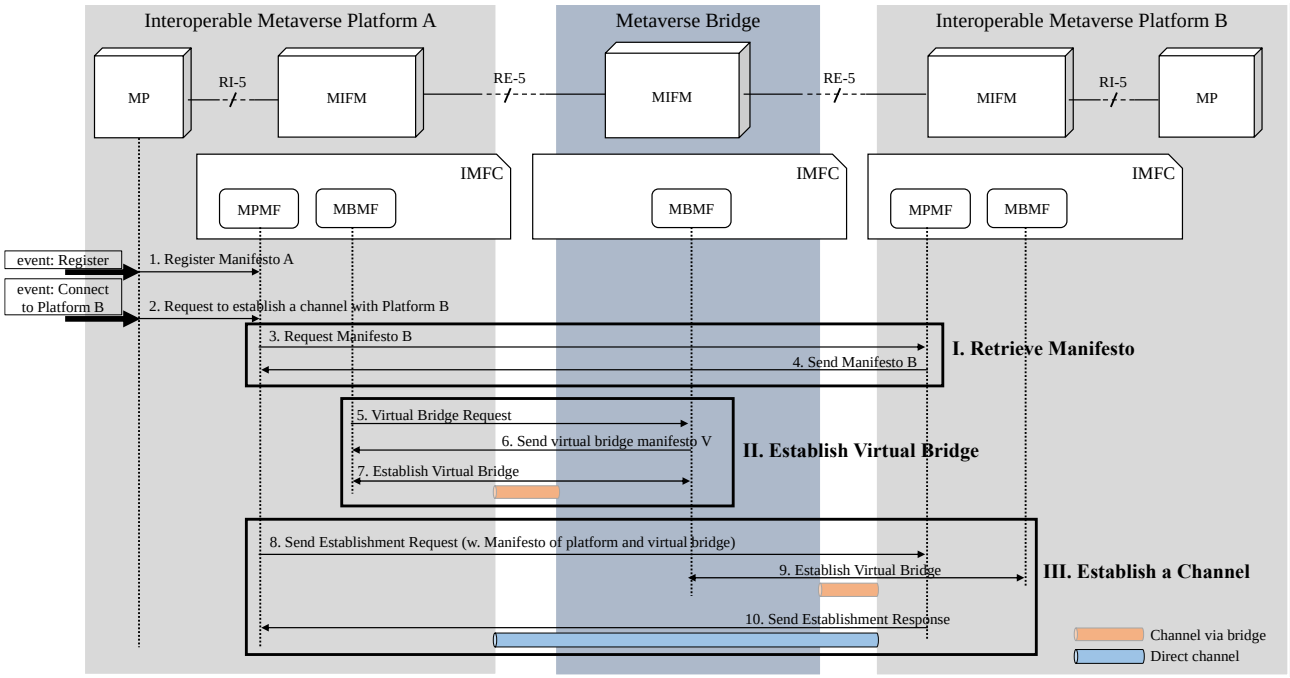


Figure 9-5 – High-level information flows for the registration of communication channels among metaverse platforms

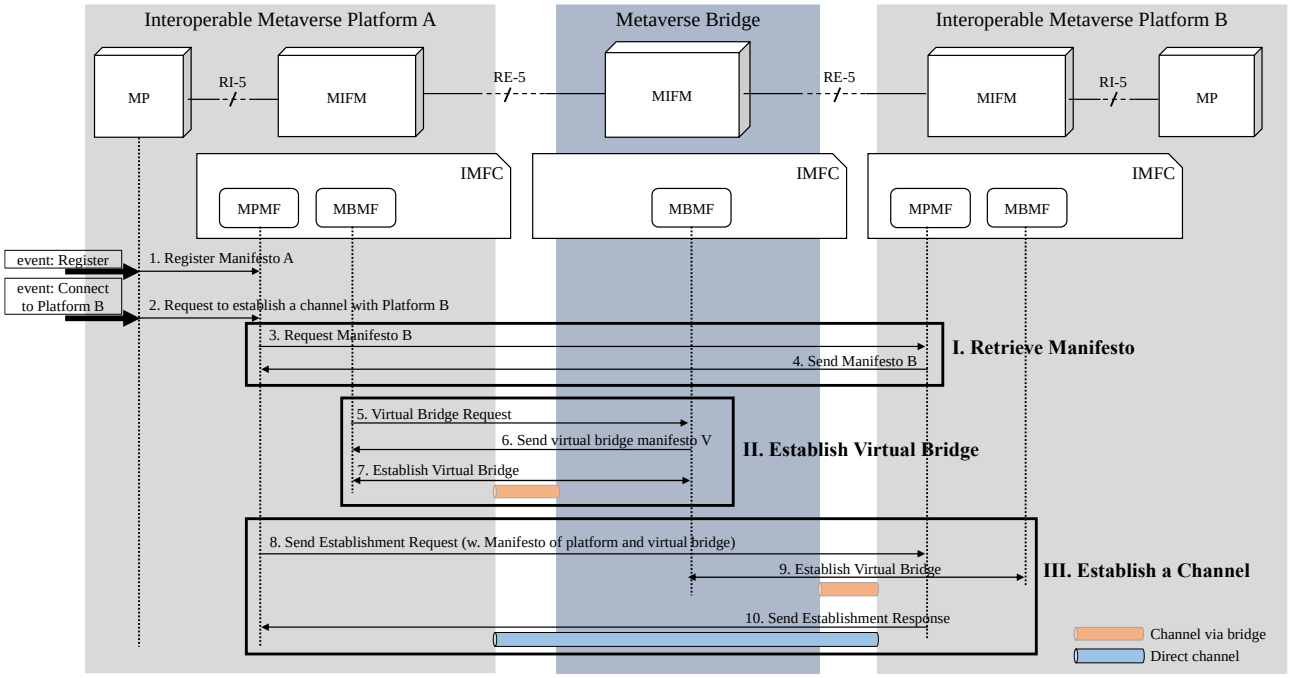


Figure **9-5** shows the information flows for the registration of a corresponding metaverse platform to establish the interoperable communication channels.

1. Each MP registers its manifesto data into its IMFC in MIFM, and the MPMF of MIFM keeps the registered manifesto data for further interactions with other metaverse platforms.
2. When MP initiates a procedure for establishing a channel with another metaverse platform *B*, it sends a request for the manifesto information of the metaverse platform *B* to the MPMF of the IMFC of MIFM.
3. The MPMF requests the manifesto of *B* to the MPMF of the corresponding metaverse platform *B*.
4. The MPMF of the corresponding MIFM sends its manifesto *B*.
5. The MIFM of the originating metaverse platform *A* checks interoperability by comparing the manifesto data of both platforms to identify, which features are directly interoperable and which are not. If it decides that it needs the metaverse bridge's support, it requests the metaverse bridge to establish a virtual bridge by sending the manifesto of both platforms except for directly interoperable features.
6. The MBMF of the metaverse bridge sends the manifesto *V* for the virtual bridge.
7. The MBMF of the originating MIFM *A* establishes a communication channel with the metaverse bridge.
8. The MPMF sends offer manifestos *A* and *V* that contain information of the originating platform and the virtual bridge. Manifesto *A* includes information that directly interoperates with platform B, while Manifesto *V* details information that passes through the metaverse bridge.
9. The MPMF of the corresponding metaverse platform *B* establishes a communication channel with the metaverse bridge.
10. MPMF of the corresponding metaverse platform *B* responds with the answer manifesto, which contains the information of the final negotiated manifesto.

NOTE 1 - If both platforms are completely interoperable on the protocols and capabilities, steps 5, 6, 7, and 9 will be skipped.

NOTE 2 - The bridge only prepares the resources as requested by platform A, and the metaverse platform B will connect to the bridge upon receiving the manifesto from platform A, as shown in steps 8 and 9.

Appendix I

Potential detailed requirements for the cross-platform metaverse

(This appendix does not form an integral part of this Recommendation.)

This appendix describes detailed requirements for metaverse cross-platform interoperability. The purpose of this appendix is to consider future detailed requirements for four types of interoperability aspects specified in [FGMV-19] and the necessary additional features for supporting them.

I.1 General platform interoperability requirements

This clause lists requirements regarding general platform interoperability as shown in Table I-1.

Table I- 1 Requirements related to general platform interoperability

Req.ID	Requirements
GPIR-001	It is recommended that metaverse platform provides interfaces to negotiate the capabilities of each platform.
GPIR-002	It is recommended that the metaverse bridge provides interfaces to support of interoperability among heterogeneous platforms.
GPIR-003	It is required that all inter-platform data transfers employ robust authentication mechanisms to ensure data integrity.
GPIR-004	It is recommended that all data transmitted between platforms be protected through end-to-end encryption.

I.2 Avatar interoperability requirements

Figure II-1 depicts the types of avatars in view of cross-platform interoperability. As defined in [FGMV-19], the home avatar is the original avatar managed by a user to represent the user's identity, and it can be customizable by the user within the original metaverse platform. The primary version of a user's digital representation in the metaverse resides exclusively within a specific metaverse platform or avatar service. When the home avatar moves to other metaverse platforms, it will become a roaming avatar, which is the avatar transitioning to visited metaverse platforms from the original metaverse platform, potentially undergoing alterations or transformations aligned with the destination platform's compatibility and features.

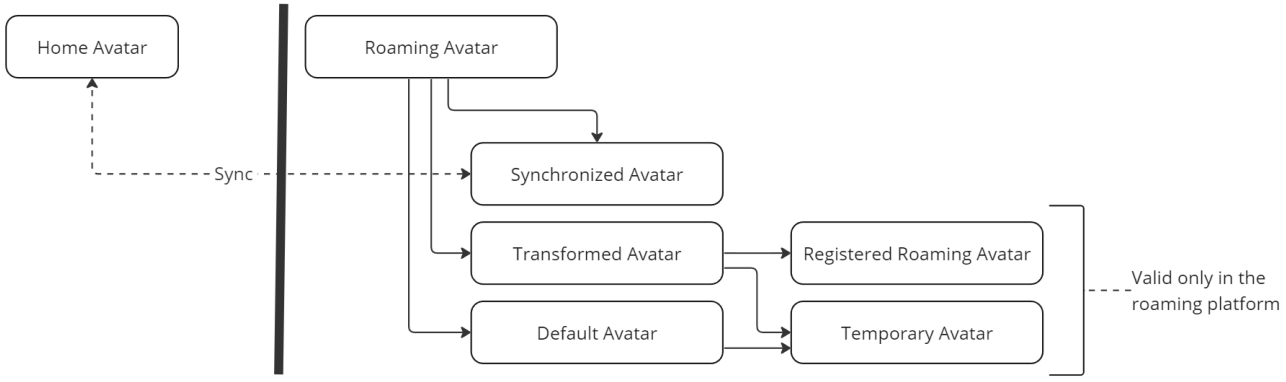


Figure I-1 – Types of avatars in view of cross-platform interoperability

The roaming avatar will take the following types:

– **Synchronized avatar:** the roaming avatar retains uniformity across metaverse platforms, mirroring the shape and attributes of the home avatar and seamlessly interchangeable among platforms. This avatar remains consistent across multiple environments through synchronization

protocols or standards, ensuring users encounter an unaltered representation regardless of the metaverse they explore

– **Transformed avatar:** the roaming avatar altered or adapted to fit into a specific metaverse platform. The changes might be due to compatibility issues or the unique requirements and characteristics of the target metaverse platform
– **Registered roaming avatar:** the roaming avatar that is registered on a metaverse platform after the user has visited it once. It may be a transformed avatar or a customized avatar that the user has created on that platform. It can be used again when the user revisits that platform
– **Temporary avatar:** the roaming avatar that is used temporarily when moving to a different metaverse platform. It may be a default avatar or a transformed avatar that does not have any connection to the user's home avatar. It may be discarded or replaced when the user leaves that platform
– **Default avatar:** the roaming avatar provided by a metaverse platform for users who have not customized their own or when their roaming avatar isn't compatible

The synchronized avatar is identical and synchronized with the home avatar. The transformed avatar is a modified version of the home avatar by the target platform. The default avatar is a basic avatar that is provided by the target platform and does not reflect the user’s identity. In the case of a transformed avatar, it is possible to register it to the target platform for reuse in the next visit. If it is not saved, it will be a temporary avatar that is volatile on leaving.

– **Avatar identity:** the identity of the avatar in a metaverse platform, which may be the same as (or bound to) the identity of its corresponding external entity.

Table I-2 Requirements related to avatar interoperability

Req.ID	Requirements
AVIR-001	The visited metaverse platforms are required to provide a default avatar for the case that the home avatar is not compatible with the roaming avatar in the visited metaverse platform.
AVIR-002	It is recommended to use the unified format, such as VRM format, for representing the avatar for exchanging the avatar model file across the metaverse platforms.

NOTE – Regarding the format for avatar, it needs further study since there are several candidates for avatar file format. However, it needs to specify default formats to guarantee cross-platform interoperability.

I.2.1 Avatar appearance

This clause lists requirements regarding avatar appearance, as shown in Table I-3. These requirements will be used to specify the protocol specifications regarding avatar migration and management.

Table I-3 Requirements related to avatar appearance

Req.ID	Requirements
AVIR-100	It is recommended to maintain the same avatar appearance across different metaverse platforms.
AVIR-101	It can optionally support the modification of the shape of avatars from other metaverse platforms, depending on the policy of the target metaverse.
AVIR-102	It can optionally discard or retain the changes to the avatar's appearance during the roaming depending on the policy of the target metaverse.

AVIR-103	It is required to be capable of recovering the previously used avatar's shape upon revisiting if the roaming metaverse platform maintains information about the roaming avatar.
AVIR-104	It is required to migrate the avatar's outfits and accessories when an avatar migrates to a different platform.
AVIR-105	It is recommended that the target metaverse platform provides a list of supported avatar features.
AVIR-106	It is recommended that the target metaverse platform provides the transformed avatar is generated based on the intersection of these features and the home avatar's features.
AVIR-107	It is recommended that the default avatar can be customized by the user within the constraints of the target metaverse platform.

I.2.2 Avatar migration and negotiation

This clause lists avatar migration and negotiation requirements, as shown in Table I-4. These requirements will be used to specify protocol specifications regarding migration procedures.

Table I-4 Requirements related to avatar migration and negotiation

Req.ID	Requirements
AVIR-201	It is recommended to proactively exchange constraints, such as the number of polygons in an avatar, considering the performance implications.
AVIR-202	It is required to deliver an error message with an explicit reason if a roaming avatar is not acceptable in the target metaverse.
AVIR-203	It is recommended that avatar migration is facilitated by a cross-platform API that integrates with multiple platforms.

I.2.3 Avatar synchronization

This clause lists avatar migration and negotiation requirements, as shown in Table I-5. These requirements will be used to specify protocol specifications regarding avatar synchronization procedures.

Table I-5 Requirements related to avatar synchronization

Req.ID	Requirements
AVIR-301	It is required to synchronize with the user’s home avatar whenever the user changes the appearance of the roaming avatar or swaps out accessories, outfits, etc., for platforms that support synchronized avatars.
AVIR-302	It is required to store and maintain the home avatar information, which includes avatar model, owner, metadata, etc., in a remotely accessible location. NOTE – The information can be stored in a home metaverse platform, avatar service platform, distributed user terminal, blockchain, etc.
AVIR-303	It is required that accessories and outfits be attached to the avatar when the avatar moves to another platform.
AVIR-304	It is recommended to comprise a database that stores the home avatar’s information for real-time synchronization across platforms.

I.2.4 Avatar delegation

This clause lists avatar delegation requirements as shown in Table I-6. These requirements will be used to specify protocol specifications regarding avatar delegation procedures.

Table I-6 Requirements related to avatar appearance

Req.ID	Requirements
AVIR-401	It can optionally delegate the behaviour of the avatar to a third party, such as an AI service provider, when the user is not online. NOTE – It is also possible to support the AI avatar by a specific metaverse platform.

I.3 Asset interoperability requirements

This clause lists asset interoperability requirements as shown in Table I-7. These requirements will be used for specifying protocol specifications regarding asset interoperability.

Table I-7 Requirements related to asset interoperability

Req.ID	Requirements
ASIR-001	It is required to ensure the portability of digital assets across platforms.

I.3.1 Asset management

This clause lists asset management requirements as shown in Table I-8. These requirements are used for developing a cross-platform digital asset management system for the metaverse, incorporating blockchain technology for secure transactions and ownership verification.

Table I-8 Requirements related to asset management

Req.ID	Requirements
ASIR-101	It is recommended to provide a way to buy, sell, exchange, rent, and lease digital assets from other metaverse platforms.
ASIR-102	It is required to enable users to set and manage the access rights and public scope of digital assets.
ASIR-103	It is recommended to integrate an API that allows real-time inquiry of digital asset transaction history and current ownership status that occurred in other metaverse platforms.
ASIR-104	It can optionally comprise a blockchain-based system for immutable recording and verifying asset history and ownership.
ASIR-105	It is recommended that users can view a comprehensive log of their asset transactions and history across the platforms.
ASIR-106	It is recommended that asset ownership is verified through multi-factor authentication before any change in ownership or status in a different platform.
ASIR-107	It is recommended that digital assets be identified and verified using distributed ledger technology such as blockchain

I.3.2 Asset migration

This clause lists asset migration requirements as shown in Table I-9. These requirements are used for developing a cross-platform digital asset management system for the metaverse, incorporating blockchain technology for secure transactions and ownership verification.

Table I-9 Requirements related to asset migration

Req.ID	Requirements
ASIR-201	It is recommended to make digital collections and accessories purchased with NFTs available to users on the platform they moved to.

I.3.3 Asset exchange

This clause lists asset exchange requirements as shown in Table I-10. These requirements are for creating a feature that enables seamless trading and cross-platform accessibility of digital assets within the metaverse ecosystem.

Table I-10 Requirements related to asset exchange

Req.ID	Requirements
ASIR-301	It is recommended for the exchange and trading of digital assets to be seamless across metaverse platforms.
ASIR-302	It is recommended that digital assets owned from other platforms should be available on the user's original metaverse platform.

I.4 Content interoperability requirements

This clause lists asset interoperability requirements that will be used for specifying protocol specifications regarding content interoperability.

I.4.1 Content management

This clause lists content management requirements as shown in Table I-11. These requirements are for developing a content discovery and management system among metaverse platforms, focusing on ease of access, clear ownership and comprehensive metadata for all forms of digital content.

Table I-11 Requirements related to content management

Req.ID	Requirements
COIR-101	It is recommended that a common interface be provided for users to easily find the content they are looking for, including images, video, digital assets, events, and services that exist in a metaverse.
COIR-102	It is recommended to provide relevant data (tags, descriptions, etc.) about the content to make it easier for users to find and understand the content.
COIR-103	It is recommended to provide clear and explicit information regarding ownership, copyright, and licensing of the content.
COIR-104	It is recommended that the system retains version histories of content, allowing creators to revert to previous versions, if necessary, after moving to a new platform.

COIR-105	It is recommended to offer a user-friendly interface for content discovery, complete with relevant metadata and clear information on ownership and licensing.
COIR-106	It is recommended that content metadata includes creator information, copyright, and usage rights.

I.4.2 Content format

This clause lists content format requirements as shown in Table I-12. These requirements are for creating a content portability and compatibility framework for user-generated or purchased digital content across various metaverse platforms.

Table I-12 Requirements related to content format

Req.ID	Requirements
COIR-201	It is recommended that user-generated or purchased digital content be portable and compatible, independent of the metaverse platform.
COIR-202	It is recommended to use a unified format, such as glTF 2.0, for representing the digital items for exchanging the 3D model file except for avatar across the metaverse platforms.
COIR-203	It is recommended for the content format to be compatible across different metaverse platforms and allow users to retain their avatars and items.
COIR-204	It is required that when moving or sharing content between different metaverse platforms, the format of the content is converted or moved with compatibility. NOTE - When a target metaverse platform doesn't support a specific content format, it's either converted, displayed alternatively, or disabled.
COIR-205	It is recommended to comprise a conversion tool that automatically adapts content to the specifications and constraints of the target metaverse platform.
COIR-206	It is recommended that content portability is facilitated through a standardized data format recognized across metaverse platforms.

NOTE – Regarding the format for digital items, it needs further study since there are several candidates for 3D model file format. However, it needs to specify default formats to guarantee cross-platform interoperability.

I.4.3 Content sharing and policy

The metaverse platform assigns an externally accessible identifier to the user's content that they want to share. This clause lists content sharing and policy as shown in Table I-13. These requirements will be used for specifying protocol specifications regarding migration procedures.

Table I-13 Requirements related to sharing and policy

Req.ID	Requirements
COIR-301	It is recommended to allow users to share their content with other platforms.
COIR-302	It is recommended that when moving content to other metaverse platforms, the permissions and access controls set by the user should also apply to other platforms.

I.5 Identity interoperability requirements

This clause lists identity interoperability requirements that will be used for specifying protocol specifications regarding identity interoperability. The deliverable [FGMV-42] includes the list of identity interoperability requirements for IoT devices.

I.5.1 identifier

This clause lists requirements regarding identifiers as shown in Table II-13.

NOTE 1 – The identifier usually points to a globally unique string of an object. Typically, an identity of an object includes one identifier and a group of associated data for identification and authentication of the object.

Table I-14– Requirements related to identifiers

Req.ID	Requirements
IDIR-101	It is required that all avatars have a distinguishable identifier to ensure uniqueness within the Metaverse. This identifier is globally unique when combined with a metaverse identifier for avatars across metaverse platforms. NOTE 2 – A user can have multiple avatars. The user may be able to select an avatar or multiple avatars for moving to the other metaverse depending on the policy of the metaverse platform.
IDIR-102	It is recommended that the assignment of the unique identifier is carried out using cryptographic techniques to ensure security and prevent tampering.
IDIR-103	It is required to provide globally unique user identifiers for consistent identification as users move to different metaverse platforms
IDIR-104	It is recommended that the unique identifier embeds metadata related to the avatar's creation date, originating platform, version information, etc.
IDIR-105	It is required to use a globally unique metaverse platform identifier on interacting with other metaverse platforms.
IDIR-106	It is recommended to use FQDN (Fully Qualified Domain Name) for the platform identifier to be routable and accessible using the identifier.
IDIR-107	It is recommended to use the URI scheme for the metaverse platform identifier. NOTE 3 – The scheme for metaverse platform needs further study
IDIR-108	It is required to use a globally unique metaverse identifier on each metaverse for cross-platform interoperability.
IDIR-109	It is required that digital items have a distinguishable identifier to ensure uniqueness within the metaverse. This identifier is globally unique when combined with a metaverse identifier for avatars across metaverse platforms.

I.5.2 Identity management

This clause lists requirements regarding identity management as shown in Table I-15. These requirements are aimed at developing a secure and transparent identity management system across platforms.

Table I-15– Requirements related to identity management

Req.ID	Requirements
IDIR-201	It is recommended to use blockchain technology to securely and transparently record creation, authentication, validation, and updating.
IDIR-202	It is recommended that the unique identifier is linked to a user's decentralized digital identity, ensuring both avatar and user authentication across the metaverse.
IDIR-203	It is recommended to comprise a centralized registry or database storing unique identifiers and their associated avatar data.

IDIR-204	It is required for users to be able to link or unlink their identity to other platforms. NOTE – If a user is linked to a metaverse platform, the platform can access the profile consented by the user.

I.5.3 Identity migration

This clause lists requirements regarding identity migration as shown in Table I-16. These requirements are for creating a cross-platform user verification system.

Table I-16 – Requirements related to identity migration

Req.ID	Requirements
IDIR-301	It is required to evaluate the reputation of users who want to move from other platforms to determine whether to allow the move.
IDIR-302	It is recommended to support a single sign-on (SSO) across platforms.
IDIR-303	It is recommended to be able to determine the eligibility for moving based on the criteria of the target metaverse, such as age and appearance, of users intending to transfer from other platforms.
IDIR-304	It can optionally check the reputation of the user belonging to another platform through the agreement between platforms.
IDIR-305	It is required that the reputation data is written in a standardized way for the compatibility of reputation evaluation between platforms.
IDIR-306	It is required for metaverse platforms to manage user access from other platforms based on the identity of the user. This identity can be received from other metaverse platforms or obtained in a variety of ways, including DID, blockchain, etc.

Appendix II

Mapping high-level requirements of FGMV-19 into Functions

(This appendix does not form an integral part of this Recommendation.)

Req.ID	Requirements	Functional Components	Functions
GENHR-001	It is recommended that metaverse platform is interoperable with other metaverse platform.	Interoperability Management Functional Component	Metaverse Platform Manage Functions
GENHR-002	It is recommended to be interoperable between metaverses on heterogeneous platforms.		Metaverse Bridge Manage Functions
GENHR-003	It is recommended to ensure secure and trust environment for exchanging information between metaverse platforms.		Metaverse Bridge Manage Functions
			Log and Audit Functions
AVIHR-001	It is recommended to enable avatars to migrate across different metaverse platforms while retaining their original characteristics.	Avatar Interoperability Functional Component	Avatar Convert Functions
AVIHR-002	It is required that each metaverse platform exchanges the constrains during the migration procedures for compliance and performance.		Avatar Convert Functions
AVIHR-003	It is recommended to synchronize attributes of avatar after experiencing by roaming avatar across metaverse platforms.		Avatar Synchronize Functions
AVIHR-004	It is recommended to ensure avatar's consistent representation across metaverse platforms.		Avatar Synchronize Functions
AVIHR-005	It is required to be accessible to the avatar-related data across the metaverse platforms.		Avatar Transfer Functions
ASIHR-101	It is recommended to ensure secure and trust environment for transforming digital assets between metaverse platforms.	Asset Interoperability Functional Component	Asset Transfer Functions
ASIHR-102	It is recommended to facilitate the seamless exchange, recognition, and use of digital assets across different metaverse platforms.		Asset Exchange Functions
			Asset Tokenize Functions
COIHR-101	It is required that content data including information for management, searchability, and interoperability, be able to transfer between metaverse platforms.	Content Interoperability Functional Component	Content Transfer Functions
COIHR-102	It is required to ensure content portability and format compatibility on moving or sharing content across metaverse platforms.		Content Convert Functions
			Content Synchronize Functions
COIHR-103	It is recommended to facilitate secure sharing of user content across metaverse platforms.		Content Synchronize Functions
IDIHR-101	It is recommended to use the same identity of digital entity in the home platform when digital entity moves to other metaverse platforms.	Identity Interoperability	Identity Migrate Function

IDIHR-102	It is required to follow the policy of identity usage of visiting metaverse platform when digital entity moves to other metaverse platforms.	Functional Component	Identity Migrate Function
IDIHR-103	It is recommended to support a variety of authentication methods for identity from visited metaverse platforms.		Identity Verify Function
IDIHR-104	It is recommended to support users to view and manage all identities of their digital entity when it moves to other metaverse platforms.		Identity Synchronize Function
IDIHR-105	It is recommended to support users to view and manage all avatars associated with their unique identities across the metaverse platforms.		Identity Verify Function
			Identity Synchronize Function

Appendix III

Use cases of the interoperability between metaverses with digital twins

(This appendix does not form an integral part of this Recommendation.)

III.1 Smart sustainable mobility

III.1.1 Description

Many cities are implementing metaverses with digital twins to facilitate urban planning, environmental management, traffic control, energy management and various other digital transformations by using IoT to collect and monitor urban data to support decision making and optimization through simulation. The Digital Twin Interoperability Functional Component (DTIFC) orchestrates the metaverses with digital twins of smart environment, smart driving, and smart transportation to develop a variety of applications that promote environment-friendly mobility.

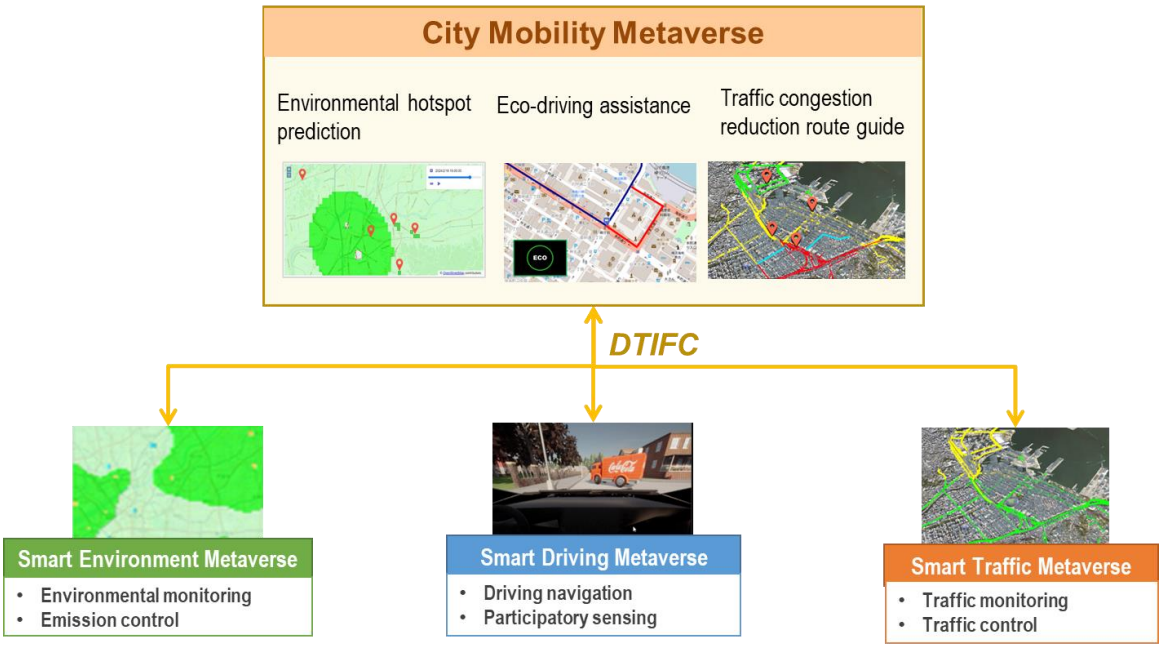


Figure III-1 – Overview of metaverse interoperability of smart sustainable mobility use case

III.1.2 Assumptions

This use case assumes the following metaverses with digital twins:

(a) Smart environment metaverse (SEMV)

- An environmental monitoring service provider monitors air pollution by collecting observation data from observation stations located at various locations, and if air pollution is expected to worsen, it seeks to improve the environment by restricting emissions at major sources.
- In the SEMV's digital twin, the observation network entity aggregates the observation data from the observation station entities. The air pollution prediction entity predicts air pollution by area based on the aggregated observation data. The emission simulation entity creates emission restriction plans for each source based on the air pollution prediction results.

(b) Smart driving metaverse (SDMV)

- A carrier or mobility-as-a-service (MaaS) provider monitors the driving conditions and driving environment of individual cars using in-vehicle sensors while guiding driving

operations and travel routes according to the conditions, thereby supporting safe and comfortable driving.
- The SDMV's digital twin consists of a car entity, environmental and driving sensor entities, and driving assistance device entities that guide driving operations and routes. The driving risk prediction entity predicts driving risks using data from the sensor entities. The driving simulation entity proposes driving operations and routes to avoid risks based on the results of driving risk prediction and instructs the driving assistance device entities.

(c) Smart transportation metaverse (STMV)
- An intelligent transportation system (ITS) operator uses closed-circuit television (CCTV) cameras and sensors installed around roads to monitor traffic flow and predict the occurrence of congestion. It also develops plans to control traffic flow to reduce congestion.
- The STMV's digital twin consists of the road network entity that make up the road entities and the vehicle entities recognized on each road. The traffic congestion prediction entity predicts traffic congestions based on the condition of vehicles on the road. The traffic simulation entity creates a traffic flow plan based on the results of the congestion prediction.

(d) City mobility metaverse (CMMV)
- Government staff monitor and simulate urban environments and activities through the city mobility metaverse, which reproduces real urban spaces in virtual space.
- In the CMMV's digital twin, various applications are developed that realize the smart sustainable mobility by orchestrating the domain-specific metaverses through DTIFC.

III.1.3 Scenario and operation flows

III.1.3.1 Environmental hotspot prediction

Environment bureau staff enable detailed environmental monitoring and emission restrictions through environmental hotspot prediction that predicts the environmental quality of high-traffic areas with a high degree of accuracy using environmental sensors attached to the vehiclesin addition to fixed observation stations. For environmental hotspot prediction, not only the observation stations of the SEMV's digital twin but also the environmental sensor attached to the car of the SDMV's digital twin is considered as a mobile observation station and incorporated into the observation network to perform air pollution prediction.

(1) Sensor data in the SDMV's digital twin containing privacy information, such as car trajectories, cannot be accessed externally. Therefore, the DTIFC conducts federated learning between SEMV and SDMV, where the SEMV transfers the air pollution prediction entity to SDMV, SDMV updates it using the locally collected sensor data, and SEMV aggregates the updated entity to refine the original entity.
(2) The DTIFC translates the location information and environmental sensor data of the SDMV's digital twin to the observation data of the SEMV's observation station entity during the step (1). This will allow the sensor data collected by the SDMV to be input into the air pollution prediction entity of the SEMV.
(3) The CMMV subscribes to the emission restriction plan that is created and published by the emission simulation entity in the SEMV's digital twin through the DTIFC.

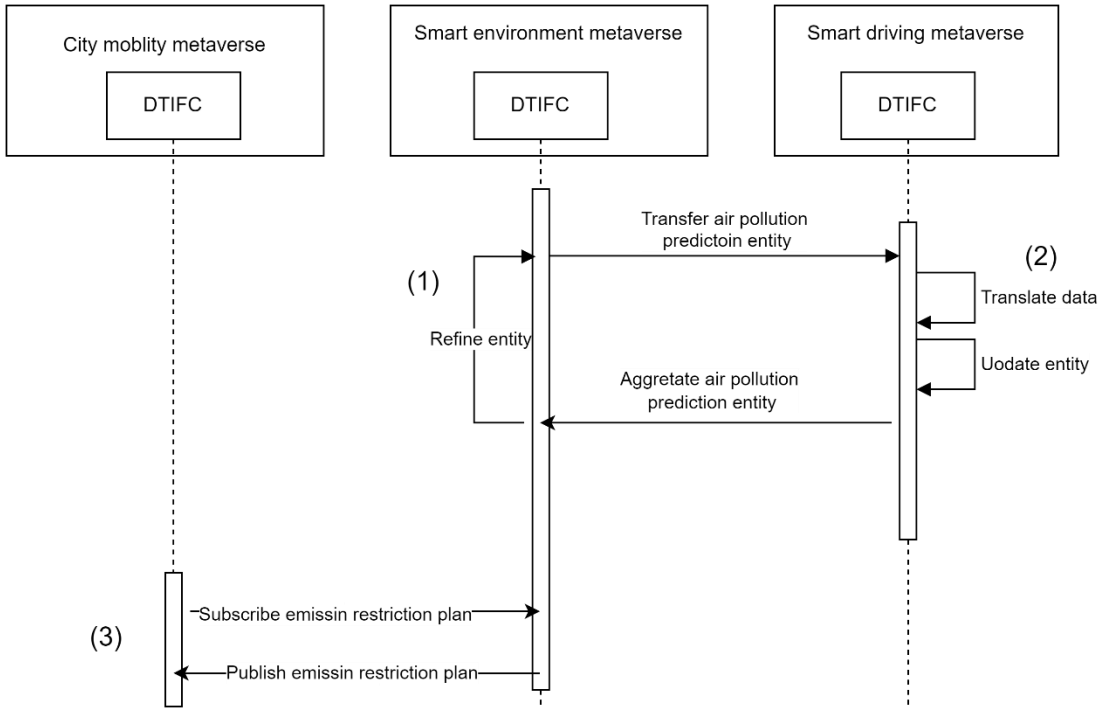


Figure III-2 – Operation flow for environmental hotspot prediction.

III.1.3.2 Eco-driving assistance

Environment bureau staff determines emission restriction plans to recommend environment-friendly driving operations to drivers in areas with poor environmental quality for improving the city's overall environment quality through eco-driving. In the eco-driving assistance, based on the emission restriction plan from the emission simulation of the SEMV's digital twin, emission restriction information is also distributed to cars driving in air pollution areas. In response, the SDMV's digital twin performs a driving simulation with the emission restriction added to the car's environmental data and instructs the driving assistance device entities to perform driving operations to control emissions. Furthermore, when combined with the environmental hotspot prediction, which enhances the air pollution prediction of the SEMV's digital twin using environmental data from cars, more detailed emission simulation becomes possible, and the effectiveness of eco-driving assistance based on emission restriction plans can be enhanced.

(1) As with the environmental hotspot prediction, the DTIFC handles federation between the SEMV and SDMV to conduct federated learning of the air pollution prediction entity of the SEMV with using the sensor data of the SDMV.

(2) As with the environmental hotspot prediction, the DTIFC transforms data from the SDMV to the SEMV to input the sensor data collected by the car entity of SDMV into the air pollution prediction entity of SEMV during the step (1).

(3) The CMMV subscribes to the emission restriction plan that is created and published by the emission simulation entity of SEMV. The CMMV determines the emission restriction for cars driving in the area of interest from the emission restriction plan and publishes it to the SDMV that subscribes to it.

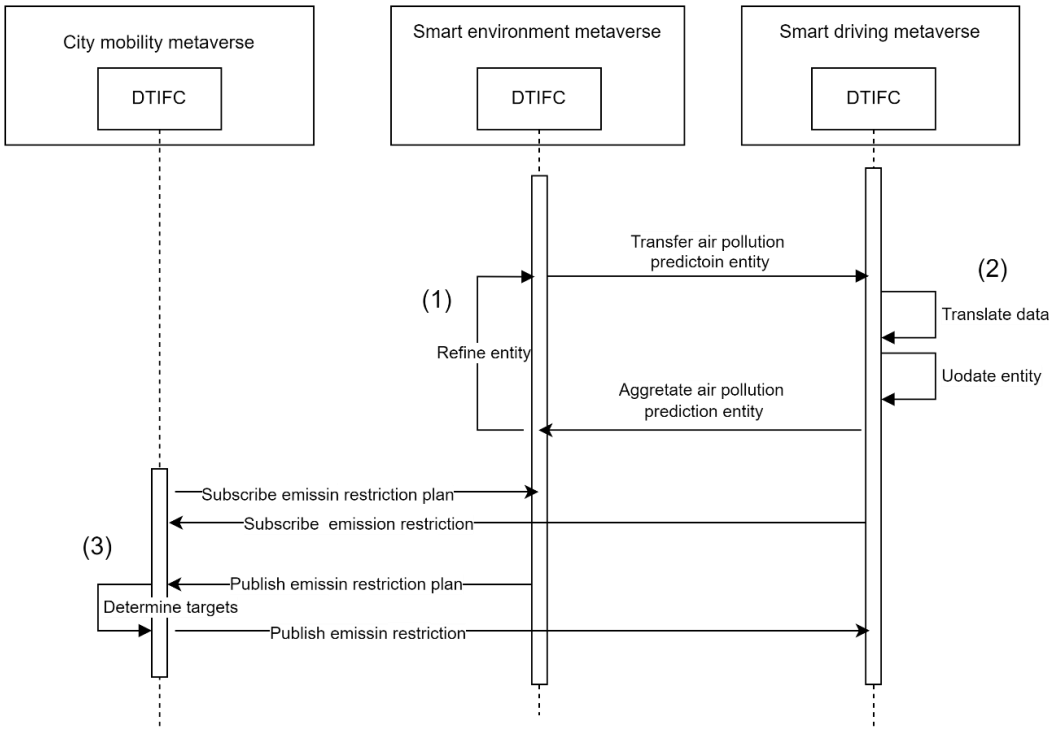


Figure III-3 – Operation flow for eco-driving support.

III.1.3.3 Traffic congestion reduction route guidance

Transportation bureau staff can prevent serious traffic congestion by recommending routes and congestion pricing that disperse traffic flow so that vehicles are not concentrated on specific roads. For congestion reduction route guidance, the application synchronizes a vehicle on a road in the STMV's digital twin with the car entity in the SDMV's digital twin in order to send the recommended route to the vehicle near the congestion reduction route. In addition, based on the traffic flow plan created by the traffic simulation of the STMV's digital twin, the recommended route and congestion pricing information is sent to the SDMV traveling on the road targeted for congestion reduction. Upon receiving this information, the SDMV uses the driving simulation entity to search for a route and directs the route to the driving assistance device entities.

(1) The DTIFC synchronizes the vehicle entity recognized by the road entity in the STMV and the car entity in the SDMV. Since vehicles on the road change from time to time, the vehicle license plate number recognized by the road entity and the license plate number of the car entity should be identical for synchronization.

(2) The CMMV subscribes to the traffic flow plan that is created and published by the traffic simulation entity of the STMV through the DTIFC. The CMMV determines from the traffic flow plan the recommended route for the vehicle on the target road, and then publishes it to the subscribing SDMV through the DTIFC. In doing so, the DTIFC identifies the SDMV of the car that has been synchronized with the target vehicle as the receiver.

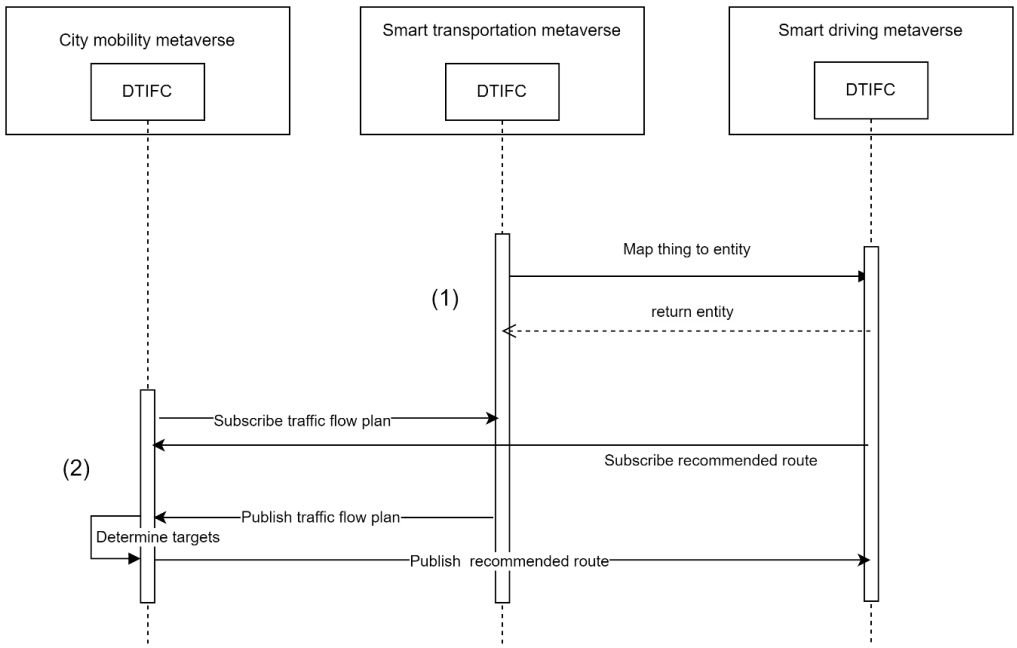


Figure III-4 Operation flow for traffic congestion reduction route guidance.

III.2 Cyber physical security

III.2.1 Description

According to the discussions so far, the classification of the metaverse includes metaverse with digital twins and metaverse with IoT devices. To interoperate these metaverses securely, it is important to ensure the security of the underlying IoT devices and cyber-physical systems, as well as the cybersecurity of the metaverse stated in [ITU FGMV-10]. Since IoT devices and cyber-physical systems integrate the cyber and physical spaces, security measures should not be limited to cyberspace or individual systems but need to consider the impact on the physical space surrounding the systems. As shown in Figure III-5, when network-connected devices are subjected to cyberattacks, it affects the surrounding physical entities, which in turn also impacts the metaverse with digital twin or IoT devices. The interoperability of digital twins is effective when evaluating the impact of cyberattacks on the physical space.

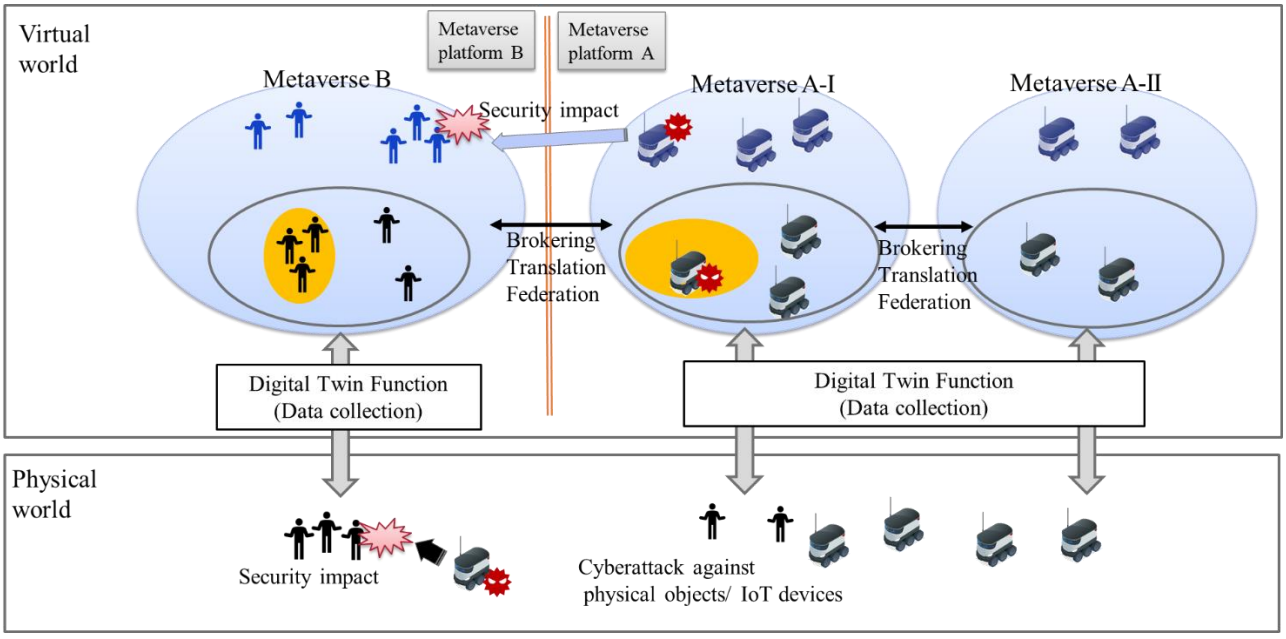


Figure III-5 – Cyberattack impact on metaverse with digital twin or IoT

III.2.2 Assumptions

This use case assumes the following context:

The physical impact of a cyberattack on a metaverse with a digital twin varies depending on the system under attack. The physical impact also causes damage to the surroundings of the system, but the degree of the damage varies depending on the affected target and situation. At this time, by controlling the metaverse with the digital twin, it is possible to simulate the impact of a cyberattack on the physical space. Furthermore, if the affected target can also be represented by the digital twin, the degree of the damage can be estimated.

Therefore, by coordinating the digital twin of the metaverse that is physically affected by a cyberattack and the digital twin that includes the target that is physically affected, it is possible to evaluate what kind of physical damage an attack on a metaverse would cause based on the surrounding circumstances.

III.2.3 Scenario and operation flows

This clause describes an application example of the DTIFC for realizing the novel cyber-physical security by ensuring interoperability among multiple digital twins that underlie the metaverse with the digital twins.

As shown in Figure III-6, digital twin interoperability functions are used for the security of the cyber-physical system that underlies the metaverse with digital twins or IoT.

(1) The DTIFC federates data obtained from various digital twins to generate and refine physical impact estimation entity. The DTIFC transfers the physical impact estimation entity from one metaverse with digital twin A-I to A-II. By aggregating the physical impact estimation entity created in other digital twins, the entire estimation entity is refined.

(2) Another kind of metaverse with digital twin B subscribes to security information from metaverse with digital twin A. When evaluating how the physical impact of an attack is estimated by one digital twin on a device controlled by another digital twin, different combinations of digital twins require different information. The DTIFC allows digital twins to select and share the necessary information for evaluation for each digital twin combination. In this process, since each digital twin has different criteria for information and different granularity of information, it is necessary to translate the information by using the DTIFC. As the result, the digital twins of multiple metaverses can estimate the impact of cyberattacks, share the estimation result, and support the countermeasure for cyberattacks on the metaverse.

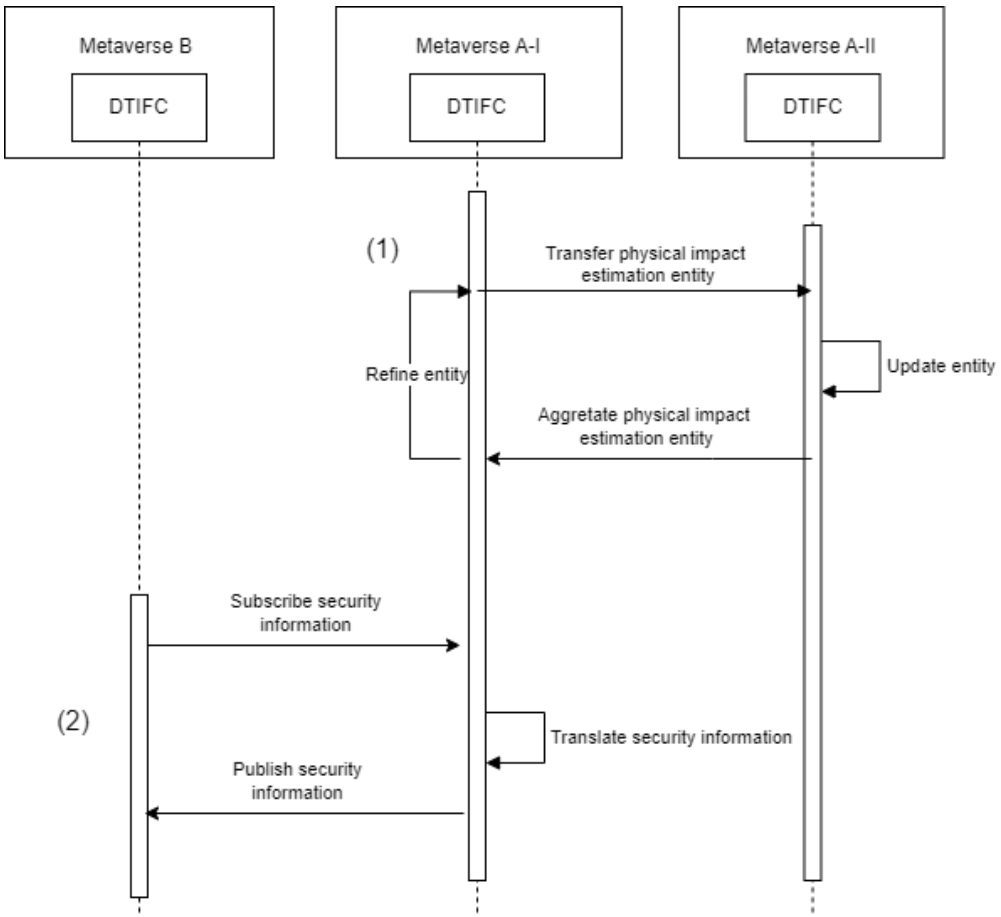


Figure III-6 Operation flow for cyber-physical security

Bibliography

[b-ITU FGMV-33] Technical Specification ITU FGMV-33, *Glossary for metaverse*. (2024)