Metaverse Standards Forum
Metaverse Universal Manifest (MUM)

Last Update: September 07, 2025

Status: Approved for Public Distribution

Version: 1.0

Reviewer	Due Date	Status	Contact
Digital Asset Management Working Group	July 17, 2025	Complete	digital_asset_management @lists.metaverse-standards.org
MSF Domains (Peer Review)	August 28, 2025	Complete	oversight@lists.metaverse-standards.org
Use Case Taskforce	September 07, 2025	Complete	use_case_task_force@lists.metaverse-standards.org

The purpose of this template is to provide a structured framework for collecting and documenting use cases within the Metaverse Standards Forum (MSF). Use cases are essential for understanding real-world scenarios where metaverse technologies are applied and where interoperability challenges may arise. This template guides MSF members in providing a concise yet comprehensive description of a use case, including its title, identifier, and summary. It also encourages contributors to list the benefits of the use case, identify actors or entities involved, and describe the use case scenario in detail, emphasizing interactions, challenges, and requirements. Additionally, it prompts the inclusion of relevant technical information, such as implementations, success metrics, and challenges faced. This template aims to facilitate the gathering of valuable use-case data to inform standards development and foster collaboration within the MSF community.

MSF members and MSF Domain Groups are invited to submit use cases.

NOTE: Organizations such SDOs who want to submit and add a use case would need a sponsor that is an MSF member. This process is established in order to have a contact person in MSF that can handle discussions and resolve open issues within regular meetings.

Eligible submitters:

- MSF Domain Groups
- MSF Members (Principal and Participant)
- External Organizations with Liaison Agreements (with the support of a MSF member that acts as sponsor)
- Standard Development Organizations (with the support of a MSF member that acts as

sponsor)

Minimum Requirements for MSF Member Submissions not part of a Domain Group:

- Minimum required number of proposers: 3
- Minimum required number of supporters: 5

NOTE: Use cases submitted by SDOs and Liaison Organizations would also need to fulfill the same requirements (and would need a sponsor) unless they are submitted by a Domain Group.

MSF: *Metaverse Standards Forum*
POG: *Pre-qualified Organizations and Groups*
SPP: *Standards Related Publications and Projects*
DWG: *Domain Working Groups*
WG: *Working Group*
SDO: *Standards Development Organization*

Use Case Title

Metaverse Universal Manifest (MUM)

Use Case Identifier

MSF2025-MUM-001

- Version 1.0
- Year of Release: 2025

Summary of Use Case

Description: The Metaverse Universal Manifest is a comprehensive, Standardized Metadata document designed to enable seamless interoperability and portability across diverse Metaverse Platforms. It serves as an extensible reference file containing links and metadata about a user's Digital Identity (DIDs, verifiable credentials), Digital Assets (NFTs, avatars, wallet data), social connections, personal preferences, and external service integrations. By leveraging decentralized technologies and user-controlled storage, the manifest facilitates Frictionless Transitions, Persistent Identities, and Consistent User Experiences across multiple Metaverse Environments.

Benefits:

- Seamless cross-platform interoperability
- Enhanced user control and privacy
- Simplified onboarding and transition between platforms
- Unified digital identity and asset portability
- Reduced redundancy and friction in identity and asset management
- Improved consistency in user experience
- Reduced friction in XR environments through pre-configured preferences

- Consistent language experience across all platform interactions
- Simplified purchasing with automatic currency conversion
- Streamlined authentication with context-appropriate security
- Unified digital wallet for loyalty and discount programs

Contributors and Supporters

- Digital Asset Management Working Group
- MSF Domains (Peer Review)
- Use Case Taskforce

Keywords

Universal Manifest, Interoperability, Metadata Standard, Decentralized Identity (DID), Verifiable Credentials (VCs), Blockchain, NFT (Non-Fungible Tokens), Digital Assets, Avatar Portability, User Privacy, Social Graph Portability, Consent Management, Cross-Platform, JSON-LD, IPFS, Zero-Knowledge Proofs (ZKPs), Language Localization, Currency Conversion, Voice Consent, Context-Aware Security, Digital Loyalty Cards, XR Input Optimization

Actors/Entities

- **End Users:** Individuals engaging across multiple metaverse environments, transporting their digital identities, assets, preferences, and social connections.
- **Metaverse Platforms:** Virtual worlds, social VR/AR spaces, gaming platforms, education-focused metaverses, and enterprise metaverse solutions adopting the Universal Manifest.
- **Identity Providers (IDPs):** Providers managing decentralized identifiers (DIDs), issuing and verifying verifiable credentials (VCs).
- **Wallet Providers:** Cryptocurrency and digital asset wallets including Fiat and crypto payment gateways (e.g., Apple Pay, Stripe, Ethereum wallets, Solana wallets) integrated within the Universal Manifest for secure, cross-platform transactions.
- **External Service Providers:** Third-party service integrations, including streaming platforms, productivity tools, fitness trackers, education providers, entertainment services, and health data services referenced via the manifest.
- **Regulatory and Compliance Authorities:** Organizations responsible for validating compliance-related credentials (e.g., KYC, AML compliance) and enforcing data protection and privacy standards across platforms.
- **Blockchain Infrastructure Providers**: Platforms (Ethereum, Polygon, XRPL, Immutable X, Solana) that offer the foundational blockchain technology enabling decentralized identity, NFT asset portability, and transaction security.
- **Interoperability Middleware Providers:** Service providers offering tools or infrastructure to facilitate asset translation, identity mapping, and metadata portability between platforms.

- **Creators**: Entities creating and distributing NFT-based or other assets (avatars, wearables, virtual property) that interact with the manifest to ensure cross-platform provenance, ownership verification, and metadata consistency.
- **Seller**: Entities selling assets that interact with the manifest to ensure currency choices and other options are used where possible.
- **Avatar Creation & Customization Services**: Providers such as Ready Player Me, MetaHuman, Decentraland, Spatial, Meta Avatars, VRChat, The Sandbox, and Roblox, ensuring consistent avatar appearance, interoperability, and behavior across platforms.
- **Data Controllers & Storage Providers:** Entities responsible for securely storing and managing user manifest data (IPFS, blockchain-based storage providers, decentralized file systems).
- **Digital Rights Management (DRM) Providers:** Organizations ensuring intellectual property rights, provenance, and usage terms are enforced consistently across platforms through metadata referencing.
- **Social Graph & Community Management Services:** Platforms and protocols (e.g., Lens Protocol, BrightID) that maintain portable user social connections and community memberships within the manifest.
- **Privacy and Security Providers:** Technology vendors providing end-to-end encryption, Zero-Knowledge Proof (ZKP) protocols, and secure credential issuance and verification solutions.
- **Cybersecurity Entities:** Organizations monitoring threats, maintaining cybersecurity frameworks, and advising or ensuring the security of implementations.

Detailed Description of Use Case/Scenario

Preconditions:

- **Secure Storage:** Users maintain an authenticated Universal Manifest securely stored in decentralized repositories.
- **Standards Compliance:** Participating platforms comply with and implement the Universal Manifest standards.
- **User Onboarding:** User onboarding onto a new metaverse platform.
- **Privacy Changes:** User performance of changes to their privacy settings.
- **Cross-Platform Activity**: Initiation of a cross-platform activity such as execution of transactions or the undertaking of compliance checks.
- **Data Integration:** User migration or synchronization of their social network and reputation data.

Main Flow:

- **Scenario 1:** Cross-Platform Identity and Asset Management:
  - **Authentication:** A user logs in to a new platform using DID-based authentication.
  - **Consent:** The user explicitly grants permission for the platform to access and share their metadata. The platform records this user consent for tracking purposes.
  - **Data Retrieval:** The platform retrieves metadata (avatars, preferences, wallet pointers) from the **Universal Manifest**.
  - **Automatic Configuration:** The platform automatically configures the user's avatar, assets, and personalized settings, allowing for a seamless entry.
- **Scenario 2:** Unified Privacy and Consent Control

  - **Adjustment:** A user adjusts their privacy preferences within their Universal Manifest.
  - **Synchronization:** The changes automatically synchronize across all connected metaverse platforms and services.
  - **Permission Update:** Platforms and services instantly update their access permissions, ensuring adherence to user privacy choices.
- **Scenario 3:** Secure and Compliant Transactions
  - **Initiation:** A user initiates a transaction that requires identity and compliance verification.
  - **Credential Supply:** The Universal Manifest supplies verifiable credentials that confirm the user's identity and compliance.
  - **Streamlined Process:** The transaction proceeds without any additional or redundant verification processes.
- **Scenario 4:** Persistent Social Graph and Reputation
  - **Platform Join:** A user joins a new metaverse platform.
  - **Data Import:** The universal Manifest enables the platform to import the user's social connections and existing reputation data.
  - **Integration:** The platform integrates the imported data and suggests contacts, which enhances social connectivity and continuity for the user.
- **Scenario 5:** User Preference and Consent Management
  - **Language Preferences:** The user sets their default language for chatbot conversations across platforms, digital signage in stores, exhibitions, and virtual spaces, and real-time human-to-human conversation translation services.
  - **Financial Preferences:** The user sets their default currency for automatic conversion in a seller's store and also specifies preferred payment methods linked to specific contexts.
  - **Logistics Preferences:** The user sets a default delivery address for virtual and physical goods and alternative addresses for different contexts (work, home, gift delivery), with preference settings designed to minimize typing in XR environments.
  - **Consent Management:** The user manages granular consent for voice recording in multiplayer environments and for microphone access. They can set specific permissions for activities like AI-powered chatbot interactions, voice-activated commands and features, real-time translation services, and the **recording or transmission** of their voice for various other activities. The user also controls data sharing on a per-platform/experience basis, including specific consent controls for voice and audio interactions.
  - **Security and Credentials:** The user can define context-specific identification methods (e.g., biometrics, PINs, MFA) and store various digital credentials like loyalty cards, membership credentials, and professional certifications.
  - **Security Configuration:** The user defines context-specific identification methods, such as biometric authentication for secure areas, a simple PIN for casual experiences, and multi-factor authentication for workplace environments, with different security levels applying per store, experience, or area.
  - **Digital Credentials:** The user can store and manage their virtual store loyalty cards, discount cards, promotional codes, membership credentials, and professional certifications relevant to specific environments.

Alternative Flow

- **Consent Withdrawal:** The user withdraws consent for specific platforms, and the Universal Manifest promptly communicates these changes.
- **Partial Data Requests:** Platforms can selectively request metadata, and users manage these requests through fine-grained permissions within the Universal Manifest.
- **Non-Compatible Platforms:** Users must manually onboard onto platforms that do not initially support the Universal Manifest standard.

Postconditions

- **Synchronization:** The Universal Manifest is consistently synchronized and recognized across all participating platforms.
- **Privacy:** User-specified privacy and consent settings are uniformly enforced.
- **Verification:** Identity, asset ownership, and compliance credentials are verified seamlessly.
- **Preference:** Social connections and user preferences are consistently applied across platforms.

Implementations and Demonstrations or Technical Feasibility

Existing Implementations

- **Ready Player Me:** Cross-platform avatar portability demonstrates practical feasibility of avatar metadata interoperability.
- **Decentraland & Spatial:** Demonstrated asset and avatar metadata portability using standardized formats such as glTF.
- **Polygon ID & Dock.io:** Decentralized identity and verifiable credential management in live blockchain-based applications.

Technical Feasibility

- **Metadata Standards:** JSON-LD schemas for interoperability and extensibility.
- **Decentralized Storage:** IPFS or blockchain-based repositories to ensure data availability, integrity, and user control.
- **Blockchain Verification:** Leveraging blockchain for secure, immutable verification of identity and asset ownership.
- **Security and Privacy:** Implementation of end-to-end encryption and selective disclosures using Zero-Knowledge Proofs (ZKPs).

Challenges:

- **Interoperability:** Integrating with diverse technical ecosystems and legacy systems presents a significant challenge, requiring flexible and seamless compatibility.
- **Data Privacy:** A primary challenge is maintaining robust user consent and preventing data exposure risks. This includes the risk of digital fingerprinting, where the manifest creates a comprehensive digital trail that could be exploited for tracking or profiling, and ensuring platforms handle manifest data only according to user permissions without creating unauthorized copies.
- **Security:** Keeping the system secure against evolving threats is a constant challenge. This requires preventing unauthorized access, protecting against tampering, and ensuring the manifest cannot be copied or misused to mitigate identity theft. It also means

preventing the unauthorized sharing or storage of sensitive manifest data to maintain data integrity.

- **Scalability:** Supporting widespread adoption without degradation of performance or user experience presents a scalability challenge that requires robust and efficient system architecture.
- **Regulatory Compliance:** Effectively navigating the complex and varied landscape of global data protection standards and compliance frameworks is a must.

Requirements:

Technical and Functional Requirements

- **Scalable Infrastructure:** The underlying infrastructure must be able to support widespread adoption without any degradation of performance or user experience.
- **Robust Security Measures:** The system must utilize advanced security mechanisms, including encryption, Zero-Knowledge Proofs (ZKPs), secure credential verification, and anti-cloning mechanisms to prevent unauthorized duplication. It must also include secure enclave support for sensitive credential storage and platform attestation to verify legitimate access requests. This functionality is supported by secure, decentralized storage mechanisms (like IPFS or blockchain storage) and a system that maintains a comprehensive manifest access log and audit trail of all interactions.
- **Reliability:** The system must ensure real-time synchronization of manifest updates across all participating platforms. It will also include conflict resolution protocols to manage concurrent updates reliably.
- **Maintenance:** This includes the necessary processes and tools for monitoring, updating, and sustaining the system over its lifecycle.
- **User Interface:** The system must provide a seamless and intuitive user experience during onboarding and cross-platform transitions. The interface will also provide robust controls for managing user preferences, consent, and privacy.
- **User Preference Management:** The system must support the storage and application of comprehensive user preferences, as outlined in Scenario 5: User Preference and Consent Management under Detailed Description of Use Case/Scenario.
- **Data Submission and Verification:** The system must securely ingest and validate all user-provided data and verifiable credentials. It should enforce data integrity and authenticity within the Universal Manifest by ensuring all submitted data is cryptographically sound and tamper-proof, thereby creating a non-repudiable record.
- **Access Control:** The system must provide comprehensive access controls that allow users to choose their authentication methods, manage their user-controlled storage (self-hosted, third-party, or platform-provided), and set granular permissions for platform access.
- **Notifications:** The system must be capable of sending notifications to users regarding manifest updates, access requests, or other relevant events.
- **Synchronization Process**: The system must implement a robust synchronization process. When a platform requests access to the user's Universal Manifest, the system checks the timestamp of the platform's cached version against an authoritative source to detect staleness. If the version is stale, the platform receives an updated manifest with a change log. The platform is then responsible for applying only authorized changes based on user permissions.

- **Version Management:** The system must allow **timestamp tracking** for all manifest updates, and should include **conflict resolution protocols** for any concurrent updates to ensure data consistency. All interactions should be logged for a comprehensive security audit trail.

Interoperability Requirements

- **Cross-Platform Compatibility:** The system must provide platforms, including legacy platforms, with multiple integration options to ensure cross-platform compatibility. Platforms are required to be able to use the manifest directly without modifications, create their own platform-specific versions, or utilize third-party API integration for updates. The system shall also support local copies with synchronization mechanisms and append-only change logs for auditability.
- **Standardized Protocols:** adoption of widely supported interoperability and metadata standards (e.g., JSON-LD) and compliance with established decentralized identity standards (e.g., W3C DID, VC).

Other Key Considerations:

- **Privacy:** The system must uphold user privacy by enforcing data minimization, and all manifest data shall be handled strictly according to user-granted permissions.
- **Identity Verification:** The system shall utilize Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to establish trust in a decentralized manner, ensuring that all identity claims are cryptographically verifiable without relying on a central authority. This process must be seamless and secure for the user.
- **Networking and Latency:** The system must ensure the Universal Manifest is accessible in real-time by utilizing an efficient, distributed network for data retrieval and storage.
- **Ownership:** provide users with the ability to maintain oversight on their data usage, storage and sharing to ensure continuous compliance with the consent they have granted.
- **Digital Ethics:** address ethical considerations by establishing or affiliating with an Ethics Board tasked with providing oversight, including regularly reviewing and guiding the ethical use of Manifest Data.
- **Provenance:** accurate tracking of data sources and changes to maintain the integrity and trustworthiness of the Universal Manifest.
- **Accessibility:** ensuring that the Universal Manifest is accessible to users and concerned stakeholders, with varying levels of technical expertise and accessibility requirements.

Relevant Domain Working Group (WGs):

- Digital Fashion Wearables for Avatars WG
- Privacy, Cybersecurity & Identity (PCI) WG
- Interoperable Characters/Avatars WG

Relevant Pre-qualified Organizations and Groups (POGs):

- **Open Metaverse Alliance for Web3 (OMA3):** develop standards for key areas, including virtual world interoperability, avatars, and portable digital assets like NFTs (www.oma3.org).
- **World Wide Web Consortium (W3C):** develops standards for the web, including those related to privacy, security, and identity management (for e.g. Decentralized Identifiers and

Verifiable Credentials), which are crucial for the interoperability of metaverse technologies (www.w3.org).

- **Ethereum Foundation:** facilitates a community-driven development of blockchain standards, such as Ethereum Improvement Proposals (EIPs) and Ethereum Request for Comments (ERCs), to ensure interoperability across the ecosystem with key examples like EIP-721, EIP-1155, and ERC-6551 (ethereum.org).
- **Decentralized Identity Foundation (DIF):** develops open protocols and standards for decentralized identifiers (DIDs), secure messaging, authentication, data storage, and interoperability to enable effective and secure exchange of identity-related data across decentralized systems and platforms (https://identity.foundation).
- **Khronos Group:** creates open standards for 3D graphics, AR, and VR; its key standards, such as **glTF** for 3D asset delivery and **OpenXR** for high-performance XR applications, are foundational to ensuring interoperability across virtual worlds and devices
- **VRM Consortium:** standardize 3D avatar formats for the metaverse. Its primary specification, the VRM format, provides a standard for handling humanoid models, expressions, and clothing, ensuring that a single avatar can be used across different virtual worlds and applications.
- **IEEE Metaverse Standards Committee (IEEE MSC):** focuses on creating interoperability standards for the metaverse. The committee is actively working to establish guidelines for connectivity, identity, privacy, security, and ethics to ensure a technically sound and cohesive virtual environment.
- **XR Safety Initiative (XRSI):** develops safety, security, and privacy standards for the extended reality (XR) ecosystem. The organization's work is critical for ensuring user protection and addressing key health, privacy, and safety risks within the metaverse.
- **Trust Over IP Foundation (ToIP):** provides a common architecture for decentralized identity, secure data exchange, and verifiable credentials across different systems, which is foundational to the metaverse.
- **World Economic Forum (WEF) Metaverse Initiative:** guides the development of a safe, ethical, and inclusive metaverse. The initiative focuses on addressing the high-level economic, governance, and societal questions surrounding the technology, working to shape its development in a responsible way.

Relevant Specifications, Publications and Projects (SPPs):

- **Ethereum Attestation Service** (https://attest.sh/)
- **OpenRank by Karma3Labs** (https://karma3labs.com)
- **Ceramic Network** (https://ceramic.network/)
- **Covalent** – Unified API for Blockchain Data (https://messari.io/report/covalent-a-unified-api-for-retrieving-blockchain-data)
- **Masa Decentralized Data Marketplace** (https://www.theblock.co/post/268051/decentralized-google-launch-zk-powered-data-marketplace-avalanche)
- **Inter World Portaling System (OMA3)** – avatar and asset portability demonstration between independent worlds.
- **IEEE P3812 (Decentralized Identity in Metaverse)** – Standardization effort addressing decentralized identity frameworks.
- **Real/Virtual World Integration (ISO/IEC 23894)** – Identity and certification interoperability between real-world credentials and virtual metaverse environments.
- **OpenSimulator Hypergrid / Open Metaverse Interoperability (OMI)** – Community-driven efforts demonstrating cross-platform avatar, inventory, and metadata portability.
- **Metaverse Metadata Directory (MVMD)** – MVMD.org provides guidelines and examples for structuring metadata related to 3D models, virtual locations, events, and other metaverse-specific entities.

Related Use Cases

- Humanity Attestation in Metaverse Environments Use Case (MSF2024-001-POH)
- Related Forthcoming Use Case Publications:
  - NFT Metadata for Avatars in the Metaverse (MSF2024-NFTMAM-001)
  - NFT Metadata for Wearables in the Metaverse (MSF2024-NFTMW-001)

Additional Comments

- Future considerations for the Universal Manifest include:
  - **Governance Model:** Establish clear governance and version management policies for ongoing standards evolution.
  - **Granularity of Metadata:** Evaluate optimal depth and modularity of metadata details included in the manifest.
  - **Legacy Compatibility:** Address compatibility strategies for integrating non-conforming or older platforms.
- This document is a living artifact and may be subject to revisions on a periodic basis to reflect the future state of Metaverse Universal Manifest, and or based on feedback received from MSF stakeholders that warrants an update in the future.