Metaverse Standards Forum
Interoperable User Agreement Compliance across Metaverse Platforms

Last Update: May 11, 2025

Status: Approved for Public Distribution

Version: 1.0

Reviewer	Due Date	Status	Contact
Digital Asset Management Working Group	December 17, 2024	Complete	digital_asset_management @lists.metaverse-standards.org
MSF Domains (Peer Review)	March 05, 2025	Complete	oversight@lists.metaverse-standards.org
Use Case Taskforce	May 11, 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

Interoperable User Agreement Compliance across Metaverse Platforms

Use Case Identifier

MSF2024-UAC-001

- Version 1.0
- Year of Release: 2025

Summary of Use Case

Description: This use case focuses on establishing a seamless process for Verifying that Users across various Metaverse Platforms have met specific compliance requirements. The aim is to facilitate interoperability and consistency in how Platforms verify User compliance with governmental regulations and corporate policies.

Benefits: Implementing this seamless Verification process will enhance User mobility across platforms without repeated compliance checks, thereby improving User experience and trust. It also benefits Platform Operators by reducing the redundancy of compliance efforts and ensuring a standardized safety and legal framework.

Contributors and Supporters

- Digital Asset Management Working Group

- MSF Domains (Peer Review)
- Use Case Taskforce

Keywords

User Compliance, Interoperability, Verification Process, Government Regulations, Metaverse Platforms, User Safety, Legal Compliance

Actors/Entities

- **Human Users:** individuals who engage with various Metaverse Platforms, providing necessary information and consenting to compliance checks as required by each Platform's User Agreement policies.
- **Metaverse Platforms Operators:** entities that manage and operate individual Metaverse environments, responsible for implementing Verification processes to ensure all Human Users meet the stipulated compliance requirements.
- **Compliance Verification Service Providers:** third-party services or integrated technologies that assist Platforms in Verifying compliance, offering technical solutions to ensure accurate and efficient compliance Verification across different regulatory requirements.
- **Standardization Bodies:** organizations that facilitate the development and adoption of standardized compliance Verification processes, promoting seamless experiences for Human Users across Platforms.

Detailed Description of Use Case/Scenario

Preconditions:

- Compliance standards, set by both governmental regulations and platform-specific policies, must exist.
- Metaverse Platforms should have integrated compliance Verification systems in place, supported by Compliance Verification Service Providers.

Main Flow:

1. **User Registration:** a Human User signs up on a Metaverse Platform, providing necessary personal information and consenting to Platform policies and compliance checks.
2. **Compliance Verification Request:** the Platform automatically sends a verification request to a Compliance Verification Service, including the User's provided information.
3. **Compliance Data Check:** the Compliance Verification Service checks the information against a database that includes government regulations and agreed-upon Platform policies.
4. **Verification Outcome:** the service returns the Verification result to the Metaverse Platform. If compliant, the User gains access; if not, the User is prompted to resolve any discrepancies or provide additional information.

5. **Continuous Compliance Update:** actors periodically update compliance requirements. The compliance service ensures that all User profiles are checked against these updates, maintaining ongoing compliance.
6. **Multi-Platform Registration:** once a User is verified on one Platform, they can opt to have their compliance status shared with other Platforms, streamlining their access without needing repeated checks.

Alternative Flow

- **Discrepancy Handling:** if information supplied by a User does not meet the set compliance standards during the initial check, the Platform will provide specific feedback on what is missing or incorrect. The User will have the opportunity to update the information or contest the finding with appropriate evidence.

Postconditions

- Human Users successfully Verified will enjoy seamless access across participating Platforms.
- Metaverse Platforms should maintain up-to-date compliance records for all active Users.

Implementations and Demonstrations or Technical Feasibility

Existing Implementations

- While no universal system currently exists that fulfills the seamless Verification across multiple Metaverse Platforms as envisioned, several Platforms have developed proprietary systems that provide insights into potential approaches:
  - **Fortis Identity Management by VirtuaVerse:** this system provides robust age and identity Verification processes tailored to comply with various regional laws, including General Data Protection Regulation (GDPR) in Europe and Children's Online Privacy Protection Act (COPPA) in the United States. It uses biometric data and AI-driven checks to ensure User authenticity.
  - **ComplyChain by MetaWorlds:** specifically designed to handle compliance with financial regulations including Office of Foreign Assets Control (OFAC), this Platform integrates real-time monitoring and reporting features that track transactions and User activities across its environment, ensuring adherence to international trade laws.

Technical Feasibility

- **Blockchain Technology:** utilizing blockchain technology provides a decentralized and transparent approach to manage and Verify compliance data across Platforms. This ensures enhanced security, User privacy, and immutable records of compliance.
- **Smart Contracts:** Smart Contracts on blockchain Platforms can automatically enforce compliance rules and agreements across different Platforms without the need for central oversight.
- **Decentralized Identifiers (DIDs):** these offer a Self-Sovereign Identity mechanism that allows Users to control their identity and personal data independently from any centralized registry, facilitating privacy-centric compliance Verification.
- **Interplanetary File System (IPFS):** using IPFS to store compliance documents ensures that documents are decentralized and tamper-proof, improving the integrity and availability of compliance data across platforms.

Challenges:

- **Data Privacy and Security:** ensuring the protection of sensitive User information while managing compliance across decentralized platforms poses significant challenges. The need to balance accessibility with security and comply with various international data protection regulations like GDPR complicates the implementation.
- **Interoperability of Verification Systems:** creating a system that is compatible across various Metaverse Platforms, each with their own underlying technologies and standards, is inherently challenging. This includes technical hurdles related to the integration of blockchain technologies and smart contracts.
- **Standardization of Compliance Protocols:** developing and enforcing standardized compliance protocols that are universally accepted and implemented across different Platforms can be difficult. This challenge is exacerbated by differing legal and regulatory requirements in different jurisdictions.
- **User Adoption and Experience:** convincing Users to adopt new Verification processes and ensuring that these processes do not degrade the User experience is essential. There's a risk that complex Verification procedures might deter users from engaging with the Platform.
- **Scalability and Performance:** as Metaverse Platforms grow in number and scale, ensuring that the compliance Verification system can handle increasing loads without compromising performance is a critical challenge.
- **Update and Maintenance of Compliance Information:** keeping the compliance Verification system up-to-date with the latest legal regulations and Platform policies requires a robust update and maintenance mechanism, which can be resource-intensive.
- **Indemnification/Trust:** Platform Operators take a risk by trusting an external process during Multi-Platform Registration, so robust standards and checks must be in place.

Requirements:

Technical and Functional Requirements

- **Data Privacy and Security Protocols:** implement advanced encryption and anonymization techniques to protect user data, utilizing blockchain for secure, immutable data storage.
- **Scalable Infrastructure:** design the system to efficiently handle increased loads from growing user numbers and platform expansions, incorporating cloud services and distributed computing solutions.
- **User-Friendly Verification Processes:** ensure the Verification process is simple and minimally invasive, with features for users to update their information and resolve disputes.
- **Continuous System Update and Maintenance:** establish mechanisms for regular system updates and maintenance to adapt to changing regulations and platform policies.

Interoperability Requirements:

- **Standardized Compliance Ruleset:** create a centralized, real-time updatable repository of compliance rules that accommodates different legal requirements across jurisdictions.
- **Unified Compliance Verification Interface:** develop a standardized API for easy integration with various metaverse platforms, supporting diverse blockchain technologies.

Other Key Considerations:

- **Privacy:** implement privacy enhancing technologies and practices that protect privacy during collection, processing, storage and sharing of required User information with authorized parties, and only after securing appropriate consent from the User.
- **Cybersecurity:** robust cybersecurity measures to safeguard User information from vulnerabilities, including unauthorized access, data breaches and illicit activities such as data trading or fraud.
- **Identity Verification:** reliable and secure Verification of Users, fostering trust in the Digital Asset ecosystem.
- **Networking and Latency:** architect the system to minimize latency, ensuring smooth operation across geographically dispersed platforms.
- **Ownership:** provide Users with the ability to control their data, including updating their Verification and compliance details as a requirement arises and in line with the User Agreement and Platform policies.
- **Digital Ethics:** address ethical considerations in collecting, processing, storing and sharing User data, while ensuring traceability option is made available for Users to monitor the flow of their compliance and Verification data with authorized parties.
- **Provenance:** tools and protocols are needed to validate the authenticity of compliance details provided by Users as part of fulfilling Platform Verification requirements.
- **Accessibility:** ensuring the compliance requirements are accessible to Users from diverse backgrounds, with varying levels of technical expertise and accessibility requirements.

Relevant Domain Working Group (WGs):

- NA

Relevant Pre-qualified Organizations and Groups (POGs):

- NA

Relevant Specifications, Publications and Projects (SPPs):

- NA

Related Use Cases

- This use case aims at advancing compliance across Metaverse Platforms through the application of Interoperable User Agreements, and hence might be applicable to many current and upcoming Metaverse use cases.

Additional Comments

- This document is a living artifact and may be subject to revisions on a periodic basis to reflect the future state of Interoperable User Agreement Compliance across the Metaverse, and or based on feedback received from MSF stakeholders that warrants an update in the future.