Metaverse Standards Forum
Shared KYC/AML Verification in the Metaverse

Last Update: May 10, 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 10, 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

Shared KYC/AML Verification

Use Case Identifier

MSF2024-REPSKA-001

- Version 1.0
- Year of Release: 2025

Summary of Use Case

Description: This use case outlines a framework for a shared Know Your Customer (KYC) and Anti-Money Laundering (AML) Verification process that allows Users to undergo Verification once and leverage this status across various platforms and applications within the metaverse. This approach aims to streamline User Experiences, enhance regulatory compliance, and build trust within digital environments.

Benefits:

- Reduces redundancy and User friction by eliminating the need for multiple KYC/AML verifications across Metaverse Platforms.
- Enhances security and trust across platforms by utilizing a standardized Verification process.
- Supports interoperability and seamless User experience within the Metaverse.
- Encourages wider participation by lowering barriers to entry for new Users.
- Enables financial use cases in the Metaverse.

Contributors and Supporters

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

Keywords

Shared KYC/AML, Interoperability, Security, Trust, User Experience, Metaverse, Verification, Identity Validation.

Actors/Entities

- **End Users (Metaverse Participants):** individuals who engage with various platforms within the Metaverse for leisure, work, or commerce. They usually complete the KYC/AML Verification process through a designated Verification service and must provide necessary documentation and consent for Verification to be used across platforms.
- **Verification Service Providers:** entities that perform KYC/AML checks, Verify the identity of Users, and issue a Verification status or credential that can be recognized by Platform Operators. They also Verify User identities in compliance with global KYC/AML standards. Verification Service Providers must also securely manage and share Verification statuses with authorized platforms, respecting User privacy and consent.
- **Platform Operators (Virtual Worlds, DApps, Services):** operators of various platforms within the Metaverse that require KYC/AML Verification for Users to access certain services or functionalities. They integrate with Verification Service Providers for accessing shared KYC/AML statuses, enabling seamless access for Verified Users across platforms. They must also ensure they adhere to privacy regulations and standards in handling Verification data.
- **Regulatory and Standards Bodies:** organizations, such as governments, that define the rules and standards for KYC/AML processes, as well as data protection and privacy within digital environments. They establish and update KYC/AML and privacy standards that Verification Service Providers and Platform Operators must comply with.

Detailed Description of Use Case/Scenario

Preconditions:

- **User Registration:** Users have created accounts on various Metaverse Platforms but have not yet undergone KYC/AML Verification.
- **Partnership and Integration:** Platform Operators have established partnerships with Verification Service Providers and integrated their systems to accept shared KYC/AML Verification statuses.

- **Regulatory Compliance:** Verification Service Providers are compliant with global KYC/AML regulations and have the infrastructure to securely manage and share Verification data.

Main Flow:

1. **User Initiates KYC/AML Verification:** an End User decides to access a platform within the Metaverse that requires KYC/AML Verification and is prompted to undergo the process.
2. **Selection of Verification Service Provider:** the User is given the option to select a preferred Verification Service Provider from a list of partners integrated with the Metaverse Platform, or the Platform Operator dictates the Verification Service Provider.
3. **Verification Process:** the User completes the Verification process with the chosen Verification Service Provider, submitting necessary documentation and information through a secure portal.
4. **Verification Status Issued:** upon successful Verification, the Service Provider issues a Verification status or credential, securely associating it with the User's Digital Identity within the Metaverse.
5. **Shared Verification Across Platforms:** the Verification status is made available (with User consent) to other platforms within the Metaverse, allowing the User to access other Platforms without needing to repeat the KYC/AML process.
6. **Verification Reuse:** the User accesses a second Platform that requires KYC/AML and leverages their Verification status with the previous Verification Service Provider.
7. **Optional:** other Service Providers may request proof of compliance with a specific regulation, such as OFAC, and the Service Provider is able to prove the compliance without compromising the privacy of the User (e.g., a zero-knowledge proof).
8. **Optional Verification Update:** Platform Operator or Verification Service Provider requests that a User go through the KYC/AML process again, and this updated Verification can also be Shared with the second and other Platforms.

Alternative Flow

- **Verification Failure:** if the User fails the Verification process (e.g., due to insufficient documentation), they are prompted to retry or contact support for further assistance. This ensures Users have the opportunity to address any issues and complete the Verification process.

Postconditions

- **Seamless Access Across Platforms:** Users who have completed the KYC/AML Verification can seamlessly access services across various Platforms within the Metaverse, enhancing their overall experience.

Implementations and Demonstrations or Technical Feasibility

Implementations and Demonstrations

- **Blockchain-Based Identity Verification Platforms:**
  - **Examples:** Platforms like Civic, SelfKey, KYC Credential Ecosystem Initiative by Polimec, and Sovrin offer Blockchain-Based Identity Verification services that enable users to own and control their identity data, including KYC/AML credentials. These

Platforms allow users to share their Verified Identity with participating services without needing to undergo Verification for each new platform.

- **Technical Feasibility:** the use of decentralized identity (DID) technology and blockchain ensures secure, tamper-proof storage and sharing of KYC/AML data. Smart contracts automate the Verification status sharing process, maintaining user privacy and consent.

- **Financial Sector Consortia:**
  - **Examples:** initiatives like the Global Legal Entity Identifier Foundation (GLEIF) and the SWIFT network's KYC Registry provide standardized, shared KYC services for the financial industry. These systems allow banks and financial institutions to access and share Verified entity information, reducing duplication of effort and enhancing compliance efficiency.
  - **Technical Feasibility:** leveraging centralized databases and standardized identifiers (e.g., LEIs), these systems demonstrate the feasibility of shared KYC/AML across organizations. Interoperability standards and APIs facilitate secure data exchange among participants.
- **Cross-Platform Verification Services:**
  - **Examples:** services such as Trulioo and Onfido offer cross-industry KYC/AML Verification solutions that can be integrated into various digital platforms. These services use a mix of document Verification, biometric analysis, and database checks to Verify Users' identities.
  - **Technical Feasibility:** these services showcase the application of advanced technologies like artificial intelligence and biometrics for efficient and accurate Identity Verification. API integrations allow for flexible incorporation into existing digital platforms, supporting shared Verification practices.
- The existing implementations demonstrate the technical feasibility of shared KYC/AML Verification systems, leveraging technologies such as blockchain, smart contracts, decentralized identities, APIs, and biometrics. These technologies ensure secure, efficient, and user-consented sharing of Verification statuses across different platforms and industries.
- Blockchain and DIDs provide a secure, decentralized method for managing and sharing digital identities and Verifications, fostering trust and reducing reliance on centralized authorities.
- Smart Contracts and APIs automate and secure the process of Verification status sharing, ensuring interoperability between disparate systems and platforms.
- Advanced Verification Technologies (e.g., document scanning, biometric analysis) enhance the accuracy and reliability of Identity Verification processes.

Challenges:

- **Interoperability Across Platforms:** ensuring seamless interoperability of KYC/AML Verification statuses across diverse platforms and applications within the Metaverse, each potentially using different standards and technologies. Without standardized protocols and formats, the utility of shared KYC/AML verification could be limited, resulting in fragmented user experiences.

- **Privacy and Data Protection:** balancing the need for thorough KYC/AML checks with the users' right to privacy, especially in jurisdictions with strict data protection laws (e.g., GDPR). Ensuring user consent and secure data handling practices are critical to maintain trust and comply with global privacy regulations.
- **Security and Fraud Prevention:** preventing fraudulent activities and ensuring the security of the KYC/AML verification process, especially against, financial harm, surveillance, adverse effects on rights and freedoms, harassment, identity theft and data breaches. Remediation of lost or stolen credentials. The integrity of the shared verification system relies on robust security measures to protect sensitive user information and maintain trust.
- **Scalability and Performance:** designing the system to efficiently handle a large volume of verification requests across the metaverse, without significant delays or bottlenecks. Scalability challenges could lead to poor user experiences, especially during peak times or rapid growth phases of metaverse platforms.
- **Regulatory Compliance:** navigating the complex and often varying regulatory requirements for KYC/AML across different countries and regions. Platforms and verification service providers must ensure compliance with all applicable laws, which can be challenging given the global nature of the metaverse.
- **Indemnification/Trust:** Platform Operators take a risk by trusting an unknown process during Verification Reuse, so robust standards and checks must be in place. Processes can get lax over time, compromising the system.

Requirements:

Technical and Functional Requirements

- **Robust Security Measures:** employ advanced security protocols, encryption, and fraud detection mechanisms to safeguard the Verification process and User data.
- **Scalable Infrastructure:** build a scalable and high-performance infrastructure capable of supporting a global User base and handling peak loads efficiently.
- **Regulatory Engagement:** collaborate with regulatory bodies to ensure the Shared KYC/AML system complies with international and local regulations.
- **Usability:** User can perceive and investigate that the KYC/AML verification systems are legitimate

Interoperability Requirements:

- **Standardization:** develop and adopt interoperable standards for KYC/AML Verification processes and data formats across the Metaverse.

Other Key Considerations:

- **Privacy:** implement privacy enhancing technologies and practices that protect user privacy, such as zero-knowledge proofs, to share verification statuses without exposing sensitive data.
- **Cybersecurity:** robust cybersecurity measures to safeguard the verification system against hacking, identity theft, and fraud.

- **Identity Verification:** reliable and secure KYC/AML Verification of Users, fostering trust in the Digital Asset ecosystem.
- **Networking and Latency:** efficient network architecture to ensure fast and reliable KYC/AML Verification processes, minimizing latency.
- **Ownership:** provide Users with the ability to control their Verification data, including revocation and/or deletion of their Verification details
- **Digital Ethics:** address ethical considerations in processing, storing and sharing Users KYC/AML data, while ensuring traceability option is made available for Users to monitor the flow of their data across Platforms.
- **Provenance:** tools and protocols are needed to validate the authenticity of Users profiles and Identity sources supplied by Users to fulfill KYC/AML Verification requirements.
- **Accessibility:** ensuring the Verification process is accessible to Users from diverse backgrounds, with varying levels of technical expertise and accessibility requirements.

Relevant Domain Working Group (WGs):

- Interoperable Characters / Avatars WG
- Privacy, Cybersecurity and Identity WG

Relevant Pre-qualified Organizations and Groups (POGs):

- World Wide Web Consortium (W3C)
- Decentralized Identity Foundation (DIF)

Relevant Specifications, Publications and Projects (SPPs):

The following standards and specifications can enable Identity Verification and credential exchange between agents leveraging cryptography and Blockchain-Based Identity Verification techniques:

- W3C Decentralized Identifiers (DID)
- W3C Verifiable Credentials
- DIDComm Protocol by DIF

Related Use Cases

- This use case advances interoperability by facilitating exchange of Verified KYC/AML profiles across Metaverse Platforms. Therefore, it augments all types of Use Cases deployed in the Metaverse and particularly ones that provide financial service, including Digital Asset Trading Marketplaces, backed by Blockchain-based Identity Verification Services and Advanced Cryptographic Techniques.

Additional Comments

- This document is a living artifact and may be subject to revisions on a periodic basis to reflect the future state of Shared KYC/AML Verification in the Metaverse, and or based on feedback received from MSF stakeholders that warrants an update in the future.