Metaverse Standards Forum
Identity Verification for Digital Asset Creators

Last Update: May 09, 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 09, 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

Identity Verification for Digital Asset Creators

Use Case Identifier

MSF2024-IDVER-001

- Version 1.0
- Year of Release: 2025

Summary of Use Case

Description: This use case outlines the essential procedures and technological infrastructure required to verify the real-world identities of Creators issuing Non-Fungible Tokens (NFTs) or other Digital Assets. It emphasizes the development of a robust verification system to ensure the authenticity of Creator identities, which is crucial for maintaining trust, security, and the integrity of copyright and provenance in Digital Asset transactions.

Benefits:

- **Trust and Security Enhancement:** by ensuring the authenticity of Creator identities, the system strengthens trust and security in Digital Asset transactions.
- **Fraud Mitigation:** it plays a critical role in reducing fraud and the circulation of counterfeit Digital Assets, protecting both Creators and investors.
- **Intellectual Property Protection:** the verification process supports copyright integrity and intellectual property rights, crucial for the sustainable growth of the Digital Asset market.

Contributors and Supporters

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

Keywords

NFT Creator Verification, Digital ID Authentication, Verification Service Provider, Royalty Distributions, Copyright Protection, Blockchain-based Identity Verification Services, Digital Asset Trading, Anti-Fraud Mechanisms, Digital Economy Trust, NFT Intellectual Property

Actors/Entities

- **Creators (Digital Artists, Developers):** individuals or entities who create Digital Assets, such as NFTs, seeking to authenticate their real-life identities to ensure rightful creation attribution. Their primary responsibility is to initiate the Identity Verification process.
- **Creation Mechanism:** the tools a Creator controls and uses to create Digital Assets (e.g., wallet).
- **Digital Asset:** the assets created by a Creator using a Creation Mechanism.
- **Verification Service Provider:** a third-party entity or platform that provides Digital Identity Verification Services. This actor is responsible for verifying the authenticity of Creators' identities using various methods (e.g., biometric verification, document validation) and ensuring the information is securely linked to the Digital Assets created by them (e.g., the identity has control of a minting wallet). The Verification Service Provider may also track the historical data of a Creator for additional provenance.
- **Marketplaces:** online platforms where verified Digital Assets are listed, bought, sold, or traded. These entities rely on the Verification Service Provider to ensure that listed Digital Assets are created by verified Creators, enhancing trust and security for buyers and sellers. Marketplaces may also be Verification Service Providers.
- **Buyers/Collectors:** individuals or entities purchasing or investing in Digital Assets. They are concerned with the authenticity of the asset's Creator and the legitimacy of the ownership and rights associated with the Digital Assets.

Detailed Description of Use Case/Scenario

Preconditions:

- Creators have Digital Assets (e.g., NFTs) they wish to mint and sell on marketplaces.
- Verification Service Providers have established, secure, and privacy-compliant processes for Identity Verification.
- NFT Marketplaces have mechanisms to integrate verification statuses and display them to buyers.

Main Flow:

1. **Identity Submission:** the Creator initiates the process by applying for verification through a Verification Service Provider, submitting required information such as identity documents and proof of ownership of the Creation Mechanism.
2. **Verification Process:** the Verification Service Provider reviews the submissions for authenticity using a combination of manual checks and automated systems, such as AI-driven facial recognition for biometric verification and visual confirmation for document authenticity.
3. **Verification Status:** upon successful verification, the Creator’s identity is cryptographically linked to their Creation Mechanism, establishing a verifiable chain of ownership of any assets created by the Creation Mechanism. The Verification Service Provider updates the verification status, which is accessible to Marketplaces, including the mechanisms used during the Verification Process.
4. **Asset Creation:** Creator creates Digital Assets using the Creation Mechanism verified by the Verification Process.
5. **Listing on Marketplaces:** Creators list their verified Digital Assets on Marketplaces, with the verification status of the Creation Mechanism prominently displayed to potential buyers.
6. **Purchase by Buyers:** buyers select and purchase Digital Assets, prioritizing those with verified Creator identities. The marketplace facilitates the transaction, ensuring the buyer receives the Digital Asset and the Creator receives Royalty Distributions / payment.

Alternative Flow

- If a Creator's identity cannot be verified due to insufficient or fraudulent documentation, the Verification Service Provider notifies the Creator of the rejection, offering guidance on resolving the issues.
- Instead of verifying the Creator’s Creation Mechanism the Verification Service Provider verifies the Creator owns the Digital Assets directly.
- A Buyer goes to another source separate from the Marketplace to verify the owner of the Creation Mechanism.

Postconditions

- Creators have their identities verified and linked to their Digital Assets or Creation Mechanism, gaining trust from buyers.
- Buyers are assured of the authenticity of the Digital Assets and their Creators.

Implementations and Demonstrations or Technical Feasibility

The concept of linking a Creator's verified real-world identity to their Digital Assets, specifically NFTs, is a burgeoning area of interest within the blockchain and Digital Asset communities. As of now, there are a few platforms and initiatives that have begun to address the need for Creator verification, albeit in varying degrees of complexity and integration.

Known Implementations

- **Blockchain-Based Identity Verification Services:** several blockchain projects focus on Identity Verification, leveraging the technology's inherent security and transparency. Platforms like Civic and uPort offer decentralized Identity Verification solutions that could be adapted for Creator verification in the NFT space. However, direct integration with NFT marketplaces to standardize Creator Identity Verification across platforms is still in developmental stages.

- **NFT Marketplaces with Verification Features:** some NFT marketplaces have started implementing their own verification processes for Creators and their Digital Assets. For instance, platforms like Rarible and OpenSea offer a verification badge to Creators who have completed a verification process. These processes vary but generally involve manual checks and may include social media verification, portfolio review, and in some cases, identity documentation. Yet, these are not universally adopted standards and often lack the depth of verifying real-life IDs against Digital Assets directly.

Technical Feasibility

The technical feasibility of implementing a comprehensive Creator ID verification system is high, given the existing blockchain technologies and smart contract capabilities. The challenge lies in creating a standardized, cross-platform system that can be adopted universally by all NFT marketplaces and Digital Asset platforms. Such a system would need to respect privacy laws, be secure against fraud, and be scalable to accommodate the growing Digital Asset economy.

Challenges:

Technical Challenges

- **Interoperability:** developing a system that is interoperable across different blockchain platforms and NFT marketplaces is crucial. This requires standardized protocols that ensure compatibility and seamless integration, facilitating the widespread adoption of ID verification systems.
- **Privacy and Security:** balancing the need for transparent verification with the right to privacy and data protection is a significant challenge. Implementing secure, privacy-preserving technologies that comply with global data protection regulations (e.g., GDPR) is essential. Additionally, safeguarding the verification system against fraudulent activities and identity theft is critical.
- **Technological Scalability:** the system must be scalable to handle the growing volume of Digital Assets and users within the Metaverse. This involves addressing the challenges of blockchain scalability, such as transaction speeds and costs, to maintain an efficient verification process.

Legal and Regulatory Challenges

- **Global Compliance:** Digital Assets and NFTs operate on a global scale, making compliance with diverse legal and regulatory requirements complex. The verification system must adapt to various jurisdictions' anti-money laundering (AML) and know your customer (KYC) laws.
- **Intellectual Property Rights:** ensuring that the verification system supports the protection of intellectual property rights in the digital realm. This includes navigating the complexities of copyright laws as they apply to Digital Assets and NFTs.

Requirements:

Technical and Functional Requirements:

- **Standardized Protocols:** development and adoption of standardized protocols for ID verification across blockchain platforms and NFT marketplaces, ensuring interoperability and seamless integration.
- **Privacy-Preserving Technologies:** implementation of technologies such as zero-knowledge proofs to enable verification without exposing sensitive personal information, ensuring compliance with global privacy regulations.
- **Secure Data Storage:** mechanisms for secure, encrypted storage of verification data, with robust access controls to protect against unauthorized access and data breaches.
- **Blockchain Scalability Solutions:** adoption of scalability solutions that can handle increased transaction volumes and users, reducing transaction costs and speeds to maintain an efficient verification process.
- **Advanced Cryptographic Techniques:** leveraging advanced cryptographic techniques, such as zero-knowledge proofs are key, to enable verification without exposing personal data.
- **User-Friendly Verification Process:** the process must be straightforward and accessible for Creators, requiring minimal technical knowledge to complete ID verification.
- **Real-Time Verification Status:** platforms and marketplaces should be able to access and display a Creator's verification status programmatically in real-time, enhancing trust and transparency for buyers.
- **Compliance with Regulatory Standards:** the system should adapt to various legal frameworks and regulations across jurisdictions, including AML and KYC standards, without compromising the efficiency of the verification process. Establishing partnerships with regulatory bodies and legal experts to ensure compliance and address the legal intricacies of Digital Asset ownership and Creator rights.

Interoperability Requirements:

- **Cross-Platform Compatibility:** the verification system must be compatible across different blockchain platforms and NFT marketplaces, facilitating a universal standard for Creator ID verification.

Other Key Considerations:

- **Privacy:** adoption of privacy-preserving verification methods to protect Creators' personal information, adhering to applicable privacy regulations such as GDPR.
- **Cybersecurity:** deploy robust cybersecurity measures to safeguard the verification system against hacking, identity theft, and fraud.
- **Identity Verification:** reliable and secure verification of Creators' real-life identities, establishing trust in the Digital Asset ecosystem.
- **Networking and Latency:** efficient network architecture to ensure fast and reliable verification processes, minimizing latency.
- **Ownership:** clear linkage of verified identities with Digital Asset ownership, supporting copyright and intellectual property rights.

- **Digital Ethics:** address ethical considerations in the use and storage of personal data, ensuring fairness and transparency in the verification process.
- **Provenance:** tools and protocols are needed to track the authenticity of Digital Assets, linking them unequivocally to verified Creators.
- **Accessibility:** ensuring the verification process is accessible to Creators 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):

- W3C

Relevant Specifications, Publications and Projects (SPPs):

The following standards and specifications can enable Identity Verification leveraging cryptography and blockchain-based Identity Verification techniques:

- W3C Decentralized Identifiers (DID)
- W3C Verifiable Credentials

Related Use Cases

- This use case augments “NFT Royalties” and other “Reputation in the Metaverse” use cases, as it centers around the provision of secure access to, Metaverse Platforms and 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 Identity Verification for Digital Asset Creators, and or based on feedback received from MSF stakeholders that warrants an update in the future.