Metaverse
STANDARDS FORUM™

Metaverse Standards Forum
Cybersecurity Reputation Data Storage

Last Update: May 12, 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 12, 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

Cybersecurity Reputation Data Storage

Use Case Identifier

MSF2024-REPCDS-001

- Version 1.0
- Year of Release: 2025

Summary of Use Case

Description: This use case focuses on the storage and accessibility of Cybersecurity Reputation Data for hardware and software used in the Metaverse. This data includes Cybersecurity Certifications, Audits, Penetration Tests, Bill of Materials, Secure Storage of Credentials, and Vulnerability Reports. It is intended to provide Metaverse participants with insights into the trustworthiness of various hardware and software components, such as blockchain validator clients, game clients, smart contracts, server applications, and Non-Playable Character (NPC) engines. This Reputation Data can be queried by participants directly or through third-party tools, and is stored and queried with the developer's permission.

Benefits:

- Enhanced visibility into the cybersecurity posture of Metaverse components.
- Improved trust and safety for Metaverse participants.
- Facilitation of informed decision-making based on verifiable Cybersecurity Data.
- Encouragement of cybersecurity best practices among developers.

- Support for interoperability by providing a standardized method for querying Cybersecurity Reputation Data.

Contributors and Supporters

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

Keywords

Cybersecurity Reputation, Metaverse Software, Cybersecurity Certifications, Vulnerability Reports

Actors/Entities

- **Developers:** entities that build the hardware and software components used in Metaverse Platforms. Developers also provide permission for associating Cybersecurity Reputation Data with their software product and supplying necessary information to Third-Party Tools. They also handle the fixing of hardware and software vulnerabilities.
- **Metaverse Participants:** Users, Third-Party Tools, and Owners.
- **Third-Party Tools/Services:** entities that provide interfaces or services to facilitate the querying of Reputation Data. Develop and maintain tools that allow participants to query and interpret Cybersecurity Reputation Data. This may include creating a rating system.
- **Cybersecurity Assessors:** organizations or individuals conducting audits and assessments, including Test Labs and Auditors.
- **Regulatory Bodies:** authorities overseeing cybersecurity standards and compliance. They approve the results of Cybersecurity Assessors; provide Certifications; enforce Cybersecurity Regulations and Standards, and Store Certification Results.
- **Owners**: entities that own and/or manage the software but may not be directly involved in its development and are alerted of any cybersecurity issues with the software and take recommended remediation actions, such as performing updates. This includes Operations Security (OPSEC) processes.
- **Users:** entities that use the hardware and software and are alerted of any cybersecurity issues with the software and make decisions on whether to use the software. They could also provide Cybersecurity Reputation Data with their actions; in which case their permission must be given.
- **Installers:** entities that configure hardware and software for Owners and Users. They install and configure software in the correct manner and reconfigure it to deal with any changes in cybersecurity posture.

Detailed Description of Use Case/Scenario

Preconditions:

- The Developer has agreed to provide cybersecurity reputation data.
- Regulatory Bodies have created certification programs.

Main Flow:

- **Data Collection, Assessment and Certification:**
    - Developers initiate the collection of Cybersecurity Reputation Data, including Cybersecurity Certifications, Audit Results, Penetration Tests, Software Bill of Materials, Secure Storage of Credentials, and Vulnerability Reports.
    - Cybersecurity Assessors perform necessary audits and assessments, generating detailed reports on the software's security posture.
    - Regulatory Bodies review the assessment reports and provide relevant certifications.
- **Data Storage:**
    - The collected Reputation Data is securely stored in a repository that supports querying by actors. This storage is done with the permission of the developers.
    - The reputation data repository ensures the integrity and confidentiality (in the case of proprietary data) of the stored information.
- **Access Control:**
    - Developers control who has access to the Reputation Data associated with their products.
    - Developers can grant access to Owners only or make the data available to the general public, based on their discretion. This access control can be fine grained to give access to only the necessary information to provide a certain level of trust.
- **Data Querying:**
    - Metaverse Participants, either directly or indirectly, query the Reputation Data repository to access the Cybersecurity Reputation of specific components (e.g., blockchain validator clients, game clients, smart contracts, server applications, NPC engines).
    - The query results provide detailed insights into the cybersecurity posture of the component, helping participants make informed decisions about its trustworthiness.
    - Only the information required for the query is revealed, honoring confidentiality of developers.
- **Alert and Remediation:**
    - Developers, Participants, and Installers are alerted of any identified cybersecurity issues with their software through the Reputation Data repository.
    - Developers, Participants, and Installers take recommended remediation actions, such as performing updates or applying patches, to address the identified issues.

Postconditions

- Users have access to up-to-date Cybersecurity Reputation Data, enabling them to make informed decisions about the software they use.

- Developers, Participants, and Installers have mechanisms in place to respond to cybersecurity alerts and take remediation actions promptly.

Implementations and Demonstrations or Technical Feasibility

Existing Implementations

- **Reputation Data Repository:** a secure repository that supports storing and querying Cybersecurity Reputation Data.
    - **Example:** CyberGRX – a platform that provides third-party cyber risk management by collecting and assessing cybersecurity data from various organizations.
    - National Vulnerability Database (NVD).
    - Graph for Understanding Artifact Composition (GUAC).
- **APIs and Interfaces:** developed by third-party tools/services to facilitate the querying and interpretation of Reputation Data.
    - **Example:** SecurityScorecard – an API that provides access to security ratings and allows for querying cybersecurity posture information.
    - RiskRecon

Demonstrations

- **End-to-End Process Prototypes:** demonstrations showing the process of collecting, storing, and querying cybersecurity reputation data.
    - **Example:** BitSight – demonstrates how security ratings can be used to assess the cybersecurity posture of organizations through a comprehensive scoring system.
    - Code scanning tools and databases.
- **Sample Data Usage:** illustrations using sample data to show how metaverse participants can query the reputation data repository and interpret the results.
    - **Example:** OpenVAS – an open-source vulnerability scanning tool that generates detailed security reports which can be used as sample data for demonstrations.

Technical Feasibility

- The reputation data repository should ensure data integrity, confidentiality, and availability.
    - **Example:** AWS Artifact – a secure portal that provides on-demand access to AWS's security and compliance reports.
- The system should support scalability to handle large volumes of data and queries from numerous metaverse participants.
    - **Example:** Splunk – a data analytics platform that can scale to handle large volumes of machine-generated data.
- Security measures such as encryption, access control, and audit logging should be in place to protect the reputation data.
    - **Example:** HashiCorp Vault – a tool for securely storing and accessing secrets and sensitive data.

Challenges:

- **Data Privacy:** ensuring the privacy of sensitive cybersecurity data while making it accessible for querying.
- **Data Integrity:** maintaining the integrity and accuracy of the Reputation Data to prevent tampering and unauthorized modifications.
- **Scalability:** handling the increasing volume of Reputation Data and queries as the Metaverse ecosystem grows.
- **Interoperability:** ensuring compatibility between different systems and platforms involved in collecting, storing, and querying the Reputation Data.
- **Reputation Scores:** ensuring scoring systems have the appropriate scope. If scoring systems are inappropriate this will lead to bad decisions.
- **Remediation:** responding to breaches in a timely manner, and remediating breaches (e.g., proper insurance for losses).

Requirements:

Technical and Functional Requirements

- **Robust Security Measures:** implement secure privacy-preserving data storage with encryption to prevent unauthorized access and breaches during Cybersecurity Reputation Data storage and accessibility management.
- **Data Consensus:** techniques applied for decentralized data stores to ensure accurate, tamper-resistant cybersecurity reputation scoring across distributed nodes.
- **User Interface:** a user-friendly interface for querying and interpreting Cybersecurity Reputation Data.
- **Notifications:** real-time alert mechanisms for notifying on Cybersecurity Reputation Data issues, ensuring that users are informed of updates in a timely manner.
- **Access Control:** fine-grained access controls mechanisms that allow Developers to manage who can access their Cybersecurity Reputation Data.
- **Data Capture and Storage:** effective techniques that enable queried Cybersecurity Reputation Data to be maintained in the respective Metaverse Platform repository, while ensuring the provision of access to auditors to verify stored data.

Interoperability Requirements:

- **Cross-Platform Compatibility:** the Cybersecurity Data Reputation system must be compatible with existing Metaverse Platforms and tools
- **APIs Development:** for Cybersecurity Reputation Data querying and integration with third-party tools.
- **Standardized Data Formats:** developing and implementing standardized data formats to facilitate interoperability and enable efficient Cybersecurity Reputation data exchange.

Other Key Considerations:

- **Privacy:** secure handling and protection of sensitive Cybersecurity Reputation data, ensuring that private information is only shared with explicit consent.

- **Cybersecurity:** robust cybersecurity measures to safeguard Cybersecurity Reputation Data against breaches and unauthorized access. This includes encryption, secure access controls, and provision of audit trails for regular security audits.
- **Identity Verification:** ensure reasonable identification and authorization of users prior to providing Cybersecurity Reputation Data, to verify that their usage aligns with approved terms and intended boundaries
- **Networking and Latency:** efficient storage mechanisms without latency issues, while ensuring that Reputation Data is accessible in real-time.
- **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 Cybersecurity Reputation Data.
- **Provenance:** accurate tracking of data sources and changes to maintain the integrity and trustworthiness of Cybersecurity Reputation Data.
- **Accessibility:** ensuring Cybersecurity Reputation Data is accessible to users, with varying levels of technical expertise and accessibility requirements.

Relevant Domain Working Group (WGs):

- NA

Relevant Pre-qualified Organizations and Groups (POGs):

- **National Institute of Standards and Technology (NIST):** provides standards and guidelines to improve the cybersecurity of organizations, contributing to the development of frameworks and best practices (www.nist.gov).
- **International Organization for Standardization (ISO):** develops and publishes international standards, including those for information security (ISO/IEC 27001) (www.iso.org).
- **Internet Engineering Task Force (IETF):** The IETF develops and promotes voluntary Internet standards and protocols, particularly the standards that comprise the Internet protocol suite (TCP/IP) (www.ietf.org).
- **Open Web Application Security Project (OWASP):** provides resources and standards for improving the security of software, including guidelines and tools for developers (www.owasp.org).
- **Cloud Security Alliance (CSA):** promotes the use of best practices for providing security assurance within cloud computing and offers education on the uses of cloud computing to help secure all other forms of computing (www.cloudsecurityalliance.org).
- **Institute of Electrical and Electronics Engineers (IEEE) Standards Association:** develops global standards for a wide range of industries, including cybersecurity standards that are relevant to software and hardware used in the Metaverse (https://standards.ieee.org).

- **W3C (World Wide Web Consortium):** develops standards for the web, including those related to privacy, security, and identity management, which are crucial for the interoperability of metaverse technologies (www.w3.org).
- **Open Source Security Foundation (OpenSSF):** part of the Linux Foundation, is a community of software developers and security engineers who collaborate to define best practice across key cybersecurity domains, including securing open source and building tools for software security scoring (www.openssf.org).
- **Lumian Foundation:** Lumian offers software update certification that enables verification of the security of a product's remote software update functionality and the status of an individual device's trust profile (www.lumian.org).

Relevant Specifications, Publications and Projects (SPPs):

- NIST Cybersecurity Framework
- ISO/IEC 27001
- OWASP Standards: Top 10, Application Security Verification Standard (ASVS), Software Assurance Maturity Model (SAMM), Mobile Top 10, and Cloud-Native Application Security Top 10
- CSA Security Guidance
- FedRAMP Annual Assessment Guidance
- System and Organization Controls 2 (SOC 2)
- International Electromechanical Commission (IEC) 62443
- Various Industry Cybersecurity Certifications such as: PCI, UL, SunSpec, CTIA, ARM PSA, and Intertek

Related Use Cases

- Unified Reputation Management for Metaverse Entities (MSF2024-REPUMME-001)

Additional Comments

- This document is a living artifact and may be subject to revisions on a periodic basis to reflect the future state of Cybersecurity Reputation Data Storage, and or based on feedback received from MSF stakeholders that warrants an update in the future.