ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Report

(06/2024)

ITU Focus Group on metaverse
(FG-MV)

FGMV-46

The essential components of trusted data use in building a trustworthy metaverse

Working Group 6: Security, Data & Personally identifiable information (PII) Protection

PREPUBLISHED

Version

Technical Report ITU FGMV-46

The essential components of trusted data use in building a trustworthy metaverse

Summary

In an era in which digital realities are increasingly as significant as physical ones, the rise of the metaverse offers exciting opportunities as well as formidable challenges. As users delve into these expansive virtual worlds, the foundation element of their interactions – trust – becomes crucial for seamless integration into daily activities. The nature of data usage within the metaverse can vary greatly; it can be trusted, untrusted, or not utilized at all. Employing trusted data involves the responsible, ethical and secure management of information. This not only enhances the confidence of users and stakeholders but also enriches the overall metaverse experience, fostering a community where trust is paramount.

This technical report is dedicated to establishing a comprehensive understanding and outlining the essential components necessary for integrating trusted data within the metaverse to ensure its trustworthiness. The report starts by discussing three key aspects required to understand a trustworthy metaverse and conducts a comprehensive examination of characteristics of trusted data. It then outlines the essential groundwork needed to understand the symbiotic relationship that facilitates the use of trusted data in establishing and maintaining a trustworthy metaverse. Essential components proposed include strategies for the construction of trusted data, trusted data interactions, trusted execution environments, and trusted management policies.

Keywords

trustworthy metaverse; trusted data; data use

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1.0 of the ITU Technical Report on "*The essential components of trusted data use in building a trustworthy metaverse*" approved at the 7th meeting of the ITU Focus Group on metaverse (FG-MV) held on 12-13 June 2024.

Acknowledgements

This Technical Report was researched and written by Xiaoshuang Jia (Renmin University of China, China), Xiaomi An (Renmin University of China, China) and Jinfa Li (Renmin University of China, China) as contributors to the ITU Focus Group on metaverse (FG-MV). The development of this document was coordinated by Vincent Affleck (DSIT, United Kingdom), as FG-MV Working Group 6 Chair, and Gyu Myoung Lee (LJMU, UK) as Chair of Task Group on issues on trustworthiness related to the metaverse.

The editors extend their heartfelt thanks to Renmin University of China for its steadfast and unwavering support throughout the project. Additionally, thanks to Heung Youl Youm (Korea (Republic of)), Junhyung Park (Korea (Republic of)), Sungchae Park (Korea (Republic of)), Jaenam Ko (Korea (Republic of)), Da Eun Hyeon (Korea (Republic of)), Radia Funna (Build n Blaze, LLC), DongYang (China), Niu Li (China), Jia Xiaojun (Singapore), Yujue Wang (China), Jinghua Min (China), Meijie Zhang (China), Jie Huang (China), Miaomiao Kuang (China) for their valuable contributions.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.

Editor:	Xiaoshuang Jia Renmin University of China China	Tel: +86 15652635770 E-mail: jiaxs1219@sina.com
Editor:	Xiaomi An Renmin University of China China	E-mail: anxiaomi@ruc.edu.cn
Editor:	Jinfa Li Renmin University of China China	E-mail: ljf020607@ruc.edu.cn
Editor & TG Chair:	Gyu Myoung Lee LJMU United Kingdom	E-mail: gyumyoung.lee@gmail.com
WG6 Chair:	Vincent Affleck DSIT United Kingdom	E-mail: Vincentaffleck2@hotmail.com

Table of Contents

Page

Technical Report ITU FGMV-46

The essential components of trusted data use in building a trustworthy metaverse

1 Scope

The scope of this technical report is to establish a comprehensive understanding, and it outlines the essential components necessary for integrating trusted data within the metaverse to ensure its trustworthiness. The detailed scope includes:

- *Relationship Analysis:* This section provides a comprehensive examination of trustworthy metaverse and trusted data. It lays the essential groundwork needed to understand the symbiotic relationship that enables the use of trusted data to establish and maintain a trustworthy metaverse.
- *Essential Components:* This section discusses the utilization of trusted data within the metaverse. It identifies and elaborates on the essential elements for the effective integration of trusted data. These include trusted data construction, trusted data interaction construction, trusted execution environment construction, and trusted management policies construction.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 data [b-ITU-T FG-DPM0.1]: Representation of facts of objective reality in a formalized manner. Example: Data can be signs and symbols, and can be in analogue form, digital form or both.

NOTE – Data can be used for communication, interpretation or processing by human beings or automatic means.

3.1.2 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.3 Identity [b-ISO/IEC 24760-1]: Set of attributes related to an entity.

NOTE – Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.1.4 metaverse [b-ITU-T FGMV-20]: An integrative ecosystem of virtual worlds offering immersive experiences to users, that modify pre-existing and create new value from economic, environmental, social and cultural perspectives.

NOTE – A metaverse can be virtual, augmented, representative of, or associated with the physical world.

3.1.5 security assurance [b-ITU-T X.1404]: Grounds for justified confidence that a claim about meeting security objectives has been or will be achieved.

3.1.6 trust [b-ITU-T X.1252] [b- ITU-T FG-DPM0.1]: The reliability and truth of information or the ability and disposition of an entity to act appropriately, within a specified context.

3.1.7 trustworthiness [b- ISO/IEC 22989:2022, 3.5.16]: ability to meet stakeholder expectations in a verifiable way.

NOTE 1– Depending on the context or sector, and also on the specific product or service, data and technology used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

NOTE 2– Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality and usability.

NOTE 3– Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

3.2 Terms defined here

None

4 Abbreviations

This Technical Report uses the following abbreviations and acronyms:

AI Artificial Intelligence

CCPA California Consumer Privacy Act

GDPR General Data Protection Regulation

HSMs Hardware Security Modules

IEC International Electrotechnical Commission

ISO International Organization for Standardization

ITU-T ITU Telecommunication Standardization Sector

NFTs Non-Fungible Tokens

TCB Trusted Computing Base

TEE Trusted Execution Environment

5 Conventions

None

6 Relationship between trusted data and trustworthy metaverse

A total of 16 pertinent standards from ISO and IEC were seriously gathered and analysed. These standards are essential to enhance the understanding of the key aspects necessary for understanding a trustworthy metaverse and for conducting a comprehensive examination of trusted data. Detailed information of the standards is presented in Appendix A. The review of these documents provides a comprehensive understanding of the mutual benefits that trusted data and a trustworthy metaverse offer to each other. This analysis highlights the symbiotic relationship proposition of each, establishing the essential groundwork necessary for leveraging trusted data to build and maintain a trustworthy metaverse.

6.1 Overview of trustworthy metaverse

A trustworthy metaverse, as a complex digital ecosystem, comprehensively integrates essential aspects to ensure security, compliance and inclusivity. This integration defines the comprehensive requirements necessary for establishing a trustworthy metaverse, which include robust technical foundations, stringent legal frameworks, and thoughtful social considerations. By addressing these three essential aspects, the metaverse cultivates a trustworthy environment that not only enhances the user experience but also ensures adherence to ethical standards and legal requirements (see Figure 1).

For robust technical foundations, a trustworthy metaverse leverages advanced digital technologies to enhance functionality and elevate user engagement. For instance, it utilizes blockchain technology to ensure security and transparency, thereby creating a trustworthy environment. Artificial Intelligence (AI) is employed to create adaptive environments that respond dynamically to user interactions. Additionally, immersive technologies such as virtual and augmented reality are utilized to deliver compelling and engaging user experiences. Furthermore, the integrity of data is maintained meticulously, and robust encryption methods are implemented to protect user privacy and secure interactive spaces within the metaverse. These technical strategies are essential for fostering a safe and immersive digital ecosystem, thereby establishing a trustworthy metaverse.

For stringent legal frameworks, a trustworthy metaverse operates within a complex regulatory environment that spans international, national and local regulatory environment to safeguard user data and intellectual property, while simultaneously fostering innovation. It is crucial that these legal frameworks align with stringent data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This alignment ensures the privacy and security of personal data. Additionally, the legal frameworks should clearly define the rights associated with digital asset management and usage within the metaverse. By doing so, they create a well-regulated environment where users can have confidence in the legal system to protect their virtual interactions, thereby enhancing trust in the digital ecosystem.

For thoughtful social considerations, a trustworthy metaverse can actively cultivate an inclusive environment that promotes ethical interactions among its users. It is crucial to provide equitable access to all users, including those with disabilities, and to support diverse cultural expressions. This commitment to accessibility and diversity helps in building a genuinely inclusive digital ecosystem. Additionally, encouraging user participation and feedback in its governance processes can facilitate community-driven development, ensuring that the metaverse truly reflects the needs and values of its diverse user base. By prioritizing these social values, the metaverse transcends being merely a platform for entertainment, evolving into a community that respects and represents its global audience.

This integrated approach ensures that the metaverse transcends being merely a platform for engaging digital interaction. It becomes a secure, equitable, responsible and welcoming space that aligns with the ethical standards and legal requirements of a global audience. By harmonizing these elements, the metaverse fosters a truly trustworthy environment that supports a dynamic, inclusive, and ethical digital community, setting a standard for future digital ecosystems.

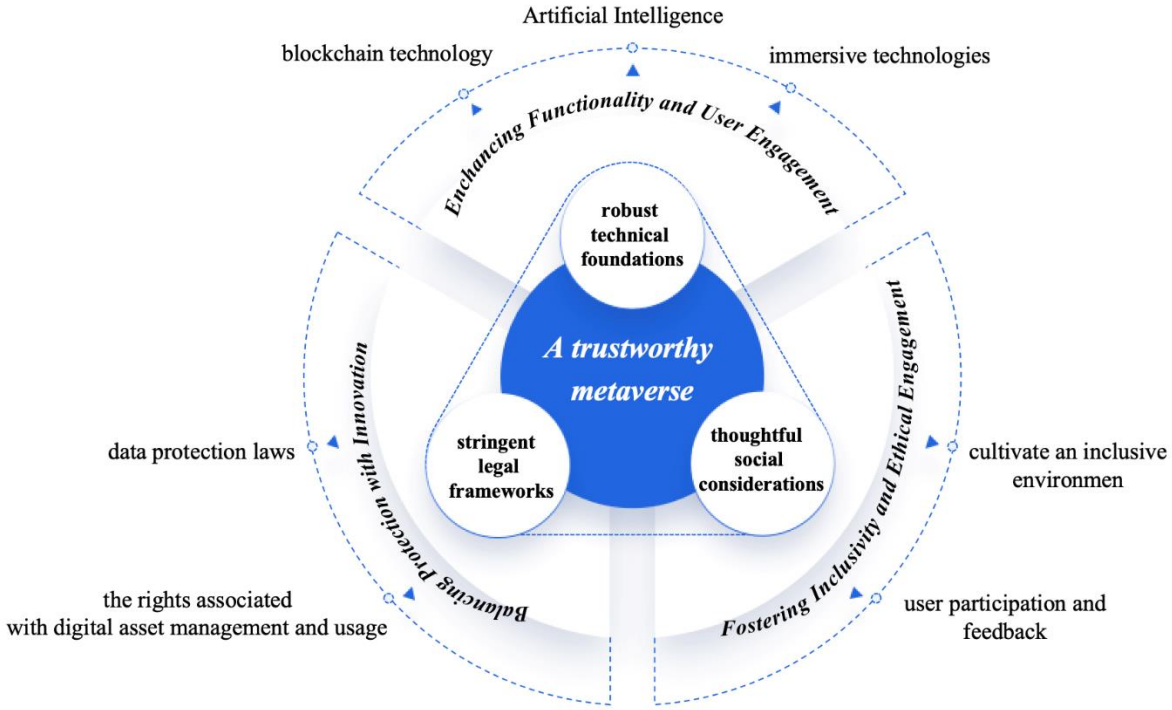

Figure 1 – Essential aspects of a trustworthy metaverse

6.2 Overview of trusted data

Understanding trusted data is crucial for maintaining the integrity and efficacy of digital systems and environments. Based on the analysis existing of standards and documents, trusted data embodies certain essential characteristics that ensure its reliability, security and utility across various applications and platforms. These attributes include:

- Accuracy: Data should accurately represent its source or the real-world phenomena it describes, ensuring decisions based on these data are valid.
- Authenticity: The origin of data should be verifiable, and it should be maintained over time without unauthorized alterations, preserving a traceable lineage.
- Availability: Data should be readily accessible to authorized entities when needed, facilitating its intended use without impediments.
- Compliance: Adherence to applicable legal, regulatory, and standards frameworks is critical, ensuring data use within ethical boundaries and legal stipulations.
- Confidentiality: Protects sensitive data from unauthorized access and exposure, crucial for maintaining privacy and trust.
- Integrity: Data should remain consistent, accurate, and reliable throughout its lifecycle, safeguarding against unauthorized changes.
- Reliability: Data should consistently provide a dependable basis for decision-making, supporting predictable outcomes.
- Security: Protective measures should be deployed to shield data against cyberthreats and vulnerabilities.
- Transparency: Clear communication regarding the methodologies used for data collection, processing, and management is essential for accountability. These attributes are fundamental for establishing and maintaining trust in digital interactions and operations.

It is critical to consider not only the inherent attributes of trusted data but also its comprehensive lifecycle management – including its creation, capture, storage, sharing and implementation. Effective lifecycle management ensures that data remain accurate, secure and useful throughout their usage. To ensure that data remain trustworthy throughout their lifecycle, they should be governed by trusted environments and policies, even as they move through various states and interactions. The environments in which the data operate should be equipped with advanced security technologies and measures, ensuring robust protection throughout the data's lifecycle. These measures are crucial for safeguarding the data's integrity and trustworthiness at every stage.

A Conceptual Model of Trusted Data is proposed (see Figure 2). This model takes a holistic process approach to ensure that throughout the data lifecycle – from creation to implementation – attributes of trusted data remain protected, reliable and compliant with established management policies in their execution environment. This comprehensive approach supports efficient and reliable operations, thereby creating a secure and trustworthy environment for user interactions.

By adhering to this conceptual model, the digital ecosystems are not only functional but also fundamentally secure and compliant. This commitment to the model cultivates an environment where trust, security and compliance are integral to the trusted data use, thereby enhancing the overall user experience and ensuring reliability. This model serves as a critical framework for developing digital infrastructures that prioritize data integrity and user trust.

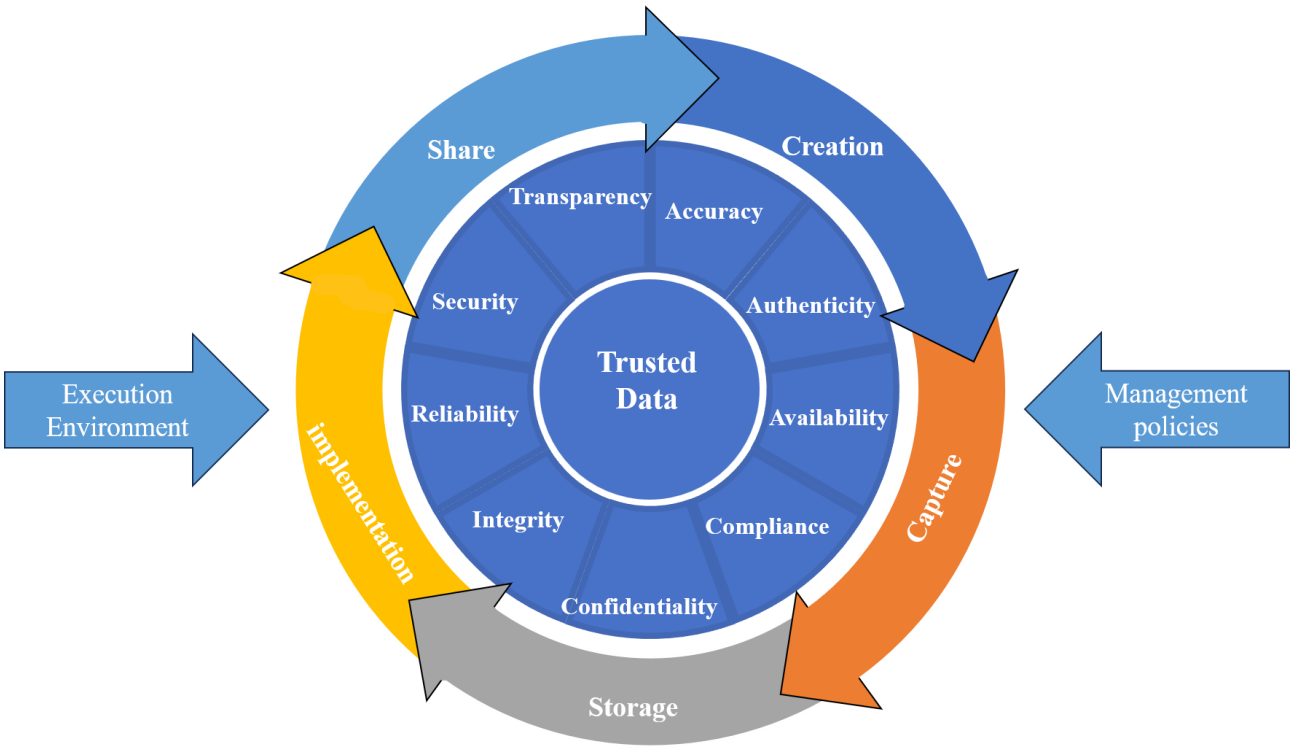

Figure 2 – The conceptual model of trusted data

6.3 Symbiotic relationship of trusted data and trustworthy metaverse

Trusted data and trustworthy metaverse share a symbiotic relationship, each enhancing the value and functionality of the other. Trusted data enhances the metaverse's functionality, security and reliability, thereby improving user confidence and engagement. Conversely, a well-regulated and secure metaverse ensures that the data remain protected and is used responsibly, further increasing its value and trustworthiness. This interdependence forms a virtuous cycle, where enhancements in one aspect strengthen the other, continuously improving both data integrity and the user experience within the metaverse. This dynamic interplay is crucial for fostering a digital environment where trust, security, and compliance are seamlessly integrated, enhancing overall user satisfaction and engagement.

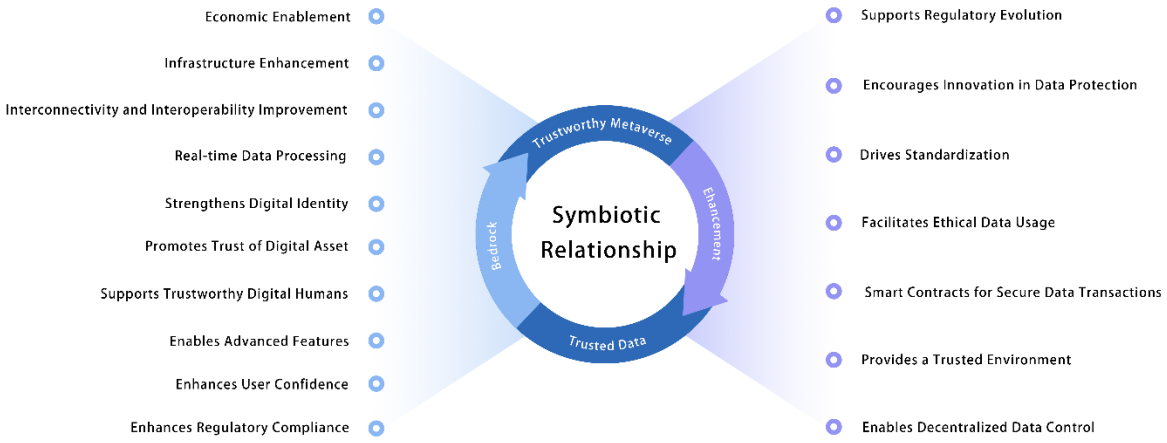

Figure 3 – Symbiotic relationship of trusted data and trustworthy metaverse

6.3.1 Functionality of trusted data to trustworthy metaverse

Trusted data serves as the bedrock upon which the security, functionality, and reliability of a trustworthy metaverse are built. Here are key ways in which trusted data adds value:

- **Economic Enablement:** Trusted data underpin the metaverse's digital economy by ensuring transparency in transactions and the secure exchange of digital assets like cryptocurrencies and non-fungible tokens (NFTs). It supports reliable, secure data handling, fostering innovative business models and sustaining economic growth.
- **Infrastructure Enhancement:** Trusted data fortify the foundational infrastructure of the metaverse by ensuring that network connectivity, computing resources, and storage operate securely and efficiently. This level of trust is crucial for maintaining high standards of data protection, preventing unauthorized access and ensuring consistent service delivery.
- **Interconnectivity and Interoperability Improvement:** While you touch on infrastructure, expanding on the specific role of trusted data in facilitating interoperability between different metaverse platforms could be insightful. Trusted data can ensure seamless and secure interactions across diverse systems, which is crucial for a unified metaverse experience.
- **Real-time Data Processing**: Mentioning the role of trusted data in real-time data processing and its implications for real-time decision-making could add another layer to its functionality. This is particularly relevant for dynamic environments in the metaverse where decisions and interactions occur instantaneously.
- **Strengthens Digital Identity:** By leveraging trusted data, digital identity management within the metaverse ensures user authentication and reduces impersonation risks. This fosters confidence in digital interactions, enabling secure and personalized experiences while safeguarding privacy.
- **Promotes Trust of Digital Asset:** Trusted data reinforces trust in digital assets like NFTs and cryptocurrencies through transparent, secure frameworks. It ensures asset authenticity and transaction traceability, enhancing confidence in digital economies.
- **Supports Trustworthy Digital Humans:** Trusted data ensure that digital humans within the metaverse can be represented accurately and can interact securely. By maintaining data integrity and implementing stringent privacy controls, it enables the digital humans that users can trust.

This trust facilitates meaningful interactions and ensures that users' digital identities are protected and used ethically in the metaverse.

- **Enables Advanced Features:** Trusted and reliable data allow for the deployment of advanced technologies such as AI and machine learning within the metaverse. These technologies can personalize and enhance user experiences, making the metaverse more engaging and interactive. For example, AI can be used to create dynamic content that adapts to user preferences, enhance virtual interactions, and provide predictive analytics to improve the overall user experience.
- **Enhances User Confidence:** When users are aware that their data are managed responsibly and with respect for privacy, their trust in the metaverse platform increases significantly. This trust is vital for user retention and engagement, encouraging users to interact more frequently and deeply within the platform. It also fosters a sense of community and loyalty, as users are more likely to return to a platform they trust.
- **Enhances Regulatory Compliance:** Adhering to trusted data practices ensures that the metaverse complies with international laws and regulations. This not only protects the platform from potential legal challenges but also reassures users that the platform is reputable and adheres to high standards of data protection. Compliance with regulations like GDPR, CCPA, and others helps avoid penalties and builds credibility with users and stakeholders alike.

By using trusted data, the metaverse can achieve higher levels of security, compliance, and user satisfaction, which are essential for its long-term success and scalability. This not only makes the metaverse more attractive to users but also to investors and developers looking to innovate within a stable and trusted framework.

6.3.2 Functionality of trustworthy metaverse to trusted data

A trustworthy metaverse significantly enhances the quality and reliability of trusted data, primarily by ensuring compliance with a broad spectrum of laws and regulations that span international, national, and regional jurisdictions. Compliance in the metaverse is not just a legal requirement, it is a crucial factor in building user trust. The dynamic and global nature of the metaverse necessitates agile compliance strategies that can adjust to evolving legal landscapes, ensuring continuous adherence without disrupting the metaverses operational dynamics.

- **Enables Decentralized Data Control:** The decentralized structure of a trustworthy metaverse, often built on blockchain or similar technologies, provides enhanced control over data ownership and access. This decentralized approach ensures data traceability, transparency, and protection against unauthorized changes.
- **Provides a Trusted Environment:** A trustworthy metaverse offers a secure and compliant environment for data processing, storage, and transmission. This trusted environment ensures that data integrity is maintained and aligns with global regulatory standards, thereby reinforcing the reliability and accuracy of data used across various applications.
- **Smart Contracts for Secure Data Transactions:** Smart contracts are an integral part of the metaverse, providing automated and secure transactions for data exchanges. These contracts enforce predefined rules for data sharing, thereby reducing errors and ensuring that data transactions adhere to agreed standards, fostering greater trust.
- **Facilitates Ethical Data Usage:** In a metaverse that maintains high ethical standards, data usage is governed by principles that ensure fairness, accountability, and transparency. This ethical commitment not only protects user data from misuse but also cultivates a culture of trust and respect. Such a culture is essential for the long-term sustainability of the metaverse as it encourages more engagement and investment from users who feel their values are reflected and respected.

- **Drives Standardization:** By establishing and adhering to stringent standards in data management and security protocols, a trustworthy metaverse promotes consistency in how data are handled across various platforms. This standardization enhances interoperability among different systems within the metaverse, reducing the risk of data breaches and ensuring a seamless user experience.
- **Encourages Innovation in Data Protection:** As the metaverse continues to evolve, it drives the need for innovative solutions in data protection. A trustworthy environment acts as a catalyst for the development of advanced data security technologies and management strategies. This innovation pushes the boundaries of what can be achieved in terms of data privacy and security, leading to more robust protection measures that can be adopted across industries.
- **Supports Regulatory Evolution:** Demonstrating effective data governance and compliance within a trustworthy metaverse sets a benchmark for regulatory bodies. It helps influence the development of future regulations by providing a practical model that regulators can observe. This influence is critical in shaping policies that more accurately reflect the complexities and unique challenges of virtual environments, ensuring regulations remain relevant and effective as the digital landscape evolves.

A trustworthy metaverse not only benefits its users and creators by providing a secure and ethical platform but also plays a pivotal role in enhancing the trustworthiness and utility of the data it generates and processes.

7 Essential components of trusted data use in building the trustworthy metaverse

Identifying the essential components for integrating trusted data into constructing a trustworthy metaverse involves addressing specific aspects crucial for the digital realm's security, privacy, and reliability. These aspects include trusted data construction, trusted data interaction, trusted execution environment, and trusted management policies. Each component is carefully tailored to meet the unique demands of the metaverse environment, ensuring comprehensive coverage of all necessary security and privacy measures. These essential components are depicted in Figure 4. Subsequent sections will detail each of these four essential components, highlighting their significance and implementation within a trustworthy metaverse.

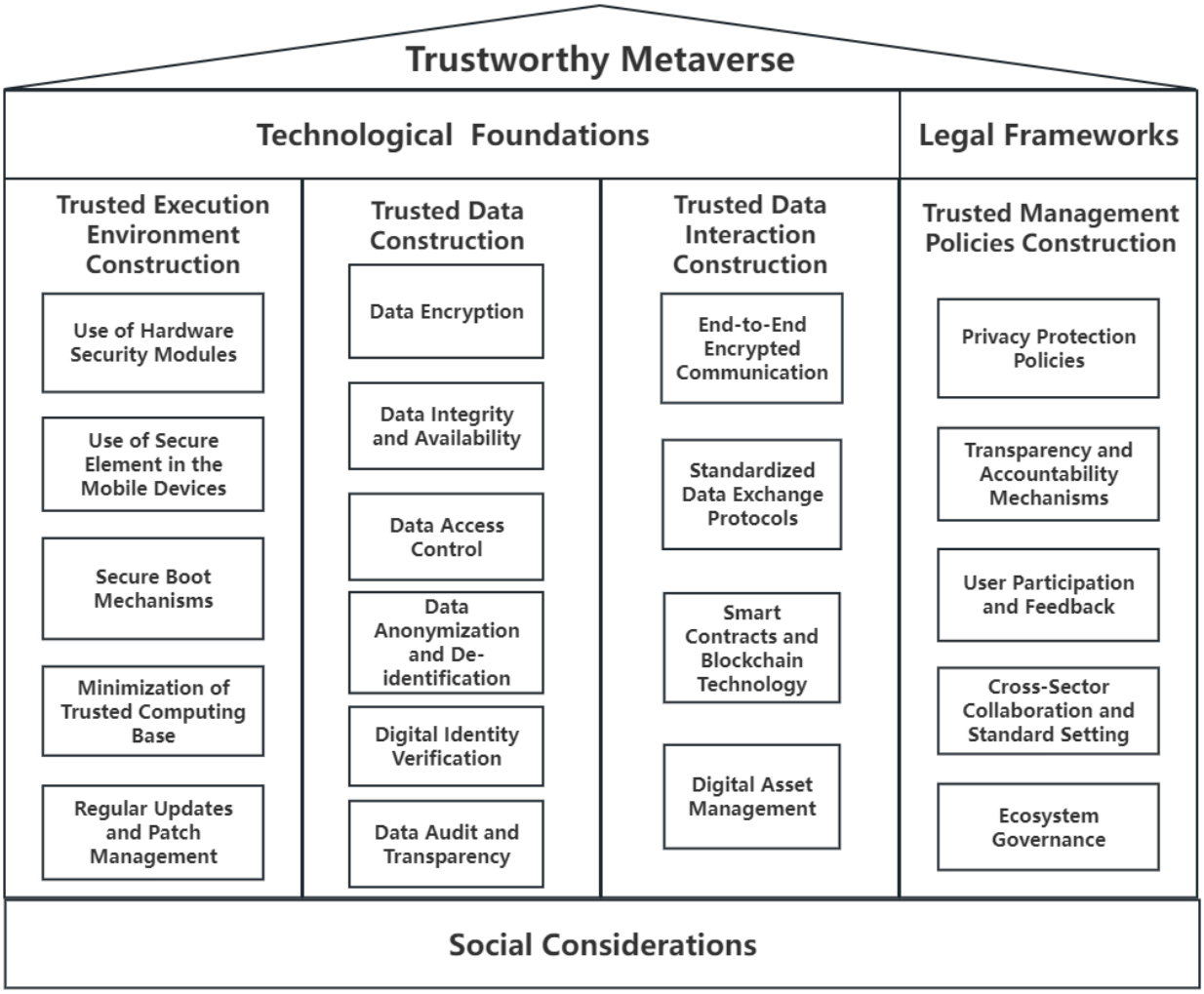

Figure 4 – Essential components of trusted data use in building a trustworthy metaverse

7.1 Trusted data construction in a trustworthy metaverse

Constructing trusted data are essential for ensuring the metaverse remains a secure, private and reliable digital realm. This segment is specifically designed to address the unique complexities of a trustworthy metaverse interactions and storage solutions. It focuses on upholding data integrity and confidentiality, which are essential for maintaining the trust and safety of users engaged in this expansive virtual environment. The approach integrates advanced techniques and technologies designed to protect data against unauthorized access and corruption, ensuring a robust foundation for metaverse operations. Below are the key aspects of trusted data construction that are crucial for ensuring a secure and trustworthy metaverse.

7.1.1 Data encryption

The purpose of utilizing robust encryption algorithms within a trustworthy metaverse is to secure data at rest and in transit. Encryption serves as a fundamental barrier, transforming sensitive data within a trustworthy metaverse into indecipherable formats that are accessible only to entities possessing the correct decryption keys. This practice is essential for maintaining the confidentiality and integrity of data in the metaverse, ensuring it remains protected from unauthorized access and tampering. By implementing strong encryption, the metaverse can establish a secure environment where user data are safeguarded, supporting a trusted and continuous virtual experience.

7.1.2 Data integrity and availability

The purpose of integrating data integrity and availability is to ensure that data remains unaltered and accessible to authorized users, thereby bolstering the security and reliability of the metaverse. By deploying mechanisms that preserve data integrity, we ensure that the data remain unaltered and genuine unless modified in an authorized manner. Simultaneously, ensuring data availability guarantees that these reliable data are accessible and usable upon demand by authorized entities.

7.1.3 Data anonymization, de-identification and pseudonymization

The purpose of data anonymization, de-identification and pseudonymization within a trustworthy metaverse is to protect user privacy and reduce compliance liabilities. These processes involve modifying personal data so that they cannot be associated with specific individuals, thus minimizing the risk of privacy breaches. Implementing these techniques effectively reduces the exposure of personal data, enhancing user trust and ensuring compliance with privacy regulations. This approach is critical in a trustworthy metaverse, where user interaction and data exchange are pervasive and sensitive data must be safeguarded to maintain a secure and trustful environment.

7.1.4 Data access control

The purpose of establishing granular access control policies within a trustworthy metaverse is to ensure that only authorized users can access sensitive information. By implementing detailed access control measures, which include defining clear permissions and roles, and utilizing robust authentication and authorization protocols, we can safeguard sensitive data effectively. These policies prevent unauthorized access and ensure that each user has access only to the information necessary for their role, thereby maintaining the security and integrity of the digital environment. This level of control is crucial for supporting a secure and trustworthy metaverse, where privacy and data protection are paramount.

7.1.5 Data audit and transparency

The purpose of maintaining an audit trail for data access and processing activities within a trustworthy metaverse is to ensure operational transparency and accountability. This involves systematically tracking and logging all data interactions to create a verifiable history that can be analysed for compliance, monitoring, and security purposes. Enhancing data transparency not only strengthens trust among stakeholders but also ensures that any unauthorized or suspicious activities can be promptly identified and addressed. By implementing robust audit mechanisms, the metaverse can uphold high standards of integrity and reliability, essential for fostering a secure and trusted virtual environment.

7.1.6 Digital identity verification

The purpose of implementing digital identity systems within a trustworthy metaverse is to secure user identities and facilitate safe interactions. This involves leveraging advanced technologies such as AI and machine learning for dynamic identity management and fraud detection. By using these technologies, the metaverse can ensure that all users are who they claim to be, greatly reducing the risk of impersonation and fraud. These systems are critical for maintaining the integrity of interactions within the metaverse, providing a secure foundation for users to engage confidently in various activities and transactions.

7.2 Trusted data interaction construction in a trustworthy metaverse

In the metaverse, maintaining the integrity of data interaction is paramount. Identifying the essential components for these interactions involves securing the pathways and protocols through which data are exchanged, ensuring that every transaction is secure and transparent. Here are the key aspects of trusted data interaction construction that are crucial for ensuring a secure and trustworthy metaverse.

7.2.1 End-to-End encrypted communication

The purpose of end-to-end encrypted communication within a trustworthy metaverse is to safeguard the privacy and integrity of data in transit. This method ensures that data are encrypted at their source and decrypted only by the intended recipient, making the data inaccessible to any intermediaries, including service providers. Such a mechanism is crucial for maintaining confidential and secure communications within a trustworthy metaverse, as it protects user data from eavesdropping and tampering during transmission.

7.2.2 Smart contracts and blockchain technology

The purpose of utilizing smart contracts and blockchain technology within a trustworthy metaverse is to provide a decentralized and transparent framework for data interactions. Smart contracts automate and enforce the terms of data exchanges without the need for a trusted intermediary, thereby streamlining operations and reducing potential for error or fraud. This combination significantly enhances the trustworthiness and auditability of data interactions, ensuring that they are executed precisely as agreed upon. This setup is vital for maintaining integrity and transparency in the complex ecosystem of the metaverse.

7.2.3 Standardized data exchange protocols

The purpose of adopting standardized protocols for data exchange within a trustworthy metaverse is to ensure compatibility and security across different systems and platforms. These protocols facilitate the efficient and secure transfer of data, supporting interoperability and seamless integration between diverse digital environments. Moreover, standardization promotes consistency and reliability in data interactions, which are essential for maintaining a trusted ecosystem. This ensures that all transactions and interactions within the metaverse occur smoothly and without discrepancies, reinforcing the overall security and user trust.

7.2.4 Digital asset management

The purpose of developing robust digital asset management systems within a trustworthy metaverse is to ensure the secure and efficient management, exchange and trade of digital assets such as NFTs and virtual goods. These systems are designed to make digital assets uniquely identifiable and securely exchangeable, while integrating them into the metaverse’s economic framework with clear ownership and rights management. Effective digital asset management supports a dynamic and thriving digital economy by providing a reliable infrastructure that ensures asset integrity and legal compliance, thereby fostering trust and engagement among users.

7.3 Trusted execution environment construction in a trustworthy metaverse

The establishment of a trusted execution environment (TEE) is pivotal in securing the foundational elements of a trustworthy metaverse, ensuring the safeguarding of its digital interactions and infrastructural integrity. A TEE provides a secure area of the main processor, where sensitive data can be processed in isolation from the rest of the system, thus providing a higher level of security against software attacks. This integration of various security measures spans hardware to software components, creating a robust defence against a wide range of threats and vulnerabilities. Here are the key aspects of a TEE that are crucial for ensuring a secure and trustworthy metaverse.

7.3.1 Use of hardware security modules

The purpose of implementing use of Hardware Security Modules（HSMs）within a trustworthy metaverse is to enhance the security management of cryptographic keys, which are fundamental to the metaverse's operations. HSMs act as a fortified hardware barrier, safeguarding sensitive operations and cryptographic key management from physical and logical threats. Their deployment is crucial for preserving the confidentiality, integrity and availability of critical data. By providing a secure environment for handling cryptographic operations, HSMs help ensure that key management

processes are isolated from other system operations, significantly reducing the risk of unauthorized access and data breaches. This robust protection is essential for maintaining trust and security within the expansive digital ecosystem of the metaverse.

7.3.2 Use of secure element in the mobile devices

Leverage secure element in the mobile devices, which is a chip that is protected from unauthorized access by design and is used to run restricted applications and store confidential and encrypted data. Smartphones and tablets, hardware cryptocurrency wallets, and other devices use cryptographic elements.

7.3.3 Secure boot mechanisms

The purpose of secure boot process within a trustworthy metaverse is to establish a verifiable and trusted computing environment from the initial system start-up. This critical security measure ensures the integrity of the metaverse's software stack by validating the digital signature of each component, ranging from the firmware to the operating system. By doing so, it guarantees that only authenticated and untampered software is loaded and executed. Such stringent validation is essential for protecting the system against potential threats by preventing the execution of unauthorized or malicious software, thereby maintaining a secure and reliable operating environment within the metaverse.

7.3.4 Minimization of trusted computing base

The purpose of streamlining the Trusted Computing Base（TCB) within a trustworthy metaverse by including only essential security-critical components is to reduce the system's exposure to potential attacks. This strategic minimization enhances the security posture of the TEE by limiting potential vulnerabilities and simplifying security management. By reducing the complexity and scope of the TCB, the potential attack surface is significantly decreased, thereby fortifying the trustworthiness of the metaverse’s operational environment. This focused approach ensures that each component within the TCB is necessary and justified, contributing directly to maintaining a secure and reliable digital infrastructure.

7.3.5 Regular updates and patch management

The purpose of regular updates and patch management within a trustworthy metaverse is to mitigate known vulnerabilities and enhance the security integrity of the TEE. An effective patch management protocol is crucial for ensuring that all components within the TEE remain resilient against evolving cyberthreats. By systematically updating software and applying security patches, the system can defend against the exploitation of recently discovered vulnerabilities, thereby maintaining a high level of security and trustworthiness. Regular updates also ensure that the TEE adapts to the latest security standards and practices, which is essential for safeguarding the metaverse’s operational environment from emerging threats.

7.4 Trusted management policies construction in a trustworthy metaverse

Trusted Management Policies Construction is a critical aspect of maintaining the integrity and reliability of the metaverse. These policies serve as the backbone of data governance, ensuring that data are used ethically, transparently and in compliance with regulatory standards. Establishing strong management policies is essential for fostering trust among users and maintaining the operational legitimacy of the metaverse. Here are the key policies in building trusted management policies.

7.4.1 Policy related to privacy protection

The purpose of developing comprehensive privacy protection policies within a trustworthy metaverse is to safeguard personal data and uphold user rights. These policies should clearly define how data are collected, used, stored and shared, adhering to stringent privacy standards and regulatory requirements. Establishing clear guidelines and obtaining informed consent from users are crucial steps in ensuring respectful and lawful handling of personal information. By implementing these

policies, the metaverse can demonstrate a commitment to privacy, enhancing trust and compliance with specific data protection regulations such as GDPR and CCPA. This approach not only protects users but also strengthens the integrity and credibility of the metaverse as a secure digital environment.

7.4.2 Policy related to transparency and accountability mechanisms

The purpose of establishing transparency and accountability mechanisms within a trustworthy metaverse is to provide users with clear insights into how their data are being used, processed and protected. This transparency, coupled with robust accountability measures, is essential for addressing any concerns or discrepancies in data handling. Such mechanisms enhance trust between users and metaverse providers by ensuring that data practices are open to scrutiny and that there are reliable processes in place to address and rectify any issues. By fostering an environment where users feel informed and in control of their data, the metaverse can build a stronger, trust-based relationship with its user community, ultimately enhancing the overall integrity and credibility of the platform.

7.4.3 Policy related to user participation and feedback

The purpose of encouraging active user participation in shaping data policies within a trustworthy metaverse is to foster a user-centric environment. By actively collecting and considering user feedback, policymakers can tailor data management strategies to better meet the community's needs and expectations. This collaborative approach not only improves the relevance and effectiveness of policies but also strengthens user trust and engagement. Engaged users are more likely to feel a sense of ownership and commitment to the platform, which enhances the overall health and sustainability of the metaverse. By integrating user insights into policy development, the metaverse can ensure that its operations remain aligned with user values and evolving digital rights.

7.4.4 Policy related to cross-sector collaboration and standard setting

The purpose of engaging in cross-sector collaboration within a trustworthy metaverse is to develop and enforce robust data security and privacy standards. This collaboration brings together various stakeholders from different sectors, facilitating the exchange of best practices and fostering innovation in policy formulation. Establishing a broad consensus on data management norms through such multistakeholder dialogues enhances the development of a comprehensive and coherent framework for trusted data management. By aligning with global standards and continuously engaging in these collaborations, the metaverse can ensure its data management policies are not only current but also forward-thinking, making the digital environment safer and more reliable for all users.

7.4.5 Policy related to ecosystem governance

The purpose of establishing ecosystem governance within a trustworthy metaverse is to preserve its integrity and reliability. These governance policies serve as the backbone of data governance, ensuring that data are used ethically, transparently and in compliance with regulatory requirements. Establishing management policies is essential for fostering trust among users and maintaining the operational legitimacy of the metaverse.

Appendix A
List of ISO, IEC standards relevant to trusted data and trustworthy metaverse

NO.	Standards	Year	SDOs	Related topics
1	ISO/IEC 15945:2002 Information technology — Security techniques — Specification of TTP services to support the application of digital signatures	2002	JTC 1	Trusted
2	ISO/IEC 11889-2:2015 Information technology — Trusted Platform Module Library — Part 2: Structures	2015	JTC 1	Trusted
3	ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)	2008	JTC 1	Trusted Data
4	ISO/IEC 13888-2:2010 Information technology — Security techniques — Non-repudiation — Part 2: Mechanisms using symmetric techniques	2010	JTC 1	Trusted Data
5	ISO/IEC 20008-1:2013 Information technology — Security techniques — Anonymous digital signatures — Part 1: General	2013	JTC 1	Trusted Data
6	ISO/IEC TR 23186:2018(en) Information technology — Cloud computing — Framework of trust for processing of multi-sourced data	2018	JTC 1	Trusted Data
7	ISO/IEC TS 19608:2018 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	2018	JTC 1	Trusted Data
8	ISO/IEC 20889: :2018 Privacy enhancing data de-identification terminology and classification of techniques	2018	JTC 1	Trusted data
9	ISO 19626-1 2020 Processes, data elements and documents in commerce, industry and administration — Trusted communication platforms for electronic documents— Part 1: Fundamentals	2020	ISO	Trusted Data
10	ISO 19626-2:2021(en) Processes, data elements and documents in commerce, industry and administration — Trusted communication platform for electronic documents — Part 2: Applications	2021	ISO	Trusted Data
11	ISO/TR 21186 -3:2021 Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards	2021	ISO/TR	Trusted Data
12	ISO/IEC 16363：2022 Space data and information transfer systems —	2022	JTC 1	Trusted Data

	Requirements for bodies providing audit and certification of candidate trustworthy digital repositories			
13	ISO/IEC 27553-1:2022 Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes	2022	JTC 1	Trusted Data
14	ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components	2022	JTC 1	Trusted Data
15	ISO/IEC 27556:2022	2022	JTC 1	Trusted data
16	ISO 22376 Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object	2023	ISO	Trusted Data

Bibliography

[b-ISO/IEC TR 23186]	International Standard ISO/IEC TR 23186：2018, Information technology — Cloud computing — Framework of trust for processing of multi-sourced data.
[b-ISO/IEC TS 19608]	International Standard ISO/IEC TS 19608: 2018, Guidance for developing security and privacy functional requirements based on ISO/IEC 15408.
[b-ISO/IEC 16363]	International Standard ISO/IEC 16363：2022, Space data and information transfer systems — Requirements for bodies providing audit and certification of candidate trustworthy digital repositories.
[ISO/IEC 13888-2]	ISO/IEC 13888-2:2010, Information technology — Security techniques — Non-repudiation.
[ISO/IEC 11889-2]	ISO/IEC 11889-2:2015, Information technology — Trusted Platform Module Library-Part 2: Structures.
[ISO 15489-1]	ISO 15489-1:2016, Information and documentation — Records management-Part 1: Concepts and principles.
[b-ISO/IEC TS 22237-7]	ISO/IEC TS 22237-7:2018, Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information.
[b-ISO/IEC 24760-1]	ISO/IEC 24760-1:2019, IT security and privacy – A framework for identity management – Part 1: Terminology and concepts.
[b-ISO/IEC TR 27550]	ISO/IEC TR 27550:2019, Information technology – Security techniques – Privacy engineering for system life cycle processes.
[b-ISO 17090-1]	ISO 17090-1:2021, Health informatics public key infrastructure Part 1: Overview of digital certificate services.
[b-ISO 19626]	ISO 19626-2:2021, Processes, data elements and documents in commerce, industry and administration-Trusted communication platform for electronic documents-Part 2: Applications.
[b-ISO 8000-2]	ISO 8000-2:2022, Data quality Part 2: Vocabulary.
[b-ISO/IEC 22989]	ISO/IEC 22989:2022,3.5.16, Information technology-Artificial intelligence-Artificial intelligence concepts and terminology.
[b-ISO/IEC 27002]	ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection-Information security controls.
[b-ISO/IEC 27556]	ISO/IEC 27556:2022, Information security, cybersecurity and privacy protection User-centric privacy preferences management framework.
[b-ISO/IEC/IEEE 32765]	ISO/IEC/IEEE 32675:2022, Information technology — DevOps — Building reliable and secure systems including application build, package and deployment.
[b-ISO 22376]	ISO 22376:2023, Authenticity, integrity and trust for products and documents-Authenticity, integrity and trust for products and documents-Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object.
[b-ITU-T TR Trust]	ITU-T Technical Report -- Trust in ICT (2017).

[ITU-T X.1058]	ITU-T X.1058(03/2017), Information technology - Security techniques - Code of practice for personally identifiable information protection.
[b-ITU-T FG-DPM 4.3]	Recommendation ITU-T FG-DPM 4.3(2019), Overview of technical enablers for trusted data.
[b-ITU-T FGMV-06]	Recommendation ITU-T FGMV-06 (2023), *Guidelines for consideration of ethical issues in standards that build confidence and security in the metaverse.*
[b-ITU-T FGMV-07]	Recommendation ITU-T FGMV-07 (2023), *Policy and regulation opportunities and challenges in the metaverse*.
[b-ITU-T FGMV-20]	Recommendation ITU-T FGMV-20 (2023), *Definition of metaverse.*
[b-ITU-T FGMV D.WG1-01]	Recommendation ITU-T FGMV D.WG1-01(2023), *Exploring the metaverse: opportunities and challenges.*
[b-ITU-T X.1252]	Recommendation ITU-T X.1252(2010), Baseline identity management terms and definitions.
[b-ITU-T Y.3052]	Recommendation ITU-T X.3052 (2017), Overview of trust provisioning for information and communication technology infrastructures and services.
[b-ITU-T X.1276]	Recommendation ITU-T X.1276(2018), Authentication step-up protocol and metadata Version 1.0.
[b-ITU-T Y.3053]	Recommendation ITU-T X.3053 (2018), Framework of trustworthy networking with trust-centric network domains.
[b-ITU-T Y.3054]	Recommendation ITU-T X.3054 (2018), Framework for trust-based media services.
[b-ITU-T X.1404]	Recommendation ITU-T X.1404(2020), Security assurance for distributed ledger technology.
[b-ITU-T Y.3055]	Recommendation ITU-T X.3055 (2020), Framework for trust-based personal data management.
[b-ITU-T Y.3057]	Recommendation ITU-T X.3057 (2021), A trust index model for information and communication technology infrastructures and services.