GBA

Government Blockchain Association
Identity Management Working Group

Blockchain
Maturity
Model

Supplement for Blockchain Identity Management Systems

Date: July 6, 2025
Version: 1.3

Approval

____________________ Director, Standards __________
Title Date

____________________ Identity Management Working Group Lead __________
Title Date

Contents

Introduction

1.1 Purpose

This document acts as a supplement to the Blockchain Maturity Model (BMM), for further reviews of solutions that are based on blockchains[1][2][3][4][5][6][7][8][9] supporting identity management systems (in all forms).

1.2 [Use]Use

When performing a BMM assessment of a blockchain identity management system, the lead assessor will review the supplemental requirements defined in this document with the Solution Point of Contact (SPoC), to determine which requirements are applicable as "Domain" requirements. When a solution meets the requirements defined in this supplement, it will receive an identity management designation on the BMM rating, which expands the scope of the assessment.

1.3 Assessment Ratings Considerations

BMM Supplement requirements are either satisfied or not satisfied. The supplement requirements are not expressed in terms of maturity levels. The supplement designation is appended to the BMM level achieved in the assessment.

[1] https://www.w3.org/TR/did-core/
https://www.itu.int/t/aap/recdetails/10295

[2] https://www.w3.org/TR/vc-data-model-2.0/

[3] https://www.iso.org/standard/82208.html

[4] https://www.iso.org/standard/80805.html

[5] https://www.iso.org/standard/81773.html

[6] In the context of "digital identity" solutions supported by blockchain technology, it is important to clarify that "decentralized identifiers (DIDs)" stored on the blockchain typically serve as unique cryptographic keys or addresses, rather than containers for personal identifiable information (PII). DIDs are designed to enhance privacy and security by acting as references to off-chain data, which may include verifiable credentials or attestations. The actual PII associated with a DID is often stored off-chain in secure and user-controlled repositories (i.e., Digital Wallets). This allows users to maintain control over their data, and selectively disclose them for sharing information on a need-to-know basis without revealing unnecessary details.

[7] https://www.iso.org/standard/75061.html

[8] Identity wallets may take various forms, such as dedicated hardware wallets, mobile applications, or even paper wallets (private keys are simply printed out and kept in a safe location). They may also come natively in a browser, an operating system, or as extensions. Wallets that are proposed "as a service" by a third-party holder that controls a user's private keys are called custodial wallets.

[9] *In the context of blockchain identity management systems, wallets can be considered as a type of service that manages digital identities and interacts with the blockchain.*
Wallets store private keys, which are used to sign transactions and prove control over associated digital identities. They also facilitate interactions with decentralized applications (dApps) and smart contracts on the blockchain.

[Use]

1.4 Terms & Definitions

See the annexes for diagrams, terms, and definitions used throughout this document.

1.5 References

This BMM supplement aims to provide guidance for assessing the maturity of Blockchain-based Identity Management Systems (BIMS). To achieve this purpose, the document primarily relies on the National Institute for Standard and Technologies (NIST) Cybersecurity White Paper "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020, available at https://doi.org/10.6028/NIST.CSWP.01142020. Additional references include publications issued by the International Organization for Standardization (ISO), International Telecommunications Union (ITU), and the World Wide Web Consortium (W3C).

1.6 Scope: Identity Management and Digital Identity

1.6.1 Identity Management

In accordance with the framework issued by ISO[10], "Identity Management" pertains to the *processes and policies involved in managing the lifecycle and value, type, and optional metadata of attributes in identities known in a particular domain.* The same framework further emphasizes that *identification applies verification to claimed or observed attributes,* as part of *interactions between an entity and the services in a domain and to access resources.*

1.6.2 Digital Identity

Digital identity refers to the online or digital representation of an individual's identity. It involves the collection and use of electronic credentials and attributes to establish and verify identity in digital transactions and interactions. Some of the most authoritative definitions of "digital identity" from the ITU, NIST, and W3C, are included in Annex A.

From the scope of the above definitions, it derives that digital identity management encompasses the entire process of managing and controlling access to resources based on the identity of users. It includes roles, policies, technologies, and processes used to ensure that the right people have the right access to the right resources at the right time.

1.6.3 Key characteristics, limitations, and risks of digital identity management solutions

As the reliance on digital platforms grows, understanding and assessing the reliability of the technologies supporting digital identity management systems becomes essential for ensuring the integrity and reliability of digital interactions and protection of privacy.

Considering the authoritative definitions of different organizations and initiatives[11], digital identities should be:

[10] ISO Technical Committee 292, https://www.iso.org/committee/5259148.html

[11] These organizations and initiatives include:

- Independent of service providers.
- Unique to the individual or entity[12] it represents.
- Verifiable, meaning that they can be linked back to the real-world entity they represent.
- Persistent, ensuring both availability and continuity.
- Portable.
- Transparent to the individual or entity it represents.
- User-controlled.
- User-consent.

The most common limitations and risks associated with digital identities include:

- Cybersecurity threats: Digital identities may be vulnerable to hacking, phishing, and other cyber threats. If not adequately protected, unauthorized access to digital identity information can lead to identity theft and fraud.

- Privacy issues and data breaches: Incidents of data breaches can compromise personal information, leading to privacy concerns. Organizations handling digital identities need robust measures to protect user data from unauthorized access.

- Centralized systems as single points of failure: Digital identity solutions could be centralized, relying on a single point of control. If the central authority is compromised, it could result in widespread identity theft or misuse.

- Lack of interoperability and fragmentation: Digital identity systems are often fragmented and lack interoperability. Users may need different credentials for numerous services, making the management of multiple digital identities cumbersome.

- Limited user control and consent: Users may have limited control over their digital identity, especially in systems where data is collected and managed by third parties.

- Identity theft and impersonation: Even with secure authentication methods, stolen credentials (such as passwords) can lead to identity theft.

- Quantum computing presents significant risks to blockchain technology primarily due to its potential to break the cryptographic algorithms that secure blockchain networks. Quantum

- World Economic Forum “MyData Global,” promoting user control over personal data and advocates for self-sovereign identity”.
- W3C Decentralized Identifiers (DIDs), emphasizing uniqueness, verification, and user control.
- World Bank “ID4D” initiative, stressing the importance of “reliable, inclusive, and affordable digital identities”, promoting uniqueness, persistence, and security.
- OECD and FATF Guidance on Digital Identity: Joint guidance emphasizing the need for digital identities to be "sufficiently reliable and independent" for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) purposes, highlighting aspects like independence and security.

[12] Per the definition of W3C, the term “entity” refers to persons, organizations, or devices (see Annex A, Glossary)

computers, with their ability to perform complex calculations at unprecedented speeds, could undermine the cryptographic foundations of blockchains, such as the RSA encryption and digital signature schemes.

- The complexity of blockchain technology can make it challenging for users to understand and manage their digital identities, potentially hindering the adoption of these solutions.
- Potential scalability and performance issues.
- Inclusion and accessibility (i.e., digital divide): Some individuals may lack access to digital technologies or face challenges in managing digital identities, leading to issues of exclusion and inequality, as well as the persistence of multiple systems or processes if a paper trail still is required to be maintained.
- Data quality issues: Digital identity systems may be affected by biases present in the data used to create them. Biases can lead to discrimination and unequal treatment based on inaccurate or incomplete information.
- Use of AI in feeding input to blockchains, particularly through Retrieval-Augmented Generation (RAG) optimization of the Language Model (LLM), could pose potential risks due to the technical complexity and scalability/performance limitations of blockchain systems, as well as interoperability, privacy, and biases issues.
- Technological obsolescence: As technology evolves, digital identity systems may become outdated. Hence, the need to determine how strategically agile is the vendor/solution/system in the event of identity revolution where the solution tech may be out of date.
- Regulatory compliance: Adherence to diverse legal frameworks and regulations concerning digital identity can be complex.
- Social engineering: Users may be susceptible to social engineering attacks, where attackers manipulate individuals to divulge sensitive information, posing a threat to the integrity of digital identities.

1.7 Blockchain Identity Management Systems[13] and Digital Identity

[13] NIST Cybersecurity White Paper A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (nist.gov), provides a comprehensive overview of blockchain identity management systems (IDMSs). The paper identifies and describes the key components, model, building blocks, and system architectures of blockchain IDMSs, and it also discusses the potential benefits and challenges of using blockchain technology for identity management.

The use of blockchain to manage digital identity introduces features that address some of the limitations and risks of traditional digital identity systems. BIMS are about the use of blockchain technology as "trust anchors"[14], to manage and secure digital identities, by offering:

- Decentralization, making blockchain-based digital identities more resistant to fraud and censorship.
- Immutability, ensuring that digital identities are tamper and reliable.
- Security, making blockchain-based digital identities less vulnerable to cyberattacks.
- Transparency and traceability, making it possible to audit and track the use of digital identities, preventing identity theft and other forms of fraud, while maintaining privacy of individual as well as adherence to applicable regulations.
- Self-sovereignty, enabling individuals to control their own digital identities.
- Interoperability, supporting interoperable digital identities that can be used across different platforms and applications, making it easier for individuals to use their digital identities to access a variety of services.
- Storing and verifying identity information[15] in a secure and decentralized manner, where it can then be verified by anyone who needs access to it, without the need of a central authority.
- Issuing and managing digital credentials, such as diplomas, degrees, and licenses. This can ensure that credentials are authentic and cannot be tampered with.
- Proving identity for access control to physical or digital resources, such as buildings, computers, and data.

Some examples of how blockchain technology is being used to support the self-sovereign-identity principles, include[16]:

[14] The concept of "blockchain" being a "trust anchor" of "identity management systems" is described in the ISO/TR 23644:2023 document, which provides an overview of trust anchors for DLT-based identity management systems. This document explains that blockchain and distributed ledger technologies (DLTs) can serve as trust anchors for identity management systems, ensuring the integrity and security of digital identities.

[15] Storing and verifying digital identity on blockchains is achieved through:
- Decentralized identifiers (DIDs): A type of digital identity that is stored on a blockchain and supports self-sovereign; and
- Verifiable credentials (VCs): A type of digital credential that is issued by a trusted entity and can be verified on a blockchain, used to prove an individual's identity, qualifications, or other attributes.

[16] Relevant examples of DLT supporting identity management systems are described in ISO/TR 23249:2022(E), *Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management*

- Alastria ID (https:// alastria .io/) - The digital identity project of the Identity Commission of Alastria, known as Alastria ID, a multi-sector consortium involving various partners, including large companies, SMEs, public administration, and academic institutions. The project is based on the Alastria digital identity model, which – at the time of writing - is considered a de facto standard and the basis of the formal UNE 71307 standard. It has also been raised to other international standardization bodies, such as CEN/CENELEC and the European Commission's self-sovereign identity initiative, ESSIF.

- Estonia: Although the Estonian electronic ID-Card system does not directly use blockchain technology, the electronic ID-card system used by the Estonian e-Health Record uses blockchain technology to ensure data integrity and mitigate internal threats to the data. (https://toolbox.estonia.ee/assets/423219)

- Known Traveler Digital Identity (KTDI, https:// ktdi .org/) - An initiative of the World Economic Forum, which aims to leverage advances in emerging technologies, such as blockchain and decentralized key management systems, to enhance the security capabilities in the travel continuum while improving the passenger experience.

- LACChain ID Framework (https://www.lacchain.net/home) - An initiative led by IDB Lab, which is part of the Inter-American Development Bank Group, with the goal of developing and promoting the use of blockchain technology in Latin America and the Caribbean. LACChain is built using Hyperledger Besu, an enterprise Ethereum client, and has become the world's largest public permissioned blockchain network, with participation from 15 countries. It supports over 190 nodes and more than 60 projects, many of which focus on financial and social inclusion. https://publications.iadb.org/en/lacchain-id-framework-set-recommendations-blockchain-based-interoperable-privacy-preserving

- Massachusetts Institute of Technology – The pilot "Digital Diploma" known as Blockcerts, uses blockchain technology to secure and verify academic credentials, which allows for the issuance and verification of blockchain-based certificates, ensuring the authenticity and integrity of the certificates (https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017)

- uPort (https://github .com/uport -project/ethr -did) - The City of Zug decentralized identity platform (uPort Serto App and SDK,), built on the Ethereum blockchain to enhance the efficiency, security, and user control of digital identities for residents.

- VON (https://github.com/bcgov/TheOrgBook)- The provinces of British Columbia and Ontario in Canada using the Verifiable Organizations Network (VON), designed to provide digital identity for businesses, creating a trusted digital network of verifiable data about organizations that is interoperable, secure, and easy to join. The foundational information about an organization is derived from British Columbia's Corporate Registry and is supplemented by various other "verifiable credentials" issued to TheOrgBook.

- WeIdentity (https:// fintech .webank .com/ en/ weidentity/ https:// fintech .webank .com/ en/ weid/) - A blockchain solution on Open Consortium Chain developed by WeBank. It serves as a hub for identity authentication by establishing the identity of entities, such as persons or objects, on the chain. The system allows for the interchange of such information among organizations when authorized. WeIdentity offers a complete set of W3C Verifiable Credentials based solutions designed to standardize and transform credentials into a verifiable and interchangeable format.

- Other examples include:
    - Dubai KYC platform: https://mediaoffice.ae/en/news/2021/June/27-06/Dubai-Economy-and-HSBC-strengthen-UAE-KYC-Blockchain-Platform
    - KUBE ID (KYC): https://www.kube-kyc.be/en/
    - RNS ID: https://rns.id/

1.8 Architecture models and core components of a Blockchain Identity Management System

The annexes of this document include further definitions, examples, and diagrams to further assist the assessment – or self-assessment – of BIMS. These annexes include:

Annex A: Graphical representation of main identity models

Annex B: Graphical representation of a Blockchain Identity Management System

Annex C: Mind map diagram of Identifier Architecture Design Models

Annex D: Mind map diagram of Credentials Architecture Design Models

Annex E: Key Components of a Blockchain Identity Management System, with definitions from ISO, ITU, NIST, and W3C

Annex F: AI and Depp Fakes Risks to Identities

1.9 Blockchain Identity Management Lifecycle

A blockchain identity management lifecycle encompasses the creation, management, and use of a self-sovereign identity solution that is anchored on a blockchain. This lifecycle involves several key components and steps, as outlined below:

(i) DID Creation: The DID owner generates a DID and publishes its DID document to the DLT. The DID document includes the DID owner's public keys, which are used to verify the authenticity of the DID and its associated VCs.
(ii) DID Management: The DID owner can manage their DID by updating the DID document, adding or revoking public keys, and associating new VCs. This process is typically done through dedicated DID management tools and applications.

(iii) VC Issuance: Trusted entities issue VCs to the DID owner, providing verifiable claims about the DID owner's identity or attributes. VCs are digitally signed by the issuer and linked to the owner's DID.

(iv) VC Presentation: The DID owner can present their VCs to relying parties to prove their identity or claims. Relying parties can verify the authenticity of VCs using the DID owner's public keys and the DID document.

(v) VC Verification: Relying parties verify the authenticity and validity of VCs presented by the DID owner. This involves checking the VC's signature, issuer's credentials, and the DID's validity using the DLT.

Blockchain & Digital Identity Management Use Cases

1.10 Cross-border identity verification

Blockchain can be used to verify identity across borders (travel, immigration, and financial services).

1.11 Vital records

Blockchain can be used to manage the issuance, storage, and release of vital records referring to official government documents that record important life events. These events typically include births, marriages, divorces, and deaths. Vital records are crucial for various legal, statistical, and genealogical purposes.

1.12 Proving identity for access control

Blockchain can be used to prove identity for access control purposes to physical or digital resources, including assets, buildings/infrastructure, computers, and data.

1.13 Issuing and managing digital credentials

Blockchain can be used to issue and manage digital credentials, such as diplomas, degrees, and licenses, to ensure that credentials are authentic and cannot be tampered with. Other use cases include social media identity, title/property/land registry, and intellectual property management.

1.14 Decentralized authentication

Blockchain can be used to provide decentralized authentication, which means that individuals can authenticate themselves without the need for a central authority for applications where security and privacy are critical, such as financial services and healthcare.

1.15 Self-Sovereign Identity (SSI)

Blockchain can be used to support SSI, which is a model of identity management where individuals have control over their own identity data. This means that individuals can own their own identity information and decide who has access to it.

1.16 Souldbound tokens (SBTs)

In the context of digital identity, SBTs can be used to store and verify personal data, credentials, and commitments in a decentralized and secure manner. They can serve as a digital resume, showcasing an individual's education, work history, and other achievements. SBTs can also be used to represent social relations, such as membership in a community or affiliation with an organization.

1.17 Voting and election

Blockchain can be used to secure and audit elections, to prevent voter fraud and ensure that elections are fair and transparent.

1.18 Supply-chain management

Blockchain can be used to track the authenticity and provenance of goods and products in the supply chain, preventing counterfeiting.

1.19 Healthcare

Blockchain can be used to store and share patient medical records (i.e., Medical Certificates related to permanent conditions) securely, improving the quality of care and protecting patient privacy.

1.20 Financial Services

Blockchain can be used to verify the identity of customers and transactions, preventing fraud, money laundering, and supporting KYC requirements.

Identity Management Solution Requirements

1.21 Confidentiality

The confidentiality requirement in digital identity management solutions pertains to the protection of personal identifiable information (PII) and other sensitive data from unauthorized access or disclosure.

The solution shall:

- **Provide encryption.**
- **Prohibit the disclosure of on-chain or off-chain information based on defined rules.**
- **Ensure that disclosure rules about user information are made available to users.**
- **Data minimisation**

1.22 Authentication

Authentication in a blockchain-based digital identity solution can be implemented using a combination of cryptography and distributed ledger technology.

The solution shall provide controls for the following steps:

- **Creation of the digital identity. The identity is typically represented by a public/private key pair. The public key is used to verify the user's identity, while the private key is used to sign transactions.**
- **Adoption of Zero-Knowledge-Proof (ZKP) technology.**
- **User registration of digital identities in a blockchain network. This process involves storing the user's public key on the blockchain.**
- **When the user wants to authenticate themselves to a service, they present their public key to the service.**
- **Multi-factor authentication.**
- **Service verification of the user's public key by checking it against the blockchain.**
- **Service issuance of a token to the user representing their authenticated identity.**
- **Procedures for the re-issuance of private keys in case of loss or destruction.**

Notes:

- Biometric Authentication is the process of verifying the identity of an individual based on their physiological or behavioral characteristics.

- ISO/IEC 24745:2022 – “Biometric information protection” provides guidance on the security and privacy of biometric information.

- According to the US National Institute for Standards & Technology (NIST), biometrics is the measurement of physiological characteristics like – but not limited to – fingerprints, iris patterns, or facial features that can be used to identify an individual. NIST has been conducting research in biometrics for over 60 years, with work on fingerprint technologies for the FBI to support law enforcement and forensics dating back to the 1960s.

- The security of authentication in blockchain-based digital identity solutions could be supported by:

A. Zero-knowledge proof: Zero-knowledge proof allows users to prove their identity without revealing their actual identity.

B. Homomorphic encryption: Homomorphic encryption allows data to be encrypted and then processed without decrypting it first. This can help to protect the confidentiality of sensitive data during processing. Core capabilities:

- Fully Homomorphic Encryption (FHE): Enables computation on encrypted biometric templates and credentials without exposing sensitive information.
- BGV Scheme Implementation: The Brakerski-Gentry-Vaikuntanathan scheme, based on Ring Learning with Errors (RLWE), provides practical FHE for identity management with manageable noise accumulation.
- Privacy-Preserving Verification: Allows authentication systems to verify identity claims against encrypted databases while maintaining complete confidentiality.

C. Secure hardware wallets: Secure hardware wallets are devices that store users' private keys in a secure manner.

D. Multi-Party Computation (MPC) enhances authentication security through distributed trust models:
Distributed Authentication Mechanisms:

- Threshold Authentication: Requires minimum number of parties to participate, providing robust protection against individual node compromise.
- Privacy-Preserving Consensus: Multiple identity providers jointly verify credentials without revealing individual contributions.
- Secure Identity Federation: Cross-domain verification where organizations validate claims without sharing sensitive authentication data.

1.23 Access Controls

The solution shall support access controls to restrict who has access to sensitive data. Access controls can be implemented at the user, group, and role levels.

Notes:

3rd Party Access[17] is the authorizing and providing external entities or organizations with access rights to specific resources or systems within a network. This access is granted to entities that are not directly involved in a transaction.

The solution may have "3rd Party Access" control rules for monitoring 3rd party access, ensuring compliance with security policies, which may include:

- Access Permission
- Authentication – The rules shall specify policy regarding the use of Multi-Factor-Authentication (MFA) by the 3rd party.
- Authorization
- Audit Trail
- Real-time Monitoring
- Compliance
- Data Encryption
- Periodic Access Reviews
- Incident Response
- User Activity Monitoring
- Training and Awareness
- Data Residency
- Data privacy
- Revocation and De-provisioning
- Notification – Describes when and how first and second parties are notified when third parties access data.

1.24 Access Notification

The solution shall include notification rules. Access notification is the function of notifying an entity when their record has been read from or written to the blockchain solution. Notification rules shall describe when and how first and second parties are notified when third parties access data for third-party users.

[17] Example:
- A user can grant a third-party access to their identity data by signing a verifiable credential (VC) with their private key. The VC can then be shared with the third party, who can verify it using the user's public key.
- A user can revoke access to their identity data by sending a revocation message to the third party. The revocation message can be signed with the user's private key to ensure its authenticity.
- A solution can offer a consent management system allowing users to grant and revoke access to their identity data to different third parties. The consent management system can be integrated with the digital identity solution to provide a seamless user experience. A digital identity solution can use self-sovereign identity principles to give users control over their own identity data.

1.25 Anonymity

The solution shall support anonymity through pseudonymization, encryption, and decentralization. Anonymity in an identity management system is the state of being unidentifiable. This means that the user's real identity is not linked to their digital identity.

- Pseudonymization is the process of replacing a user's real identity with a pseudonym. This pseudonym can then be used to interact with online services without revealing the user's real identity.
- Encryption is the process of scrambling data so that it cannot be read by unauthorized individuals. This can be used to protect a user's personal information, such as their name, address, and date of birth.
- Decentralization and distribution of data across multiple nodes. This can make it more difficult for attackers to track and identify users.
- Anonymity in a blockchain based identity solution is a characteristic that only provides selected information about an entity without revealing identifying information. Hence, the need to evaluate the criteria adopted to determine "On-chain" vs "Off-chain" data.

The solution shall also include safeguards and controls to mitigate the risk of de-anonymization.

Note:
- "Zero Knowledge Proof (ZKP)" is a method to ensure Anonymity. See Glossary for definition of ZKP.

- "Fully homomorphic encryption (FHE)" ensures the privacy and security of sensitive data while allowing for computations to be performed on encrypted data.

1.26 Integrity

The solution shall ensure the integrity of data and transactions through:

- Encryption
- Distribution
- Consensus mechanisms
- Hashing functions
- Digital signatures
- Merkle trees

Notes:

- Encryption: Mathematical techniques to encrypt and decrypt data (See previous note)
- Consensus mechanisms: Used to ensure that all nodes on the network agree on the state of the blockchain. This makes it difficult for unauthorized individuals to change the data stored on the blockchain.

- Hashing: A mathematical function that takes an input of any length and produces an output of a fixed length. The output of a hash function is called a hash value, hash code, or simply a hash.
- Merkle trees: Data structures that can be used to efficiently verify the integrity of data stored on the blockchain.

1.27 Encryption

The solution shall adopt and implement encryption mechanisms to:

- Protect the privacy of user data.
- Secure user identities.
- Ensure the authenticity of data.
- Facilitate transactions.

Note:
The main encryption methods used in blockchain are:

- Symmetric encryption: Uses the same key to encrypt and decrypt data. This is a simple and efficient way to encrypt data, but it requires that the key be shared between the sender and receiver of the data. This can be a security risk if the key is compromised.
- Asymmetric encryption: Uses two keys: a public key and a private key. The public key is used to encrypt data, and the private key is used to decrypt data. This makes it much more secure than symmetric encryption, as the private key is not shared with anyone else. However, it is also less efficient, as it requires two keys to encrypt and decrypt data.
- Hashing: A one-way encryption method that cannot be reversed. This means that data cannot be decrypted after it has been hashed. Hashing is often used to verify the integrity of data, as any changes to the data will result in a different hash value.
- Homomorphic encryption, which allows data to be encrypted and then processed without decrypting it first. This can help to protect the confidentiality of sensitive data during processing.

1.28 Availability

The solution shall ensure that users can access their digital identities when they need to conduct transactions and access services.

Availability is one of the three main pillars of cybersecurity, along with confidentiality and integrity. Availability refers to the ability of systems and data to be accessed by authorized users when needed.

Blockchains need to be able to withstand various threats, such as cyberattacks, data tampering, and network disruptions, to maintain the integrity and availability of the blockchain network. Resilience strategies like redundancy, access control, and tamper-evident logging can help blockchains defend against attacks and minimize the impact of failures. Additionally, blockchains must have well-designed recovery plans to quickly restore operations and recover data in the event of a system-wide failure or catastrophic event. This could involve mechanisms like secure data backups, multi-signature governance, and the ability to migrate assets across different blockchain networks.

1.29 Accountability

The solution shall support control mechanisms ensuring that users are responsible for their actions, to prevent fraud, improve security, and compliance.

Notes: There are several ways to ensure accountability in blockchain-based digital identity solutions, including:

- Using pseudonymous identities: Pseudonymous identities can be used to protect users' privacy while still allowing them to be held accountable for their actions. This is because pseudonymous identities are not linked to real-world identities.
- Using audit trails: Audit trails can be used to track and audit user activity. This can help to identify and investigate fraudulent or unauthorized activity.
- Using penalties: Organizations can implement penalties for users who violate the terms of service. This can help to deter users from engaging in fraudulent or unauthorized activity.

1.30 Auditability

The solutions shall support control mechanisms to track and record its own activity, which, in turn, can be independently tested and verified.

Auditability is an important consideration for any system that handles sensitive data or that is subject to regulatory requirements. Furthermore, the importance of real-time auditability for blockchains includes:

- Immutable Audit Trail: Blockchains create an immutable, tamper-evident record of all transactions that have occurred on the network. This provides a comprehensive audit trail that can be accessed and verified in real-time, unlike traditional accounting systems where audits are typically conducted periodically.
- Increased Trust and Transparency: The real-time auditability of blockchains enhances trust and transparency, as all participants can verify the integrity of the data and transactions.
- Continuous Monitoring and Auditing: Blockchains enable continuous monitoring and auditing, as the audit trail is updated in real-time with each new transaction (any type of transactions, not limited to financials). This allows for more frequent and thorough audits, reducing the risk of errors or fraudulent activities going undetected.
- Efficiency and Cost Savings: Real-time auditability can streamline the audit process, as auditors can access the entire transaction history directly from the blockchain, rather than relying on manual data collection and sampling. This can lead to significant cost savings and improved efficiency in the audit process.
- Regulatory Compliance: The real-time auditability of blockchains can help organizations meet regulatory requirements more effectively, as the audit trail provides a transparent and verifiable record of all activities.

1.31 Unique Identity

The solution shall ensure the issuance of unique digital identities and avoid the need for users to create multiple digital identities for different services or applications.

Note:
Unique identity is a basic requirement necessary to ensure that individuals can control their own identities, protect themselves from fraud, and improve the security of online transactions.

1.31.1 Independent Attestation

The solution shall have mechanisms whereby third-party can:

- Verify identity credentials.
- Generate a secure attestation record with cryptographic proof.
- Store relevant data on the blockchain.

Notes:

- Independent attestation refers to the process of verifying and validating an individual's identity and attributes by a defined trusted third party or authority that is separate and independent from the individual and the relying party. It involves the use of external entities to attest to the accuracy and authenticity of the information provided by the individual. These may include government agencies, educational institutions, employers, or other trusted entities that possess authoritative data about the individual. Independent attestation plays a crucial role in enhancing the trustworthiness and reliability of the identity management process by reducing the risk of fraud or misrepresentation. Through independent verification by trusted third parties, such as cross-referencing information with official records, conducting background checks, or employing other authentication mechanisms, organizations can attain a higher level of assurance. This becomes especially significant in scenarios involving regulatory compliance, financial transactions, or accessing sensitive resources, where organizations can rely on independent attestation to gain greater confidence in the accuracy and integrity of individuals' identities and attributes.
- Independent attestation may introduce additional complexities and dependencies in the identity management process, such as establishing secure connections with external authorities and managing the exchange of information. However, these challenges are often outweighed by the increased trust and reliability achieved through independent verification and attestation.

1.31.2 Self-Attestation

The solution shall support self-attestation by:

- Providing a tamper-proof record of identity data.
- Allowing users to control their own identity data.
- Providing a secure way to share identity data.
- Enabling the use of digital signatures.

Notes:

- Self-attestation, from an identity management perspective, refers to the process in which individuals or users assert or declare certain attributes or information about themselves, without requiring explicit verification or validation by a third party. It involves individuals taking responsibility for providing accurate and truthful information about their identity, attributes, or credentials.
- Self-attestation can be implemented in various scenarios, such as user registration processes, consent management, or when requesting access to certain resources or services. Users are typically required to provide information about themselves, such as their name, date of birth, address, or other relevant attributes. They affirm the accuracy and validity of the provided information by digitally signing or accepting the terms and conditions.
- While self-attestation allows for a more streamlined and user-centric approach to identity management, it does introduce a certain level of trust and potential risk. Organizations implementing self-attestation processes need to carefully consider the potential consequences of relying solely on user-provided information and shall have mechanisms in place to detect and mitigate fraud or misrepresentation. Additional layers of verification or authentication may be necessary in critical or high-risk scenarios to ensure the integrity of the identity management system.

1.32 Identity Verification

The solution shall support identity verification through different methods, such as:

- Document verification: This involves checking the authenticity of documents such as passports, driver's licenses, and birth certificates.
- Biometric verification: This involves using biometric data such as fingerprints, facial recognition, or iris scans to verify the identity of an individual.
- Knowledge-based authentication: This involves asking the individual questions about their personal information, such as their date of birth or mother's maiden name.
- Multi-factor authentication: This involves using two or more different methods to verify the identity of an individual, such as a password and a biometric scan.

Notes:

- Identity Verification is the process of comparing the identity of a person or entity claims compared to the supporting documentation or data. This process may include the verification of other claims/attributes related to gender, age, credentials, etc.
- Identity attribute verification is an important part of identity management, as it helps to ensure that only authorized individuals can access resources and systems. It can be used to verify the identity of individuals in a variety of contexts, such as when they are logging in to a computer system, applying for a job, or opening a bank account.
- The International Organization for Standardization (ISO) defines it as *“..the process of determining the correctness and validity of the identity attributes of an entity*." This

process typically involves checking that the required attributes are present, have the correct syntax, and exist within a defined validity period.

- See Annexes for a list of attributes and references.
- See Annex F: AI & Deep Fake Risks to Identities

1.33 Non-Repudiation

The solution shall support the non-repudiation of transactions using digital signatures and timestamps.

Non-repudiation is the assurance that the sender of a message cannot deny having sent the message or the recipient cannot deny having received the message.

Note: Non-repudiation is an important concept in cybersecurity because it helps to prevent fraud and other malicious activity

1.34 Key Management

The solution shall support key management.

Key management is the process of managing cryptographic keys. Cryptographic keys are used to encrypt and decrypt data, and they are essential for protecting sensitive information.

Notes:

There are several technologies that can be used to manage cryptographic keys in blockchain-based digital identity solutions, including:

- Public key infrastructure (PKI): PKI is a system for managing cryptographic keys. It uses a public key and a private key to encrypt and decrypt data. The public key is published for anyone to see, while the private key is kept secret.
- Hardware Security modules (HSMs): HSMs are physical devices that are used to store cryptographic keys. They are designed to be very secure, and they are often used to store the private keys of blockchain-based digital identity solutions.
- Key Management servers (KMS): KMSs are software applications that are used to manage cryptographic keys. They provide a centralized repository for keys, and they can be used to automate key management tasks.
- Multi-signature wallets (multisig): A way to recover keys and add security to keys in blockchains, utilizing multiple private keys to access and authorize transactions, rather than relying on a single private key. Multisig wallets enhance the security of blockchain-based assets by requiring multiple parties to authorize transactions.

- Shamir's Secret Sharing provides mathematically robust key management enhancing both security and availability with: (i) Threshold Cryptography: Divides cryptographic keys into multiple shares using polynomial interpolation, where any k-of-n shares can reconstruct the original key; (ii) Information-Theoretic Security: Provides perfect secrecy—fewer than threshold shares reveal nothing about the secret key regardless of computational power. (iii) Polynomial-Based Construction: Uses Lagrange interpolation over finite fields for mathematical security properties. Implementation in Identity Systems: Master Key Protection: Split master private keys across multiple secure locations, trusted parties, or hardware security modules. Distributed Recovery: Enables robust key recovery using any valid subset of shares, providing resilience against hardware failure or custodian unavailability. Trust Distribution: Key shares distributed among identity providers, family members, or institutional custodians eliminate single points of failure

- Hierarchical Deterministic (HD) Wallets for Secure Key Management: HD wallets, standardized in BIP32, provide advanced key derivation and management capabilities: Technical Architecture: Master Seed Derivation: Generate all keys from single master seed using BIP39 mnemonic phrase standard (2048-word list). Hierarchical Key Structure: Keys organized in tree structure using deterministic key derivation functions. Extended Key System: Generates extended private keys (xprv) and extended public keys (xpub) enabling secure derivation without exposing master private keys.

1.35 Data Privacy

The solution shall support controls for allowing users to control which information is revealed to a verifier.

Notes:

- ISO/IEC 18370-2:2016 specifies several blind signature mechanisms that can be used to achieve selective disclosure. These mechanisms are based on the discrete logarithm problem, and they provide an elevated level of security. This can be achieved through a variety of techniques, such as encryption, pseudonymization, and attribute-based access control.
- Selective disclosure allows the disclosure of required information in compliance with privacy standards and regulations. Examples of Selected Disclosure are:
  - Verifying age criteria without disclosing a birthdate.
  - Disclosing residence criteria without disclosing an address
  - Confirming educational credentials without disclosing grade performance.

1.36 Secure Communication

The solution shall be supported by secure communication controls, such as:

- Encryption: Encryption can be used to protect the confidentiality of data that is transmitted over the communication layer.
- Authentication.

- Authorization: Used to control who has access to specific data or resources.
- Intrusion detection and prevention systems: Intrusion detection and prevention systems (IDS/IPS) can be used to monitor the communication layer for suspicious activity.
- Firewalls: Used to restrict access to the communication layer from unauthorized sources.
- Using secure protocols: Transport Layer Security (TLS) and Secure Sockets Layer (SSL), can be used to protect the confidentiality and integrity of data that is transmitted over the communication layer.

1.37 Smart Contract Security

In those instances where the solution uses smart contracts, the solution shall include controls mechanisms to provide assurance on their reliability.
Smart contracts are self-executing contracts that are stored on a blockchain. They are written in code and can be used to automate a variety of tasks, such as transferring money, exchanging assets, and verifying identities. They can be programmed to trigger certain actions based on specific life events recorded in vital records.

Smart contract controls include:

- Smart contract auditing: The process of reviewing the code of a smart contract to identify potential security vulnerabilities.
- Formal verification: A mathematical technique that can be used to prove the correctness of a smart contract. This is a more rigorous approach to assurance than smart contract auditing.
- Code reviews: Used to identify potential security vulnerabilities in the code of a smart contract. This is a manual process that involves having a team of developers review the code for errors.
- Testing: To ensure that the smart contract functions as intended. This can be done by manually testing the contract or by using automated testing tools.
- Security assessments: Used to identify potential security vulnerabilities in a smart contract's environment. This includes the blockchain network, the smart contract's dependencies, and the hardware and software that is used to deploy and run the smart contract.

1.38 Scalability

The solution shall support control mechanisms for:

- High transaction throughput: The solution shall be able to handle a high volume of transactions because digital identity is often used in high-traffic applications, such as online banking and e-commerce.
- Low latency: The solution shall also have low latency because users expect to be able to verify their identities quickly and easily.

Notes:
Some of the scalability solutions that can be used to address the scalability requirements for blockchain-based digital identity solutions include:

- Sharding: A technique that divides the blockchain into smaller pieces, called shards, helping to increase the transaction throughput of the blockchain.
- Off-chain scaling: Off-chain scaling refers to moving some of the data and computations off the blockchain, reducing the load on the blockchain and improving scalability.
- Layer-2 scaling: Layer-2 scaling refers to building additional layers on top of the blockchain that can be used to process transactions off-chain and then submit the results to the blockchain.

1.39 Interoperability

The solution shall support control mechanisms for:

- Interoperability with other blockchains for allowing users to use their digital identities across different applications and platforms.
- Interoperability with traditional (legacy) identity systems for allowing users to use their digital identities in the real world.
- Interoperability with different standards for allowing different organizations to use the same digital identity solution.

Notes:
Some of the solutions that can be used to address the interoperability requirements for blockchain-based digital identity include:

- Standards: There are several standards that can be used to ensure the interoperability of blockchain-based digital identity solutions. These standards include the Decentralized Identity Foundation (DIF)'s Verifiable Credentials Data Model and the W3C's Decentralized Identifiers (DIDs).
- Protocols: There are several protocols that can be used to ensure the interoperability of blockchain-based digital identity solutions. These protocols include the DIF's DIDComm protocol and the W3C's WebAuthn protocol.
- Repositories: There are several repositories that can be used to store and share digital identities. These repositories include the DIF's Verifiable Credentials Repository and the W3C's DID Repository.

1.40 Compliance

The solution shall support control mechanisms to address applicable compliance requirements, including:

- Examples of data privacy regulations include:
  - European General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
  - Brazil's General Data Protection Law (LGPD)
  - India's Personal Data Protection Bill
  - Singapore's Personal Data Protection Act (PDPA)
- Data security regulations, such as the Payment Card Industry Data Security Standard (PCI DSS).

- Regulatory compliance, such as those governing financial services and healthcare.

Notes:

Some of the compliance solutions that can be used to address the compliance requirements for blockchain-based digital identity solutions include:

- Privacy-preserving technologies: These technologies include homomorphic encryption, zero-knowledge proof, and secure multi-party computation.
  Security protocols: These protocols include Transport Layer Security (TLS), Secure Sockets Layer (SSL), and OAuth 2.0.
- Regulatory frameworks: These frameworks include the GDPR, the PCI DSS, and the Health Insurance Portability and Accountability Act (HIPAA).

1.41 Human Centricity

The solution shall support a "human centricity" approach, based on:

- User control: Users shall have control over their digital identities. This means that users shall be able to create, update, and delete their digital identities as they see fit.
- Transparency: Users shall be able to understand how their digital identities are being used. This means that users shall be able to see what data is being collected about them and how that data is being used.
- Privacy: Users shall have the right to privacy. This means that users shall be able to control who has access to their digital identities and what data is being shared with them.
  - Security: Users shall be able to trust that their digital identities are secure. This means that users shall be confident that their data is not being tampered with or stolen.
- Accessibility: The solution shall be accessible to everyone and be available to people of all abilities.

Note:
Human-centric technology is a design approach that puts people at the center of the technology. It focuses on the needs of people and how technology can be used to meet those needs. Human-centric technology is about designing technology that is easy to use, accessible, and inclusive.

Annexes

Annex A: Identity Models

From NIST Cybersecurity White Paper *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (nist.gov)*

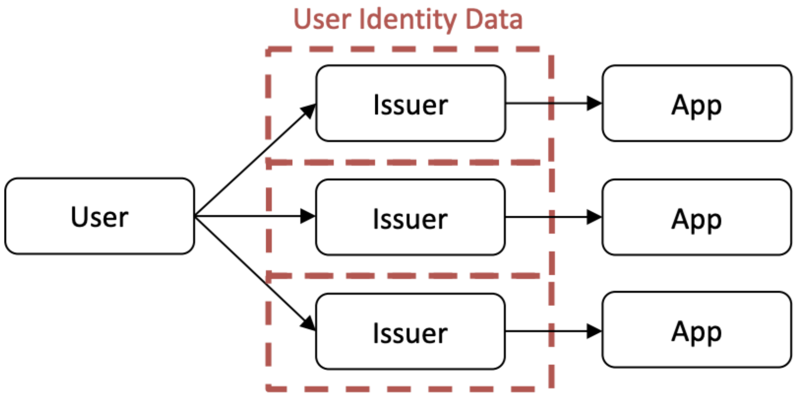


Figure 1: Traditional Identity Management

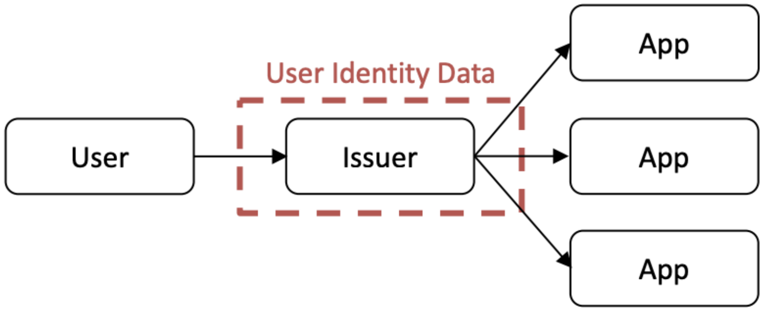


Figure 2: Federated Identity Management

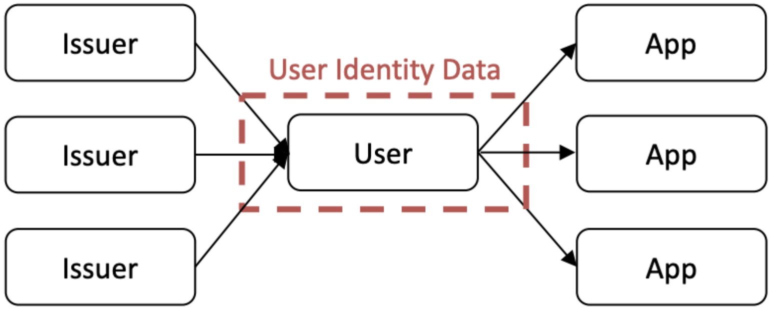


Figure 3: User-Centric Identity Management

Annex B: Blockchain Identity Management System

From NIST Cybersecurity White Paper “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (nist.gov)”

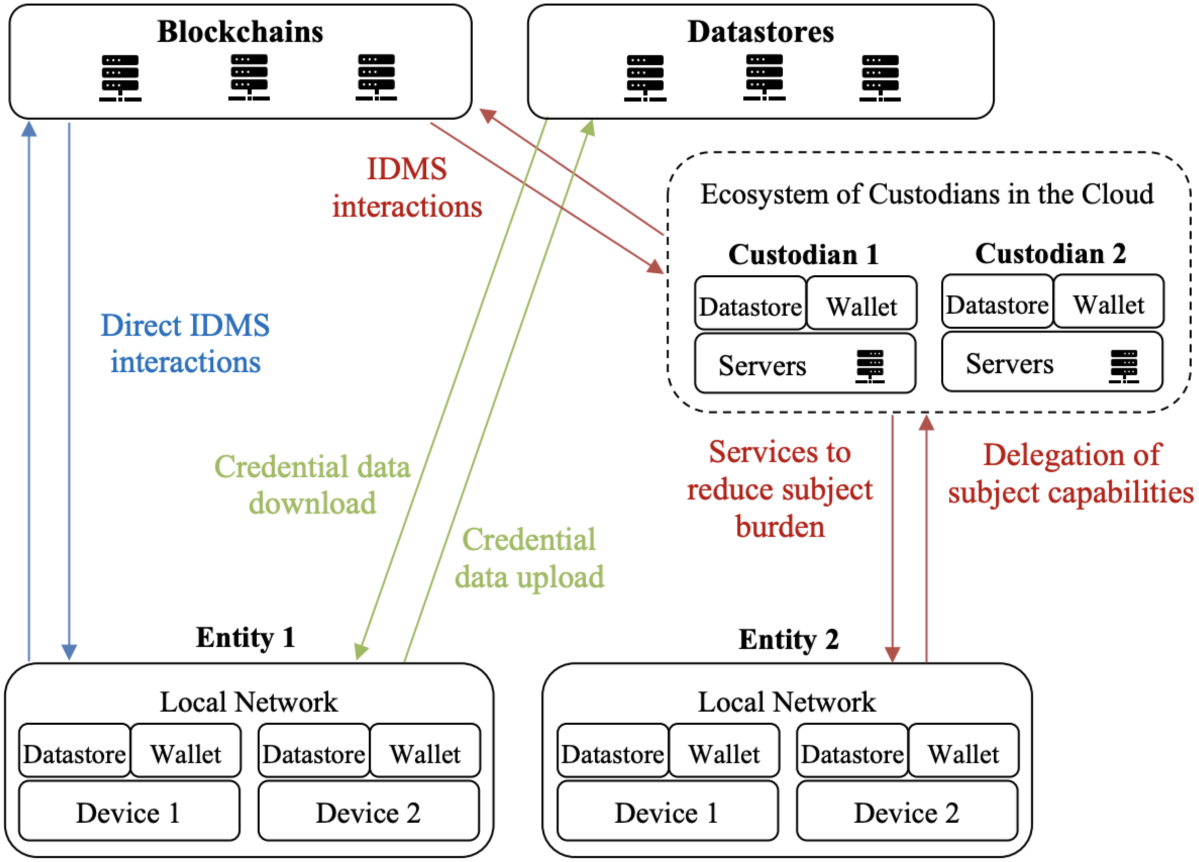
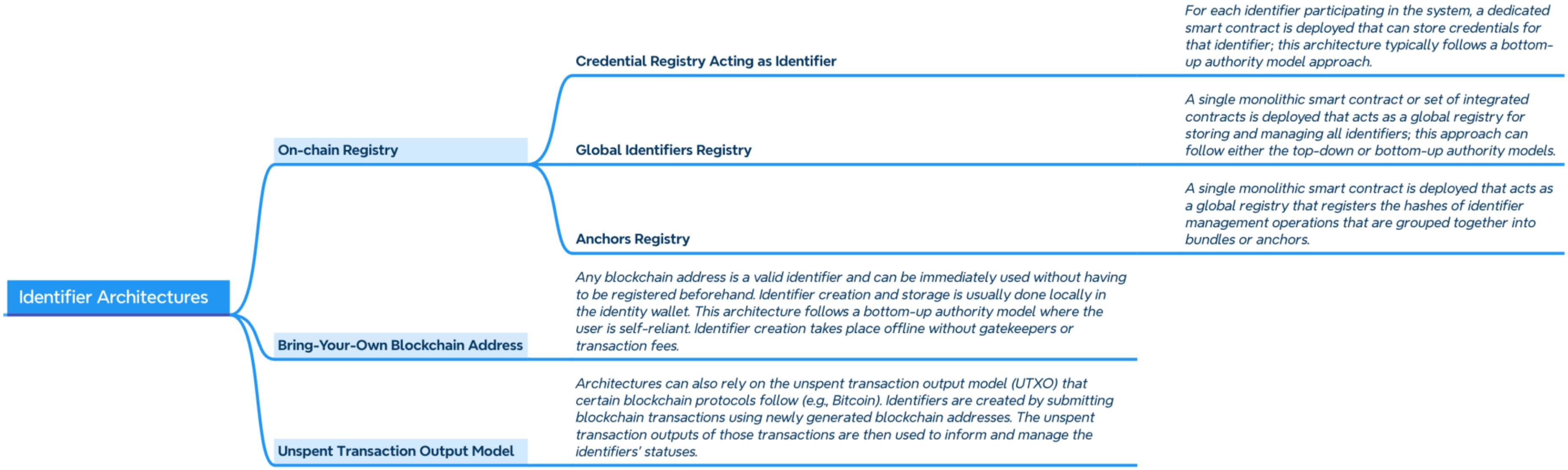


Figure 8: Interactions Between Subjects, Custodians, and Blockchains

Annex C: BIMS System – Identifier Architecture Design Models



Identifier Architectures

On-chain Registry

Credential Registry Acting as Identifier

For each identifier participating in the system, a dedicated smart contract is deployed that can store credentials for that identifier; this architecture typically follows a bottom-up authority model approach.

Global Identifiers Registry

A single monolithic smart contract or set of integrated contracts is deployed that acts as a global registry for storing and managing all identifiers; this approach can follow either the top-down or bottom-up authority models.

Anchors Registry

A single monolithic smart contract is deployed that acts as a global registry that registers the hashes of identifier management operations that are grouped together into bundles or anchors.

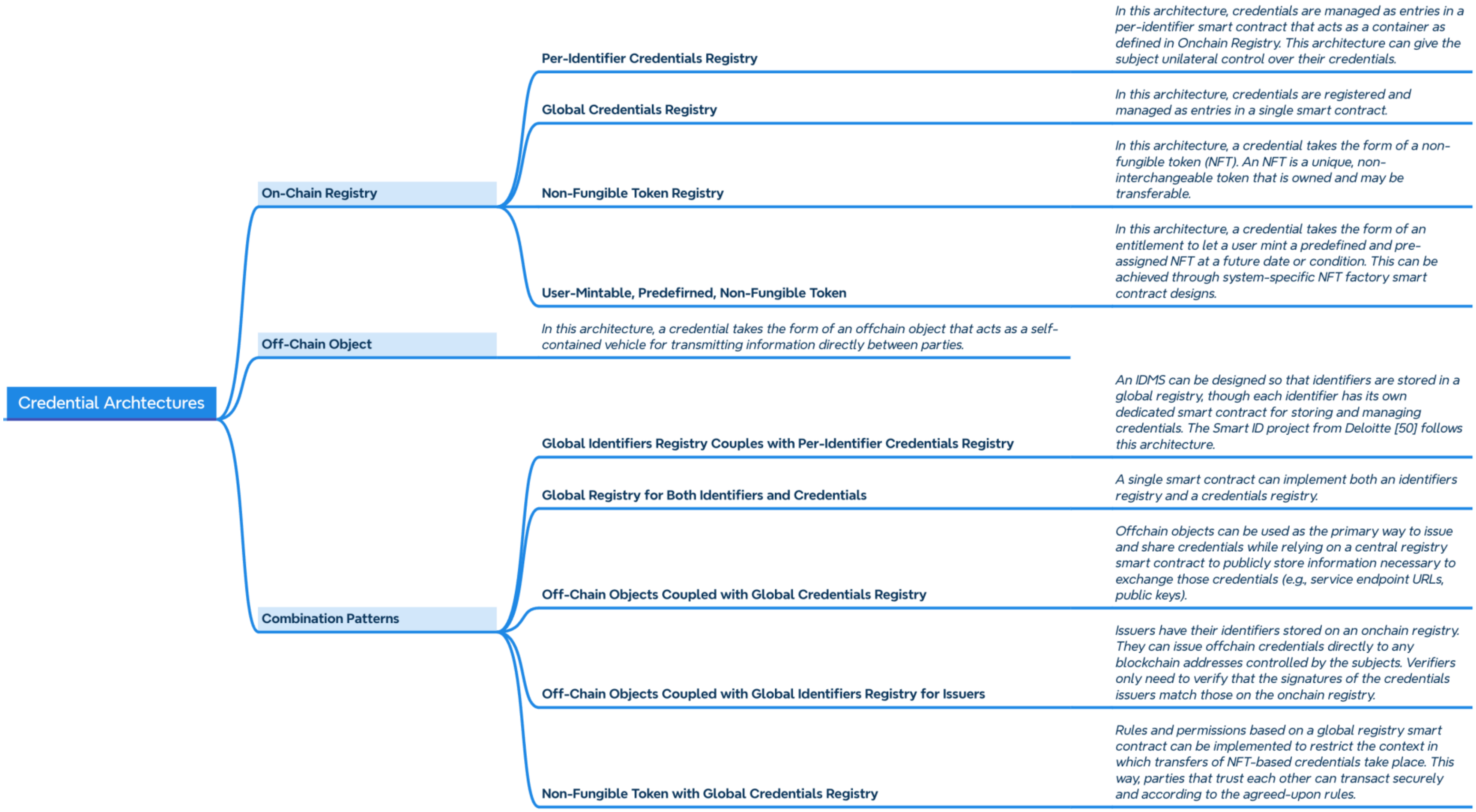
Bring-Your-Own Blockchain Address

Any blockchain address is a valid identifier and can be immediately used without having to be registered beforehand. Identifier creation and storage is usually done locally in the identity wallet. This architecture follows a bottom-up authority model where the user is self-reliant. Identifier creation takes place offline without gatekeepers or transaction fees.

Unspent Transaction Output Model

Architectures can also rely on the unspent transaction output model (UTXO) that certain blockchain protocols follow (e.g., Bitcoin). Identifiers are created by submitting blockchain transactions using newly generated blockchain addresses. The unspent transaction outputs of those transactions are then used to inform and manage the identifiers' statuses.

Annex D: BIMS System – Credentials Architecture Design Models



- Credential Archtectures
  - On-Chain Registry
    - Per-Identifier Credentials Registry — *In this architecture, credentials are managed as entries in a per-identifier smart contract that acts as a container as defined in Onchain Registry. This architecture can give the subject unilateral control over their credentials.*
    - Global Credentials Registry — *In this architecture, credentials are registered and managed as entries in a single smart contract.*
    - Non-Fungible Token Registry — *In this architecture, a credential takes the form of a non-fungible token (NFT). An NFT is a unique, non-interchangeable token that is owned and may be transferable.*
    - User-Mintable, Predefirned, Non-Fungible Token — *In this architecture, a credential takes the form of an entitlement to let a user mint a predefined and pre-assigned NFT at a future date or condition. This can be achieved through system-specific NFT factory smart contract designs.*
  - Off-Chain Object — *In this architecture, a credential takes the form of an offchain object that acts as a self-contained vehicle for transmitting information directly between parties.*
  - Combination Patterns
    - Global Identifiers Registry Couples with Per-Identifier Credentials Registry — *An IDMS can be designed so that identifiers are stored in a global registry, though each identifier has its own dedicated smart contract for storing and managing credentials. The Smart ID project from Deloitte [50] follows this architecture.*
    - Global Registry for Both Identifiers and Credentials — *A single smart contract can implement both an identifiers registry and a credentials registry.*
    - Off-Chain Objects Coupled with Global Credentials Registry — *Offchain objects can be used as the primary way to issue and share credentials while relying on a central registry smart contract to publicly store information necessary to exchange those credentials (e.g., service endpoint URLs, public keys).*
    - Off-Chain Objects Coupled with Global Identifiers Registry for Issuers — *Issuers have their identifiers stored on an onchain registry. They can issue offchain credentials directly to any blockchain addresses controlled by the subjects. Verifiers only need to verify that the signatures of the credentials issuers match those on the onchain registry.*
    - Non-Fungible Token with Global Credentials Registry — *Rules and permissions based on a global registry smart contract can be implemented to restrict the context in which transfers of NFT-based credentials take place. This way, parties that trust each other can transact securely and according to the agreed-upon rules.*

Annex E: Key Components of a BIMS, with definitions from ISO, ITU, NIST, and W3C

Decentralized Identifiers (DIDs) v1.0

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
Application Layer		*Application layer:* *This layer provides applications, e.g., the web services or decentralized applications, or network services, based on the Self-controlled identity (SCid). It provides service interfaces for direct interaction with the entities about the SCid, e.g., applying to create an SCid.*		
DLT/Blockchain	ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary *3.6 Blockchain* *Distributed ledger with confirmed blocks organized in an append-only, sequential chain using hash links.* ISO/TR 23249:2022 Blockchain and distributed ledger	*Distributed ledger* *[b-ITU-T X.1400]:* *A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.* *Blockchain* *[b-ITU-T X.1400]:* *A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and*	*Used to support the mapping of keys to identifiers by acting as an integrity-protected "bulletin board" for public key infrastructure (PKI). Blockchains may be application-specific, such as Hyperledger Indy, and/or may support native smart contract platforms.*	*Decentralized Identifiers (DIDs) v1.0* Distributed ledger *(DLT)* *A non-centralized system for recording events. These systems establish sufficient confidence for participants to rely upon the data recorded by others to make operational decisions. They typically use distributed databases where different nodes use a consensus protocol to confirm the ordering of cryptographically signed transactions. The linking of digitally*

[18] https://www.itu.int/t/aap/recdetails/10295

Core Components	ISO	ITU	NIST	W3C
		ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework[18]	*"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	*Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
	technologies – Overview of existing DLT systems for identity management In accordance with Section 5.3 "Functional role of DLT in identity systems", DLT could be used to: - Associate identifiers with public keys ("Decentralized PKI") - Attest credentials, similar to digital signature or timestamping on credential as found in traditional systems. - Support credentials revocation – Store common credential templates, supporting interoperability. - Act as trust anchors.	*hardened against tampering and revision.* *Identity layer: This layer is decentralized as it adopts blockchains as underlay storage. It provides services for SCid life-cycle management, SCid discovery and resolution management, and SCid data access control management. The layer includes multiple function blocks, i.e., for discovery, registry, endorsements, verification and data access management of the identity.*		*signed transactions over time often makes the history of the ledger effectively immutable.* Decentralized Identifiers (DIDs) v1.0 *Ref.* decentralized identifier *(DID)* *……..Many—but not all—DID methods make use of distributed ledger technology (DLT) or some other form of decentralized network.*
Infrastructure Layer		*This layer provides the networks and computing or storage resources for self-controlled identities and services (ITU Y.3081 Self-controlled identity based on blockchain: requirements and framework)*		

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
Decentralized Identifiers (DIDs)	ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary *3.18 Decentralized Identifier DID Identifier that is issued or managed in a decentralized system and designed to be unique within a context.* In accordance with ISO/TR 23644:2023(E) Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management *From a technical perspective.... verifiable, self-sovereign digital identifier is based on a type of identifier called a "decentralized identifier" (DID),...in technical terms, it is a URL, i.e. an identifier universal or uniform resource locator, with its own rules of syntax and processing, that relates a subject with a DID document, and which describes how such DID is used, and, in particular, how the DID document*	Decentralized identifier (*DID*) *[b-ITU-T X.1252]: A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network. A DID is associated with exactly one DID object descriptor.*	*Unique identifiers that serve as the public representation of the DID owner's identity. DIDs are stored () on the blockchain and can be used to verify the authenticity of the DID owner's credentials. They are unique identifiers that are not tied to a central authority. DIDs empower individuals with control over their own digital identities, allowing them to create, manage, and selectively disclose their identity information.*	*Decentralized Identifiers (DIDs) v1.0:* *A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically. The generic format of a DID is defined in 3.1 DID Syntax. A specific DID scheme is defined in a DID method specification. Many—but not all—DID methods make use of distributed ledger technology (DLT) or some other form of decentralized network.* *A Decentralized Identifier, or DID, is a URI composed of three parts: the scheme did:, a method identifier, and a unique, method-specific identifier specified by the DID method. DIDs are resolvable to DID documents. A DID URL extends the syntax of a basic DID to incorporate other standard URI components such as path, query, and fragment in order to locate a particular resource—for example, a cryptographic public key inside a DID document, or a resource external to the DID document (Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations)*

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
	supports the authentication of the subject associated with the DID.			
DID Document			*A JSON-based document that contains metadata about the DID, including the DID owner's public keys, authentication methods, and service endpoints. It is stored on the blockchain and can be accessed by anyone to verify the DID's validity.*	*Decentralized Identifiers (DIDs) v1.0:* *A set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID. A DID document might have one or more different representations as defined in 6. Representations or in the W3C DID Specification Registries [DID-SPEC-REGISTRIES].*
Verifiable Credentials (VCs)			*Claims about the identity of the DID's owner, such name, date of birth, or educational qualifications. VCs are issued by trusted entities and can be verified using the DID owner's public keys.*	*Decentralized Identifiers (DIDs) v1.0:* *A standard data model and representation format for cryptographically-verifiable digital credentials as defined by the W3C Verifiable Credentials specification [VC-DATA-MODEL].*
Second Layer Protocol		*The main purpose of L2 blockchain technology is to scale blockchain transaction capacity while retaining the benefits decentralization brings to a distributed protocol. Solving the scalability problem will significantly*	Used to: • *Build scaling solutions by offloading operations away from the blockchain layer (i.e., SideTree protocol); and*	

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
		help with blockchain's mainstream adoption. Layer 2 blockchain technology systems are those that connect to and rely on blockchain systems as a base layer of security and finality. L2 solutions include plasma, state channel, sharding, raiden network and lightening network (ITU F.751.2 Reference framework for distributed ledger technologies)	● *Help promote the development of interoperable, blockchain-agnostic systems.*	
Smart Contracts	ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary *3.88 Smart contract Computer program stored in a distributed ledger technology (DLT) system wherein the outcome of any execution of the program is recorded on the distributed ledger.*	*A smart contract can be used to operate the data stored in the blockchain…..The blockchain ledger is leveraged to record identity information for discovery, the reference of the data stored off-chain and digests of credentials and attestations. In the meantime, the smart contract can implement many functions formerly assumed by a traditional credential Service Provider (SP), such as ID registry and authentication.*	*Can be used to implement data processing logic.*	
Credentials Storage Methods	*ISO/TR 23244:2020(E) "Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations"*	*The blockchain ledger is leveraged to record identity information for discovery, the reference of the data stored off-chain and digests of credentials and attestations. In the meantime, the smart contract can implement many functions formerly*	*Storage of credentials can be implemented using a blockchain or off-chain. Off-chain credentials may be stored by a subject in a wallet application (i.e., Digital Wallet).*	Verifiable Credentials Data Model v2.0 - W3C Working Draft 26 January 2024: *8.13 Storage Providers and Data Mining* ….

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
	5.6.2.3 Off-chain storage *Where data is held off-chain, privacy and PII protection can be addressed by adopting the approach of ISO/IEC 29100.* *Blockchain and DLT systems typically use hashes of files to allow the actual data to be held off-chain whilst a record of the file, confirming the existence of the file at a certain moment in time and its provenance and authenticity and enabling verification of its integrity, is held on the blockchain*	*assumed by a traditional credential SP, such as ID registry and authentication. The blockchain enables the entity to control and manage its ID and credentials while leaving the SPs or networks to focus on authentication and verification.*	*There are both onchain and offchain credentials storage and management methods, though they present different usability, privacy, and security implications. Onchain credentials often only require onchain storage for the hashes of the credentials with the non-hash data being stored on any data store a subject has access to, be it a designated custodian or a decentralized storage system such as IPFS [40]. The integrity of the data may be checked by the receiving party by hashing the credential and comparing the hash with the one found on the blockchain. The hashes are often stored as state variables or blockchain logs, the latter being sometimes cheaper than onchain storage (e.g., Ethereum events).*	*When a holder receives a verifiable credential from an issuer, the verifiable credential needs to be stored somewhere (for example, in a credential repository). Holders are warned that the information in a verifiable credential is sensitive in nature and highly individualized, making it a high value target for data mining. Services that advertise free storage of verifiable credentials might in fact be mining personal data and selling it to organizations wanting to build individualized profiles on people and organizations. Holders need to be aware of the terms of service for their credential repository, specifically the correlation and data mining protections in place for those who store their verifiable credentials with the service provider. Some effective mitigations for data mining and profiling include using:* • *Service providers that do not sell your information to third parties.* • *Software that encrypts verifiable credentials such that a service provider cannot*

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *"A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
				view the contents of the credential. • *Software that stores verifiable credentials locally on a device that you control and that does not upload or analyze your information beyond your expectations.*
User-Controller Identity Wallet	*ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary* *3.100 Wallet:* *Application or mechanism used to generate, manage, store or use private keys and public keys or other digital assets.* *Note 1 to entry: A wallet can be implemented in software, implemented as a hardware module, or written onto non-digital media such as paper or metal*	*Wallet (identity wallet) [b-ITU-T X.1252]: An application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys on the user device.*	*A user-controlled identity wallet is an application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys. It also serves as an interface for entities to interact with one another.* *Identity wallets can act as control centers since entities can receive and decide whether to approve requests for verifiable information, thereby giving their consent to perform some action.*	*Decentralized Identifiers (DIDs) v1.0:* *Services:* *Means of communicating or interacting with the DID subject or associated entities via one or more service endpoints. Examples include discovery services, agent services, social networking services, file storage services, and verifiable credential repository services.*
User Profile Data Management Protocols			*External protocols used for managing user profile data with blockchain-based IDMSs to control access rights to that data. With such protocols, user profile data created when using an application*	

Core Components	ISO	ITU *ITU-T Y.3081, Self-controlled identity based on blockchain: Requirements and framework*[18]	NIST *“A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems”, dated January 12, 2020*	W3C *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations, 19 JULY 2022; and* *Verifiable Credentials Data Model v2.0*
			would not have to be stored by the application itself. Instead, users could rely on encrypted vaults and decentralized storage protocols.	
Data Exchange Models			*To request, issue, disclose, and verify credentials and/or presentations (e.g., for authentication), blockchain-based IDMSs commonly leverage data exchange formats such as JSON, JWT, Security Assertion Markup Language (SAML), and eXtensible Data Interchange (XDI).*	
Application Libraries and Interfaces			*Application libraries and APIs that facilitate the integration of applications supporting various identity management roles (e.g., requester, issuer, relying party, and verifier roles).* ￼	
Infrastructure layer		*Infrastructure layer: This layer provides the networks and computing or storage resources for self-controlled identities and services.*		

Annex F: AI & Deep Fake Risks to Identities

1. Synthetic Identity Fraud

Threat: AI can be used to create fake but believable identities using a blend of real and fabricated data.
Potential Mitigations:

- Use **identity verification platforms** that incorporate device fingerprinting and behavioral biometrics.
- Implement **document verification with cryptographic validation** (e.g., ePassports, verifiable credentials).
- Cross-check against **authoritative sources** (e.g., government or credit databases).

2. Deepfake Impersonation

Threat: Attackers may use AI-generated video or audio to impersonate real people.
Potential Mitigations:

- Deploy **liveness detection** in video and voice recognition systems (e.g., detecting eye blinks, 3D depth, challenge-response).
- Require **multi-factor authentication (MFA)** beyond biometrics—such as physical security keys.
- Use **context-aware verification** (e.g., time, location, or device-based access patterns).

3. Credential Phishing Automation

Threat: AI can be used to craft convincing phishing messages mimicking real contacts.
Potential Mitigations:

- Implement **zero-trust policies** that verify all user and system behaviors continuously.
- Train users with **realistic phishing simulations** and **AI-generated threat awareness**.
- Use **email authentication protocols** (SPF, DKIM, DMARC) and **secure email gateways** with AI threat detection.

4. Bypassing Biometric Authentication

Threat: Deepfakes can be used to spoof facial/voice recognition systems.
Potential Mitigations:

- Require **multi-modal biometrics** (e.g., face + voice + fingerprint).

- Employ **anti-spoofing algorithms** that detect replay attacks, anomalies, or static imagery.
- Prefer **on-device biometric processing** with secure hardware elements (e.g., Apple Secure Enclave).

---

5. Undermining Trust in Digital Evidence

Threat: Authentic media is questioned due to rise of deepfakes.
Potential Mitigations:

- Adopt **digital content provenance** standards (e.g., C2PA, Project Origin).
- Use **timestamped cryptographic signatures** and **decentralized ledgers** to track source authenticity.
- Require **chain-of-custody metadata** in legal and regulatory contexts.

---

6. Scalability of Attacks

Threat: AI allows low-cost, mass-scale identity-based attacks.
Potential Mitigations:

- Employ **AI-driven fraud detection** that monitors large-scale behavioral anomalies.
- Use **rate limiting and bot detection** tools to stop automated abuse.
- Conduct **continuous identity risk assessments** across users and endpoints.

---

7. Reputation Hijacking

Threat: Deepfakes may be used to damage reputations or manipulate events.
Potential Mitigations:

- Create **public incident response protocols** for identity or media compromise.
- Offer **media verification tools** (e.g., forensic analysis or reverse video/image search).
- Establish **legal frameworks** and **platform accountability** for deepfake misuse.
