A picture containing text, clipart

Description automatically generated

Government Blockchain Association  
Identity Management Working Group

Text

Description automatically generated with medium confidence

Decentralized Identity Management Supplement

|  |  |
| --- | --- |
| Date: | November 13, 2023 |
| Version: | 0.2 |

**Approval**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Director, Standards | |  |  |
| Meiyappan Masilamani |  | Title |  | | Date |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Identity Management Working Group Lead | |  |  |
| Dino Cataldo Dell’Accio |  | Title |  | | Date |

© 2023 Government Blockchain Association (GBA)

Contents

[1 Introduction 1](#_Toc150633264)

[1.1 Purpose 1](#_Toc150633265)

[1.2 Scope: Decentralized Digital Identity 1](#_Toc150633266)

[1.2.1 Directory Services 1](#_Toc150633267)

[1.2.2 Self-sovereign identity (SSI) 1](#_Toc150633268)

[1.2.3 Decentralized identifiers (DIDs) 1](#_Toc150633269)

[1.3 Use 2](#_Toc150633270)

[1.4 Assessment Ratings Considerations 2](#_Toc150633271)

[2 Terms & Definitions 2](#_Toc150633272)

[3 Blockchain & Digital Identity Management Use Cases 2](#_Toc150633273)

[3.1 Cross-border identity verification 3](#_Toc150633274)

[3.2 Vital records 3](#_Toc150633275)

[3.3 Proving identity for access control 3](#_Toc150633276)

[3.4 Issuing and managing digital credentials 3](#_Toc150633277)

[3.5 Decentralized authentication 3](#_Toc150633278)

[3.6 Self-Sovereign Identity (SSI) 3](#_Toc150633279)

[3.7 Voting and election 3](#_Toc150633280)

[3.8 Supply-chain management 3](#_Toc150633281)

[3.9 Healthcare 3](#_Toc150633282)

[3.10 Financial Services 3](#_Toc150633283)

[4 Identity Management Solution Requirements 4](#_Toc150633284)

[4.1 Security 4](#_Toc150633285)

[4.1.1 Confidentiality 4](#_Toc150633286)

[4.1.2 Authentication 4](#_Toc150633287)

[4.1.3 Access Controls 5](#_Toc150633288)

[4.1.4 Access Notification 5](#_Toc150633289)

[4.1.5 Anonymity 6](#_Toc150633290)

[4.1.6 Encryption 6](#_Toc150633291)

[4.1.7 Integrity 7](#_Toc150633292)

[4.1.8 Availability 7](#_Toc150633293)

[4.1.9 Accountability 7](#_Toc150633294)

[4.1.10 Auditability 8](#_Toc150633295)

[4.1.11 Authenticity 8](#_Toc150633296)

[4.1.12 Unique Identity 8](#_Toc150633297)

[4.1.13 Independent Attestation 8](#_Toc150633298)

[4.1.14 Self-Attestation 9](#_Toc150633299)

[4.1.15 Identity Verification 9](#_Toc150633300)

[4.1.16 Non-Repudiation 10](#_Toc150633301)

[4.1.17 Key Management 10](#_Toc150633302)

[4.1.18 Data Privacy 11](#_Toc150633303)

[4.1.19 Secure Communication 11](#_Toc150633304)

[4.1.20 Smart Contract Security 12](#_Toc150633305)

[4.2 Scalability 12](#_Toc150633306)

[4.3 Interoperability 13](#_Toc150633307)

[4.4 Compliance 13](#_Toc150633308)

[4.5 Human Centricity 14](#_Toc150633309)

[Appendixes 1](#_Toc150633310)

[Appendix A: Glossary 1](#_Toc150633311)

[Appendix B: Identity Attributes 1](#_Toc150633312)

# Introduction

## Purpose

This document acts as a supplement to the Blockchain Maturity Model (BMM)i for further reviews of solutions that are designed to support identity management (in all its forms) based on blockchain technologies.

## Scope: Decentralized Digital Identity

This document applies to decentralized digital identity solutions that are usually supported by blockchain technology and provides further guidance for the assessment of relevant controls processes.

There are three main approaches in the adoption of blockchain technologies in support of decentralized digital identity solutions.

### Directory Services

A directory service is a database of identities that can be used to verify the identity of individuals and organizations. Traditional directory services are centralized, meaning that they are controlled by a single entity. This can lead to problems with security and privacy. Blockchain-based directory services are decentralized, meaning that they are not controlled by any single entity, making them more secure and private. In this scenario, blockchains are used to create a distributed directory that support the verification of the identity of individuals and organizations. Examples of blockchain-based directory services include Bitcoin, ION, and Hyperledger Indy.

### Self-sovereign identity (SSI)

SSI is a model of identity management where individuals have control over their own identity data. This means that individuals can own their identity information and decide who has access to it. SSI can be implemented using blockchain technology, allowing individuals to store their identity information on the blockchain, where it is secure and tamper-proof. Examples of blockchain-based SSI solutions include Sovrin and uPort.

### Decentralized identifiers (DIDs)

DIDs are unique identifiers for individuals and organizations that can be used to verify their identity without revealing their personal information. DIDs are based on blockchain technology. Examples of blockchain-based DID solutions include W3C DID and Verifiable Credentials.

**Note:** Blockchain technology can be used to support digital identity management solutions in a variety of ways, including:

* Storing and verifying identity information in a secure and decentralized manner.
* This information can then be verified by anyone who needs to access it, without the need for central authority.
* Enabling self-sovereign identity (SSI), which is a model of identity management where individuals have control over their own identity data.
* Blockchain can be used to support SSI by providing a secure and decentralized way for individuals to store and manage their identity information.
* Providing decentralized authentication, where individuals can authenticate themselves without the need for a central authority. This can be useful for applications where security and privacy are critical, such as financial services and healthcare.
* Issuing and managing digital credentials, such as diplomas, degrees, and licenses. This can help to ensure that credentials are authentic and cannot be tampered with.
* Proving identity for access control: Blockchain can be used to prove identity for access control purposes. This can be used to control access to physical or digital resources, such as buildings, computers, and data.

**Example:** Some specific examples of how blockchain is being used to support digital identity solutions include:

* The Estonian government use of blockchain for issuing digital ID cards to its citizens. These ID cards can be used to authenticate users for a variety of government services, such as voting and accessing healthcare records.
* The airline industry use of blockchain to verify the authenticity of passports and other travel documents, preventing fraud and improving security at airports.
* The healthcare industry use of blockchain to store and share patient medical records, to improve the quality of care and protect patient privacy.

## Use

When performing a BMM assessment of an identity management solution, the lead assessor will review the supplemental requirements defined in this document with the Solution Point of Contact (SPoC)1 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.

## Assessment Ratings Considerations

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

# Terms & Definitions

See [Appendix A](#_Appendix_A:_Glossary) for the terms and definitions used throughout this document.

# Blockchain & Digital Identity Management Use Cases

## Cross-border identity verification

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

## Vital records

Blockchain can be used to manage the issuance, storage, and release of vital records refer 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.

## 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.

## 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.

## 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.

## 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.

## Voting and election

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

## Supply-chain management

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

## 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 protect patient privacy.

## 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

## Security

### 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, disclosure, or modification.

The solution shall:

* Prohibit the disclosure of on-chain or off-chain information based on defined rules.
* Ensure that disclosure rules about user information is made available to users.

### 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.
* 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.
* 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.

**Notes:**

1. **Biometric Authentication** is the process of verifying the identity of an individual based on their physiological or behavioral characteristics.
2. **I**SO/IEC 24745 provides guidance on the security and privacy of biometric information.
3. 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.
4. The security of authentication in blockchain-based digital identity solutions could be supported by:  
   A. Zero-knowledge proofs: Zero-knowledge proofs allow 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.

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

### 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 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" controls to:

* Establish rules for monitoring 3rd party access, ensuring compliance with security policies. Rules may include:
* Authentication – The rules shall specify policy regarding the use of Multi-Factor
* Authentication (MFA) by the 3rd party.
* Authorization
* Compliance
* Data privacy
* De-provisioning
* Federation
* Notification – Describes when and how first and second parties are notified when third parties access data.

for third-party users.  
  
3rd Party Access also facilitates the authentication of third-party participants using cryptographic keys, digital signatures, or similar methods to ensure their legitimacy.

### Access Notification

Access Notification is the function of notifying an entity when their record has been read from or written to the blockchain solution.

### Anonymity

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. The solution shall support anonymity through pseudonymization, encryption, and decentralization.

* 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 is the process of distributing 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.  
    
  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.

### 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: U**ses 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.

### Integrity

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

* Encryption
* Distribution
* Consensus mechanisms
* Hashing functions
* Merkle trees

**Notes:**

* **Encryption**: Mathematical techniques to encrypt and decrypt data (See previous note)
* **Consensus mechanisms:** Consensus mechanisms are used to ensure that all nodes on the network agree on the state of the blockchain. This makes it very 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.

### Availability

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.

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

### 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 a number of 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.

### Auditability

Auditability is an important consideration for any system that handles sensitive data or that is subject to regulatory requirements.

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

### Authenticity

### Unique Identity

The solution shall:

* Ensure that individuals are able to control their own identities. If multiple people have the same digital identity, it can be difficult for individuals to prove who they are. This can lead to problems when individuals are trying to access services or make transactions.
* Protect individuals from fraud. If individuals share their digital identity with others, it can be used to impersonate them. This can lead to problems such as identity theft and financial fraud.
* Secure online transactions. When individuals use a unique digital identity to authenticate themselves, it can help to prevent fraud and protect their personal information.
* Prevent duplications complement the creation of unique digital identities and avoid the need for users to create multiple digital identities for different services or applications.
* Reduce the risk of fraud, preventing duplications can help to improve the user experience and increase overall security.

**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.

### Independent Attestation

The solution shall have mechanisms whereby third-party can:

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

**Notes:**

1. **Independent attestatio**n 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.
2. It's worth noting that 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.

### 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:**  
**1. 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.  
**2. 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.  
**3. 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.

### 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:**

1. **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.
2. **Identity attribute verification** is an important part of identity management, as it helps to ensure that only authorized individuals are able to 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
3. **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.
4. See Appendixes for a list of attributes and references.

### Non-Repudiation

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.

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

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

### 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.

The solution shall support key management.

**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.

### Data Privacy

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

**Notes:**

1. 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 a high level of security. This can be achieved through a variety of techniques, such as encryption, pseudonymization, and attribute-based access control.
2. **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

### 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.

### Smart Contract Security

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.  
Smart contracts can be programmed to trigger certain actions based on specific life events recorded in vital records. For example, an insurance payout could be automatically initiated upon the confirmation of a person's death.

In those instances where the solution uses smart contracts, the following controls mechanisms are used to provide assurance on their reliability:

* **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.

## 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 improve 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.

## 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 a number of 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 a number of 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 a number of 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.

## Compliance

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

* Data privacy regulations, such as:
  + **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:

* **Privacy-preserving technologies:** These technologies include homomorphic encryption, zero-knowledge proofs, 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).

## Human Centricity

The solution shall support "human centricity", including:

* **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 and from all walks of life.

**Note:**  
Human-centric technology is a design approach that puts people at the center of the technology. It is an approach that 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.

# Appendixes

## 

## Appendix A: Glossary

The following table describes the terms and definitions used throughout this document.

|  |  |
| --- | --- |
| Digital Identity | Digital identity is a broader term that refers to any method of identifying an individual or organization in the digital world. This can include things like usernames, passwords, biometrics, and verifiable credentials.  International Organization for Standardization (ISO): According to the International Organization for Standardization (ISO), “digital identity” is a term that refers to a set of electronically captured and stored attributes and credentials that can uniquely identify a person or an entity in an information system.  ISO has developed several standards for digital identity, such as:  - ISO/IEC 24760-1, which defines terminology and concepts for identity management2.  - ISO/IEC 24760-1 also provides a framework for understanding the relationships between different aspects of identity, such as identity attributes, identity tokens, identity claims, identity proofing, and identity verification.  NIST: According to NIST “digital identity” is the online persona of a subject and how that subject is represented online, adding that: “Digital identity is the unique representation of a subject engaged in an online transaction.” This definition is part of the NIST Special Publication 800-63-3 Digital Identity Guidelines, which provide technical requirements for federal agencies implementing digital identity services2. The publication covers topics such as enrollment and identity proofing, authentication and lifecycle management, and federation and assertions. The publication also establishes risk-based processes for the assessment of risks for identity management activities and selection of appropriate assurance levels and controls. NIST is currently working on the fourth revision of the publication, which is expected to address emerging challenges and opportunities in the digital identity landscape, such as privacy-enhancing technologies, decentralized identifiers, verifiable credentials, and biometric presentation attack detection.  W3C According to the World Wide Web Consortium (W3C), digital identity is defined as: A set of claims about an entity, such as a person, organization, or device, that can be used to verify its identity. Digital identities can be used to prove who you are to other people and organizations online. They can also be used to access services and resources, and to make payments. The W3C has developed a number of standards for digital identity, including: - Decentralized Identifiers (DIDs): DIDs are unique and persistent identifiers that can be used to represent anything, such as a person, a device, or a piece of data. DIDs can be used to create self-sovereign identities, which are identities that are owned and controlled by the individual or organization that holds them. - Verifiable Credentials (VCs): VCs are cryptographically signed documents that contain claims about an individual or organization. VCs can be used to prove your identity, skills, or qualifications to anyone who needs to verify them. The W3C is working to develop additional standards for digital identity, such as: Digital Identity Trust Framework: This framework will define the requirements for trust frameworks for digital identity. Digital Identity Wallets: This specification will define the requirements for digital identity wallets. Digital Identity Governance Framework: This framework will define the requirements for governance of digital identity systems. |
| Verifiable Credentials | Verifiable credentials (VCs) are a type of digital identity that is based on blockchain technology. They are cryptographically signed documents that contain claims about an individual or organization. VCs can be used to prove your identity, skills, or qualifications to anyone who needs to verify them.  Key features of verifiable credentials are: - Tamper-proof: VCs are digitally signed, which means that they cannot be tampered with without invalidating the signature. This makes them a secure way to store and transmit identity information. - Interoperable: VCs are based on open standards, which means that they can be used by any application or service that supports verifiable credentials. This makes them a scalable and flexible way to manage identity information. - Privacy-preserving: VCs only contain the information that is necessary to verify the claim. This means that personal information is protected, and the identity owner only has to share the information that is relevant to the specific transaction. |
| Decentralized Identity (DID) | ISO: According to the International Organization for Standardization (ISO),  Decentralized Identity is a standard for the design and use of decentralized and self-sovereign identification of subjects (legal entities and natural persons) and objects, assets within the design of Blockchain and DLT Systems, in conjunction with Verifiable Credentials (VCs).  NIST According to the Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), Decentralized Identifier (DID) is a globally unique identifier that does not require a centralized registration authority because it is registered with a decentralized system1.  Decentralized identity, or self-sovereign identity, is a model for identity management that gives individuals control over their own data. It uses digital identifiers and verifiable credentials that are self-owned, independent, and enable trusted data exchange. It does not rely on a centralized authority to verify a person or entity to interact and transact with an online service  W3C A Decentralized Identifier (DID) is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. DIDs are typically associated with cryptographic material, such as public keys, and service endpoints, for establishing secure communication channels. DIDs are useful for any application that benefits from self-administered, cryptographically verifiable identifiers such as personal identifiers, organizational identifiers, and identifiers for Internet of Things scenarios. For example, current commercial deployments of W3C Verifiable Credentials heavily utilize Decentralized Identifiers to identify people, organizations, and things and to achieve a number of security and privacy-protecting guarantees. This document is an introduction to the concept of Decentralized Identifiers. |
| Digital Identity Protocols | A digital identity protocol is a set of rules and standards that govern the creation, management, and use of digital identities. Digital identity protocols are used to ensure that digital identities are secure, reliable, and interoperable.  Examples of digital identity protocols used in blockchain implementations are: - Verifiable Credentials (VCs): VCs are a type of digital credential that is based on blockchain technology. VCs are cryptographically signed documents that contain claims about an individual or organization. VCs can be used to prove your identity, skills, or qualifications to anyone who needs to verify them. - W3C Decentralized Identifiers (DIDs): DIDs are a type of digital identifier that is based on blockchain technology. DIDs are unique and persistent identifiers that can be used to represent anything, such as a person, a device, or a piece of data. DIDs can be used to create self-sovereign identities, which are identities that are owned and controlled by the individual or organization that holds them. - Sovrin: Sovrin is a public blockchain-based ecosystem that enables self-sovereign identity (SSI). SSI is a decentralized approach to identity management that gives individuals control over their own identity data. Sovrin uses DIDs and VCs to allow individuals to share their identity data with organizations in a secure and privacy-preserving manner. - Uport: Uport is a private blockchain-based platform that enables self-sovereign identity (SSI). Uport uses DIDs and VCs to allow individuals to share their identity data with organizations in a secure and privacy-preserving manner. - Blockstack: Blockstack is a decentralized application platform that uses blockchain technology to store user data. Blockstack uses DIDs to allow users to control their own identity data. |
| Identity Data Sources | An identity data source is a repository of information about an individual or organization that can be used to verify their identity. This information can include things like names, addresses, phone numbers, email addresses, date of birth, and government-issued identification numbers.  Examples of identity data sources include: - Government databases: Government databases often contain information about individuals, such as their names, addresses, and date of birth. This information can be used to verify identity for things like voter registration, passport applications, and driver's licenses. - Commercial databases: Commercial databases contain information about individuals and organizations, such as their names, addresses, phone numbers, and email addresses. This information can be used to verify identity for things like credit card applications, employment background checks, and insurance claims. - Social media profiles: Social media profiles can contain information about individuals, such as their names, photos, and contact information. This information can be used to verify identity for things like online accounts and social media verification. - Biometric data: Biometric data is unique physical characteristics of an individual, such as fingerprints, facial scans, and voiceprints. This data can be used to verify identity for things like access control and payments. |
| Identity Attributes, Device | Identity attributes for devices are the characteristics of a device that can be used to uniquely identify it. This can include things like the device's serial number, MAC address, IP address, operating system, and hardware configuration.  Examples of identity attributes for devices include: - Serial number: The serial number is a unique identifier that is assigned to a device by the manufacturer. It is typically a 12-digit number that is printed on the device or in the device's documentation. - MAC address: The MAC address is a unique identifier that is assigned to a device's network interface controller (NIC). It is typically a 12-digit hexadecimal number that is burned into the NIC's hardware. - IP address: The IP address is a unique identifier that is assigned to a device by a network. It is typically a 4-byte number that is used to route traffic to the device. - Operating system: The operating system is the software that controls the device's hardware and software. It is typically a unique identifier that can be used to identify the device. - Hardware configuration: The hardware configuration is the set of hardware components that make up the device. This can be used to uniquely identify the device, especially if the device is custom-built. |
| Identity Attributes, Personal | Identity attributes for human beings are the characteristics of a person that can be used to uniquely identify them.   Examples of identity attributes for human beings include: - Name: The name is a unique identifier that is assigned to a person at birth. It is typically a combination of first, middle, and last names. - Date of birth: The date of birth is a unique identifier that is assigned to a person at birth. It is typically a day, month, and year. - Address: The address is a physical location where a person resides. It can be used to uniquely identify a person, especially if the address is unique. - Phone number: The phone number is a unique identifier that is assigned to a person by a telecommunications company. It can be used to uniquely identify a person, especially if the phone number is not shared with anyone else. - Email address: The email address is a unique identifier that is assigned to a person by an email service provider. It can be used to uniquely identify a person, especially if the email address is not shared with anyone else. - Government-issued identification number: A government-issued identification number is a unique identifier that is assigned to a person by a government agency. This can be used to uniquely identify a person, especially if the identification number is not shared with anyone else. - Biometric data: Biometric data is unique physical characteristics of a person, such as fingerprints, facial scans, and voiceprints. This data can be used to uniquely identify a person, even if they change their name, address, or phone number. |
| Self-Sovereign Identity (SSI) | Self-sovereign identity (SSI) is a type of digital identity that is owned and controlled by the individual or organization that holds it. This means that the individual or organization has complete control over their identity data, including who has access to it and how it is used.  SSI is a decentralized approach to identity management that is in contrast to the traditional approach, where identity data is stored and controlled by centralized organizations, such as governments or social media platforms.  The term "self-sovereign identity" was coined by the Sovrin Foundation, a non-profit organization that is developing a public blockchain-based ecosystem for SSI. The Sovrin Foundation defines SSI as: |

## Appendix B: Identity Attributes

Annex…: The Identity Life-Cycle  
  
(From: ID4D - The World Bank: Technical Standards for Digital Identity - Draft for Discussion

Annex B: Digital Identity Models

Annex C: ISO Standards on Digital Identity

Annex D: NIST Definition of Digital Identity

Annex E: W#C Definition of Digital Identity

Annex F: Digital Identity Protocols

Identity Attributes, Device

Identity Attributes, Personal

Annex D: References