International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1403

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Distributed ledger technology security

Security guidelines for using distributed ledger technology for decentralized identity management

Recommendation ITU-T X.1403

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	**X.1400–X.1429**
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1403

Security guidelines for using distributed ledger technology for decentralized identity management

Summary

Distributed ledger technology (DLT) and its specific implementations such as blockchain offer a unique opportunity for utilizing a trust infrastructure and a platform that could be useful in enabling trusted federation for exchanging identity attributes and identity information. Recommendation ITU-T X.1403 provides a telecom-specific privacy and security considerations for using DLT data in identity management.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1403	2020-09-03	17	11.1002/1000/14264

Keywords

Distributed ledger technology, identity management.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1403

Security guidelines for using distributed ledger technology for decentralized identity management

1 Scope

Distributed ledger technology (DLT) provides a trusted infrastructure that is useful for enabling decentralized identity management systems for the exchange of identity attributes and identity information.

This Recommendation provides an overview of using DLT for decentralized identity management. The scope of the work includes:

– a brief overview of using distributed ledgers for the management of identity and identity data,

– discussion on security benefits of decentralized identity,

– guidance concerning necessary controls that should be used to mitigate threats to identity data.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

[ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework*.

[ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 claim [ITU-T X.1252]: To state as being the case, without being able to give proof.

3.1.2 credential [ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.3 DID document [b-W3C-2]: A set of data describing the DID subject, including mechanisms, such as public keys and pseudonymous biometrics, that the DID subject can use to authenticate itself and prove their association with the DID.

3.1.4 entity [ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

3.1.5 federation [ITU-T X.1252]: An association of users, service providers, and identity service providers.

3.1.6 identity service provider (IdSP) [ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 decentralized identifier (DID): A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology (DLT) or other form of decentralized systems.

NOTE – Based on definition from [b-W3C-2].

3.2.2 DID subject: The entity the DID document is about. That is, the entity identified by the DID and described by the DID document.

NOTE – Based on definition from [b-W3C-2].

3.2.3 key-chain: Refers to the task of securing the storage of private keys or data on a trusted hardware unit in a device.

3.2.4 service endpoint: A distributed ledger address at which a service operates on behalf of a DID subject. Examples of specific services include discovery services, social networks, file storage services, and verifiable claim repository services. Service endpoints might also be provided by a generalized data interchange protocol, such as extensible data interchange.

NOTE – Based on definition from [b-W3C-2].

3.2.5 trust framework: A legally enforceable set of specifications, rules, and agreements that governs an identity system.

3.2.6 wallet (identity wallet): An application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys on the user device.

3.2.7 zero knowledge proof: A proof that uses special cryptography and a master secret to permit selective disclosure of information in a set of claims. A zero knowledge proof proves that some or all of the data in a set of claims is true without revealing any additional information, including the identity of the prover.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDO	DID Document
DID	Decentralized Identifier
DIdAm	Decentralized Identity and Access Management
DLT	Distributed Ledger Technology
IdAM	Identity Access and Management
IdSP	Identity Service Provider
IT	Information Technology
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
RP	Relying Party

SAML Security Assertion Markup Language

SP Service Provider

SSI Self-Sovereign Identity

SSO Single Sign On

URL Uniform Resource Locator

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

a) "Shall" indicates a requirement,

b) "Should" indicates a recommendation,

c) "May" indicates a permission,

d) "Can" indicates a possibility and a capability.

6 Towards decentralized digital identity

Distributed ledger technology plays a critical role in advancing the evolution and maturity of decentralized identity systems.

The proliferation of mobile devices and the Internet of things increases the pressure on traditional identity and access management systems (IdAMs) to evolve towards agile and intelligent platforms that are capable of supporting mobile and cloud-based systems.

Traditional identity management systems are built on top of centralized authorities such as corporate directory services, certificate authorities or domain name registries. Each of these organizationally centralized authorities serves as their own trust domains. In a traditional IdAM system, centralized authority could represent a single point of failure. Identity federation [ITU-T X.1252] emerged as a stopgap solution that enabled IdAM systems to work across systems with different organizations controlling their own domains.

The emergence of DLT provides an opportunity for the development of decentralized identity and access management (DIdAm) solutions. DLT provides a means for the management of trust without a centralized authority thus avoiding any single point of failure. Furthermore, DLT enables any entity to create and manage its own identifiers on any number of distributed ledgers.

Digital identity models have been continually evolving in order to meet changing business needs. There are three basic identity models as described in clause 6.

6.1 Centralized identity model

This is the oldest digital identity model and currently the most used [ITU-T X.1252]. In a centralized identity model, organizations act as identity service providers (IdSP). In this model, an organization establishes a point-to-point trusted relationship with each of its users. This model is a traditional, siloed model whereby, an organization issues a credential to a user that allows the user to access services of this organization.

In this model each organization acts as an IdSP. The organization manages the user's digital identity and decides on the accepted trust relationships. Trust between the user and the IdSP is typically established through use of shared secrets such as use of a username and a password. In some cases, shared secrets are augmented with multi-factor authentications such as hardware tokens, biometrics or FIDO [ITU-T X.1277] and [ITU-T X.1278] based solutions.

In a centralized model, the IdSP can store and collect data about users. The data can be monetized, shared or sold to other parties based on the identity service provider's (IdSP)'s business model. Users have to trust the IdSP to do the right thing when it comes to managing their data. Although end users benefit from the organization's services, in most cases they do not have control over the management of their own identities, personal data or their personal identity attributes. In this model, the IdSP is the owner of the users' identity. Users do not have the ability to port their data to other providers.

Centralized identity model requires a user to create and manage separate credentials for each of his business relationship with each IdSP. An organization requires the creation of these credentials before a user is permitted access to its resources. This model overwhelms user with many online identities. The lack of mutual authentication at login make this model vulnerable to phishing and credential harvesting attacks. The model encourages user to reuse passwords, which lead to further security risks and vulnerabilities.

The centralized model places a burden on IdSP when it comes to the life cycle management of identity. In particular, the model requires each IdSP to perform identity vetting [ITU-T X.1254] as part of the identity enrolment phase in the identity life cycle management. Identity vetting is needed in order to establish a level of trust in the claimed identity. This process may be repeated during the whole life cycle of a given identity. This step is problematic from a user perspective since the centralized model requires user to go through the identity vetting step separately with each identity provider. Additionality, data breach threat increases the risks of account-takeover due to the reliance of organizations on centralized data stores that are targeted by hackers on a regular basis.

6.2 Federated identity model

Organizations have realized the limitations of centralized identity model as discussed in clause 6.1 and have acted to develop federated identity model to address these challenges. The federated identity model aims to reduce the burden on users by enabling them to use their identity from one domain in another domain. The security assertion markup language (SAML) [ITU-T X.1242] provides more convenience for individuals with single sign on (SSO) functionality.

Federated identity management systems can provide authentication and authorization capabilities across organizational and system boundaries. It requires the establishment of business and trust agreements so that a user identity at one provider is recognized by other providers (members of the federation). In general, a trust agreement also includes a contractual agreement on data ownership, usage of personally identifiable information (PII) and compliance [ITU-T X.1242].

Federation model benefits the user since an identity service provider usually provides a single sign-on experience to a user. It reduces the number of separate credentials that a user needs to maintain and acquire. In this model, relying parties participating in the federation, including their users, are dependent on the availability of a given IdSP's services and its willingness to stay in the federation.

As with the centralized identity model, authentication in the federation model is not mutual and suffers from the same limitations.

6.3 Decentralized identity model

Decentralized identity could be implemented using DLT or other emerging standard based technologies like verifiable claims [b-W3C-1] and decentralized identifiers (DIDs) [b-Sovrin], [b-W3C-1] and [b-W3C-2]. A decentralized identity model can build on top of a distributed ledger (DLT) and a relationship between a user and an organization [b-Sovrin] and [b-W3C-17]. In this model, the user and the organization are peers.

Decentralized identity allows users to assume control and ownership over their identities. The degree of ownership can vary depending on the decentralized model. In particular, in a self-sovereign identity (SSI) model, it assumes that entities would be able to have control of their own digital identity.

Most identity solutions today have limited support for control over identity, transparency and portability, as identity providers with proprietary systems facilitate such solutions. An identity system fully compliant with an SSI model may exist in the near future, but this does not preclude the need to define its founding principles as discussed in clauses 6.3.1 and 6.3.2. Using DLT for decentralized identity management is further discussed in clause 7.

6.3.1 Decentralized identifiers

DIDs [b-W3C-2] are a type of identifier for verifiable, decentralized identity systems. The format of DIDs allow them to be under the control of the DID subject, which makes them independent from any centralized registry, identity provider, or a certificate authority. DIDs are uniform resource locators (URLs) that relate a DID subject to means for trustable interactions with that subject. The standard elements of a DID document (DDO) [b-W3C-2] include:

1) DID (for self-description)
2) Set of public keys (for verification)
3) Set of authentication protocols (for authentication)
4) Set of service endpoints (for interaction)
5) Timestamp (for audit history)
6) Signature (for integrity)

The task of resolving a DID [b-W3C-2] results with a DDO, which is a simple document that describe how to use that specific DID. Each DID document contains at least three elements: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate a DID subject (which is the user that is related to the DDO). Examples of authentication options are public keys and pseudonymous biometric protocols. Service endpoints enable trusted communications with the DID subject.

To use a DID [b-W3C-2] with a particular distributed ledger, it is required that a DID method be defined. The DID method specification can be based on [b-RFC 8141]. A DID method specifies the set of rules that govern how a DID is registered, resolved, updated and revoked on a specific DLT. All DIDs are specified and resolved on a distributed ledger.

The use of a DLT-based DID [b-W3C-2] reduces the dependence on centralized registries for identifiers as well as centralized certificate authorities for key management. As DIDs reside on a distributed ledger, each entity may serve as its own trust domain resulting in a decentralized trust infrastructure. This creates an interoperability bridge between the worlds of centralized, federated, and decentralized identifiers.

DID has a public and private cryptographic key pair [b-W3C-2]. The ownership of a DID is proven by cryptographic algorithms that relies on a private key, which only the owner of the DID should possess. Hence, DIDs can be published, changed, queried or deleted. Since each DLT may have its own implementation of the DID method, there will be, in practice, different implementations of the "create, read, update and delete (CRUD)" operations for the DID.

6.3.2 Verifiable credentials

Verifiable credential [b-W3C-1] solves the problem of exchanging credentials such as driver's license, proofs of age, education qualification and healthcare data, over a communication network in a way that is verifiable yet protects individual PII. In this approach, credentials are composed of statements called verifiable claims. Verifiable claims [b-W3C-1] are useful when an entity needs to prove that they are, for example:

- Above a certain age,
- Capable of driving a particular motor vehicle,
- Require a particular medication,

- Trained and certified as an electrician,
- Professionally licensed to practice medicine,
- Cleared to travel internationally.

The verifiable credential ecosystem is composed of four primary roles:

1) The issuer, who issues verifiable credentials about a specific subject,
2) The holder, who stores credentials on behalf of a subject. Holders are typically also the subject of a credential,
3) The verifier, who requests a profile of the subject. A profile contains a specific set of credentials. The verifier confirms that the credentials provided in the profile are fit-for-purpose,
4) The identifier registry, which is a mechanism that is used to issue identifiers for the subjects.

A claim [b-W3C-1] is a statement about a subject, expressed as a subject-property-value relationship. Claims may be merged together to express a graph of information about a particular subject.

When an issuer sends data to a holder, it bundles a set of claims into a data structure called a credential and digitally signs the data structure [b-W3C-1]. When a verifier requests data from a holder, the holder typically bundles a set of credentials into a data structure called a profile and digitally signs the data structure [b-W3C-1].

7 Decentralized identity using DLT

Decentralized identity can be perceived as an identity that is anchored by a DLT. In this approach, zero knowledge proof [b-W3C-1] can link identities in a universally discoverable manner. A decentralized identity allows a user to prove his or her identity once to a trusted third party and store the proof of their identifier in a DLT. The DLT acts as the identity trust vault. The DLT offers identity infrastructure services in support of peer-to-peer communications, DLT based public key infrastructure (PKI) services and verifiable claim exchange protocols among others.

Decentralized identity allows users to access services in a straightforward process. For example, a user interacts with an IdSP that in return uses a DLT to create a user DID that points to a DLT location that the user can use. This step is transparent to the end user. This step is equivalent to creating a pair of private and public keys for the user. The private key is stored with the user in some form of a digital wallet. The corresponding public key is stored on the DLT. The public key acts as a wallet identifier (aka user identity on the DLT) and is hashed and securely stored in the ledger. As part of the services offered by a DLT, claims can be issued and signed for a particular user by DLT issuers and provided to the user. These claims can be stored in the user's wallet.

In this model, a user can access a service by presenting their identifier to a service provider in the form of a token. The service provider verifies the identity by comparing the hash values of identifiers with their corresponding hash records that is stored on the DLT. The service provider grants or reject access based on the verification result.

7.1 Wallet initiation

The work in [b-Sovrin] and [b-W3C-1] provides an example of interactions in support of an identity-based service. A user decides to interact using the decentralized identity services of a DLT based identity trust system. In this regard, the DLT provides services to enable the end user to establish a DID and a relationship with the ledger. The task of establishing a DID for the user concludes by saving a ledger address for that user and the creation of public private key pairs for interacting with the user. The ledger can also provide services that can be used to create the DID document and establish the required document links as specified by the user. The ledger provides

core identity services that enable services to discover how to interact with the user wallet in order to make enquiries about available claims under the user control.

The act of creating a DID on the ledger leads to the creation of a wallet to be used by the user to provide verified claims to the relying party (RP). The wallet holds the user's private keys, public keys and other identity profiles as determined by the DID method. The use of zero knowledge techniques [b-Sovrin] ensures that claims can be verified in a manner that is PII preserving and in line with the current usage of traditional paper-based credentials and documents. For example, a user can prove their age with a driving licence at an establishment without the need of the issuing authority of the driving licence participating in the transaction. The wallet can be a virtual wallet where one part of the wallet is on the user mobile device and another part of the wallet could be in the cloud. This configuration enables the creation of agents to act on behalf of the user and perform services without the need for the direct involvement of the user.

The following steps are relevant to the process:

1) DID register: The user downloads the wallet that is associated with the DLT service provider and register their DID on the ledger. The DLT generates the private and public key pairs associated with the identity wallet. An address is created and stored on the DLT as part of the registration process.
2) Identity initiation: For a DLT to be used in decentralized identity systems, a trust framework is assumed to exist that specifies a list of available identity services for the participants. In this regard, a user can rely on the availability of an issuer (a trusted party) that can validate the identity of the users. Initially, users can start with self-asserted claims. Users can then build on their wallet initial claims to collect additional claims from multiple providers to include in their wallet and to enhance their identity validity within the system. Every relationship is protected by mutual DID between the issuer, the holder (user) and the verifier.
3) Verification: If a holder (user) wants to access a service from a relying party, the RP (verifier) will request the user to provide access to available claims in their wallet. The verifier then consults with the DLT in order to validate the signed claims by using the public keys corresponding to the DID as stated in the transaction. The system assumes that the wallet is the source of truth in terms of the knowledge of the holder's private keys. The system assumes that appropriate authentication has occurred to ensure that the legitimate wallet owner is the entity that is performing the transaction.
4) Claim validation: The RP uses the provided claims from the wallet to verify the user's identity and attribute using the DLT PKI based signature and hash validation techniques.
5) Authorization: RP determines what services can be accessed based on the result of identity verifications.

7.2 DID resolution and authentication

The DID concept [b-W3C-2] can facilitate the creation of a universal resolver [b-DIF] for any DID. The universal resolver can participate in an interoperable DID authentication layer. DID authentication enable an identity owner to take control of a DID during its interaction with a RP. This requires the following steps to be executed by the relying party:

1) The relying party resolves the identity owner's DID on a DLT to a DID document,
2) The relying party attempts to authenticate the identity owner using the authentication object(s) found in the DID document on the DLT,
3) The authentication object(s) may include or make reference to a public key object, in cases where the identity owner's proof is established as a cryptographic signature.

7.3 Benefits of using DLT for decentralized identity and access management system (DIdAm)

The use of DLT as a trust framework for decentralized identity systems paves the way for providers to design frameworks that allows providers to act as a middleware abstraction layer between the user and various ledgers. These interactions require traditional identity and access management systems to establish proper framework to support decentralized systems. In essence, the merger of centralized and decentralized systems can be referenced as decentralized identity management system (DIdAm) [b-Angelov et al.]. In this regard, a DIdAm [b-Angelov et al.] is a system of systems that can interact with many DLTs that support decentralized identity models based on DIDs. This is depicted in Figure 1.

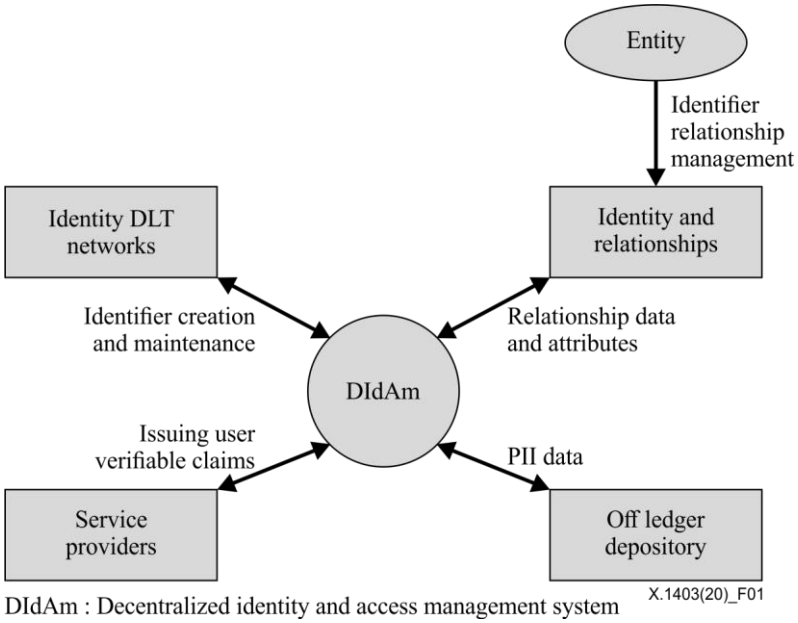

Figure 1 – DIdAm framework

The components of a DIdAm using DLT are:

1) Decentralized identity owner: This is an entity that manages its decentralized identities using services offered by DIdAm across multiple ledgers.

2) Service providers (SPs): The issuers who offer services to identity owners (bootstrapping identity). For example, government agencies such as the department of motor vehicle or private companies like financial institutions.

3) Off ledger identity depository: This is a database in which the user identity attributes, claims and general information are stored. The user is in control of where the data should be stored. This is typically data that is PII sensitive and should be stored off ledger. The depository should provide the ability to read and write the data at the discretion of the user.

4) Identity systems that are based on DLT can be thought of as separate identity systems with different trust boundaries and cryptography keys. Therefore, the DIdAm must facilitate interactions across ledgers on behalf of the user.

The services of the DIdAm can be performed internally by the enterprise or some third party can play the role of such providers.

7.3.1 Support of decentralized identity across multiple DLT ledgers

There are many interface requirements [b-Angelov et al.] that is needed to support decentralized identity using DIDs across multiple DLT. The difficulty arises due to varying requirements of the trust framework such as the type of DLT whether it is public or private. The DIdAm should be able to support the user irrespective of the user preferences for the type of communication access network that they are using. Figure 1 shows the DIdAm in the capacity of a unified interface towards the identity owner, being able to operate on multiple ledgers.

DIdAm [b-Angelov et al.] acts as an abstraction layer to the end user. It enables the user to interact with many DLTs while using a single virtual interface. DIdAm will also act as an abstraction layer to the enterprise where legacy based IdM systems can interact with it in support of centralized IdM internal functions. A benefit of this abstraction would be the ability of a user to manage identities on any number of ledgers. This will enable the user to create relationships with providers and be able to have better control over their identity.

7.3.2 Support for identity services

In traditional IdAm systems the identity service provider is able to attest to a relying party for the identity of a user. The DIdAm [b-Angelov et al.] should be able to support this role in particular to be backward compatible with legacy systems. The following actions can support the attestation requirement:

1) The DIdAm should act as a trusted partner. It should ensure that the identity owner acquires accurate and valid assertions through correct verifiable claims procedures for issuers.
2) Reduce identity vetting friction for users. Typically, a user will need to go through an identity vetting stage with each issuer. A properly designed DIdAm can help the user to overcome this limitation by being an active trusted participant in the interaction.
3) Real time data validation. Inaccurate data is a problem in legacy systems. This problem can be alleviated by the DIdAm through the offering of services that help relying parties in determining that the user attributes are not stale.
4) Consent management. Consent is an integral part of compliance. The DIdAm can offer services to users and relying parties to ensure that consent compliance is accounted for.

7.3.3 Managing key chain

The term key-chain refers to the task of securing the storage of the private keys associated with a wallet on the user device. There is a direct one to one relationship between DID, verifiable credential and service provider. The device can be a mobile device or a browser-based device. Since in this current security model, access to private keys is used for validating the user's identity. The task of protecting the key pairs is crucial for the prevention of identity fraud attacks. In dealing with multiple DID over many DLTs, users are faced with the task of protecting a collection of private keys that are used to unlock their identities across the whole identity space.

The key-chain is the structure where the private key corresponding to the user DIDs are securely stored. It is a structure that is owned by the identity owner and is in control of the private keys that translates to owning the DIDs. A DIdAm should be able to manage the key chain on behalf of the user. In particular:

1) The user should be able to use the key chain functionality and storage while operating within the domain of the DIdAm.
2) Management of keys should be under the control of the user.
3) Access to the key-chain should be managed and auditable.
4) Services that enable user to save and restore wallet could be offered by the DIdAm.

8 Security guidelines for using DLT for DIdAm

Decentralized identity solves some of the key issues associated with centralized and federated identity models. Distributed ledger technology is vulnerable to cybersecurity risks. Security risks include those resulting from human errors such as software coding errors.

In general, user DID(s) should not be published on a permissionless ledger even if in some cases there might be a need to have a unique ID made available for all its users. However, data that help users to trust the ledger such as IdSP public keys, revocation lists, and data that enhance interoperability such as variable credential schemas can be made to be public information on ledgers.

This clause address security benefits, challenges and security risks for decentralized identity models.

8.1 Distributed ledger security considerations

There are two broad types of distributed ledgers, which are categorized as permissionless and permissioned. Permissionless ledgers allow any entity to access, view, propose new data or validate existing data on the ledger as long as they are following the ledger established protocols. The ledger ensures the confidentiality, integrity, availability and consistency of the data with consensus protocols to create trust among participants who may not trust each other. In general, permissionless ledgers operate without any central authority.

A permissioned ledger is a system that is comprised of trusted parties that are granted usage rights as needed for their role in the trust framework. In this model, selected participants can change the ledger data. Depending on the trust agreements, some ledger can allow open read access to the ledger.

Permissionless ledger ensures trust through consensus protocols that are computational expenses and does have a direct impact on the throughput and performance of an identity system running on them. On the other hand, permissioned ledgers rely on trust among the ledger creators to ensure that the security of the ledger data including identity data. Permissioned ledgers are generally faster and more economical than permissionless ledgers.

8.2 Benefits of using DID for DLT

Decentralized identity provides the following benefits:

1) Identity portability: Decentralized DID ensure control by individuals over their digital identities. It eliminates the reliance on centralized IdSP. In theory, individuals can own, control and manage their own identifiers and their relationships.
2) Encourages relationship-based identity services: DID enable entities to establish digital identifiers for almost all relationships. Pairwise, pseudonymous DIDs preserve PII.
3) Minimize security risk: DID requires the owners of an identifier to prove ownership by demonstrating knowledge of the private key associated with the corresponding public key. Claim validation is checked dynamically on the DLT in real time. Validation can be done without the need to centralized servers, which reduces the attack surface.
4) Cost distribution: Identity validation on a DLT can benefit from the ability of using DID to re-use identity proofing across the DLT participants. This reduce the cost and enhance security.
5) PII by design: Decentralized sovereign DID services distribute the risk resulting from using central data stores for storing user information and hence it increases the difficulty for attackers.
6) Consented and tracked sharing of personal data: DID provide the ability of sharing data between users and providers based upon agreed policies, which improves the user ability to protect their data.

7) Dynamic and improved federation: The use of DID within a DLT extend trust to all organizations participating in the ecosystem. Participants can focus on providing services as opposed to focusing on the details of the federation and how to set it up.

8) Fault tolerance: The decentralized nature of DLT provides a level of fault tolerance and infrastructure resilience.

8.3 Threats and vulnerabilities

Distributed ledgers have inherited capabilities that mitigates cybersecurity risk to an information and communication technology system. Examples of improved security features are:

1) Increased system resiliency: the distributed architecture of a DLT that prevents it from being a single point of failure.

2) Improved robustness: consensus mechanisms improve the overall integrity of distributed ledgers, because consensus among participants is required before accepting any new data in the ledger.

3) Improved transparency: It is more difficult for malware to work within DLT since the system have many separate layers of security at the ledger infrastructure level.

Decentralized identity systems that are built using DLT will inherit the security risks from those technologies. In addition, there are additional risks for using DLT for identity management.

8.3.1 Identity data management

CRUD stands for Create-Read-Update-Delete. These are the basic operations of traditional storage database. In DLT, specifically with permissioned blockchain, implementations entities cannot delete written transactions on a blockchain. Even updating existing transactions cannot be done, since they are immutable. Therefore the 'CRUD' operations cannot be considered as a normal operation for handling user data.

Instead, operations on blockchain can be described as CRAB: Create, Retrieve, Append and Burn. The Append, which replaces Update, means that implementers can only append new transactions to a blockchain technology, therefore changing the 'world state' (sum of all past events/transactions up until now). The Burn operation in CRAB means that you throw away the encryption keys, so you are unable to append new transactions or make any further change to the ledger state of the asset.

It is therefore important to pay careful attention to writing personal data on a DLT or blockchain since the data cannot be taken out or be forgotten in the future. In this regard, it is best to write the data off chain with pointers in the DLT to the outside data. However, storing data off ledger also has drawbacks. In particular:

- The benefit of transparency is reduced since users will not know if they are not authorized to access the off-ledger data.
- The benefit of data-ownership with blockchain is reduced since once the data is off ledger, it can be owned by any entity that can access it.

8.3.2 DID key linkability

There is a potential for DIDs to be correlated. This can happen if the same DID is used among more than one relationship. DLT ledgers can mitigate this risk by using pairwise unique DIDs for relationships. This means that each pair of used DID is different for every relationship. In this scenario each DID acts as a pseudonym [b-W3C-2]. A pseudonymous DID need only be shared with more than one party when the DID subject explicitly authorizes correlation between those parties.

As a point of caution, even pseudonymous DIDs can be correlated [b-W3C-2] if the data in the corresponding DID documents can be correlated. For example, using common service endpoints names in multiple DID documents can be used to correlate information about the same DID. Therefore, the DID document for a pseudonymous DID also needs to use pairwise unique public keys.

8.3.3 DID key protection

The management of private keys is important. If a master key is stored in a non-secure location even on a single device, then identity theft is likely to occur. Use of secure storage facilities on devices should be a requirement.

8.3.4 PII preserving techniques

It is recommended that there should be no storage of sensitive information on the ledger. The advent of quantum computing will ensure that every two-way encryption technique can be cracked over time, the aim is to never store any sensitive information on the ledger.

Although hashes are one-way functions, they can be potentially sensitive since hackers have unlimited time to try to brute-force the digest. For this reason, there should be no hashes stored on the ledger.

Instead of storing raw data such as date of birth on the ledger, answers to questions stating, for example, that an individual is above 21 years old could be stored within a smart contract on a ledger. It can be seen as a claim complying to a requirement.

It is recommended to store only hashes of private or sensitive data on the DLT. PII data should not be stored on the ledger even if it is encrypted. Sensitive data should be stored off-ledger and should be exchanged between approved entities that need to consume the data. This approach reduces the risk that a DLT breach will result in the loss of sensitive data. Secure peer-to-peer technology should be used for data exchanges supporting off ledger access. Appropriate off ledger data storage techniques should be used including plans for data archiving and recovery. For example, if an identity owner claims that they are a licensed insurance provider, that claim can be verified by an entity that plays the trusted provider role in the decentralized identity system and the proof is stored on the DLT in a hashed form. The proof can be the hash of the digitally signed claim from the claimant. The security of the off-ledger depository should be ensured.

8.3.5 Vendor lock-in

Ledgers can be standardized, however software components are specific to a given solution and could be proprietary and non-interoperable.

8.3.6 Identity-based attacks

A distributed ledger is vulnerable to identity-based attacks similar to those targeting traditional information technology infrastructure, such as spoofing and Sybil attacks. Malicious actors can deploy such attacks to take over a majority of the nodes in a ledger. If successful, an attacker can undermine the consensus validation and distributed architecture protections of a ledger. This risk can be mitigated using strong authentication solutions for cloud-based directory services.

8.3.7 Communication network effects

The distributed structure of DLT can create operational problems when dealing with the involvement of many players each with their own communication infrastructure protection solutions. This structure poses challenges in managing identities, access control, security configuration, PKI key storage and management.

DLT operations requires running nodes that use differing communication network topologies, software code and protocols which may be vulnerable to security threats. The impact of these threats varies depending on the nature of the DLT (private or public). As such, identity management systems and identity data are vulnerable to communication network level attacks that target the DLT. Designers of identity management systems should take into consideration communication network level issues that include:

1) Impact on identity data in the event that the DLT consensus algorithm fails.
2) How to deal with DLT or blockchain collisions?
3) What is the disaster recovery plan for identity data?
4) What are the threats to identity data in the event that a small group of participants control the DLT consensus mechanisms?

8.3.8 Identity data encryption

Identity data stored off ledger is considered confidential and private for the identity owner. The user should be able to get help from the ledger for assistance with encrypting data whether in bulk or during transmission in particular when sharing data among various providers.

8.3.9 Backup

There are risks to the user when it comes to protecting its device and its content in terms of verifiable claims or private keys and personal data.

There is a need for proper data recovery and restoration for the user wallet.

Additionally, the user will need assurance that their data is protected and backed up on the ledger. Techniques that ensure no data corruption or loss should be available as services to the end user.

8.3.10 Smart contracts

The use of smart contracts may be required in the implementation of decentralized identity systems. Smart contracts are written by developers using computer programming languages. These programs are susceptible to development and programming errors in particular as the complexity of smart contracts increases. The uncertainties with the accuracy of smart contracts requires the development of governance framework that ensures the decentralized identity systems have proper processes and procedures to address any limitations resulting from inaccurate smart contract whether it was intentional or non-intentional.

8.3.11 DLT certificate management

Identity management systems include the task of managing the identity life cycle which include identity vetting tasks. Identity management related tasks include creating, issuing, storing, revoking and replacing credentials and fraud detection.

The use of certificates in the ledgers poses some unique challenges to security practitioners. In decentralized identity systems, there is a higher price to be paid for lost or misplaced private keys than traditional access systems. For example, if a user wallet private keys are lost then the user's access to their DLT is permanently disabled. Greater damage will occur if the keys are stolen, since proving passion of private keys is equivalent to identity theft. The difficulty of the recovery mechanisms is also a function of the nature of the DLT. It is easier to deal with these issues in private ledgers as opposed to permissionless ones that require consensus on transactions.

These issues should be included in the design of governance systems for DLT since there are no central authority for handling fraud or technical difficulties. This requires trust governance frameworks to ensure that all states of an identity life cycle are covered from the onset and proper procedures are agreed upon by DLT participant beforehand in the support of identity recovery services such as: key life cycle management, what parts of a block pay load is encrypted, how are keys revoked, how are private keys protected and recovered, and what happens if fraud is detected.

Bibliography

[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, April 2017.

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen, *Decentralized Identity Management System for Self-Sovereign Identity*, https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf.

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*, https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[b-Blog] Blockchain platforms, https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b.

[b-DIF] Decentralized Identity Foundation (DIF), https://identity.foundation/#wgs.

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, Published 1 December 2017 – ID G00324208, By Analysts Homan Farahmand.

[b-Sovrin] Sovrin Foundation, https://sovrin.org/.

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*, https://www.w3.org/TR/2019/CR-vc-data-model-20190725/.

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, August 2019, https://w3c-ccg.github.io/did-spec/.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021