International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3081

(09/2022)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Self-controlled identity based on blockchain: Requirements and framework

Recommendation ITU-T Y.3081

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3081

Self-controlled identity based on blockchain: Requirements and framework

Summary

Recommendation ITU-T Y.3081 presents the motivations and principles for self-controlled identity based on blockchain in future networks including networks beyond IMT-2020. It provides the high-level framework and requirements of self-controlled identity based on blockchain. It specifies the capability requirements of the self-controlled identity based on blockchain accordingly in the context of future networks including networks beyond IMT-2020. Detailed descriptions of the use cases and business models are listed in the appendix.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3081	2022-09-29	13	11.1002/1000/15051

Keywords

Blockchain, decentralization, framework, future networks, networks beyond IMT-2020, self-controlled identity.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3081

Self-controlled identity based on blockchain: requirements and framework

1 Scope

This Recommendation specifies for self-controlled identity (SCid) based on blockchain targeting network applications in future networks including networks beyond international mobile telecommunications-2020 (IMT-2020):

- roles and principles analysis:
- high-level framework and requirements;
- capability requirements.

Detailed use cases and business models are listed in an appendix.

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 Y.2015] Recommendation ITU-T Y.2015 (2009), *General requirements for ID/locator separation in NGN*.

[ITU-T Y.2022] Recommendation ITU-T Y.2022 (2011), *Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks*.

[ITU-T Y.2057] Recommendation ITU-T Y.2057 (2011), *Framework of node identifier and routing locator separation in IPv6-based next generation networks*.

[ITU-T Y.2342] Recommendation ITU-T Y.2342 (2019), *Scenarios and capability requirements of blockchain in next generation network evolution*.

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[ITU-T Y.3031] Recommendation ITU-T Y.3031 (2012), *Identification framework in future networks*.

[ITU-T Y.3032] Recommendation ITU-T Y.3032 (2014), *Configurations of node identifiers and their mapping with locators in future networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.2 claim [b-ITU-T X.1252]: [*noun*] Digital assertion about identity attributes made by an entity about itself or another entity. [*verb*] To state as being the case, without being able to give proof.

NOTE – The terms assertion and claim [noun] are agreed to be very similar.

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

NOTE – [b-ISO/IEC 29115] is a similar text to [b-ITU-T X.1254] and contains the same definition of credential that was developed by the groups involved.

3.1.4 decentralized application [b-ITU-T X.1400]: Application that runs in a distributed and decentralized computing environment.

3.1.5 decentralized identifier (DID) [b-ITU-T X.1252]: A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network. A DID is associated with exactly one DID object descriptor.

3.1.6 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

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

3.1.8 identity [ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

3.1.9 identifier [ITU-T Y.2091]: A series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.10 identity provider [ITU-T Y.2720]: An entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations, and devices) and offers identity-based services based on trust, business and other types of relationship.

3.1.11 identity verification [b-ITU-T X.1252]: The process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information.

3.1.12 issuer [b-ITU-T X.1252]: The entity that issues a claim.

3.1.13 private key [b-ITU-T X.509]: (In a public-key cryptosystem) that key of an entity's key pair which is known only by that entity.

3.1.14 public key [b-ITU-T X.509]: That key of an entity's key pair which is publicly known.

3.1.15 revocation [b-ITU-T X.1252]: The annulment of something previously done by someone having the authority.

3.1.16 verification [b-ITU-T X.1252]: Process of establishing that identity information associated with a particular entity is correct.

3.1.17 verifier [b-ITU-T X.1252]: Entity that performs verification.

3.1.18 wallet (identity wallet) [b-ITU-T X.1252]: An application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys on the user device.

3.1.19 zero knowledge proof [b-ITU-T X.1403]: 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 self-controlled identity (SCid): An identity created, controlled and managed in a decentralized manner by the entity itself. The self-controlled identity includes the identifiers and associated explanatory profiles.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
APP	Application
DID	Decentralized Identifier
ID	Identifier
IMT-2020	International Mobile Telecommunications-2020
KYC	Know Your Customer
LOC	Locator
SCid	Self-Controlled identity
SP	Service Provider
SSO	Single Sign On
URL	Uniform Resource Locator

5 Conventions

In this Recommendation:

The phrase "is required" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

The phrase "is recommended" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

The phrase "can optionally" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service provider (SP). Rather, it means the vendor may optionally provide the feature and still claim conformity with this Recommendation.

In the body of this Recommendation and its annexes, the words "shall", "shall not", "should", and "may" sometimes appear, in which case they are to be interpreted respectively as, "is required to", "is prohibited from", "is recommended", and "can optionally". The appearance of such words or phrases in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction

6.1 Background and motivations

Identity [ITU-T Y.2720] is information about an entity that is sufficient to identify that entity in a particular context. The entity could be users or subscribers, groups, user devices, organizations, network and SPs, network elements and objects, and virtual objects. Usually the identity is issued by an identity provider, which is a centralized authority. For example, the telecommunication network operator assigns an E.164 number to a subscriber, or the SP offers its user a local account with username and password, such as the website or mobile application (APP) account. However, the centralized identity solution leads to several disadvantages: 1) hard to remember 10s of username-password pairs as users must maintain identities for every SP to which they register; 2) increase in the risk of private data leakage as SPs may differ in security level; 3) raising privacy concerns through inadvertent personal information sharing and the data monetization of the SPs; 4) hard to share services between SPs for users.

To eliminate isolation of identities among SPs, federated identity management systems enable some SPs to maintain user credentials on behalf of other SPs. This enables single sign-on (SSO) capabilities where a user utilizes one identity issued by an SP to access a large number of services provided by others. SSO frees users from remembering lots of passwords, but at the price of security and privacy data abuse; e.g., the SSO provider may present a single point of failure and control the access of other SPs. The mobile phone number is another kind of generic identity that could be accepted by most SPs as it is unique and can be authenticated easily leveraging the SMS code. An identity based on a mobile phone number is frequently used for user login the first time and for performing important actions online; however, the know-your-customer (KYC) procedure is still necessary for each SP to build a user profile related to the identity. Although a generic user identity reduces password memory issues and isolation of SPs, identity-related private data is still held by SPs and users lack control over their own data.

Furthermore, from the network perspective, the identity of a node has multiple options, such as in identifier/locator (ID/LOC) separation [ITU-T Y.2015] [ITU-T Y.2022] [ITU-T Y.2057] [ITU-T Y.3032] that is used to improve mobility management and address aggregation. As the demand for network node cooperation and network infrastructure sharing continues to increase, such as the unmanned aerial vehicle and connected vehicles, network resource sharing and collaboration has gradually become a new trend, e.g., in computing resource sharing. The identity of the network node is necessary to provide more attributes, e.g., identifying the ownership of the resource and trustworthy verification. Additionally, as the number of entities in the network is seeing explosive growth in the IMT-2020 era, especially for terminal and sensor devices, identity allocation and issuance would be a burden to both networks and SPs.

Thus, a self-issued and SCid is considered as a promising method to construct an independent identity layer, which provides opportunities to separate resource ownership validation, service provision and access control from identification management for SPs, and establishes trust between users and (network) SPs. The SCid is also expected to generate new business models and a promising new ecosystem.

6.2 Self-controlled identity overview

An SCid is an identity created, controlled and managed in a decentralized manner by the entity itself. The SCid includes the ID and associated explanatory profile to identify the entity and confirm their eligibility to access a service or network, or to perform a particular task or own a specific resource. An SCid promises to provide direct verified information interactions between entities with a generic permanent identity or temporary identities, allowing the entity to control how to use data. The SCid enables the SPs or networks to verify the entity without having to store the entity

information themselves, which reduces privacy leakage and security burdens. Figure 6-1 shows the components and their interactions in the SCid system.

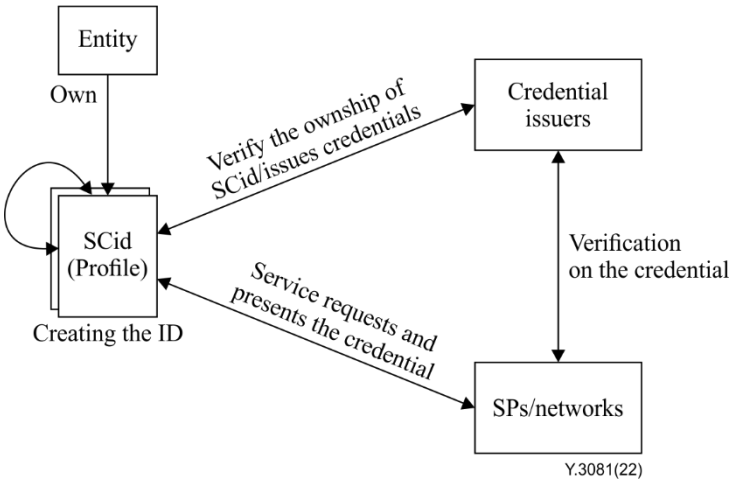


Figure 6-1 – Components and their interaction in the SCid system

The blockchain [ITU-T Y.2342] leverages its structure to store data and records in a distributed fashion to achieve consistent data storage, anti-tampering or non-repudiation and failure resistance. A smart contract can be used to operate the data stored in the blockchain. The blockchain is a promising technology to support SCid management. The blockchain ledger is leveraged to record identity information for discovery, the reference of the data stored off-chain and digests of credentials and attestations. In the meantime, the smart contract can implement many functions formerly assumed by a traditional credential SP, such as ID registry and authentication. The blockchain enables the entity to control and manage its ID and credentials while leaving the SPs or networks to focus on authentication and verification.

7 Roles and principle analysis of self-controlled identity

7.1 Roles and relationships of self-controlled identity

Figure 7-1 provides a high-level overview of the four main roles in an SCid system.

– **Subject**: An entity that is the basic component in the SCid system and owns one or multiple IDs. A subject can be a user or subscriber, organization, network and SP, network element and object. A subject can create IDs or entrust a trusted entity to create IDs. A subject can apply credentials from other subjects and issue credentials to other subjects in SCid systems. The subjects in an SCid system may perform different functions according to the roles offline, e.g., general member, authority issuer and committee member who manages authority issuers.

– **Issuer**: An entity that issues credentials about subjects. An issuer can be an organization, an individual or network object. The credentials issued by the authority issuer are authoritative. The identification of an authority issuer depends on the specific business scenario and the offline function of the issuer.

– **Verifier**: An entity that verifies whether the data of credentials of a specific subject have been tampered with and whether it has been endorsed by a certificate issuer. The verifier includes the functions necessary for engaging in authentication exchanges.

– **Identifier registry repository**: A blockchain-based repository that is used to record ID-related data, such as the explanatory profiles (e.g., DID documents [b-W3C-DID]) with the public key, the hash value of a specific credential, etc. The ID registry repository can also provide specific data management service over the blockchain ledger leveraging smart

contracts, e.g., SCid revocation list, SCid-associated explanatory profiles creating, updating or deactivating access control to SCid explanatory profiles and credentials.

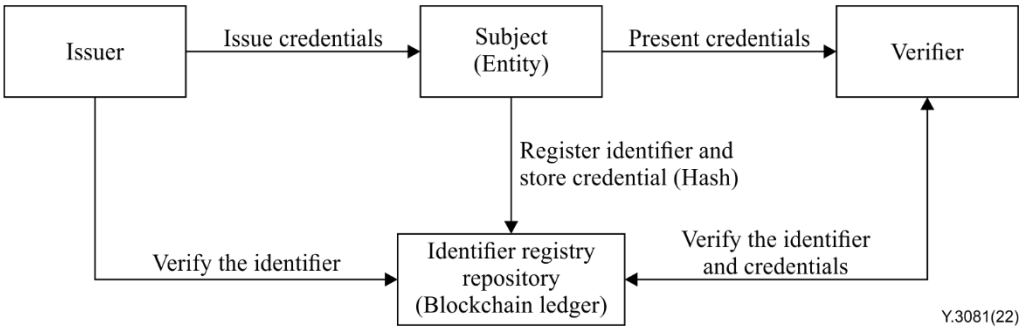


Figure 7-1 – Roles in the SCid system

7.2 The principles of self-controlled identity based on blockchain

The design principles of an SCid follow.

– **Portability**: The SCid is system independent and the information related to identities must be portable and transportable.

– **Self-controlled**: Entities have entire control of their identities, including life cycle management of the IDs and attestation data disclosure.

– **Privacy**: The SCid can enhance privacy as well as possible and disclosure of data must be minimized.

– **Extensibility**: The SCid mechanism and resolution system are scalable.

– **Discoverability and resolvability**: The self-controlled identities can be discovered and resolved in a resolution system globally.

– **Credential-based**: Interoperability between entities with self-controlled identities is based on credentials.

– **Decentralization**: The SCid can eliminate centralized ID management, including ID generation, registration, update, revocation, storage of credentials and metadata, as well as service retrieval.

– **Regulatory compliance**: The SCid is regulation compliant to avoid liability for identity data management, e.g., the geographical distribution of specific data.

7.4 Analysis of identifiers considered in an SCid system

The ID in the current network can be categorized based on different attributes, e.g., the readability and hierarchy [ITU-T Y.3031]:

– human-readable IDs and non-readable IDs (e.g., public key-based IDs);

– hierarchical IDs and flat IDs.

Human-readable IDs are easier to understand for human users, e.g., the domain name and email address, while non-readable IDs are meaningless and based on hash algorithms in most cases, e.g., a public blockchain address generated from a public key. Hierarchical IDs are scalable both in ID spaces and in fine-grained management, therefore many IDs in the network adopt hierarchical format, e.g., uniform resource locator, Internet protocol address, mobile subscriber international integrated services digital network/public switched telephone network number, international mobile subscriber identity, universally unique identifier and DID.

However, the readability and hierarchy of an ID are not mutually exclusive. The hierarchy of an ID is beneficial to embed the resolution methods, the applied domain, group or community, version

information, indicators for specific actions, etc. At the same time, public key-based IDs, which are non-readable and flat, can provide self-certifiable ability natively. Thus, the combination of the hierarchical structure and flat IDs based on a public key can provide an ID with global uniqueness, security and decentralization, as well as partially relieve readability issues as discussed in [b-Zooko's triangle] at the resolution level.

Therefore, the preferred composition of an ID of an SCid is of two parts. The first part is a globally unique prefix with a hierarchical structure, which could be used to instruct: ID discovery; ID resolution methods; the specific domain, group or community policy; the blockchain instance; etc. The second part is a flat string composed of alphanumeric characters generated by a specific hash process based on a public key that is recorded on the SCid-associated explanatory profile. It needs to be emphasized that the flat string aforementioned may also contain some fields with predefined semantics.

Note that the analysis in this clause only provides a guideline on how to design the ID of an SCid; the detailed scheme of the ID of an SCid and the data model of SCid-associated explanatory profiles lie outside the scope of this Recommendation.

8 High-level framework of the self-controlled identity

8.1 High-level framework of self-controlled identity

8.1.1 General framework of SCid

Figure 8-1 shows a high-level framework for an SCid, which is supposed to converge diverse SCid instances. The high-level framework of an SCid includes the following three layers.

- **Application layer**: This layer provides applications, e.g., the web services or decentralized applications, or network services, based on the SCid. It provides service interfaces for direct interaction with the entities about the SCid, e.g., applying to create an SCid.
- **Identity layer**: This layer is decentralized as it adopts blockchains as underlay storage. It provides services for SCid life-cycle management, SCid discovery and resolution management, and SCid data access control management. The layer includes multiple function blocks, i.e., for discovery, registry, endorsements, verification and data access management of the identity.
  - Identity discovery function: it discovers and resolves an SCid. According to the SCid ID, the identity discovery function resolves the SCid ID to the SCid-associated explanatory profile. The SCid ID can be input by the users of the application layer, or read from the online text, e.g., the verifiable credential [b-W3C-VC] representations.
  - Identity registry function: it registers SCid-related resource data, which includes the SCid-associated explanatory profile and the hash of the verifiable credentials. The identity registry function can be decentralized APPs since it builds on the smart contracts of the underlay blockchain.
  - Identity endorsement function: it issues verifiable credentials for entities in the SCid system. Any entity that endorses for other entities and issues verifiable credentials has this function.
  - Identity verification function: it verifies the SCid and the attributes of an entity (subject) according to the methods listed in the SCid-associated explanatory profile and verifiable credentials. Any entity that provides applications or communicates with other entities has this function. After verification, authorization by an entity of the SCid subject for further services or resource usage lies outside the scope of this Recommendation.

– Identity data access management function: it manages access control for SCid-related resource data stored on the blockchain ledger. The identity data access management function may have different interfaces to those of the identity registry function, depending on the types of underlay blockchains and SCid operation method, i.e., SCid and associated explanatory profile creation, resolution, update, and deactivation.

– **Infrastructure layer**: This layer provides the networks and computing or storage resources for self-controlled identities and services.

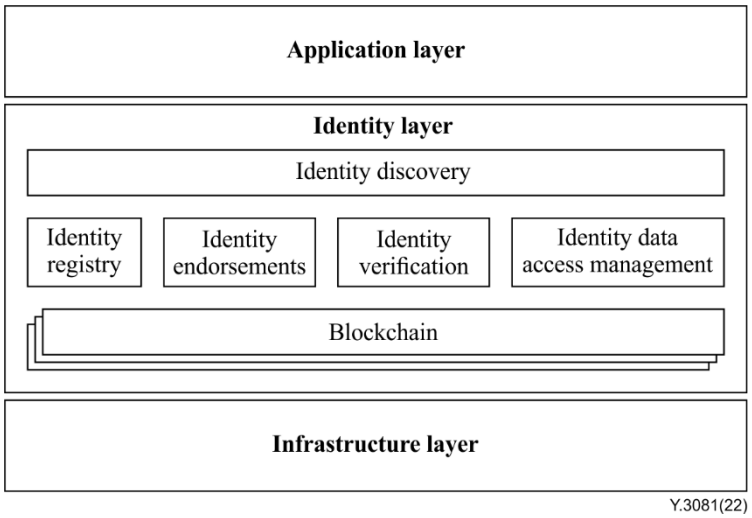


Figure 8-1 – High-level framework of the self-controlled identity

8.1.2 General mechanism and workflow of SCid

Figure 8-2 shows the general workflow of SCid based on the high-level framework. The workflow mainly includes three procedures according to a specific service instance: SCid generation and registration; SCid credential retrieval; and SCid resolution and identity verification.

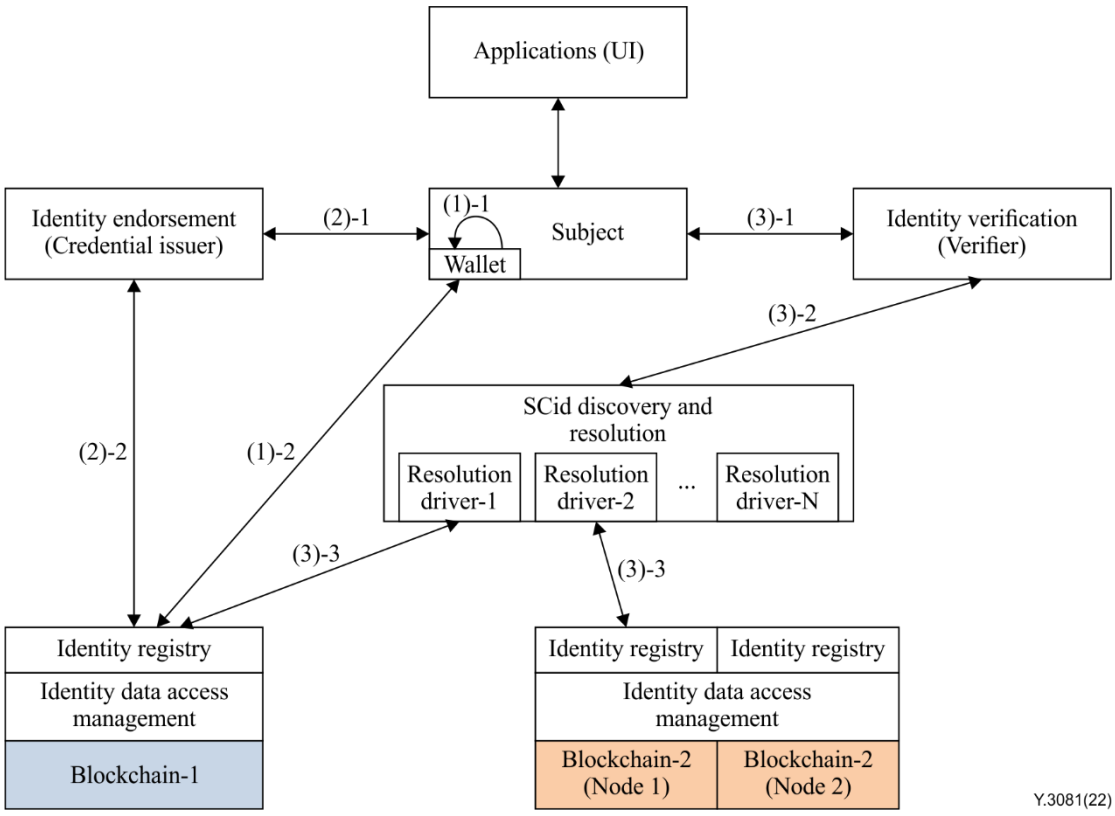


Figure 8-2 – General workflow of a self-controlled identity

1) SCid generation and registration

An entity can generate an ID of an SCid and an associated explanatory profile of the ID locally leveraging an agent (or wallet) embedded in the entity. The agent creates a pair of private and public keys associated with the ID of the SCid, records public key information, ID and reference service point and communication protocols in the associated explanatory profile, and registers the SCid in the blockchain ledger. The agent embedded in the entity can optionally have a remote part where a trusted controller generates and registers the SCid.

2) SCid credential retrieval

An entity applies credentials to the issuers in the SCid system after an SCid is created. The credentials can be issued by any entity in the SCid system, while those issued by the authority issuer is authoritative.

The issuer endorses specific features, attributes or resource ownership of an entity and generates credentials according to a predefined data format recorded in the blockchain ledger. The issuer provides the credentials to the entity and stores the hash of specific fields of the credential and information for validation in the blockchain. The original credential is only kept by the entity itself locally.

The issuer can execute a KYC procedure before issuing a credential to an entity to guarantee information consistency between online and offline. Based on authoritative credentials, the issuer can issue credentials online directly, which establishes a chain of trust in the SCid system. The entity can also make use of self-asserted claims to apply credentials to avoid offline identification. The entity might need to collect multiple credentials from different issuers to access the services of the SPs or networks.

3) SCid resolution and identity verification

When the verifier (SP/network) obtains an ID of the SCid from a service session, the verifier firstly queries a SCid resolver to resolve the ID to its associated explanatory profile recorded on the

blockchain. The verifier verifies the mapping relationship between the SCid owner and ID of the SCid leveraging the metadata and public key in the associated explanatory profile of the ID, since the verifier believes the private key is kept by the SCid owner.

The verifier retrieves the credentials of the SCid owner from the agent for authentication after SCid resolution. The verifier validates the attributes of the SCid owner based on the credentials. The integrity of the credentials and specific fields are verified if necessary based on the information recorded on the blockchain by the issuer. In addition, the entity complies with the principle of minimum disclosure when providing credential information to the verifier, e.g., using zero knowledge proof technology.

8.2 High-level requirements of self-controlled identity based on blockchain

8.2.1 SCid life-cycle management

It is required that the life-cycle management of an SCid, including the generation, registration, endorsement, update, revocation and recovery, be independent of centralized authorities.

It is required that SCid information be portable and transportable to avoid lock-in of the vendor, SP or underlying blockchain.

It is required that the ID of an SCid has multiple types, e.g., public, private and group or community ID, for different scenarios and avoiding identity correlation.

It is required that the ID of an SCid be persistent or temporary. The temporary ID can be used one or a few times in service sessions.

8.2.2 SCid discovery and resolution

It is required that the ID of SCid be unique globally.

It is required that the SCid be discovered and resolved to a SCid-associated explanatory profile in a SCid resolution system.

It is required that the SCid resolution system support multiple resolution engines to adapt to different ID schemes.

8.2.3 Credential issuance of SCid

It is required that each entity in the SCid system support credential issue for other entities.

It is required that the entity in the SCid system support credential issue based on the credentials issued by other entities in the SCid system.

8.2.4 SCid privacy protection

It is required that SCid-related original data, including the credentials data and especially the entity private data, not be stored on the blockchain.

It is required that the owner of the SCid support control and management of credentials and SCid-associated explanatory profile by itself and discloses minimum data when interacting with other entities.

8.2.5 SCid verification

It is required that the entities in the SCid system support verification and authentication directly with each other.

It is required that the entities with different kinds of SCid support interaction with each other.

8.2.6 Blockchain requirements

It is required that the SCid system support multi-vendor and multi-technology blockchain networks.

It is required that the blockchain network in the SCid system ensure that only authorized parties can set up nodes, store data and vote.

8.2.7 Compliance requirements

It is required that SCid data management be regulation compliant.

It is required that the blockchain network in the SCid system support control over geographical distribution of specific privacy data.

9 Capability requirements of the framework of the self-controlled identity

9.1 Capability requirements of the identity registry

The identity registry capability includes SCid ID creation and identity registration. SCid ID creation can be initiated by the application agent, e.g., the identity wallet, installed in the entity. After an SCid has been created, the entity registers the ID and related necessary data in the blockchain ledger of the SCid system.

It is required to provide a capability to create IDs by the entity itself in the SCid system.

It is required to provide a capability to create multiple IDs to avoid correlation by the entity itself in different SCid systems.

It is required to provide a capability to deactivate IDs by the entity itself in the SCid system.

It is required to provide a capability to recover the SCid ID in case of loss of the private key of the entity in the SCid system.

It is required to provide a capability to record the SCid IDs and related necessary data, such as the public key, authentication method, resource ownership, service entries and integrity proof, in the blockchain ledger of SCid systems in an appropriate way, e.g., an associated explanatory profile.

It is required to provide a capability to update the SCid ID-related necessary data in the SCid system, such as the authentication method and service entries.

It is required to provide a capability to record the relationship of the SCid IDs and attached verifiable credentials in the blockchain ledger of the SCid system.

It is required to provide a capability to protect the privacy of entities and to avoid the leaking of entity data in the verifiable credentials.

It is required to provide a capability to record the schemes of the SCid-associated explanatory profile in the blockchain ledger of the SCid system.

It is required to provide a capability to be compatible with centralized identities for the SCid through specific methods, such as identities binding, in the SCid system.

It is required to provide a capability to record the SCid revocation list, which can be queried during SCid resolution.

It is required to provide a capability to record the schemes of the verifiable credentials in the blockchain ledger of the SCid system.

9.2 Capability requirements of the identity discovery and resolution

Identity discovery and resolution provides an entry for verifiers to query SCid information.

It is required that a capability be provided to return the queried SCid information, such as an associated explanatory profile, based on an efficient query algorithm for identity discovery and resolution in the SCid system.

It is required that a capability be provided to converge different SCid systems and different types of IDs for identity discovery and resolution.

It is required that a capability be provided to support high availability for identity discovery and resolution in the SCid system.

It is required that a capability be provided to resolve different granularity resources, such as the SCid-associated explanatory profile or a specific authentication method, based on the input reference of the SCid for identity discovery and resolution in the SCid system.

It is required that a capability be provided to support different data interaction formats to serialize the data model of SCid information resolved through identity discovery and resolution in the SCid system.

It is required that a capability be provided to establish a decentralized identity discovery and resolution service by accessing different identity registries.

9.3 Capability requirements of the identity verification

Identity verification provides verification to the SCid subject and verifiable credentials. Multidimensional verifications are important when entities interact with each other directly.

It is required that a capability be provided to verify the entity of the SCid based on the authentication methods in the SCid-associated explanatory profile, such as the public-private pair keybased algorithms.

It is required that a capability be provided to verify the integrity of the SCid-associated explanatory profile retrieved through the resolution, e.g., private key-based digital signature or specific proof.

It is required that a capability be provided to verify the status about SCid revocation.

It is required that a capability be provided to verify the integrity of the verifiable credentials retrieved from the SCid entity.

It is required that a capability be provided to verify the attributes in the credentials without the original data, such as the zero knowledge proof.

It is required that a capability be provided to provide security communication between SCid entities when executing the verification.

9.4 Capability requirements of the identity endorsement

Identity endorsement enables any entities in the SCid system to issue verifiable credentials and build a trust chain.

It is required to provide a capability to issue verifiable credentials for any entities in the SCid system.

It is required to provide a capability to support the entity to update and revoke the verifiable credentials that have been issued by the same entity in the SCid system.

It is required to provide a capability to support the entity to issue one-time verifiable credentials.

It is required to provide a capability to support the entity to perform offline validation and a KYC procedure when issuing a verifiable credential online in the SCid system.

It is required to provide a capability to support the entity to issue a verifiable credential based on the verification on the other verifiable credentials in the SCid system.

It is required to provide a capability to support various types of verifiable credential schemes for the entities in the SCid system.

It is required to provide a capability to avoid entity privacy data in the credentials, such as the entity identifiable information, device identity and serial number, being recorded in the blockchain ledger, either in plaintext or ciphertext.

It is required to provide a capability to prevent correlation through multiple credentials' data, e.g., storage address, verification method and credential ID.

It is required to provide a capability to keep the verifiable credentials in the software or hardware (trusted execution environment) wallet(agent) of the subject to avoid private data leak.

It is required to provide a capability to record verifiable credentials in blockchain ledgers in the form of data field or file hashes.

It is required to provide a capability to support a trusted third party for subjects to hold verifiable credentials in the SCid system.

9.5 Capability requirements of the identity data access management

Identity data access management provides the application programming interfaces (APIs) for the identity registry to write or read data to or from the blockchain ledger via specific smart contracts.

It is required to provide a capability to support the authentication for writing data to the blockchain ledger, including the SCid-associated explanatory profile, the credentials hash value, the scheme of SCid-associated explanatory profile and verifiable credentials, in the SCid system.

It is required to provide a capability to return SCid information query results to the identity registry as a resolution response.

It is required to provide a capability to record specific data of SCid off-chain to comply with data management regulations, e.g., deletion of original data and local data storage, in the SCid system.

It is required to provide a capability to support exposure of common APIs to the identity registry, even over multiple types of blockchain or multiple blockchain instances.

9.6 Capability requirements of the blockchain

The blockchain is an underlay enabling technology for the ID registry repository. Tamper-proof and sequential append-only features of the blockchain are used to establish trustworthiness among entities in the SCid system.

It is required to provide a capability to support multiple types of blockchain in the SCid system.

It is required to provide a capability to support the interaction of entities over different types of blockchains in the SCid system.

It is required to provide a capability to support the unified management of smart contracts that may deployed in multiple blockchain nodes to guarantee the consistency of SCid-related data and access rights of the entities.

It is required to provide a capability to support off-line management of the joining of blockchain organizations and ledger nodes if credential issuers involve authority off-line.

10 Security considerations

Security and privacy considerations of an SCid based on blockchain in future networks, including networks beyond IMT-2020, include the following aspects.

SCid management includes security considerations of SCid resolution, SCid correlation, SCid-associated explanatory profile integrity and SCid recovery.

SCid data privacy management includes security considerations of entity data privacy, verifiable credential data privacy, off-chain data local storage and verification and identity information correlation.

Blockchain security includes security considerations of smart contract management, certificate management, private key storage and recovery of a subject, as well as multi-vendor blockchain interoperability. Additional blockchain security considerations can be optionally aligned with the capability requirements specified in [b-ITU-T X.1402].

End-to-end communication includes security considerations of the off-chain data interaction between the SCid verifier and SCid subject.

In addition, the security and privacy considerations of an SCid based on blockchain can be optionally aligned with the security guideline requirements specified in [b-ITU-T X.1403].

Appendix I

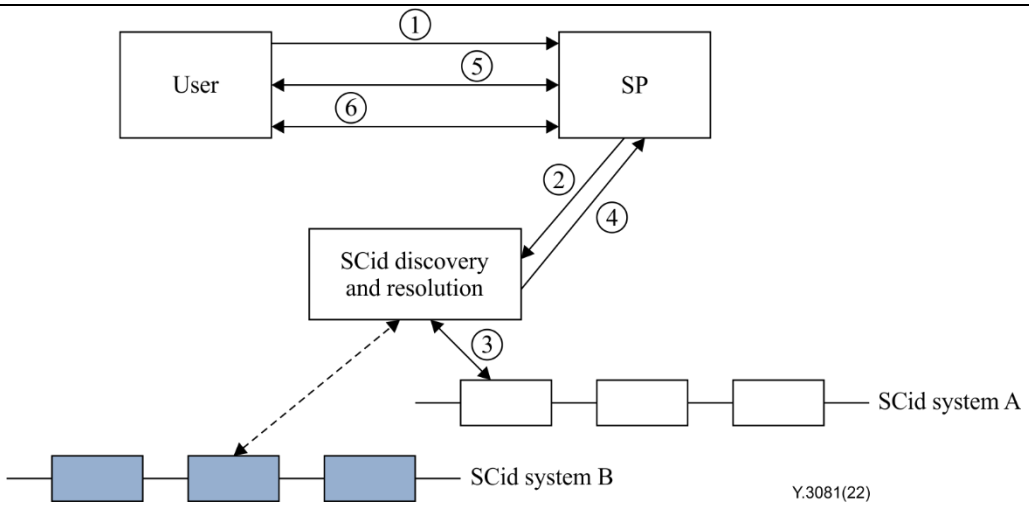
Use cases of self-controlled identity

(This appendix does not form an integral part of this Recommendation.)

I.1 SCid discovery and verification

See Table I.1.

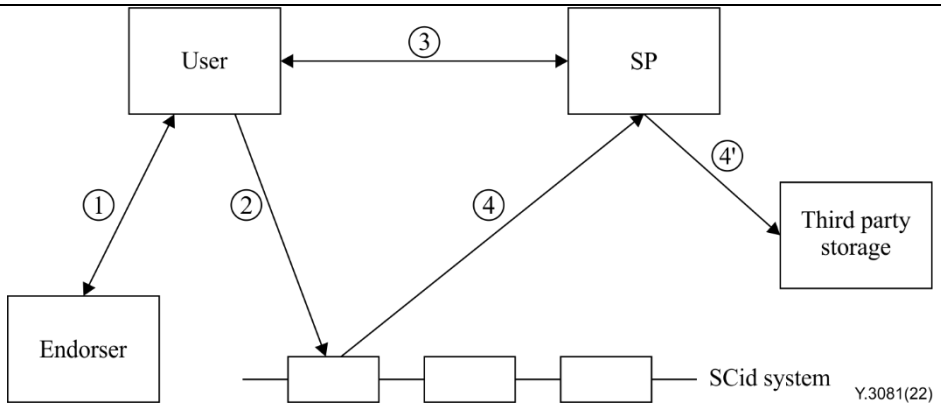
Table I.1 – SCid resolution and verification

Description	A user needs to access the SP and uses the service provided by the SP.
Pre-conditions (optional)	The user has registered its SCid.
Post-conditions (optional)	The user is allowed to access the services provided by the SP.
Figure and operational flows (optional)	 Operational flows: 1) the user discloses its SCid to the SP; 2) the SP looks up the SCid using the SCid discovery and resolution function; 3) the SCid discovery and resolution function retrieves the SCid-associated explanatory profile from the SCid system A; 4) the SCid discovery and resolution function returns the profiles to the SP; 5) the SP verifies the user; 6) the user establishes end-to-end communication with the SP.
Derived requirements	1) Identity discovery and resolution is required to address and resolve the SCid to its registered blockchain ledger.

I.2 Decentralized KYC based on SCid

See Table I.2.

Table I.2 – Decentralized KYC based on SCid

Description	A user has an SCid and related KYC information such as the age and education in a credential endorsed by the regulatory authorities. The user needs access to an SP that requires a KYC procedure.
Pre-conditions (optional)	The user already has created and registered a SCid.
Post-conditions (optional)	The user completes the KYC procedure without inputting personal information to the SP.
Figure and operational flows (optional)	 Operational flows: 1) The user acquires the endorsement for age and education from the endorser entity online or offline. The endorser issues the credential to the user based on a specific data scheme. The credential includes necessary attributes, such as the diploma as well as the required cryptographic proof (digital signature). 2) The user uploads the KYC endorsement information to the SCid system based on the blockchain as an entry in the attached profile binding with the SCid. The attached entry can only include the URI of the credential to avoid privacy leak. The original credential could be stored in user devices or a trusted third party agent. 3) The user accesses the SPs with the SCid. To avoid ID correlation, the user could utilize separate IDs to access different SPs. 4) The SP queries the SCid system by the SCid of the user to obtain and verify the credential information. 4') Optionally, the SP may only get the link of the KYC information and it needs to access the third party storage to obtain the credential information to execute the KYC procedure.
Derived requirements	1) The SCid is required to have an attached profile to record the attributes and endorsement, which could be updated if necessary. 2) The SCid is required to have multiple SCids to avoid the ID correlation. 3) The SCid is required to support data exchange between the user and SPs for the KYC without presenting the original credential data.

Appendix II

Self-controlled identity business models

(This appendix does not form an integral part of this Recommendation.)

As the application scenarios of the SCid are diverse, the business models also differ and depend on the roles. In this appendix, some but not all business models are listed.

II.1 Cross-SP digital ecosystem

There are three main roles in addition to the SCid systems in this business model, as illustrated in Figure II.1.

- The SPs who verify the SCid, authorize the access and provide the specific service to the user with the SCid.
- The credential issuers who endorse the credentials to the user and bind the credentials with the SCid. Credentials can include an ID issued by a government, driving licence, diploma, social security number and specific certificates from other reliable credential providers. In addition, credentials can also consist of online virtual objects, e.g., entities and assets.
- The user who accesses the services of SPs with the SCid.

The business model of a cross-SP digital ecosystem will benefit from the SCid since all SPs share the full amount of users and credentials and reduce the cost of developing new users and maintaining user privacy data.

In this business model, the user has an SCid and registers it on the SCid system. Credentials for the user have been issued. On user access, SPs can discover the SCid by identity discovery and resolution function, verify and provide service to the user based on the specific profile in the SPs. When necessary information, such as age, is required, SPs can apply to obtain it from credentials based on user permission.

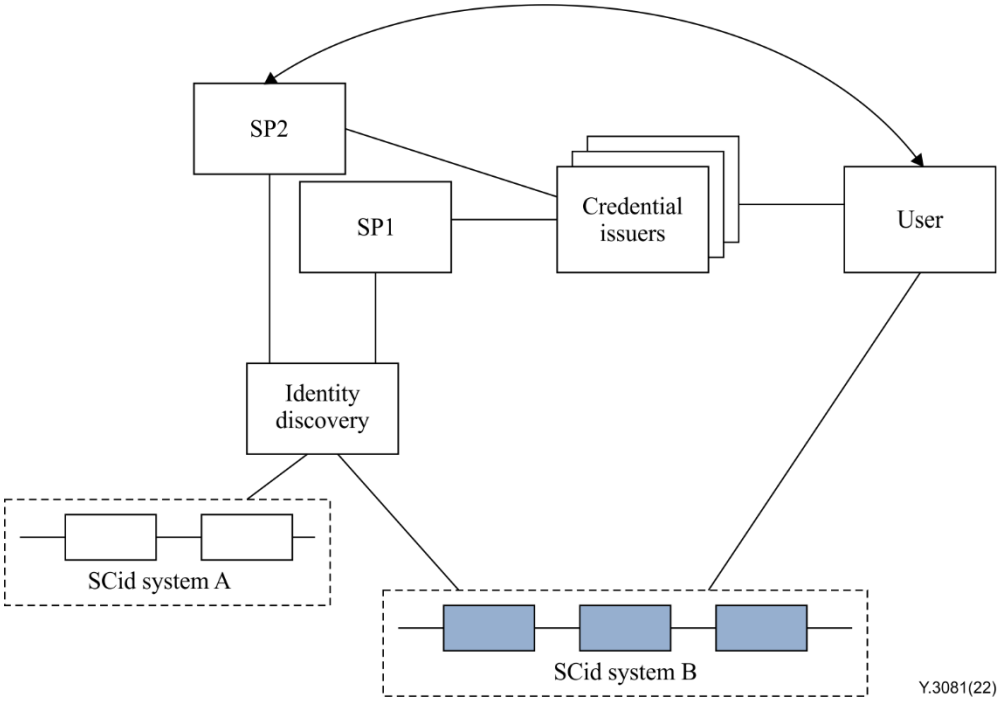


Figure II.1 – Business model of cross-SP digital ecosystem

II.2 Decentralized trustworthy marketplace

There are two main roles in addition to the SCid system in this business model, as illustrated in Figure II.2.

- The credential issuers who endorse the credentials for the user and bind the credentials with the SCid. Credentials can include an ID issued by a government, driving licence, diploma, social security number, and specific certificates from other reliabe credential providers. In addition, credentials can be an endorsement for resource ownership of the entities.
- The users who verify the SCid and mutually exchange information. Users generate transactions with each other and share resources. The user in this case can be an individual, a device, a terminal, a network operator, an SP, a third party resource provider or a regulator authority.

The decentralized trustworthy marketplace in this business model enables sharing of a heterogeneous network resource in terms of the computing, storage, network, content, spectrum, data, serverless function or virtualization function, etc., between users directly across multiple technological and administrative domains. The decentralized trustworthy marketplace improves multi-party collaboration and value delivery in future networks, including networks beyond IMT-2020.

In this business model, users register SCids on the SCid system, and obtain the necessary credentials from credential issuers, such as individual or enterprise IDs. Users associate the network resource catalogue that can be shared with the SCid. Based on the network resource catalogue, users share network resources with each other and perform billing.

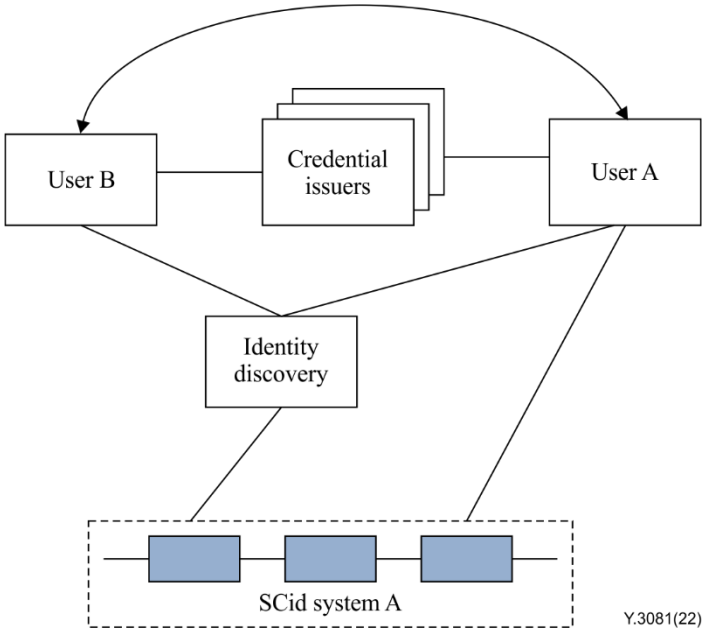


Figure II.2 – Business model of a decentralized trustworthy marketplace

II.3 Self-bootstrapping and service provision of vertical industry devices

There are three main roles in addition to the SCid systems in this business model, as illustrated in Figure II.3.

- The credential issuers who provide erifiable credentials for vertical industry devices, which may include: the product serial number; the component serial numbers of the device; the device state integrity signature; access control list configuration; and the owner. Credential issuers can be the original equipment manufacturer, vendors of physical hardware elements and software elements or distributors.

- The devices of vertical industries are mainly terminals and equipment that are connected to the network of vertical industries, including industrial sensors, vehicles, drones, cameras, factory equipment; and medical equipment.
- The mobile operator who provides the network connection service for the devices of vertical industries.

A massive number of vertical industry devices is expected to connect to the IMT-2020 network directly. Self-bootstrapping and service provision of the devices is a promising way for mobile operators and field service vendors providing like installation or maintenance to reduce costs and improve efficiency.

In this business model, the device creates the SCid and registers it on the SCid system. The device will require credentials, which can include device state integrity and ownership, from the credential issuers, when the device performs self-bootstrapping. When the device connects to the mobile operator, the mobile operator will verify the device according to the SCid and associated credentials before service provision, e.g., embedded subscriber identity module issue, billing discount and quality of service configuration.

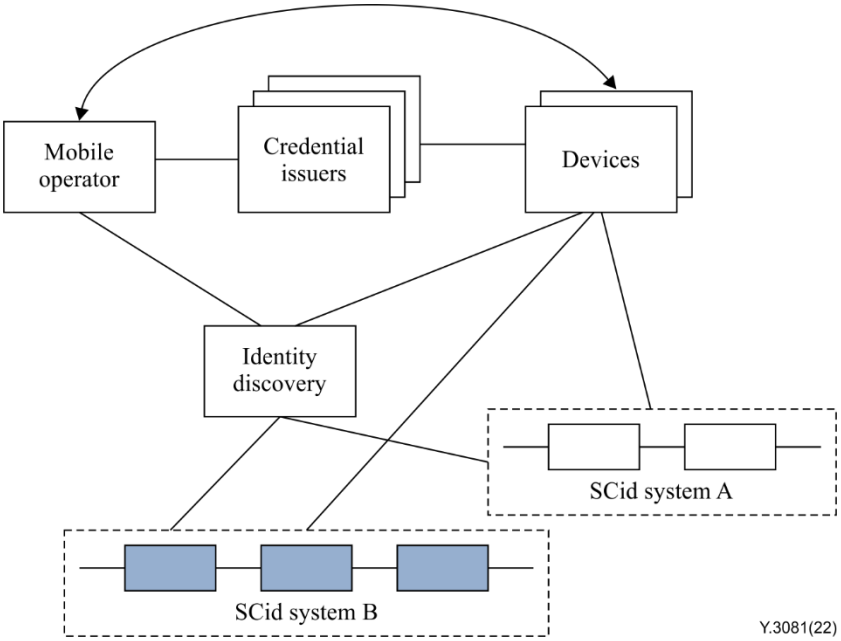


Figure II.3 – Business model of self-bootstrapping devices of vertical industry

Bibliography

[b-ITU-T E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-W3C-DID] W3C (2022), *Decentralized identifiers (DIDs) v1.0 –, Core architecture, data model, and representations.* Available [viewed 2022-11-10] at: https://www.w3.org/TR/did-core/

[b-W3C-VC] W3C (2022), *Verifiable credentials data model v1.1.* Available [viewed 2022-11-11] at: https://www.w3.org/TR/vc-data-model/

[b-Zooko's triangle] Wilcox-O'Hearn, Z (2001), *Names: Decentralized, secure, human-meaningful: Choose two.* Boulder, CO: Zooko. Available [viewed 2022-11-10] at: https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html.

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, 2022