

Recommendation

ITU-T Y.3087 (04/2025)

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 – Functional requirements and architecture

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
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	Y.1000-Y.1999
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	Y.2000-Y.2999
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	Y.4000-Y.4999
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.3087

Self-controlled identity based on blockchain – Functional requirements and architecture

Summary

Recommendation ITU-T Y.3087 specifies the functional architecture of self-controlled identity (SCid) based on blockchain, as well as the functional requirements, reference points and basic operational procedures.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3087	2025-04-29	13	11.1002/1000/16314

Keywords

Blockchain, functional architecture, functional requirements, future networks, operational procedures, self-controlled identity.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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 <https://www.itu.int/ITU-T/ipr/>.

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview.....	3
7	Functional requirements	4
	7.1 General requirements.....	4
	7.2 Application layer	4
	7.3 Identity layer.....	5
	7.4 Infrastructure layer	5
8	Functional architecture	5
	8.1 SCid subject function	6
	8.2 Identity verification function.....	8
	8.3 Identity endorsement function.....	9
	8.4 Identity registry function	9
	8.5 Identity data access management function	10
	8.6 Identity discovery and resolution function	10
9	Reference points	11
	9.1 Reference point RP-aa	11
	9.2 Reference point RP-asa	11
	9.3 Reference point RP-asv	11
	9.4 Reference point RP-cs	11
	9.5 Reference point RP-cr	12
	9.6 Reference point RP-ar	12
	9.7 Reference point RP-sar.....	12
	9.8 Reference point RP-svr.....	12
	9.9 Reference point RP-sri	12
	9.10 Reference point RP-rer	12
	9.11 Reference point RP-rr.....	12
10	Basic operational procedures.....	12
	10.1 Procedure for SCid creation	12
	10.2 Procedure for SCid resolution	13
	10.3 Procedure for SCid verification.....	14
	10.4 Procedure for verifiable credential application	15

	Page
10.5 Procedure for verifiable credential verification.....	18
10.6 Procedure for credential data model scheme registration.....	19
11 Security considerations	19
Bibliography.....	20

Recommendation ITU-T Y.3087

Self-controlled identity based on blockchain – Functional requirements and architecture

1 Scope

This Recommendation specifies the functional requirements and architecture of self-controlled identity (SCid) based on blockchain.

The scope is as follows:

- Functional requirements
- Functional architecture
- Reference points
- Basic operational procedures.

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 standalone document, the status of a Recommendation.

- [[ITU-T Y.2091](#)] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for 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.3081](#)] Recommendation ITU-T Y.3081 (2022), *Self-controlled identity based on blockchain – Requirements and framework*.

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 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.

3.1.3 digital entity [b-ITU-T X.1255]: An entity represented as, or converted to, a machine-independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; the structure helps to enable interoperability among diverse information systems in the Internet.

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

3.1.5 identifier [ITU-T Y.2091]: An identifier is 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).

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

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

3.1.8 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.

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

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

3.1.11 self-controlled identity (SCid) [ITU-T Y.3081]: 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.

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

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

3.1.14 virtual entity [b-ITU-T Y.2814]: A unit of virtualized component for reconfigurable networks. Virtual entities are categorized into four types: function, controller, device and application; while groupings of virtual entities are used to reconfigure the network.

3.1.15 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

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 self-controlled identity resolution: A function to resolve an identifier of self-controlled identity (SCid) into associated explanatory profile and relevant state information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AFOC	Attributes, Features, Ownership and Capabilities
API	Application Programming Interface
APP	Application
BC	Blockchain

DDoS	Distributed Denial-of-Service
FE	Functional Element
ICT	Information and Communication Technology
ID	Identifier
RP	Reference Point
SCid	Self-Controlled identity
TEE	Trusted Execution Environment
VC	Verifiable Credential

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which 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/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

With the development of information and communication technology (ICT) and the promotion of digital transformation of the industries, more and more digital resources and activities are carried on the ICT infrastructure of giant service providers and network providers, which leads to the continual increase of user-centric or entity-centric requirements. On the one hand, users continue to be concerned about the ownership, control and usage of their sensitive data online, which may include private data, credential information, activity information, configuration information and so on. On the other hand, users also seek the digital transport of assets and credentials across multiple applications or network ecosystems based on one (the same) identity. Furthermore, the identity of a user or entity can be endorsed on specific attributes, features, ownership, capabilities and so on, by any other user or entity leveraging the verifiable credentials. Thus, it is necessary for the user or entity to create, control and manage its identity and related data, independently of any specific identity provider or the third party.

According to [ITU-T Y.3081], SCid is defined as an identity created, controlled and managed in a decentralized manner by the entity itself. The SCid aims to meet the needs of emerging innovated services, such as aspects of self-created identity, minimum disclosure of identity-related data, the trust chain of the verifiable credentials [b-W3C-VC], virtual object identification such as digital humans [b-ITU-T F.748.15] and AI agents [b-ISO/IEC 22989], and data asset exchange and circulation.

Figure 6-1 shows the high-level framework for the SCid system.