International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4811

(11/2021)

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

Internet of things and smart cities and communities – Identification and security

Reference framework of converged service for identification and authentication for IoT devices in decentralized environment

Recommendation ITU-T Y.4811

ITU-T

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.4811

Reference framework of converged service for identification and authentication for IoT devices in decentralized environment

Summary

Recommendation ITU-T Y.4811 is intended to develop a converged identification and authentication service to overcome relevant challenges in decentralized Internet of things (IoT) identification and authentication management systems, so as to ensure efficient communication among IoT devices and services in decentralized environments. The challenges in decentralized environments are to support effective and efficient interactions (e.g., secured interoperability, scalability, low latency, etc.) among a huge number of IoT devices and IoT services, which are using different decentralized IoT identification and authentication systems.

This Recommendation introduces a converged service for identification and authentication for IoT devices in decentralized environment (CSIADE), and provides relevant common characteristics, general requirements, functional architecture, main capabilities and procedures of CSIADE. CSIADE can facilitate IoT devices and IoT services to identify and authenticate each other in IoT decentralized environments when they use the same or different types of decentralized IoT identification solutions.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4811	2021-11-29	20	11.1002/1000/14821

Keywords

Authentication, blockchain, device, identification and authentication service.

[*] 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

Page

Recommendation ITU-T Y.4811

Reference framework of converged service for identification and authentication for IoT devices in decentralized environment

1 Scope

This Recommendation specifies a converged service for identification and authentication for IoT devices in decentralized environment (CSIADE). It provides common characteristics and general requirements, functional architecture, main capabilities and procedures of CSIADE. The scope of this Recommendation includes:

– the concept, common characteristics and general requirements of CSIADE,

– the functional architecture, main capabilities and procedures of CSIADE.

NOTE – Use of conventional centralized IoT identification and authentication management systems are out of the scope of this Recommendation and this Recommendation does not contradict existing centralized IoT identification and authentication systems.

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.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of Internet of things.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 authentication [b-ITU-R M.1224-1]: The process of verifying the identity of a user, terminal, or service provider.

3.1.3 blockchain [b-ISO 22739]: Distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links.

NOTE – Blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records.

3.1.4 blockchain platform [b-ITU-T Y.4464]: A platform (or system) that is established based on blockchain-related technologies.

3.1.5 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, date capture, data storage and data processing.

3.1.6 functional entity [b-ITU-R M.1224-1]: A grouping of service providing functions at a single location. It is a subset of the total set of functions required to provide the service.

3.1.7 identification [b-ITU-R M.1224-1]: A step in a procedure used to identify a user or terminal to a service provider for the purposes of broad prevention.

3.1.8 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.9 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.10 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 Internet of things entity (IoT entity): A functional entity (e.g., IoT service, IoT gateway) or physical entity (e.g., IoT device, end user device) that participates in activities performed in Internet of things (IoT).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AM-FC	Functional Component of Authentication Management
CSIADE	Converged Service for IoT Identification and Authentication in Decentralized Environment
DID	Decentralized Identity
DLT	Distributed Ledger Technology
FC	Functional Component
GUID	Globally Unique Identifier
IDR	Identity Resolving
IOS	Identity Object Storage
IoT	Internet of Things
IR-FC	Functional Component of Identity Resolution
ITS	Intelligent Transport Service
JSON	JavaScript Object Notation
PKI	Public Key Infrastructure
PM-FC	Functional Component of Policy Management
PII	Personal Identifying Information
URI	Uniform Resource Identifier

5 Conventions

This Recommendation uses the following conventions:

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

– The keywords "is recommended" indicate a requirement that is recommended, but which is not absolutely required to claim conformance with this Recommendation.

6 Introduction of CSIADE

The converged service for IoT identification and authentication in decentralized environment (CSIADE) for IoT devices is a functional entity which leverages Internet of things (IoT) services and IoT devices to integrate and access capabilities of IoT identification and authentication provided by multiple IoT identity management systems and authentication systems. CSIADE can act as a bridge, with which IoT devices and IoT services can identify and authenticate each other in IoT decentralized environments, even though they use different decentralized IoT identification solutions or different authentication solutions.

CSIADE establishes one type of decentralized cooperation mode among IoT services and IoT devices which may be provided by the same or different operators (see Figure 6-1). IoT devices and IoT services, individually, can get identifiers and corresponding identity objects (see Appendix II) from their operators, and can also create identifiers and corresponding identity objects by themselves, and their operators can endorse the identifiers and the corresponding identity objects respectively. Then through CSIADE, IoT devices and IoT services can issue their identifiers in decentralized system(s), and store their corresponding identity objects in cloud(s) individually. The corresponding identity objects in cloud(s) can be encrypted by their owners (such as IoT devices or IoT services) and can be linked to the identifiers as stored in decentralized system(s) respectively.

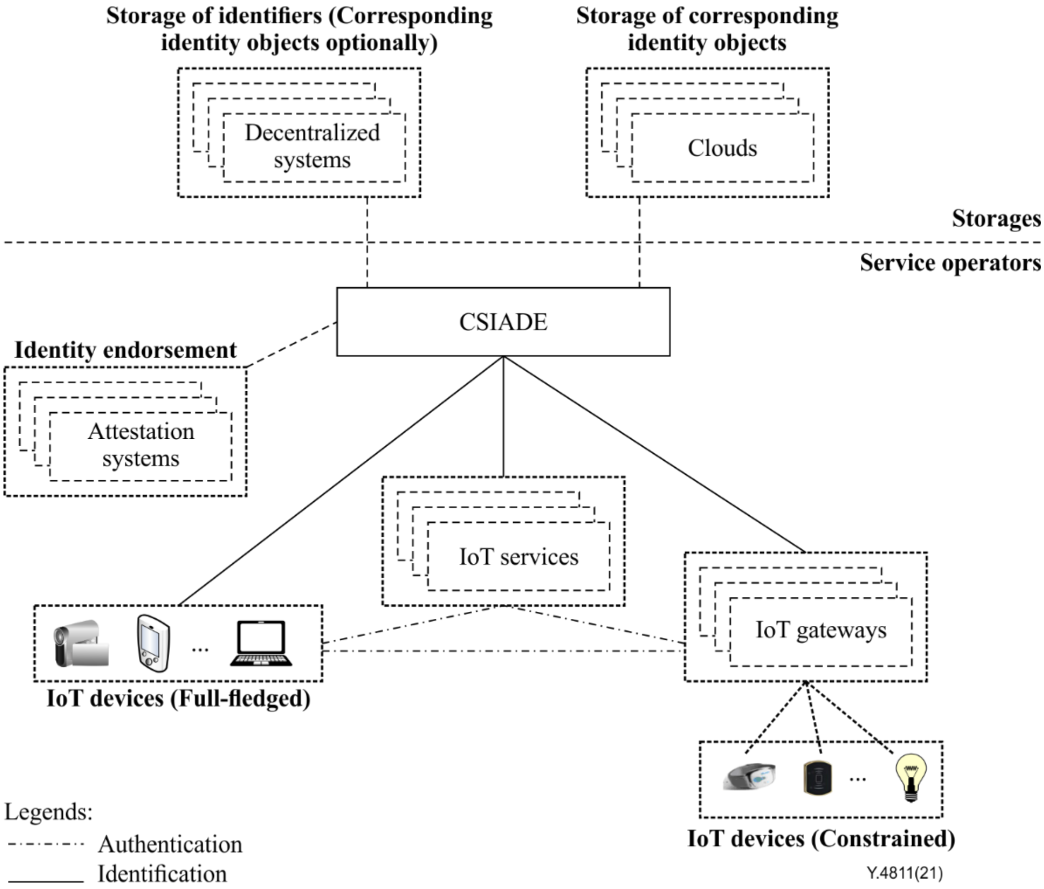

Figure 6-1 – Overview of CSIADE

When IoT devices apply to access IoT services, or IoT services apply to connect to IoT devices, through CSIADE, IoT services and IoT devices can resolve the identifiers of their counterparts enabled by the decentralized systems, and can retrieve the corresponding identity objects of the counterparts from the cloud(s). The IoT services and IoT devices can then directly identify and authenticate each other with their identifiers and corresponding identity objects. Therefore, IoT devices and IoT services identify and authenticate each other with the supports of CSIADE directly, even though they use different types of decentralized IoT identification solutions.

NOTE 1 – Appendix III provides business roles and models of CSIADE, and illustrates the relationships of the entities (such as IoT devices, IoT services, attestation systems, decentralized systems, clouds and CSIADE), involved in converged service for identification and authentication for IoT devices and IoT services in decentralized environment.

NOTE 2 – An operator can use relevant attestation system(s) (as shown in Figure 6-1) to provide an identity endorsement service to its IoT devices and IoT services, i.e., to endorse their corresponding identity objects. Typically, an attestation system may sign relevant identities by the operator's private key if using a public key infrastructure (PKI) security mechanism. It is noted that this Recommendation does not cover the solutions about identity endorsement for IoT entities.

6.1 Identifier and corresponding identity object

An identity of an IoT entity consists of one or multiple identifier(s) and one corresponding identity object. An identifier is a unique string (such as URI, GUID, or other types of unique expression), and the corresponding identity object contains compound information to support identification and authentication for the IoT entity.

Appendix II provides reference information about identifiers, identifier packages and corresponding identity objects.

6.2 Converged identification and authentication

IoT entities can create their identities by themselves, and then request their operators or owners to endorse the identities. Alternatively, attestation systems can create and endorse identities for IoT entities on behalf of the operators or owners of the IoT entities respectively, and then send the identities to the IoT entities in a secure communication channel (see clause 8.8.1).

After that and as shown in Figure 6-2, the IoT entities issue their identifiers and corresponding identity objects to CSIADE. Through CSIADE, the identifiers of IoT entities can be stored in decentralized systems, and the corresponding identity objects can be stored in cloud storages (or stored in decentralized systems as well).

The identifiers in decentralized system(s) and the corresponding identity objects in cloud storages can be linked, where one can be located via another (see Appendix II).

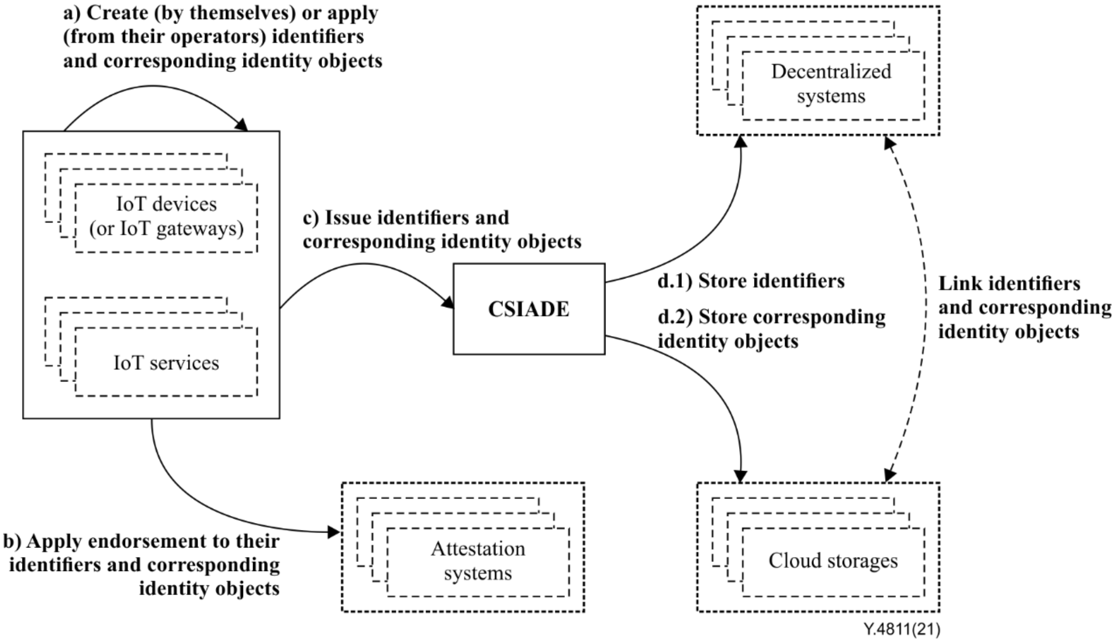
a) Create (by themselves) or apply (from their operators) identifiers and corresponding identity objects
IoT devices (or IoT gateways)
IoT services
c) Issue identifiers and corresponding identity objects
CSIADE
d.1) Store identifiers
d.2) Store corresponding identity objects
Decentralized systems
Link identifiers and corresponding identity objects
Cloud storages
b) Apply endorsement to their identifiers and corresponding identity objects
Attestation systems
Y.4811(21)

Figure 6-2 – Creation, endorsement and issuance of identifiers and corresponding identity objects

When an IoT device applies to access to an IoT service, as shown in Figure 6-3, the IoT device and the IoT service can retrieve the identifiers and corresponding identity objects of the counterpart through CSIADE. After that, with the supports of CSIADE, the IoT device and the IoT service can identify and authenticate each other directly, without the help of traditional identification systems and authentication systems. The IoT device and the IoT service can access relevant attestation system(s) to verify the endorsement(s) if needed, according to the information provided in relevant corresponding identity object(s).

In this case, with the supports of CSIADE, the IoT device and IoT service can use the same or different types of decentralized identity solutions and authentication solutions.

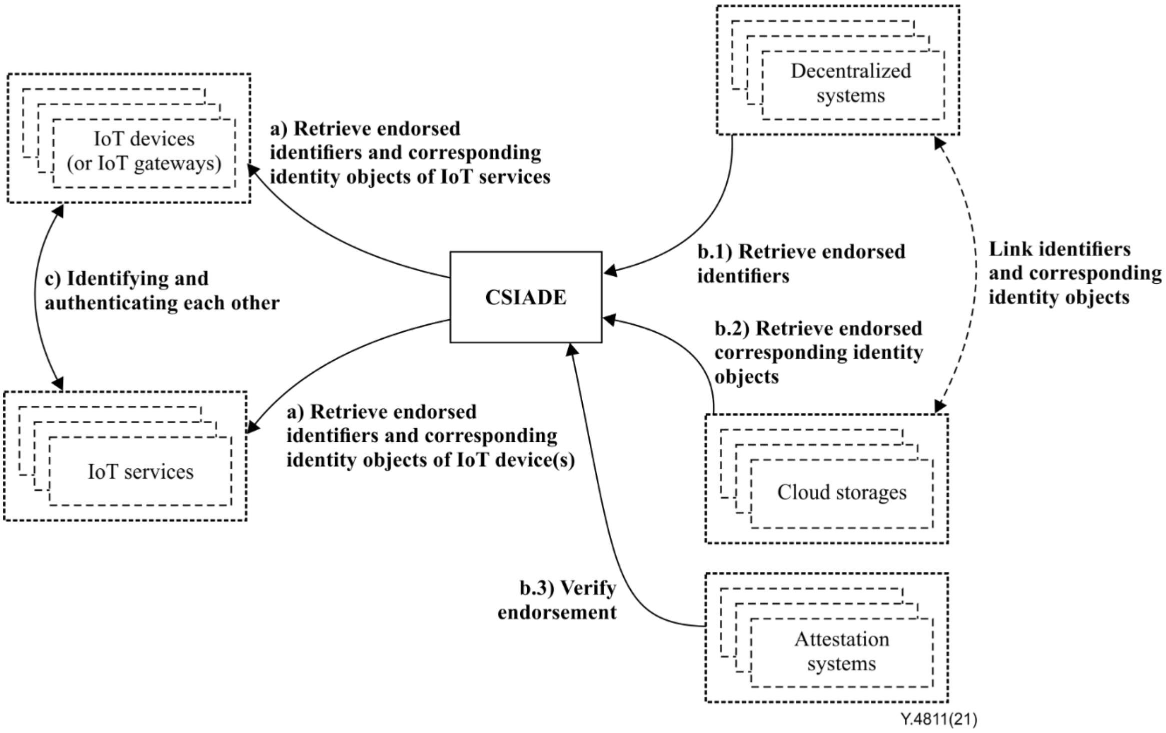
IoT devices (or IoT gateways)
a) Retrieve endorsed identifiers and corresponding identity objects of IoT services
Decentralized systems
b.1) Retrieve endorsed identifiers
Link identifiers and corresponding identity objects
c) Identifying and authenticating each other
CSIADE
b.2) Retrieve endorsed corresponding identity objects
IoT services
a) Retrieve endorsed identifiers and corresponding identity objects of IoT device(s)
Cloud storages
b.3) Verify endorsement
Attestation systems
Y.4811(21)

Figure 6-3 – Retrieving, identifying and authenticating among IoT entities

Optionally, identifiers and corresponding identity objects of IoT entities can be stored together in decentralized system(s) or in cloud storages. It is decided by IoT entities how to store their identifiers and corresponding identity objects.

NOTE 1 – CSIADE is compatible with different types of IoT identification solutions, such as W3C DID [b-W3C-DID], and can connect to decentralized system(s), such as blockchain platforms, or distributed ledger technology (DLT) systems, but it is not limited in any special decentralized system.

NOTE 2 – CSIADE is compatible with different types of authentication solutions. When the counterparts get the identifiers and corresponding identity objects, they can authenticate each other directly with supports of CSIADE.

NOTE 3 – The attestation systems can use different solutions to endorse the identifiers and corresponding identity objects. When IoT entities get the endorsed identities, they can exchange information with the corresponding attestation systems to verify the endorsements.

7 Common characteristics and general requirements of CSIADE

7.1 Common characteristics

This clause provides the common characteristics of CSIADE.

7.1.1 Supporting self-resolving identifier and corresponding identity object

The identifier and corresponding identity object of an IoT entity are self-resolving (see Appendix II). When two IoT entities interact with each other, any side can identify and authenticate its counterpart, just depending on identifiers and corresponding identity objects. CSIADE supports IoT entities to manage (including creating, issuing, storing, retrieving, updating, withdrawing, etc.) and exchange their identifiers and corresponding identity objects.

7.1.2 Supporting independent end-to-end identification and authentication in decentralized environment

Traditionally, operations about identification and authentication for IoT entities are performed by relevant centralized or distributed systems. With supports of CSIADE, IoT entities can perform independent end-to-end identification and authentication with one another. An identifier and corresponding identity object contain sufficient information to identify and authenticate an IoT entity. CSIADE ensure the authenticity, integrity, compliance and consistency of the identifiers and corresponding identity objects, and prevent illegal tampering and malicious use in decentralized environment, with the assistance of relevant systems.

7.1.3 Supporting self-controllable storages for identifiers and corresponding identity objects

In CSIADE, the owners of IoT entities decide how to store their identifiers and corresponding identity objects. An identifier and its corresponding identity object of an IoT entity can be stored separately; the identifier can be stored in a decentralized system, and the corresponding identity object can be stored in a decentralized system, or in a cloud, or even just in the IoT entity as per requests of the owner of the IoT entity (see Appendix II).

Separate storage mechanisms of identifiers and corresponding identity objects of IoT entities has the following advantages:

- Allowing an IoT entity may have multiple identifiers. One is a primary identifier, and others are aliases. The primary identifier is stored with its corresponding identity object. The aliases of the identifier can be stored in decentralized systems. Through any of the available aliases, the primary identifier and corresponding identity object can be found and retrieved. The aliases of an identifier can be expired and set as unavailable by the owner or operator, if needed.
- Supporting user-controllable storage of corresponding identity objects. The corresponding identity objects can be stored in traditional storages (such as clouds), and can be protected with specific access permissions.
- Supporting withdrawal of an identifier and its corresponding identity object. Since only aliases of the identifier are stored in decentralized systems, but the corresponding identity object is stored controllably, it is therefore easily withdrawn, such as setting the aliases of the identifier expired in the decentralized systems and setting the corresponding identity object inaccessible from its storage, if authorized.

NOTE – If an identifier and corresponding identity object of an IoT entity are stored together, usually they are stored in a decentralized system. In this case, the corresponding identity object may be stored by multiple entities of the decentralized system. This may lead to potential risks of the sensitive data in the corresponding identity object being leaked and being maliciously used.

7.1.4 Supporting online and offline endorsement for the identity

The identifier and corresponding identity object of an IoT entity are endorsed by the attestation system of its owner or operator. After endorsement, information for identification and authentication and information of the attestation system are stored in the corresponding identity object. The information in the corresponding identity object is sufficient to be used to identify and authenticate the IoT entity. Therefore, the attestation systems are usually operating offline to endorse identifiers and corresponding identity objects. Alternately, the attestation systems can provide online services to verify their endorsements.

7.1.5 Supporting multiple solutions of identification and authentication

IoT entities can use the same or different identification and authentication solutions. When IoT entities identify and authenticate each other, if they use different identification and authentication solutions, they can exchange relevant necessary information by themselves, or through CSIADE.

7.2 General requirements

This clause provides the general requirements of CSIADE.

7.2.1 Self-resolving identifier and corresponding identity object

- CSIADE is required to support self-resolving identifiers and corresponding identity objects for IoT entities.
- CSIADE is required to support IoT entities to manage (creating, issuing, storing, retrieving, updating, withdrawing, etc.) and exchange their identifiers and corresponding identity objects, in compliance with local and regional data regulations.

7.2.2 Independent end-to-end identification and authentication

- CSIADE is required to enable IoT entities to perform end-to-end identification and authentication directly, without assistance of other third parties.
- CSIADE is required to ensure authenticity, integrity, compliance and consistency of identifiers and corresponding identity objects of IoT entities, and prevent illegal tampering and malicious use, in decentralized environments.

7.2.3 Self-controllable storages for identifiers and corresponding identity objects

- CSIADE is required to enable IoT entities to control storage (e.g., through pre-defined policies) for their identifiers and corresponding identity objects, such as the former being stored in decentralized systems and the latter being stored in clouds, in compliance with local and regional data regulations.
- CSIADE is required to provide a mechanism to link identifiers and relevant corresponding identity objects if they are stored separately in different systems.
- CSIADE is recommended to enable IoT entities to store their identifiers in a decentralized system, and to store corresponding identity objects in clouds, in compliance with local and regional data regulations.

7.2.4 Online and offline endorsement for the identity

- CSIADE is required to support identifiers and corresponding identity objects of IoT entities that are endorsed by attestation systems of relevant owners or operators.
- CSIADE is recommended to support attestation systems to endorse identifiers and corresponding identity objects, offline or online.

7.2.5 Multiple solutions of identification and authentication

- CSIADE is recommended to support IoT entities to use the same or different identification and authentication solutions.

7.2.6 Synchronisation and scalability

- CSIADE is required to provide mechanisms for scalability and synchronisation to support a variable number of IoT entities, especially for huge amounts of IoT devices.

7.2.7 Security and PII protection

- CSIADE is required to provide security mechanisms when processing (such as storing, transferring, endorsing, etc.) identifiers and corresponding identity objects.
- CSIADE is required to provide personal identifying information (PII) protection when processing (such as storing, transferring, endorsing, etc.) identifiers and corresponding identity objects.

8 Functional architecture of CSIADE

CSIADE works on the service support and application support layer of the IoT reference model specified in [ITU-T Y.4000]. Figure 8-1 is a schematic diagram of the functional architecture of CSIADE.

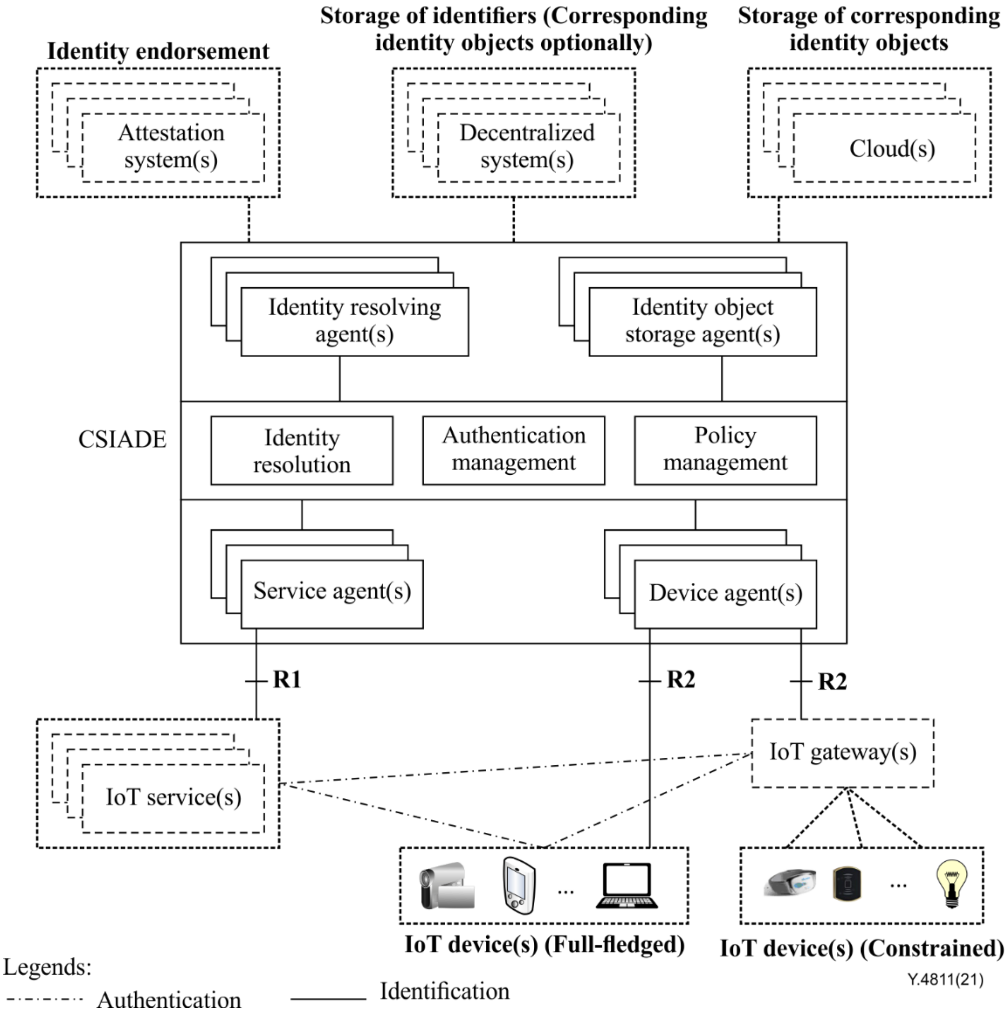
Identity endorsement
Storage of identifiers (Corresponding identity objects optionally)
Storage of corresponding identity objects
Attestation system(s)
Decentralized system(s)
Cloud(s)
CSIADE
Identity resolving agent(s)
Identity object storage agent(s)
Identity resolution
Authentication management
Policy management
Service agent(s)
Device agent(s)
R1
R2
R2
IoT service(s)
IoT gateway(s)
...
...
IoT device(s) (Full-fledged)
IoT device(s) (Constrained)
Legends:
Authentication
Identification
Y.4811(21)

Figure 8-1 – Functional architecture diagram of CSIADE

CSIADE includes three groups of logical functional components (FCs) intended for: interactions with attestation and decentralized systems and clouds, management for identity resolution and authentication, and connections to IoT entities (such as IoT devices, IoT services and IoT gateways).

- The FCs in the first group include identity resolving (IDR) agent(s) and identity object storage (IOS) agent(s).
- The FCs in the second group include identity resolution (IR-FC), authentication management (AM-FC), and policy management (PM-FC).
- The FCs in the third group include service agent(s) and device agent(s).

CSIADE exposes a group of reference points to interact with IoT entities, including:

- R1: for IoT services to process the operations;
- R2: for IoT devices to process the operations.

NOTE 1 – Service agents can be deployed in IoT services, and device agents can be deployed in IoT devices or IoT gateways.

NOTE 2 – IDR agents connect to different types of decentralized systems to store identifiers, and IOS agents connect to different types of cloud storages respectively to store corresponding identity objects. This Recommendation does not specify reference points for CSIADE to interact with attestation systems, decentralized systems and clouds.

8.1 Identity resolving agent (IDR agent)

IDR agents of CSIADE interact with attestation systems, decentralized systems and clouds, which provide capabilities related to IoT identity identification, as follows:

- connecting attestation systems to endorse identities of IoT entities, and to verify endorsements of identities of IoT entities, online or offline;
- supporting identity resolution and authentication services for IoT entities, according to relevant policies of IoT entities.

NOTE – Functionalities of end-to-end identity resolution and authentication are performed finally in IoT entities.

8.2 Identity object storage agent (IOS agent)

IOS agents of CSIADE interact with decentralized systems and clouds, which provide capabilities related to IoT identity storage, as follows:

- connecting decentralized systems to store and retrieve identifiers of IoT entities, and to store corresponding identity objects optionally, according to relevant policies of IoT entities;
- connecting clouds to store and retrieve identifiers of IoT entities optionally, and to store corresponding identity objects according to relevant policies of IoT entities;
- connecting decentralized systems and/or clouds to keep links of identifiers of IoT entities with their corresponding identity objects according to relevant policies of IoT entities;
- connecting decentralized systems and/or clouds to store and retrieve modules for identifying and authenticating IoT entities, if IoT entities using different identification and/or authentication solutions, according to relevant policies of IoT entities.

NOTE 1 – Module for identification and authentication of an IoT entity is one type of executable programme which is used to identify and authenticate the IoT entity by using the identifier and corresponding identity object of the IoT entity. IoT entity should provide a secure local environment to load and execute the modules. This Recommendation does not specify those types of modules.

NOTE 2 – Decentralized systems and clouds provide mechanisms on data synchronisation and scalability for serving IoT entities.

8.3 Functional component of identity resolution (IR-FC)

IR-FC of CSIADE provides capabilities related to identity resolution, as follows:

- supporting IoT entities to issue and withdraw their identifiers and corresponding identity objects, according to relevant policies of IoT entities, and CSIADE;
- supporting IoT entities to identify each other mutually by using their identifiers and corresponding identity objects;
- supporting IoT entities to exchange identification modules if they using different types of identification solutions.

8.4 Functional component of authentication management (AM-FC)

AM-FC of CSIADE provides capabilities related to authentication management, as follows:

- supporting IoT entities to manage their identifiers and corresponding identity objects for authentication services, according to relevant policies of IoT entities and CSIADE;
- supporting IoT entities to authenticate each other mutually by using their identifiers and corresponding identity objects;
- supporting IoT entities to exchange authentication modules if they are using different types of authentication solutions.

8.5 Functional component of policy management (PM-FC)

PM-FC of CSIADE provides capabilities related to policy management, as follows:

– supporting IoT entities to manage policies related to their identifiers and corresponding identity objects, such as where to store, how to resolve identity and how to authenticate mutually;

– performing access control for data and services for identification and authentication between IoT entities, according to relevant policies of IoT entities and CSIADE.

8.6 Service agent

Service agents of CSIADE interact with IoT services, which provide capabilities related to identification and authentication, as follows:

– supporting IoT services to manage their identifiers and corresponding identity objects (such as to create, request endorsement, request verifying endorsement, store, exchange, issue, withdraw, etc.), according to policies of CSIADE;

– supporting IoT services to manage policy related to their identifiers and corresponding identity objects, such as where to store, how to resolve identity and how to authenticate mutually;

– supporting IoT services to identify and authenticate IoT devices, end-to-end, by using their identifiers and corresponding identity objects, according to relevant policies of IoT devices and IoT services and CSIADE.

CSIADE supports multiple service agents to provide capabilities of scalability and data synchronisation to serve huge amounts of IoT services. One service agent of CSIADE can serve one or multiple IoT services. One service agent of CSIADE can support different connections and communication technologies to IoT services.

NOTE – Regulators in specific regions may require data for citizens and businesses in that region to be stored within that region. Service agents of CSIADE should be in compliance with local and regional data regulations.

8.7 Device agent

Device agents of CSIADE interact with IoT devices, which provide capabilities related to identification and authentication, as follows:

– supporting IoT devices to manage (such as to create, request endorsement, request verifying endorsement, store, exchange, issue, withdraw, etc.) their identifiers and corresponding identity objects, according to policies of CSIADE;

– supporting IoT devices to manage policy related to their identifiers and corresponding identity objects, such as where to store, how to resolve identity and how to authenticate mutually;

– supporting IoT devices to identify and authenticate IoT services, end-to-end, by using their identifiers and corresponding identity objects, according to relevant policies of IoT devices and IoT services and CSIADE.

NOTE – Regulators in specific regions may require data for citizens and businesses in that region to be stored within that region. Device agents of CSIADE should be in compliance with local and regional data regulations.

8.8 External systems

8.8.1 Attestation system

There may be one or multiple attestation systems as deployed by same or different operators. An attestation system provides capabilities related to identity endorsement, as follows:

- Receiving and endorsing identities of IoT entities if requested.
- Creating and endorsing identities for IoT entities if requested, optionally.
- Endorsing modules for identification and authentication of IoT entities if requested.
- Verifying endorsements of identities and modules for identification and authentication of IoT entities, online or offline, if requested.

NOTE – Generally, when an attestation system endorses an identity of IoT entity, it may generate a digest according to a pre-defined policy and content of a corresponding identity object of the identity, and then may sign the digest according to a pre-defined encryption strategy (such as using its private key to encrypt the digest), on behalf of the relevant operator or owner. This Recommendation does not specify an attestation system and how to endorse the identity of an IoT entity.

8.8.2 Decentralized system

There may be one or multiple decentralized systems as deployed by same or different operators. A decentralized system provides capabilities related to identity storage, as follows:

- Providing storage for identifiers and/or corresponding identity objects of IoT entities, according to requests of IoT entities and CSIADE.
- Providing storage for identification and authentication modules of IoT entities optionally, according to requests of IoT entities and CSIADE.

NOTE – The advantage of decentralized systems (such as crowding collaboration, distributed storage and data tamper-proofing, etc.) is to provide secure and trustworthy storage for identities and modules for identification and authentication of IoT entities. This Recommendation does not specify decentralized systems.

8.8.3 Cloud

There may be one or multiple clouds as deployed by same or different operators. A cloud provides capabilities related to identity storage, as follows:

- Providing storage for identifiers and/or corresponding identity objects of IoT entities, according to requests of IoT entities and CSIADE.
- Providing storage for identification and authentication modules for IoT entities optionally, according to requests of IoT entities and CSIADE.

NOTE – Usually, corresponding identity objects of IoT entities are stored in clouds, and identifiers, identification and authentication modules for IoT entities are stored in decentralized systems. It is decided by IoT entities where and how to store their identities, identification and authentication modules. This Recommendation does not specify clouds.

8.8.4 IoT service, IoT device and IoT gateway

IoT services and IoT devices connect to CSIADE to manage their identities, and identification and authentication modules; and identify and authenticate each other end-to-end by using their identities.

IoT gateways serve for constrained IoT devices and represent the constrained IoT devices to communicate with IoT services and CSIADE.

8.9 Reference points

Reference points R1 and R2 of CSIADE enable IoT entities in:

- creating, and requesting to endorse their identities, and requesting to verify endorsements of their identities;
- optionally, creating, and requesting to endorse identification and authentication modules, and requesting to verify endorsements of their identification and authentication modules;

- setting policies to managing their identities, and identification and authentication modules of IoT entities;
- storing, retrieving and exchanging their identifiers and corresponding identity objects in decentralized systems and/or clouds;
- optionally, storing, retrieving and exchanging their identification and authentication modules in decentralized systems and/or clouds;
- identifying and authenticating each other, end-to-end, by using their identifiers and corresponding identity objects mutually.

9 Main procedures of CSIADE

This clause provides the main procedures of CSIADE, based on the requirements and functional architecture of CSIADE.

9.1 Creating and endorsing identifiers and corresponding identity objects

The creation and endorsement operations for IoT entities are used to create and endorse identifiers and corresponding identity objects of IoT entities by attestation systems, according to policies of CSIADE.

There are two alternative solutions to create and endorse identifiers and corresponding identity objects of IoT entities:

- Option 1 (as shown in Figure 9-1):

  The IoT entities, by themselves, create their identifiers and corresponding identity objects according to the rules of CSIADE individually.

  The IoT entities send their identifiers and corresponding identity objects to attestation systems individually.

  The attestation systems endorse and send back the endorsed identifiers and corresponding identity objects to the IoT entities respectively.

- Option 2:

  The attestation systems create and endorse identifiers and corresponding identity objects for their IoT entities respectively.

  The attestation systems send the endorsed identifiers and corresponding identity objects to their IoT entities respectively.

The IoT entities and attestations systems can use public key infrastructure (PKI) solutions to protect their communications for transferring sensible data.

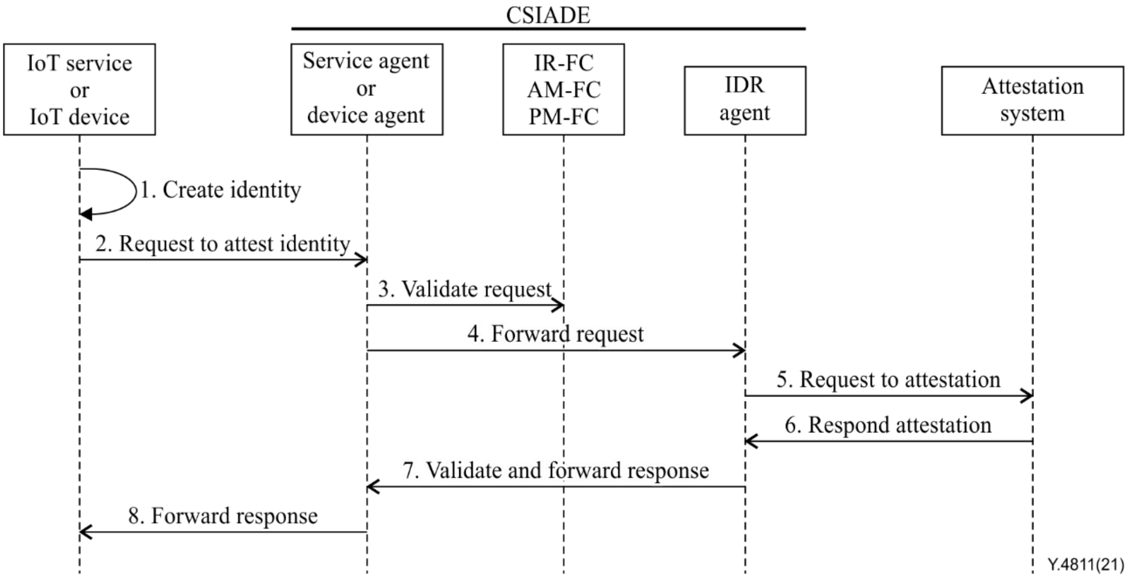

Figure 9-1 – Endorsement of identity for IoT entity

Figure 9-1 depicts a reference procedure for option 1 mentioned above. In this option, CSIADE supports creation and endorsement operations for identifiers and corresponding identity objects. The procedures mainly include:

- Steps 1 and 2: An IoT service (or an IoT device) creates its identifiers and corresponding identity objects, and sends a request to CSIADE for endorsing the identity. The request includes the identifiers and corresponding identity objects, and relevant information to identify the requestor and the target attestation system.
- Step 3: Service agent (or device agent) of CSIADE receives the request, and validates it through PM-FC, IR-FC and AM-FC according to the policy of CSIADE.
- Steps 4 and 5: If the request is accepted, CSIADE forwards the request to the target attestation system, through the corresponding IDR agents.
- Steps 6, 7 and 8: The attestation system validates the request and endorses the identifiers and corresponding identity objects if accepted, and then sends the endorsed identity to the requestor (IoT service or IoT device).

Option 2 is similar to that in option 1 for endorsing identities for IoT entities. The main difference is the requests of option 1 include identifiers and corresponding identity objects, but the requests of option 2 indicate the identities created by attestation systems.

Similarly, modules for identifying and authenticating IoT entities are endorsed by related attestation systems.

9.2 Issuing and validating identifiers and corresponding identity objects

9.2.1 Issuing

The issuance operation of IoT entities is used to store their identifiers and corresponding identity objects in decentralized systems and/or clouds, according to policies of CSIADE.

There are two alternative solutions for an IoT entity to issue its identifier and corresponding identity object through CSIADE.

- One storage for identifier and corresponding identity object:

  Identifier and corresponding identity object of IoT entity are not stored separately, but all are stored in a decentralized system, or in a cloud.

– Separate storage for identifier and corresponding identity object:

  Identifier and corresponding identity object of IoT entity are stored in different storages, usually the identifier is stored in a decentralized system, and the corresponding identity object is stored in a cloud. In this case, CSIADE provides functionalities to support making link information to link the identifier and relevant corresponding identity objects.

The storage provides security protection and privacy preservation for identifiers and corresponding identity objects. IoT entities can encrypt their corresponding identity objects before requesting to store remotely.

Similarly, modules for identifying and authenticating of IoT entities can be stored with their identifiers and/or relevant corresponding identity objects, and events are stored by IoT entities themselves.

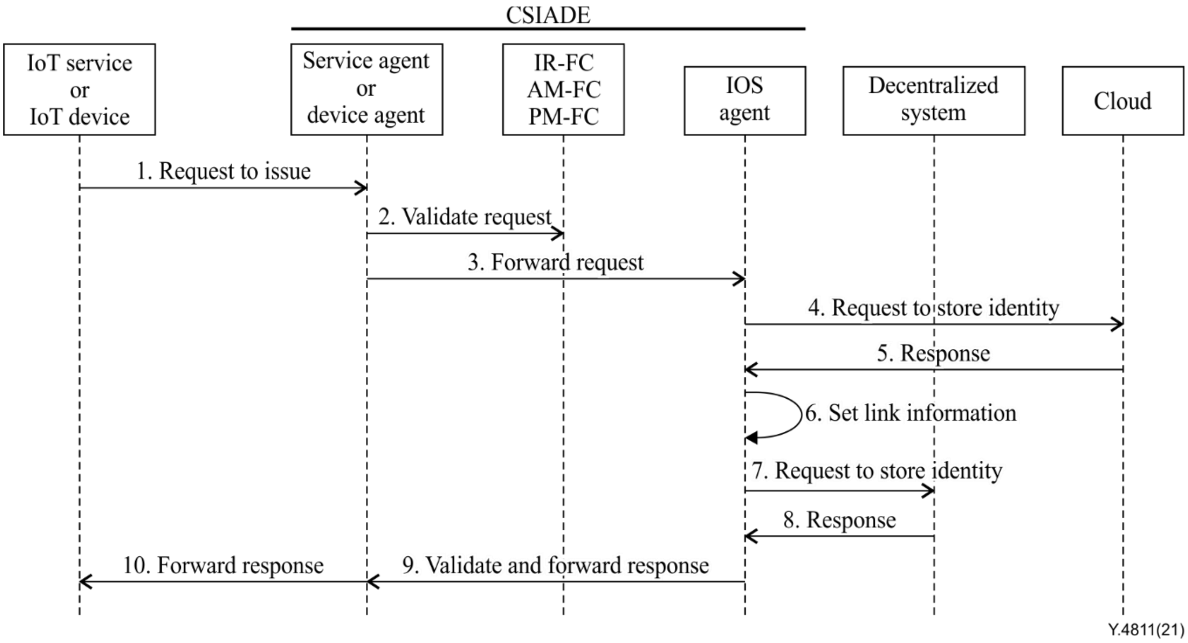

Figure 9-2 – Issuance of identity for IoT entity

Figure 9-2 depicts a reference procedure for separate storage for identifiers and corresponding identity objects for IoT devices and IoT services, identifiers stored in a decentralized system and corresponding identity objects stored in cloud. In this case, CSIADE supports issuance for identifiers and corresponding identity objects. The procedures mainly include:

– Step 1: An IoT service (or an IoT device) requests to issue its identifier and corresponding identity object. The request includes the identifier and corresponding identity object, and relevant information (such as how to store its identity).

– Steps 2 and 3: The request is received by one of the service agents (or device agents) of CSIADE, and then CSIADE validates the request through PM-FC, IR-FC and AM-FC according to the policy of CSIADE. If the requests are validated and accepted, CSIADE selects an IOS agent to subsequently process the requests.

– Steps 4 and 5: The selected IOS agent of CSIADE validates the target cloud according to the requests, and transfers the corresponding identity object to the target cloud. The target cloud stores the corresponding identity object, and responds to the request. The response includes the link information with which to access the corresponding identity object.

– Steps 6, 7 and 8: The selected IOS agent of CSIADE receives and validates the response. If the corresponding identity object was successfully stored in cloud, the selected IOS agent of CSIADE creates an identifier package according to the request, and sets the link information into the identifier package (see Appendix II), and sends the identifier package to the target decentralized system according to the requests.

The target decentralized system validates the requests and stores the identifier package if accepting the requests, and then sends response to the selected IOT agent.

– Steps 9 and 10: CSIADE validates the processed status for the request and transfers the response to an IoT service (or IoT device). Then the IoT service (or IoT devices) fulfils the issuance operation for its identity.

In the case of separate storage for identities of IoT entities, CSIADE adds links information into identifier packages to indicate where to get corresponding identity objects. Therefore, through the links information, CSIADE can facilitate IoT entities to retrieve the identifiers and corresponding identity objects.

If identifiers and/or corresponding identity objects of an IoT entity are changed, it can re-issue to update relevant information stored in decentralized systems and/or clouds, through CSIADE.

The procedures of re-issuance operation of IoT entities are similar as the issuance operation. The main difference is that the request for re-issuance operation contains information to be updated for issued identifiers and corresponding identity objects.

9.2.2 Validating and invalidating

The validation operation (or invalidation operation) of an IoT entity is to enable (or disable) its identifier and corresponding identity object in decentralized system and/or cloud, according to policies of CSIADE.

If an identifier and its corresponding identity object of an IoT entity are stored together in a cloud (or stored in the IoT entity), it is easy for them to be enabled or disabled, and even to be deleted.

If an identifier and its corresponding identity object of an IoT entity are stored separately, for example, the former stored in a decentralized system and the later stored in a cloud (or in the IoT entity), it is easy to validate or invalidate them. In view of the inherent characteristics of a decentralized system, the identifier in a decentralized system cannot be deleted and changed, but it can be enabled or disabled by adding new updating records to the decentralized system. In this case, the corresponding identity object of the IoT entity stored in cloud (or in the IoT entity) is easy to be enabled or disabled to access, and even to be moved or deleted.

NOTE – If an identifier and its corresponding identity object of an IoT entity are stored together in a decentralized system, they can be enabled or disabled by adding new updating records to the decentralized system, but the original record(s) cannot be deleted and changed and yet can be accessed. There may be potential risks to leak information, meanwhile, this method to store the identifier and corresponding identity object of an IoT entity is optional.

9.3 Identification and authentication between IoT devices and IoT services

When an IoT device requests to access an IoT service, they retrieve an identifier and corresponding identity object of their counterparts, through CSIADE, from a decentralized system or cloud. When getting identifiers and corresponding identity objects, the counterparts can identify and authenticate each other.

When an IoT service and IoT device identify and authenticate each other, they can request to verify endorsements for identifiers and corresponding identity objects of their counterparts, through CSIADE, from relevant attestation systems.

Both sides can perform end-to-end identification and authentication by using the identifiers and corresponding identity objects. The end-to-end identification and authentication solutions are pluggable and are decided by the operators of the IoT devices and IoT services.

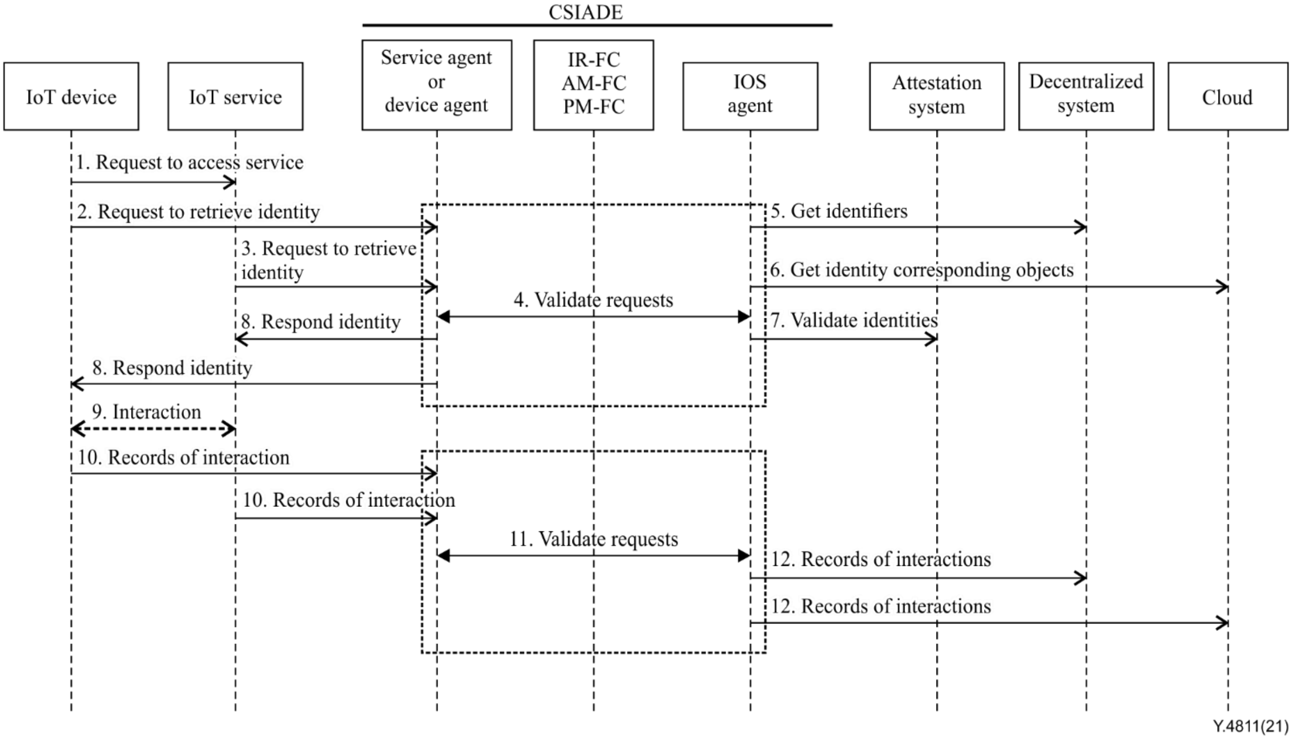
CSIADE
IoT device
IoT service
Service agent or device agent
IR-FC AM-FC PM-FC
IOS agent
Attestation system
Decentralized system
Cloud
1. Request to access service
2. Request to retrieve identity
3. Request to retrieve identity
4. Validate requests
5. Get identifiers
6. Get identity corresponding objects
7. Validate identities
8. Respond identity
8. Respond identity
9. Interaction
10. Records of interaction
10. Records of interaction
11. Validate requests
12. Records of interactions
12. Records of interactions
Y.4811(21)

Figure 9-3 – End-to-end identification and authentication between IoT devices and IoT services

Figure 9-3 depicts a reference procedure for end-to-end identification and authentication between IoT devices and IoT services. In this case, it is assumed that identifiers are stored in decentralized systems and corresponding identity objects are stored in cloud. The procedures mainly include:

– Steps 1, 2 and 3: An IoT device requests to access an IoT service, and then the IoT device and the IoT service request to retrieve the identifier and corresponding identity object of their counterpart through CSIADE individually.

  One of the service agents of CSIADE receives and processes the request of the IoT services. One of the device agents of CSIADE receives and processes the request of the IoT device.

– Step 4: CSIADE validates the requests of the IoT device and the IoT service respectively, and then selects IOS agent(s) to validate the identifiers and corresponding identity objects of the IoT device and the IoT service, if accepted.

– Steps 5, 6 and 7: IOS agent(s) of CSIADE retrieve(s) identifiers of the IoT device and IoT service from decentralized system(s), and retrieve(s) corresponding identity objects of the IoT device and IoT service from cloud(s), and request(s) to verify the endorsement of the identifiers and corresponding identity objects via the attestation system(s) if requested by the IoT device or IoT service.

  NOTE 1 – If the IoT device and the IoT service adapts to different identity solutions, there may be different IOS agents of CSIADE to serve them, and their identifiers and corresponding identity objects may be endorsed by different attestation systems, and be stored in different decentralized systems and clouds.

– Step 8: After that, CSIADE transfers the identifier and corresponding identity object of the IoT device to the IoT service, and transfers that of the IoT service to the IoT device, respectively.

– Step 9: If getting the identifier and corresponding identity object of their counterpart, the IoT device and the IoT service can identify and authenticate each other, by using the identifiers and corresponding identity objects directly. If successful, they can continuously interact with each other.

NOTE 2 – If the IoT device and IoT service are using different identification and authentication solutions, the corresponding identity object of the IoT device and IoT service will contain information to indicate where to retrieve the identification and authentication modules. In this case, the IoT device and IoT service can retrieve relevant identification and authentication modules from indicated storages. After that, the IoT device and IoT service load and execute the relevant modules to identify and authenticate each other.

- Steps 10, 11 and 12: Optionally after the interactions, the IoT device and IoT service can upload the records of interaction to decentralized systems or clouds.

10 Security consideration

CSIADE and IoT services, IoT devices, attestation systems, decentralized systems, and clouds are usually deployed in different domains and may be in untrusted environments. CSIADE should provide mutual authorization and authentication mechanisms to secure their communications.

The security mechanism of CSIADE should support security transportation technologies when exchanging identifiers and corresponding identity objects with IoT services, IoT devices, attestation systems, decentralized systems and clouds.

Additionally, IoT entities should provide secure local environments to load and execute identification and authentication modules, if they support interactions with other IoT entities which use different types of identification and authentication solutions.

Appendix I

Use cases of CSIADE for IoT devices

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

This appendix provides some use cases to illustrate the concept of CSIADE.

I.1 Use case: Supporting one IoT device to access to multiple IoT services of one service operator

This use case shows CSIADE used to promote one IoT device (camera A) to access multiple IoT services (image printing service S1 and image sharing service S2). This IoT device and two IoT services are deployed and operated by one service operator.

The service operator A deploys a CSIADE and an attestation system. The CSIADE, cooperating with the attestation system, one blockchain system and one cloud, promotes the IoT device to access to the IoT services. Here the blockchain system and cloud system act as storages. As depicted in Figure I.1, camera A and IoT services S1 and S2 can get identifiers and corresponding identity objects from the attestation system individually. Those corresponding identity objects were endorsed by the attestation system. Then, the camera A and IoT service S1 and S2, through the CSIADE, issue their identifiers in the blockchain system and store their corresponding identity objects in the cloud. The CSIADE adds "links" information into identifier packages (see Appendix II) and stores the identifier packages in the blockchain system and the corresponding identity objects in the cloud.

The identifiers can present the camera and the IoT service S1 and S2 respectively. The corresponding identity objects contain the information for identifying and authenticating the IoT device and the IoT services individually.

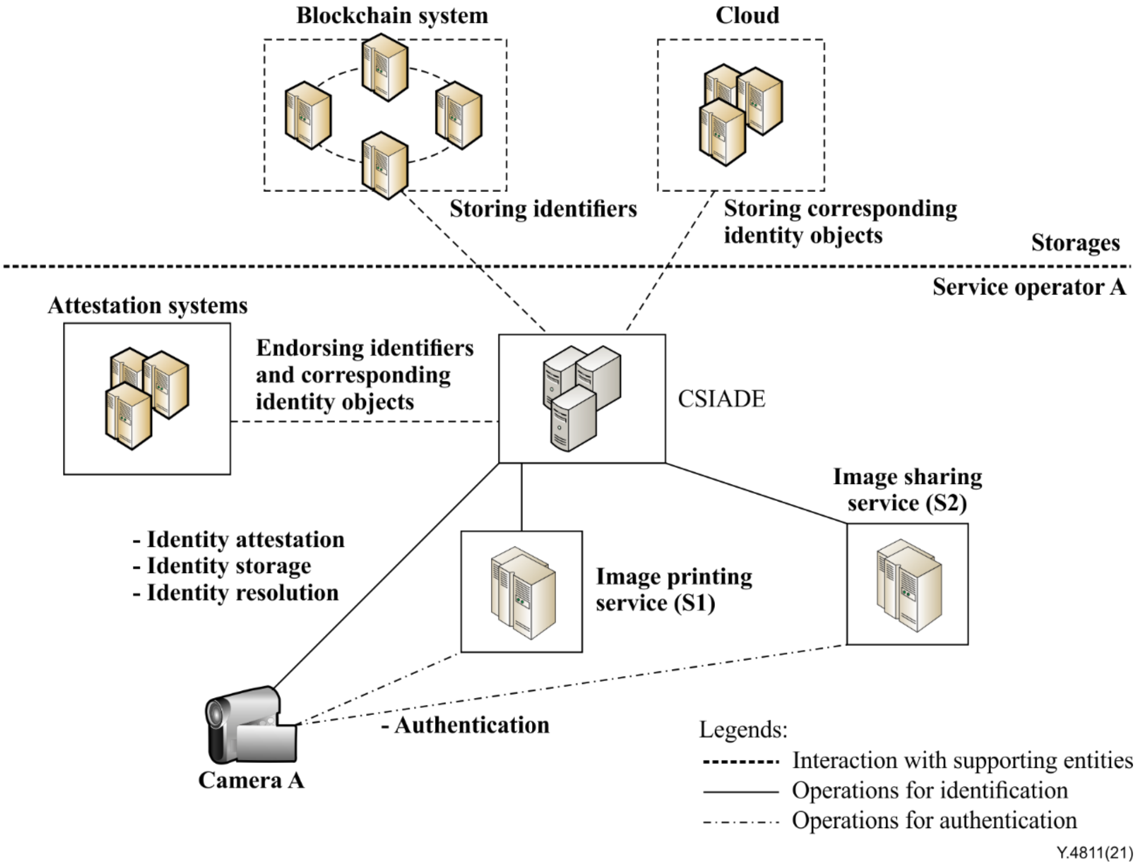
Blockchain system
Cloud
Storing identifiers
Storing corresponding identity objects
Storages
Service operator A
Attestation systems
Endorsing identifiers and corresponding identity objects
CSIADE
Image sharing service (S2)
- Identity attestation
- Identity storage
- Identity resolution
Image printing service (S1)
- Authentication
Camera A
Legends:
-------- Interaction with supporting entities
——— Operations for identification
-·-·-·- Operations for authentication
Y.4811(21)

Figure I.1 – Supporting one IoT device to access to multiple IoT services of one service operator

NOTE – The blockchain system and cloud shown in Figure I.1 can be deployed by service operator A or other service operators.

When the camera A applies to access to IoT service S1 or S2, through CSIADE, the camera A, the IoT service S1 or S2 can retrieve the identifiers and corresponding identity objects of the counterpart from the blockchain system and cloud respectively. Because the identifiers and corresponding identity objects are endorsed by the attestation system and contain enough information to perform identification and authentication, the counterparties can identify and authenticate each other directly with the supports of CSIADE.

In this case, it is not necessary that the counterparties request supports of the traditional IoT identification and authentication systems of the service operator A. Therefore, CSIADE can decrease the burdens of traditional IoT identification and authentication systems, especially when there are huge amounts of IoT devices to access various IoT services.

I.2 Use case: Supporting one IoT device to access to IoT services of multiple service operators

This use case shows CSIADE used to promote one IoT device (vehicle A) to access to IoT services (groups of intelligent transport services, ITS services) provided by different service operators (A, B, and C). The IoT device, ITS services and attestation systems are deployed and provided by the three service operators.

As depicted in Figure I.2, the supporting systems (such as blockchain systems, clouds) are used as storages. With the supports of CSIADE, this vehicle can access to those ITS services provided by different service operators when it moves from one area to another area.

CSIADE converges capabilities of the supporting systems of the three service operators, and facilitates identification and authentication between the vehicles and the ITS services. When vehicle

A is moving on the road from area 1 through area 4, it can access the ITS services provided by the service operators A, B and C. When vehicle A accesses the ITS services, vehicle A and the ITS services can identify and authenticate with each other through supports of CSIADE, even though the vehicle and the ITS services use different identity and authentication solutions.

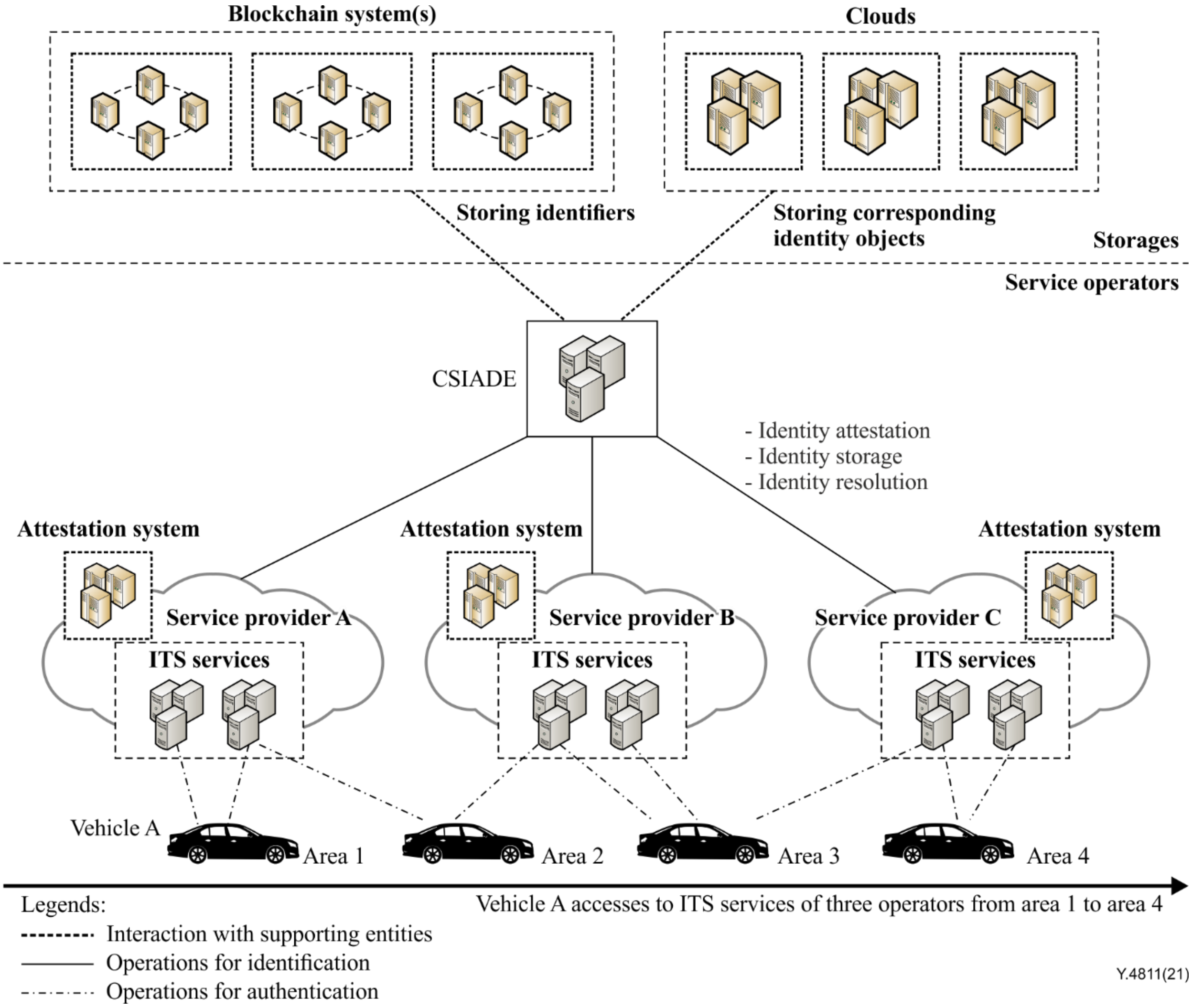

Figure I.2 – Supporting one IoT device to access to IoT services of multiple operators

In this case, CSIADE provides converged services of IoT identification and authentication for the ITS services and the vehicles, and ITS services and vehicles leverage CSIADE to identify and authenticate with each other, regardless of the traditional solutions for IoT identification and authentication.

Appendix II

Abstract model of identifier and corresponding identity object for IoT device and IoT service

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

An identity of an IoT entity consists of one or multiple identifier(s) and one corresponding identity object. An identifier is a unique string (see clause II.1), and the corresponding identity object contains compound information to support identification and authentication for the IoT entity (see clause II.3). The identifier is part of its corresponding identity object. The content of a corresponding identity object can be formatted as a JSON (JavaScript Object Notation) file or other formation.

II.1 Identifier

Identifiers of IoT entities are strings, and are as unique as other unique expressions such as uniform resource identifier (URI), globally unique identifier (GUID), etc., and can be compatible with any type of identity solution.

An IoT entity has at least one identifier, and the identifier may have multiple aliases. The identifier and its aliases of an IoT entity are bound to one corresponding identity object.

NOTE – Similar to an identifier of an IoT entity, an alias of an identifier is also a unique string. If not specified, an identifier and its aliases can be seen as identifiers of an IoT entity. Usually, the identifier of an IoT entity cannot be changed, but its aliases can be updated or destroyed. The identifier will be stored with its corresponding identity object, but aliases can be stored anywhere (such as in decentralized systems, in clouds, or in the IoT entity itself, etc.).

II.2 Identifier package

In view of the fact that an identifier of IoT entity is a unique string, if it is stored outside of its corresponding identity object, additional information needs to be stored with the identifier. An identifier package is used to store the identifier of the IoT entity, for retrieving and validating the identifier and its corresponding identity object. Table II.1 depicts the main elements of an identifier package.

An identifier package can be stored in a decentralized system, or cloud, or in the IoT entity itself. The storages should protect identifier packages from illegal tampering.

Table II.1 – Element list of identifier package

Elements	Descriptions	Note
identifier	Identifier of IoT entity, or alias of identifier	
cio-digest	Digest of the corresponding identity object, which is usually encrypted by private key of the IoT entity. Using this element to verify integrity and consistency of the corresponding identity object.	
links	URLs to retrieve the corresponding identity object.	
createdTime	Created time of the identifier.	
expiredTime	Expired time of the identifier.	optional
status	Status of the identifier, e.g., available or not available.	optional
digest	Digest of information above to prevent illegal tampering, which is usually encrypted by private key of the IoT entity.	

Table II.1 – Element list of identifier package

Elements	Descriptions	Note
NOTE 1 – More information can be added into the list, such as algorithms and methods to be used to make "cio-digest" and "digest". NOTE 2 – The abbreviation "cio" means "corresponding identity object".		

II.3 Corresponding identity object

A corresponding identity object is bound to an identifier of an IoT entity. A corresponding identity object includes compound elements to be used to identify and authenticate the IoT entity. The main elements of a corresponding identity object are listed in Table II.2.

NOTE – It is an abstract and simple model of an identifier and corresponding identity object of an IoT entity as listed in Table II.2. In practice, the abstract model could be updated accordingly.

Table II.2 – Element list of an abstract model of identifier and corresponding identity object for an IoT entity

Elements	Attributes	Description	Note
identifier	Type of identifier, Version of identifier, etc.	Identifier of the IoT entity. An entity has one or multiple identifier(s). One of the identifiers is the same as listed in Table II.1.	
subject	Name of the IoT entity, Description of the IoT entity, etc.	Information of the entity.	
identification	public key of the IoT entity, Algorithm to generate the public/private keys of the IoT entity, etc.	Identification related information.	
attestation	Identifier and public key of attestation system which endorses the identity of the IoT entity, Algorithm to generate the public/private keys of the attestation system, URI to access to the attestation system, etc.	Attestation related information	
Authentication	Identifier and public key of the service operator which provided the authentication information, Algorithm to generate the public/private keys of the authenticator, Authentication information with which to authenticate the IoT entity, URI to access to the authenticator, etc.	Authentication related information	
Authorization	Identifier and public key of the service operator who provided the authorization information, Algorithm to generate the public/private keys of the authorizer, authorization information with which to authorize the IoT entity,	Authorization related information	optional

Table II.2 – Element list of an abstract model of identifier and corresponding identity object for an IoT entity

	URI to access to the authorizer, etc.		
Storage	URI to show where to get corresponding identity object of the IoT entity, etc.	Storage related information	optional
Auxiliary	Auxiliary information such as createdTime, expiredTime, status, etc.	Auxiliary information	optional
digest	Data, type, version, algorithm of the digest, etc.	Digest of information above to prevent illegal tampering.	

The corresponding identity object of an IoT entity can be endorsed by the attestation system of its operator or owner. The attestation information should be stored in the corresponding identity object (see Table II.2). If the content of the corresponding identity object is changed, it should be endorsed again.

The corresponding identity objects can be stored in traditional storages (such as clouds) or in decentralized systems (such as blockchain platforms), according to the owners' requests. If an identifier and its corresponding identity object are stored separately, "links" information should be added to the identifier package to indicate where to get the corresponding identity object (see clause II.1).

The corresponding identity object of an IoT entity can be encrypted by the IoT entity. When two IoT entities use corresponding identity objects to identify and authenticate each other, they can exchange information to decrypt the corresponding identity objects if they were encrypted.

Appendix III

Business roles and models of CSIADE

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

III.1 Business roles of CSIADE

[ITU-T Y.4000] describes a common IoT ecosystem, business roles and groups of business models (see Figure III.1). The IoT ecosystem is composed of a variety of business players, including device providers, network providers, platform providers, application providers and application customers. Each business player plays at least one business role, but more roles are possible [ITU-T Y.4000].

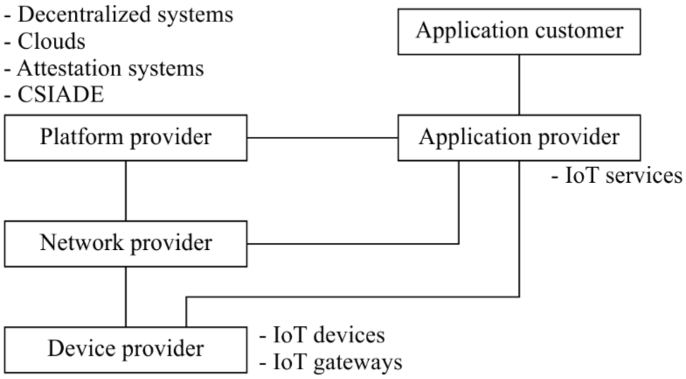

Figure III.1 – Business roles of CSIADE in IoT ecosystem (derived from [ITU-T Y.4000])

III.1.1 Device providers

IoT devices and IoT gateways are device providers.

IoT devices manage their identifiers and corresponding identity objects, which identify and authenticate IoT services when interacting with the IoT services according to users' requests.

IoT gateways, on behalf of connected constrained IoT devices, manage their identifiers and corresponding identity objects, which identify and authenticate IoT services when interacting with IoT services according to users' requests.

III.1.2 Application providers

IoT services are application providers.

IoT services manage their identifiers and corresponding identity objects, which identify and authenticate IoT devices when interacting with the IoT devices according to users' requests.

III.1.3 Platform providers

Decentralized systems, clouds, attestation systems and CSIADE are platform providers.

Decentralized systems store the identifiers of IoT devices and IoT services. The corresponding identity objects of IoT devices and IoT services can be stored in decentralized systems if requested. There may be multiple decentralized systems with the same or different solutions.

Clouds optionally store the corresponding identity objects of IoT devices and IoT services. There may be multiple clouds, with the same or different solutions.

Attestation systems endorse and validate identifiers and the corresponding identity objects on the requests of IoT devices and IoT services. The operators or owners of IoT devices and IoT services may have their own attestation systems.

CSIADE supports IoT devices and IoT services to identify and authenticate each other in decentralized environments, which interact with the decentralized systems, clouds and attestation systems.

III.2 Business models of CSIADE

The IoT ecosystem players may have a variety of relationships in practice [ITU-T Y.4000].

There are some business models of CSIADE from the perspective of operators who perform business roles. Figure III.2 depicts a sample business model of CSIADE. Typically, multiple players can deploy and operate the device providers (e.g., IoT devices and IoT gateways), platform providers (e.g., attestation systems), and application providers (e.g., IoT services). Meanwhile, one or multiple decentralized system(s) can be operated by one or multiple player(s) Bs, multiple clouds can be operated by one or multiple player(s) Cs, and CSIADE can be operated by player D.

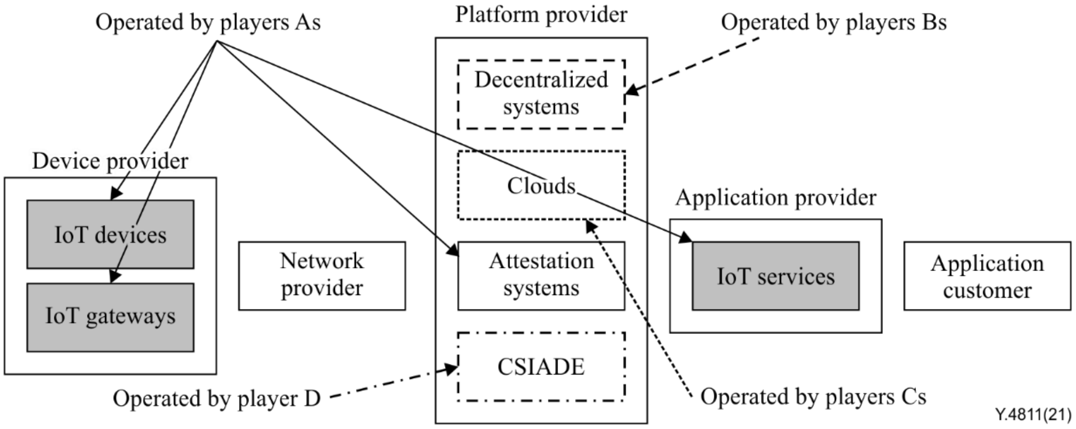

Figure III.2 – A sample business model of CSIADE

NOTE – This is a sample business model of CSIADE, there may be other business models.

Bibliography

[b-ITU-T Y.2091]	Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.
[b-ITU-T Y.4464]	Recommendation ITU-T Y.4464 (2020), *Framework of blockchain of things as decentralized service platform.*
[b-ITU-R M.1224-1]	Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT).*
[b-ISO 22739]	ISO 22739 (2020), *Blockchain and distributed ledger technologies – Terminology.*
[b-W3C-DID]	W3C Technical Report DID v1.0, *Decentralized Identifiers,* https://w3c.github.io/did-core/

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