International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4483

(08/2022)

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 – Frameworks, architectures and protocols

Reference architecture of service exposure for decentralized services for Internet of things applications

Recommendation ITU-T Y.4483

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.4483

Reference architecture of service exposure for decentralized services for Internet of things applications

Summary

Recommendation ITU-T Y.4483 introduces a service exposure for decentralized services (DSE) for Internet of things (IoT) applications and specifies its common characteristics, general requirements, reference architecture and common capabilities. A DSE is a functional entity for IoT applications in an IoT device, which integrates multiple decentralized services (such as services based on distributed ledger technologies) and exposes uniform interfaces to IoT applications. Those integrated decentralized services may support the same or different types of decentralization solutions. IoT applications can use uniform interfaces to integrate and access multiple decentralized services at the same time, regardless of their decentralization solutions. A DSE can bring efficiencies and benefits to application providers and users.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4483	2022-08-29	20	11.1002/1000/15071

Keywords

Application, decentralized service, Internet of things, service exposure.

* 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
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	2
6	Introduction to service exposure for decentralized services	2
7	Common characteristics and general requirements of DSE	3
7.1	Common characteristics	3
7.2	General requirements	4
8	Reference architecture of DSE	5
8.1	Access control management-functional component (ACM-FC)	5
8.2	Service capability management-functional component (SCM-FC)	6
8.3	Decentralized service agent management-functional component (DSAM-FC)	6
8.4	Application management-functional component (AM-FC)	6
8.5	Application agents	6
8.6	Decentralized service agents	7
8.7	Interface DSE-1	7
9	Common procedures of DSE	7
9.1	Integration and publication of service capabilities of decentralized services	7
9.2	Registration of an Internet of things application on a DSE	8
9.3	Subscription to exposed service capabilities of decentralized services	10
9.4	Access to exposed service capabilities of decentralized service with none-encrypted communication	12
9.5	Access to exposed service capabilities of decentralized service with encrypted-communication	14
10	Security considerations	14
Appendix I – Use cases of DSE for Internet of things applications		15
I.1	Uniform wallet application	15
I.2	Integrated application for smart services	15
Bibliography		17

Recommendation ITU-T Y.4483

Reference architecture of service exposure for decentralized services for Internet of things applications

1 Scope

This Recommendation introduces the concept of service exposure for decentralized services (DSE) for Internet of things (IoT) applications, analyses its common characteristics and general requirements and provides a reference architecture of DSE and its relevant common capabilities.

Additionally, use cases of DSE for IoT applications are provided 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.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the 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 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.

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

3.1.4 distributed ledger technology (DLT) [b-ISO 22739]: Technology that enables the operation and use of distributed ledgers.

3.1.5 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 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.6 ledger [b-ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACM-FC	Access Control Management-Functional Component
AM-FC	Application Management-Functional Component
API	Application Programming Interface
DLT	Distributed Ledger Technology
DSAM-FC	Decentralized Service Agent Management-Functional Component
DSE	service Exposure for Decentralized Service
FC	Functional Component
IoT	Internet of Things
PII	Personally Identifiable Information
SCM-FC	Service Capability Management-Functional Component

5 Conventions

The following conventions are used in this Recommendation:

– The phrase "is required to" 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.

6 Introduction to service exposure for decentralized services

Service exposure for decentralized services (DSE) is a functional entity for Internet of things (IoT) applications in an IoT device, which integrates multiple decentralized services and exposes uniform interfaces to IoT applications. Those integrated decentralized services may support the same or different types of decentralization solutions, such as those based on blockchain or distributed ledger technology (DLT). IoT applications that use uniform interfaces through one DSE can access multiple integrated decentralized services regardless of their decentralization solutions.

Figure 6-1 shows that a given DSE integrates a group of dedicated decentralized service agents with which to interconnect to multiple decentralized services, such as blockchain agents connecting to blockchain-based services, DLT agents connecting to DLT-based services, and so on. An agent can connect to one or multiple decentralized service(s). A DSE exposes uniform interfaces to IoT applications, with which IoT applications can use uniform approaches to integrate and access one or multiple decentralized services at the same time.

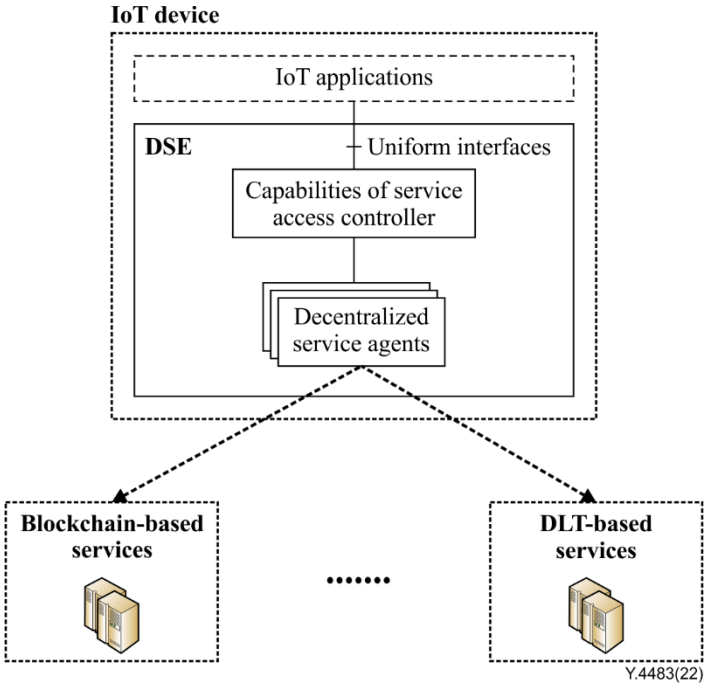

Figure 6-1 – Overview of DSE

NOTE – This Recommendation focuses on integration and exposure of capabilities of decentralized services. Decentralized services themselves lie outside the scope of this Recommendation.

7 Common characteristics and general requirements of DSE

7.1 Common characteristics

This clause describes the common characteristics of DSE.

7.1.1 Integrating multiple decentralized services

A DSE can integrate multiple decentralized services through decentralized service agents, automatically or mutually. Integrated decentralized services can be local services on IoT devices or remote services in clouds, and they can support the same or different decentralization technologies.

7.1.2 Exposing data and capabilities of integrated decentralized services

A DSE provides unified interfaces to local IoT applications, with which local IoT applications can discover, subscribe and access data and capabilities exposed by the same or different decentralized services, even if the decentralized services use different decentralization technologies.

An IoT application can subscribe to and access one or multiple decentralized services integrated by a given DSE.

7.1.3 Accessing exposed capabilities of integrated decentralized services

A DSE supports local IoT applications to access the exposed data and capabilities of integrated decentralized services. The DSE receives and verifies requests from local IoT applications and then forwards them to the corresponding decentralized services. The DSE then delivers the results from the decentralized services to the IoT applications.

Local IoT applications, by using exposed unified interfaces, can access decentralized services to which they subscribe by the same approach.

7.1.4 Security and privacy protection

A DSE provides security and privacy protection support to data and capabilities of integrated decentralized services. The DSE exposes the data and capabilities according to its own security and privacy protection policies and those of integrated decentralized services.

7.2 General requirements

This clause provides general requirements of DSE.

7.2.1 Integration of decentralized services

The integration-related requirement of a given DSE is as follows:

– DSE is required to be able to collect and integrate data and capabilities of decentralized services with the same or different decentralized technologies.

7.2.2 Publication of data and capabilities of decentralized services

The publication-related requirements of a given DSE are as follows:

– DSE is required to support the collection and publication of information (e.g., service descriptions and methods and parameters to access services) about data and capabilities of integrated decentralized services for IoT application;

– DSE is required to set access policies based on published data and capabilities of decentralized services;

– DSE is recommended to apply related access policies of integrated decentralized services.

7.2.3 Subscription to exposed data and capabilities of decentralized services

The subscription-related requirements of a given DSE are as follows:

– DSE is required to support IoT applications to discover and subscribe to exposed data and capabilities of decentralized services;

– DSE is required to support IoT applications to obtain descriptions for accessing the subscribed data and capabilities of decentralized services;

– DSE is recommended to notify IoT applications of the state (such as available or unavailable) of data and capabilities of decentralized services, as needed.

7.2.4 Access to data and capabilities of decentralized services

The access-related requirement of a given DSE is as follows:

– DSE is required to support IoT applications to access subscribed data and capabilities exposed by decentralized services, if authorized.

7.2.5 Security protection and privacy preservation

The security-related requirements of a given DSE are as follows:

– DSE is required to provide the necessary security mechanisms when exposing data and capabilities of decentralized services;

– DSE is required to provide privacy preservation of personally identifiable information (PII) when exposing data and capabilities of decentralized services.

– DSE is required to authenticate and authorize IoT applications when related IoT applications discover, subscribe to and access exposed data and capabilities of decentralized services.

8 Reference architecture of DSE

A DSE works at the device layer of the IoT reference model [ITU-T Y.4000], which is a functional entity in an IoT device, to support IoT applications in the IoT device to discover and access the exposed data and capabilities of decentralized services. A DSE consists of four functional management components for: access control management (ACM-FC), service capability management (SCM-FC), decentralized service agent management (DSAM-FC); and application management (AM-FC). In addition, a DSE includes a group of extensible functional components (FCs), application agents and decentralized service agents. The AM-FC of one DSE exposes an interface, DSE-1, to support IoT applications to discover, subscribe to and access the exposed data and capabilities of decentralized services. Figure 8-1 shows the reference architecture diagram of a DSE.

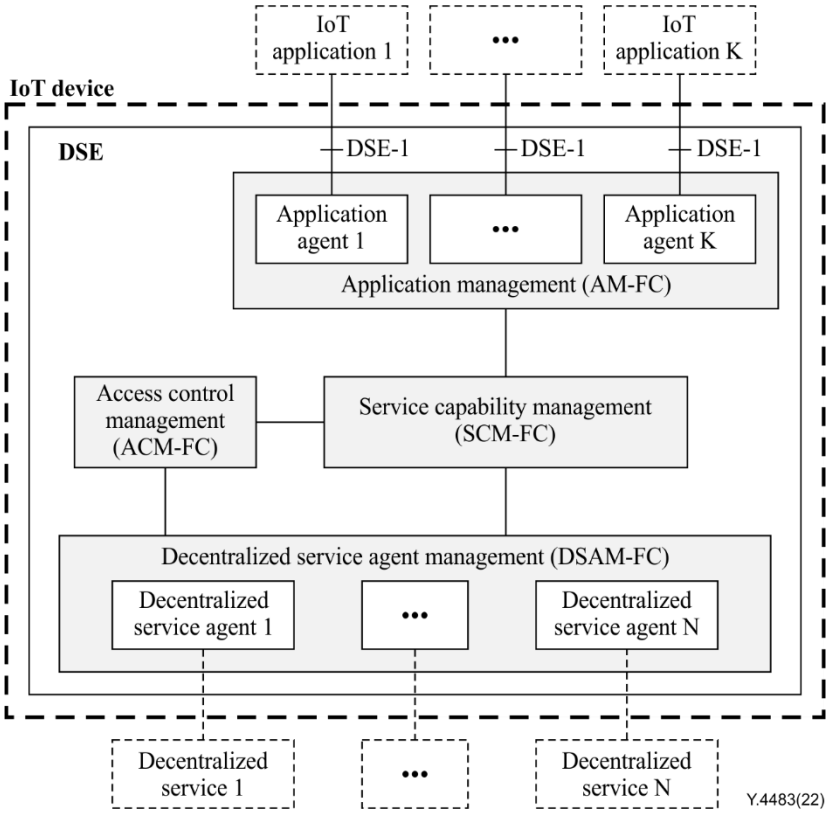

Figure 8-1 – Reference architecture of a DSE

8.1 Access control management-functional component (ACM-FC)

The access control management-functional component (ACM-FC) performs access control for IoT applications to discover, subscribe to and access the exposed data and capabilities of decentralized services.

The ACM-FC, in coordination with other FCs of a DSE, provides the following functionalities for verification of:

– IoT applications and relevant registration statuses;

– decentralized services and relevant exposure of data and service capabilities of decentralized services;

– subscription relationships of IoT applications to data and service capabilities of decentralize services;

– encryption algorithms for interaction between IoT applications and decentralized services;

– IoT applications to discover, subscribe to and access exposed data and capabilities of decentralized services.

8.2 Service capability management-functional component (SCM-FC)

The service capability management-functional component (SCM-FC), in collaboration with the ACM-FC, supports IoT applications to discover, subscribe to and access exposed data and capabilities of decentralized services.

The SCM-FC, in coordination with other FCs of a DSE, provides the following functionalities for management of:

– data and service capabilities exposed by decentralized services;

– subscription relationships of IoT applications to data and service capabilities of decentralized services;

– registration information of IoT applications;

– information about decentralized services.

8.3 Decentralized service agent management-functional component (DSAM-FC)

The decentralized service agent management-functional component (DSAM-FC) manages decentralized service agents. A DSE may have multiple decentralized service agents. When one DSE serves for an IoT application to access a decentralized service, the DSAM-FC selects the corresponding decentralized service agent to transfer information and interact with the target decentralized service.

8.4 Application management-functional component (AM-FC)

The application management-functional component (AM-FC) manages application agents, and supports IoT applications to discover, subscribe to and access exposed data and capabilities of decentralized services, in collaboration with the ACM-FC.

The AM-FC exposes interface DSE-1, with which IoT applications can use uniform approaches to interact with decentralized services through a given DSE.

The AM-FC may dynamically create application agents when interacting with IoT applications.

8.5 Application agents

The application agents of a DSE interact with IoT applications and support IoT applications to discover, subscribe to and access the exposed data and capabilities of decentralized services.

The application agents of DSE are created and managed by the AM-FC of a DSE.

The application agents of DSE interact with IoT applications by using interface DSE-1 of a DSE.

The application agent, in coordination with other FCs of a DSE, provides the following functionalities:

– support for IoT applications to discover and, subscribe to exposed data and capabilities of decentralized services on the DSE;

– support for IoT applications to access exposed data and capabilities of decentralized services to which they subscribe on the DSE;

– conversion of the format of data and protocol of requests from IoT applications and responses from the DSE;

– transfer of notifications of the status of subscribed service capabilities from the DSE.

8.6 Decentralized service agents

The decentralized service agents of a DSE are responsible for communication with corresponding decentralized services. Each decentralized service agent of a DSE may connect to one or multiple decentralized services.

The decentralized service agents of a DSE are created and managed by the DSAM-FC of the DSE.

The decentralized service agents of a DSE interact with decentralized services.

The decentralized service agents, in coordination with other FCs of a DSE, provide the following functionalities:

– interaction with corresponding decentralized services on behalf of IoT applications and the DSE;

– conversion of the format of data and protocol of requests from IoT applications and the DSE, and responses from decentralized services;

– transfer of notifications about the status of corresponding service capabilities to the DSE.

NOTE – This Recommendation does not specify the external interfaces for communications between decentralized service agents of the DSE and decentralized services.

8.7 Interface DSE-1

The interface DSE-1 is exposed by the AM-FC to allow IoT applications to discover, subscribe to and access the data and capabilities published on a DSE and to receive notifications about the updated states of the subscribed decentralized services.

9 Common procedures of DSE

9.1 Integration and publication of service capabilities of decentralized services

For each local or remote decentralized service, a given DSE can provide a proprietary decentralized service agent to interact with it. A decentralized service agent of a DSE can interact with one or multiple decentralized services.

When a decentralized service is integrated into a DSE, information about the service capabilities of the decentralized service to be exposed can be published on DSE. The information to be exposed includes, but is not limited to:

– identity of the decentralized service,

– name of the decentralized service,

– identity and description of the service capabilities of the decentralized service,

– approaches and relevant parameters for access the decentralized service,

– access profiles for IoT application for access the decentralized service,

– access profiles for DSE to interact with the decentralized service, optionally.

Alternatively, if the decentralized service supports encryption communication, the information may include its public key and certificate of the decentralized service, as well as the encryption algorithms and relevant parameters it supports.

Information about the capabilities of a decentralized service can be composed in extensible markup language or JavaScript object notation format.

The ACM-FC and SCM-FC of one DSE manage and publish information about the exposed service capabilities of integrated decentralized services, according to the policies of the DSE and the access profiles of the exposed service capabilities.

When the service capabilities of a decentralized services are published on a DSE, IoT applications can discover, subscribe to and access those service capabilities through the DSE-1 interface.

The main steps in the procedure for the integration and publication of service capabilities of a DSE are outlined as follows (see Figure 9-1).

Step 1 A decentralized service agent of the DSE checks and interacts with a decentralized service, and collects its service capabilities of the decentralized service, according to the policies of DSE and the decentralized service.

Step 2 The decentralized service agent of the DSE requests integration with the decentralized service and publishes its service capabilities, if permitted.

Step 3 and 4 The ACM-FC and SCM-FC of the DSE check the request and publish the service capabilities of the decentralized service, if available, according to the policies of DSE and the decentralized service, and then send a response to the decentralized service agent.

Step 5, 6 and 7 If the request is accepted and the service capabilities of the decentralized service are published by the DSE, the decentralized service agent may check status of the decentralized service in consequence, such as availability or unavailability of the decentralized service and service capabilities.

If the status of the decentralized service or its service capabilities change, the decentralized service agent may send relevant information to other FCs of the DSE to notify each IoT application that has subscribed to the exposed service capabilities of the decentralized service.

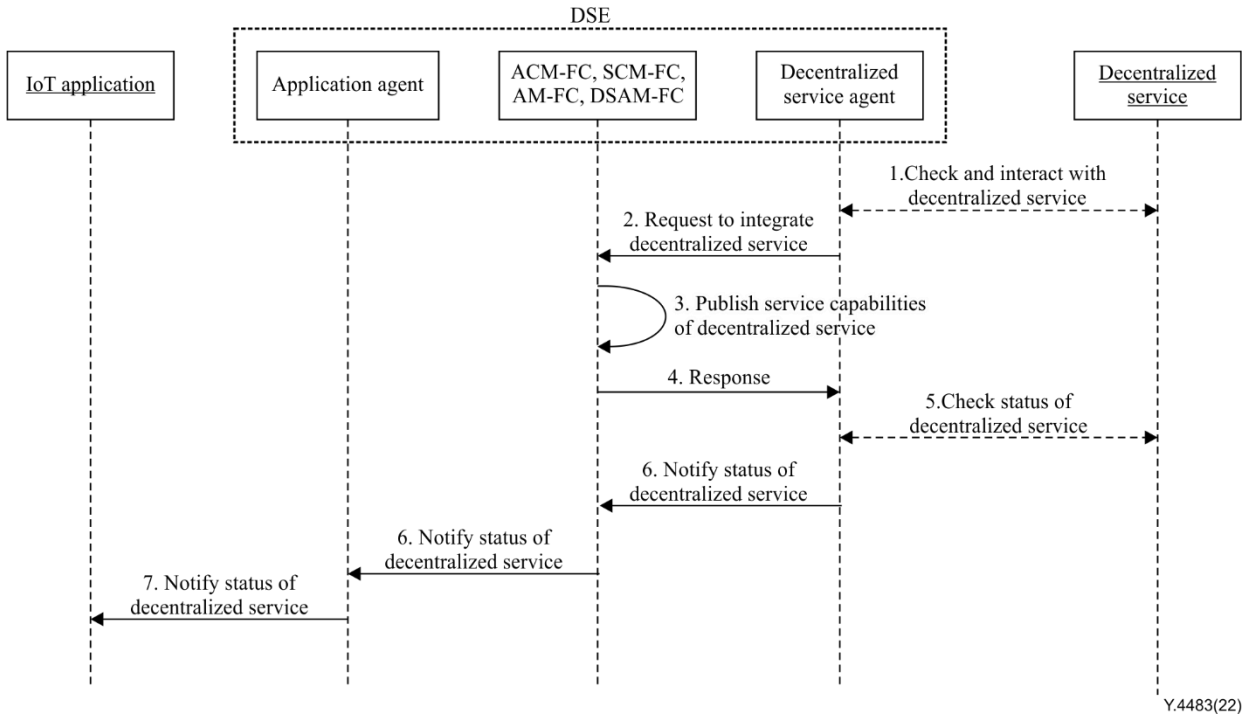

Figure 9-1 – Flow for integration and publication of service capabilities of a decentralized service

9.2 Registration of an Internet of things application on a DSE

Before an IoT application subscribes to and accesses exposed data and capabilities of decentralized service through a DSE, it should first register itself on the DSE.

If an IoT application has ever been registered successfully and the registration has expired, the IoT application should register on the DSE again. However, in practice, an IoT application can register itself on the DSE regardless of its previous registration status.

Before requesting registration, the IoT application should generate its identity, which should be a global unique string. Additionally, the IoT application can generate its public or private keys and certificate if it supports encrypted communication. In practice, the identity, public or private keys and certificate of an IoT application can be generated by its IoT application provider. The IoT application should store its private key securely.

If the registration request of an IoT application is accepted, the DSE may generate a registration identity and a specific application agent for the IoT application. The application agent serves for the IoT application. The registration identity is sent to the IoT application, and is used to facilitate the management of registration information about the IoT applications by the DSE.

If registered successfully, when the IoT application accesses the DSE, relevant requests should contain the registration identity.

The main steps in the procedure for an IoT application to request registration on a DSE are outlined as follows (see Figure 9-2):

Step 1 An IoT application sends a registration request to a DSE through interface DSE-1.

The registration request includes the identity and description of the IoT application.

If the IoT application has ever been registered successfully and the registration has not expired, the request may include previous registration information (such as registration identity).

If the IoT application supports encryption communication, the registration request may include its public key and certificate of the IoT application, as well as the encryption algorithms and relevant parameters it supports.

In the registration request, the IoT application can declare whether it supports only non-encrypted or encrypted communication, or both.

Step 2 The AM-FC of the DSE processes the request, in collaboration with other FCs of the DSE.

The AM-FC of the DSE separates the identity of the IoT application from the registration. It then checks whether the identity of the IoT application is compliant and whether it has ever been registered.

If the identity of the IoT application is already registered, the AM-FC of the DSE separates the registration identity from the registration request and checks whether it has expired. If there is no registration identity in the registration request or if the previous registration has expired, the registration request may be considered as new registration.

The AM-FC of the DSE separates and analyses the registration request of the IoT application, and verifies whether it is supported. If not, it proceeds directly to step 4 to reject the registration request.

If it is supported, the AM-FC of the DSE accepts the registration request.

Step 3 The AM-FC of the DSE checks and generates the corresponding application agent for the IoT application, in collaboration with other FCs of the DSE.

If the IoT application has ever been registered and the registration is still available, the AM-FC of DSE checks whether a corresponding application agent of the DSE for the IoT application exists. If not, the AM-FC generates a specific application agent for the IoT application.

If the IoT application has never been registered, the AM-FC directly generates a specific application agent for the IoT application.

Alternatively, a specific application agent for an IoT application may be generated when the IoT application first accesses the DSE after it has been registered successfully.

Step 4 The AM-FC of the DSE stores the registration information and sends a registration response to the IoT application, in collaboration with other FCs of the DSE.

If the registration request is accepted, the AM-FC of the DSE generates a registration identity for the IoT application, and stores the registration information, including the identity of the IoT application, registration identity, and public key and certificate of the IoT application.

The AM-FC sends a registration response, whose payload includes the registration identity if the registration request has been accepted or rejection information if it is rejected, to the IoT application.

Step 5 If the registration on the DSE is successful, the IoT application can check its registration status (i.e., available or not) any time.

When checking its status, the request includes at least the identities of both the IoT application and its registration.

Step 6 and 7 The AM-FC of the DSE checks and returns the relevant registration status according to the request of the IoT application.

NOTE – The request for registration on the DSE and request for subscription to exposed data and service capabilities of decentralized services can be combined into one request.

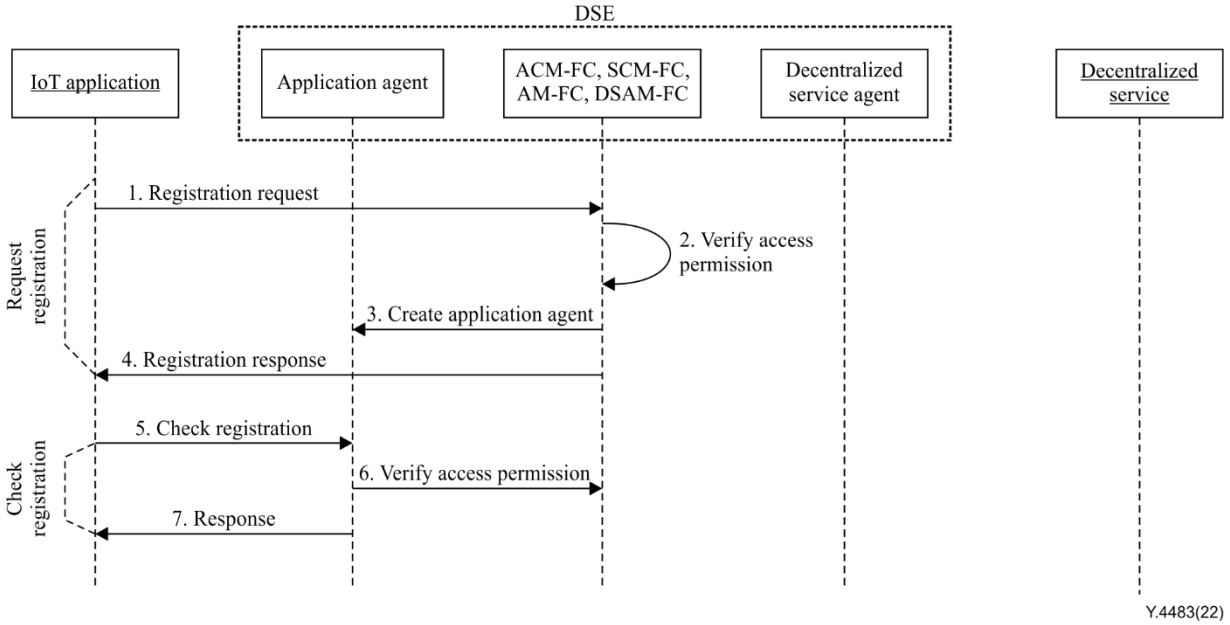

Figure 9-2 – Flow for registering an Internet of things application on a DSE

9.3 Subscription to exposed service capabilities of decentralized services

This procedure is an IoT application request to subscribe to exposed service capabilities of a decentralized service, and the given DSE sends relevant notifications to the IoT application if the subscription request is accepted.

Before subscription, the IoT application can discover the exposed service capabilities of decentralized services, and obtain the identity of that selected decentralized service, through interface DSE-1 of the given DSE.

The main steps are outlined as follows (see Figure 9-3):

Step 1 An IoT application sends a request to the given DSE through interface DSE-1 to subscribe to exposed service capabilities of a decentralized service.

The application agent processes the request, in collaboration with other FCs of the DSE.

The request for subscription includes at least the identities of the IoT application and its registration, as well as the identity of the decentralized service.

Step 2 The application agent of the DSE requests other FCs (AM-FC, ACM-FC, SCM-FC, etc.) to verify access permission.

Step 3 The AM-FC and ACM-FC and SCM-FC verify the access permission, according to the policy of the DSE.

The general policy to verify access permission may include:

a) the IoT application should be successful to be registered previously to DSE;

b) the decentralized service should be successfully registered on the given DSE, exposed to its service capabilities and available when subscribed;

c) the IoT application and the decentralized service support the same encryption algorithm if they request encrypted communication.

If only one side selects encrypted communication, the access permission is not accepted.

If both sides select encrypted communication, they should support same encryption algorithm. If not, the subscription request is rejected.

Optionally, the given DSE can negotiate with the decentralized service to further check access permission; otherwise, it proceeds to step 6 to send access permission information to the application agent.

Step 4 and 5 The corresponding decentralized service agent of the DSE sends the information to the decentralized service for its subscription, to check remote access permission.

The decentralized service verifies and returns access permission accordingly.

Step 6 The result of the access permission is sent to the application agent accordingly.

If supported, the given DSE combines local with remote to generate final access permission. Otherwise, the local access permission is final.

Step 7 The DSE processes the subscription request accordingly and sends a response to the IoT application.

If the subscription request is accepted, the DSE stores the subscription information for the IoT application, and sends information of the success to the IoT application; otherwise, it sends fail information to the IoT application.

Step 8 If the subscription request is accepted by the given DSE, it may continuously notify the IoT application about the subscribed decentralized service to which it subscribes.

When the service capabilities of a decentralized service change, it may notify the given DSE, which may send that information to IoT applications that have subscribed the decentralized service.

If the status of a decentralized service (e.g., available or unavailable) is known, the given DSE may notify IoT applications that have subscribed to the decentralized service.

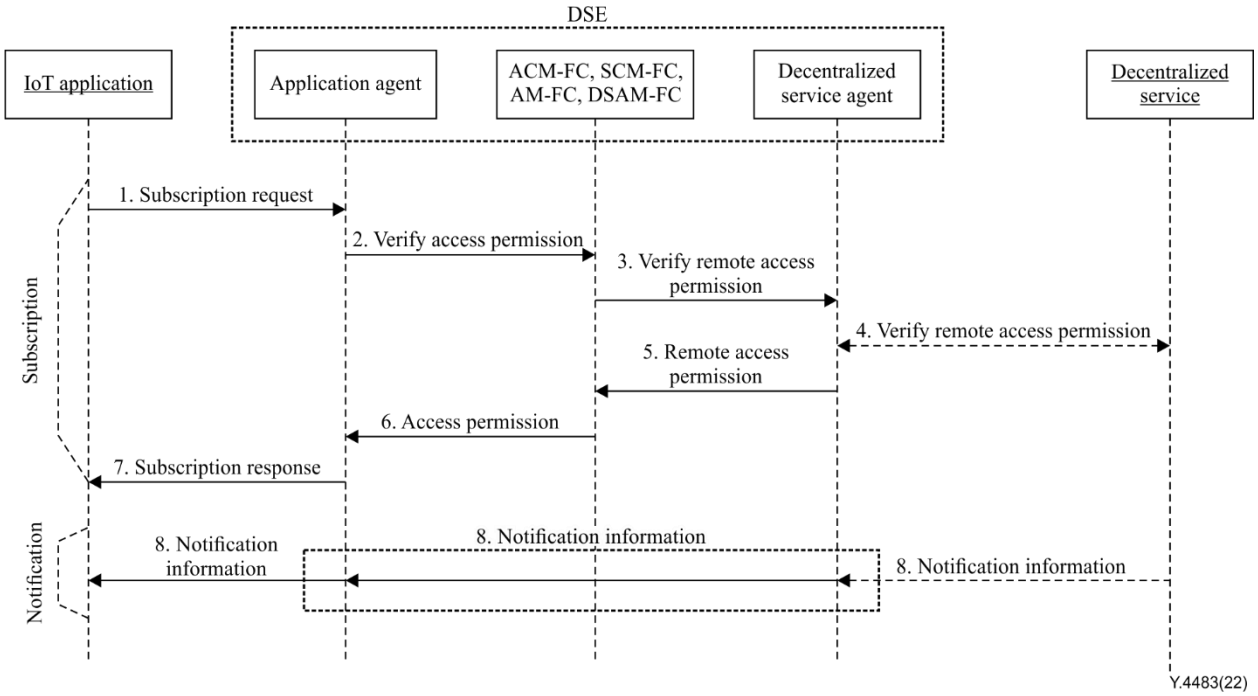

Figure 9-3 – Flow for subscribing service capabilities of a decentralized service

9.4 Access to exposed service capabilities of decentralized service with none-encrypted communication

When an IoT application is successful in subscribing to the service capabilities of a decentralized service, it can request interaction with the decentralized service through interface DSE-1. The given DSE verifies the access permission and provides support for the establishment of communication sessions between the IoT application and the decentralized services. Furthermore, the given DSE converts the data and protocol format of requests and responses in the progresses.

This procedure is an IoT application for access to service capabilities of a decentralized service to which it subscribes.

The main steps are outlined as follows (see Figure 9-4):

Step 1 An IoT application requests access to the service capability of a decentralized service to which it subscribes. This request is sent to the AM-FC through the interface DSE-1.

The request includes the identities of the IoT application and its registration, as well as those of decentralized service, and the target service capabilities. In addition, the request includes approaches and relevant parameters for access to the service capabilities. That information in the request is organized according to the rules of interface DSE-1.

The application agent of the given DSE then receives and processes the request.

Step 2 The AM-FC of the given DSE, in collaboration with its other FCs, verifies the relevant permission for the access request. If the IoT application does not subscribe to the service capabilities, the DSE rejects the request, then generates objection information and proceeds to step 12; otherwise, it goes to step 3.

Step 3 The application agent of the given DSE converts the format of information in the access request for processing by the given DSE.

Generally, interface DSE-1 provides uniform approaches to a transfer request and response. The access request from the IoT application is organized according to the rules of interface DSE-1, and it should be converted so that the given DSE can understand. Additionally, the response from the given DSE should be organized according to the rules of interface DSE-1.

Step 4 and 5 If the access request is accepted, the application agent of the given DSE transfers the request to its SCM-FC.

The SCM-FC of the given DSE then checks the request and transfers the request to the corresponding decentralized service agent of DSE.

Step 6 The corresponding decentralized service agent of DSE converts the format of the request according to the rules of the target decentralized service.

Step 7 The corresponding decentralized service agent of DSE interacts with the target decentralized service, on behalf of the IoT application and DSE.

The corresponding decentralized service agent of DSE sends converted request to target decentralized service, and receives the response.

Step 8 The corresponding decentralized service agent of DSE converts the format of the response from target decentralized service, according to the rules of the given DSE.

Step 9 and 10 The corresponding decentralized service agent of DSE transfers the converted response to the SCM-FC, and then to the application agent of the given DSE.

Step 11 and 12 The application agent of the given DSE organizes the response according to its interface DSE-1, and then sends it to the IoT application.

NOTE – Data format conversion occurs four times in this procedure: 1) on request from the IoT application for the given DSE; 2) on request from the given DSE to decentralized service; 3) in response from decentralized service to the given DSE; and 4) in response from the given DSE to the IoT application. This approach can separate IoT applications and the distant decentralized services, and the IoT applications can use a uniform method and interface to access different types of distant decentralized services.

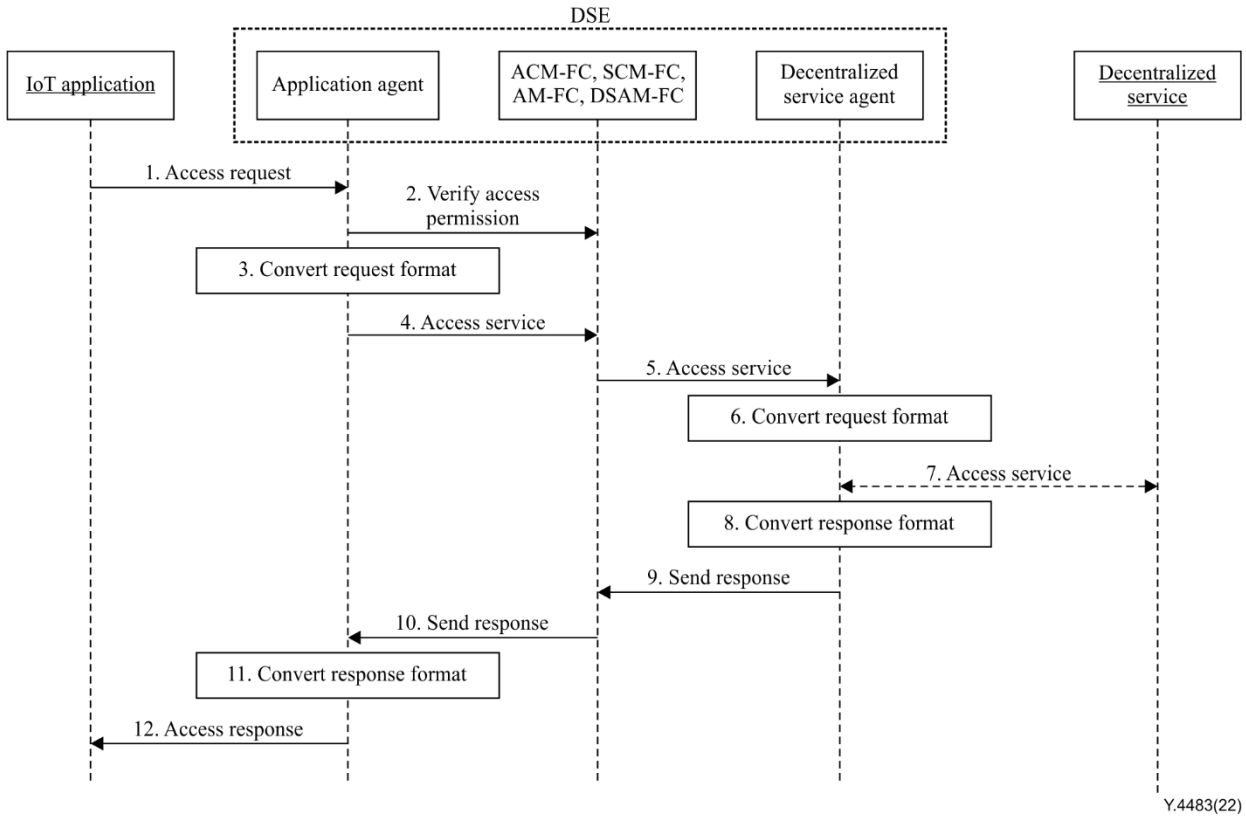

Figure 9-4 – Flow for accessing exposed service capabilities of a decentralized service

9.5 Access to exposed service capabilities of decentralized service with encrypted-communication

The procedure with encrypted communication is similar to that for non-encrypted communication. The main difference is in step 2 shown in Figure 9-4.

If the IoT application or target decentralized service are set to use encrypted communication, in step 2 in Figure 9-4, the given DSE should check whether the IoT application and target decentralized service support the same encryption algorithms. If not, the access request should be rejected.

If using encrypted communication, the given DSE also converts the format of the data and protocol.

10 Security considerations

The given DSE provides an approach to separate IoT applications and the decentralized services, and the IoT applications can use a uniform method and interface to access different types of decentralized service, by using the given DSE.

The given DSE provides a mechanism to support mutual identification, authentication and authorization not only by IoT applications, but also by decentralized services.

The given DSE supports encrypted-communication between IoT applications and decentralized services to provide data security and privacy protection of PII.

Appendix I

Use cases of DSE for Internet of things applications

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

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

I.1 Uniform wallet application

There are many types of wallet applications with different solutions, such as those based on Bitcoin [b-Bitcoin] or Ethereum [b-Ethereum]. One wallet application usually connects to a corresponding decentralized service. So, in an IoT device, there may be multiple wallet applications if the user has multiple types of tokens served by different decentralized services. If using a given DSE, users can use one wallet application to manage all their tokens (see Figure I.1).

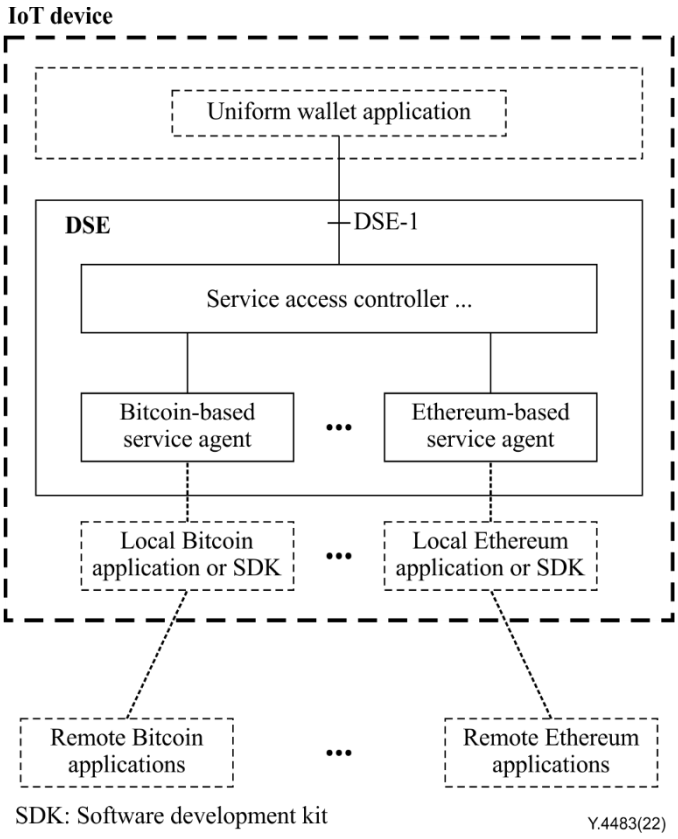

Figure I.1 – Use case of uniform wallet application – using DSE

I.2 Integrated application for smart services

Figure I.2 shows that a user can use a single integrated application, through a given DSE, to access and manage several decentralized smart services, such as those for DLT-based logistics, Ethereum-based token or blockchain-enabled detail.

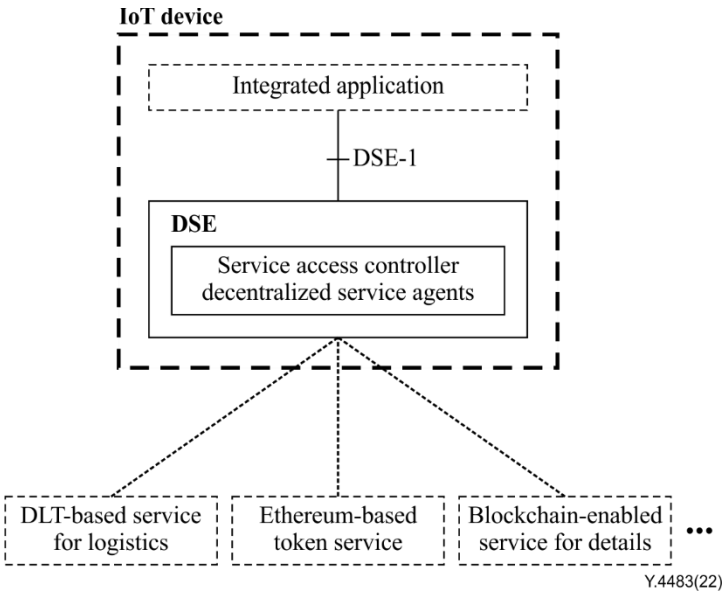

Figure I.2 – Use case of integrated application for smart services – using DSE

Bibliography

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

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

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

[b-Bitcoin] Bitcoin.com (Internet). *Your gateway to Bitcoin & beyond.* Saint Kitts and Nevis: Saint Bitts. Available [2022-06-22] at: https://www.bitcoin.com

[b-Ethereum] Ethereum (Internet). *Welcome to Ethereum.* Bern: Ethereum Foundation, Available [2022-06-22] at*:* http://www.ethereum.org.

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