ETSI GS PDL 023 V1.1.1 (2024-04)

PDL service enablers for Decentralized Identification and Trust Management

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger (PDL) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/PDL-0023_DID_Framework

Keywords
decentralized identifier, PDL

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines Permissioned Distributed Ledger (PDL) Platform services to enable a decentralized identification and trust management framework. The present document also describes the characteristics and behaviour of this framework, along with the services that it offers and ideal solutions that can be built using it.

The objective of the present document includes:

- To define PDL platform services to handle registration management of different type of entities/participants to operate over the PDL platform to accomplish their specific tasks and purpose to realize the overall decentralized identification and trust management process.
- To define PDL platform services to handle decentralized identifier(s), related documents, and verifiable credentials.
- To define PDL platform services to verify the decentralized identifier and related information to enable a specific service provision (e.g. public, and private services).

In scope:

- Definition of Functionalities, Interface Reference points, and Procedures.

The approach taken in the present document is to focus on defining what needs to happen, not how it is implemented.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS PDL 012 (V1.1.1): "Permissioned Distributed Ledger (PDL); Reference Architecture".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] W3C Recommendation 19 July 2022: "Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations".

[i.2] ETSI GR PDL 019 (V1.1.1): "PDL Services for Decentralized Identity and Trust Management".

[i.3] EIDAS: "Supported Self-Sovereign Identity", May 2019.

[i.4] ENISA: "Digital Identity, Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust", January 2022.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

applications at end-device: application (e.g. a client application or wallet) used by the DID holder or Controller to generate, manage, store, or use private and public key pairs for related security (e.g. confidentiality and/or integrity protection)

NOTE: The sensitive information (such as cryptographic materials) may need to be protected by the "secure element" within the device or wallet. In such as case, the use of the cryptographic key(s) is restricted to the DID holder or controller respectively.

Decentralized IDentifier (DID): digital identifier managed through decentralized platform where the subject (e.g. end-user/device/any entity) possess the full control over its generation and associated data exposure, independent from any centralized registry, identity provider, or certificate authority

NOTE: DIDs can be URLs/URIs that relate a DID subject which enables trustable interactions with that subject. DID can refer to any subject (e.g. a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. A DID is considered as a form of pseudonym as used in eIDAS and it is not directly linked to a formal identifier of the natural or legal person.

DID controller: controller of a DID is the entity (person, organization, or autonomous software) that has the capability as defined by a DID method and indicated in the DID document to make any changes to a DID document

NOTE: A DID holder can be the DID controller in some cases (or) a DID controller can be a different entity as authorized by the DID holder. DID controller holds the proof of possession or control of the holder's private key and will be responsible for issuance of a unique and anonymous DID to the holder.

DID document: DIDs resolve to the DID Documents, i.e. a set of simple documents that contains information associated to a DID (e.g. to verify the DID) and describes how to use a specific DID

NOTE: Each DID Document may contain at least three information such as proof purposes, verification methods (such as cryptographic public keys), and service endpoints (can also indicate services relevant to interactions with the DID holder). Proof purposes are combined with verification methods to enable mechanisms for proving various aspects related to DID holder's identification, authentication, and authorization.

DID holder: subject which is referred by the DID is called as the DID holder

NOTE: A DID holder in some cases can generate the DID and, in such cases, the DID holder is also referred as a DID controller.

DID resolver function: DIDs can be resolvable to their corresponding DID documents, where a DID Resolver function supports storage of DIDs and returns necessary data to access DID documents

DID verification: allows authentication of the subject identified by the DID

NOTE: The DID holder presents the data derived from one or more VCs, issued by one or more VC issuers, with a specific verifier (i.e. a service provider) to request and receive specific service of interest to the DID holder. A verifiable presentation is a tamper resistant/evident presentation encoded (with cryptographic methods) in such a way that authorship of the data can be trusted after a process of cryptographic verification. The DID holder authentication is facilitated with protocol exchanges between the DID holder, DID verifier and the trust management framework to verify the DID and validate the VCs (as part of authentication) to check if that can be sufficient to provide a requested service (i.e. resource access) for the DID holder.

DID verifier: it is a role that any third-party service provider or application server would perform to identify and authenticate the DID holder using the trust management framework

distributed ledgers: record of data stored by consensus with cryptographic audit trail maintained and validated by nodes in a decentralized platform based on governance

NOTE: Distributed ledger can be of two types such as permissioned distributed ledger and permission less distributed ledger. As the Permissioned Distributed Ledger (PDL) is further used in the present document, PDL service is further clarified below.

off-chain storage: privacy sensitive data associated to the DID can be stored and managed in isolation using off-chain methods or using any local/external authorized storage space as required

PDL services: it can facilitate the storage of DID related data such as DID documents, VC, etc.

NOTE: The ledgers which store the DID related data should be considered as a form of secure area (e.g. secure element or trusted platform). For example., the storage of DID can be supported through use of an agent service (such as PDL platform service if a distributed ledger is implemented for the storage) to remotely access the data from the end device and controlled through multiple authentication and authorization factors.

Verifiable Credentials (VC): are tamper-evident credentials that has authorship which can be cryptographically verified, and it includes one or more claims asserted by the VC issuer for the DID holder (i.e. subject)

NOTE: In practice, DIDs are used in combination with VCs to enable trusted digital interactions, where the required information about the subject is shared with third parties, by proving to those third parties that the DID subject has ownership of certain attestations or attributes. This proof is based on the cryptographic link between the VC, the DID subject the VC is about, and the issuer of the VC, which can be the DID subject itself (self-asserted claims), or another trusted entity.

VC Issuer: is an entity (e.g. a trusted entity or a trust service provider) that performs claims assertation about one or more subjects, creates a VC from the claims, and transmits the VC to the holder

NOTE: Trust on the VC is established either by trusting the issuer's DID (e.g. by out-of-band mechanisms, bilateral relationship, trusted lists etc,) or by any other means. The third party (e.g. service provider) can then use the presented cryptographically protected proof (i.e. the VC) to verify the ownership and trustworthiness of the claims about the subject.

VC Storage: to enable usage of VCs, the system that implements VC storage performs mediation service for the creation and verification of the identifiers, keys, and other relevant data, such as VC schemas, revocation of VC data, issuer public keys, and so on, e.g. some configurations may require correlation of identifiers for subjects

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DDRS	DID Document Registry Service
DID	Decentralized IDentifier
DLT	Distributed Ledger Technology
DPRS	DID operational Participants Registry service
DRS	DID Resolver Service
DTMF	Decentralized identification and Trust Management Framework
DVMS	DID Verification Management Service
eIDAS	electronic IDentification, Authentication, and trust Services
ID	IDentifier
L-RMS	Ledger Role-based registration Management Service
L-RMS-ID	Ledger Role-based registration Management Service IDentifier
NWK-ID	NetWorK IDentifier

PDL	Permissioned Distributed Ledger
RMS	Registration Management Service
SLA	Service Level Agreement
SSI	Self-Sovereign Identity
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VC	Verifiable Credentials
VDRS	Verifiable credentials Data Registry Service
W3C	World Wide Web Consortium

4 Introduction (informative)

With the evolution of technologies, businesses, and advanced services, a more seamless, user friendly, user controlled, and privacy preserved identity management system is most essential for the quick roll-out and success of any business and services. Meanwhile, the trust in the identity of the subject or object (i.e. a natural or legal person, entity, etc.) has become the cornerstone of all digital services and activities. Here comes the decentralized identification, where a decentralized identifier is considered as the most suitable candidate which can link various essential and limited set of attributes (specific to the end-user(s) or device) as required for any specific service that can be shared with the service provider(s) or verifier(s) in order to enable authentication of the end-user/device to offer a specific set of service(s). The present document defines various PDL platform services such as role-based registration management, DID operation participants registry service, DID registry service, DID Resolver service, DID document registry service, Verifiable credentials data registry service, and DID verification management service, to enable the overall decentralized identification and trust management process. All forms of decentralized identification methodologies can utilize the PDL platform services defined in the present document to handle related data and trust management over the PDL platform. Specific implementation details (e.g. Implementation of identity using a specific method) are out of scope of the present document.

5 ETSI-ISG-PDL Decentralized Identification and Trust management Framework

5.1 Definition of terminologies

A decentralized identification and trust management process enables authentication of the end-user(s)/device(s) (i.e. to set up the initial trust between the end-user/device being the service consumer and the service provider). The key enablers to realize a fully functional decentralized identification and trust management involves various operational aspects such as DID generation (i.e. by a DID holder or DID controller), VC issuance (by a VC Issuer), DID storage and management, VC storage and management, Verification of the DID (by a DID verifier) for identification and authentication as listed and described in detail below.

5.2 Reference Framework Overview

5.2.1 Introduction

The present document uses a functional block architecture to define various services required to enable a decentralized identification and trust management framework. A decentralized platform has the capability to facilitate a globally unique digital identifier (i.e. DID with no possibility of duplication) related data management and control of associated cryptographic verification data, service information, etc. as needed for decentralized identification and authentication of a DID holder (i.e. user/device) to setup trusted interactions between the DID holder and a service provider for any related digital service provisions. The procedural aspects of PDL based decentralized identification and trust management ranges from different participants registration along with access control over the decentralized identification system, related data storage and management operations (e.g. throughout the data lifecycle), the decentralized identifier verification, and selective data exposure to service provider(s) for end-user/device authentication respectively.

A Decentralized Identification and Trust management framework can utilize the PDL services described in the PDL reference architecture (ETSI GS PDL 012 [1]) for the governance related aspects and the decentralized identification management and operation specific PDL services as shown in Figure 5.2.1-1. The core PDL service functionalities (i.e. capabilities, behaviour, and relationships) which forms the building block of decentralized identification and trust management process includes the following as shown in Figure 5.2.1-1 and it is described in detail in clause 5.2.2:

- Ledger Role-based registration management service;
- DID Operational participants Registry service;
- DID Resolver service;
- DID Document Registry service;
- VC Data Registry service; and
- DID Verification management service.

[R1] An ETSI-ISG-PDL compliant PDL platform SHALL include Mandatory Services required by the applications using a decentralized Identification and trust management framework.

[O1] An ETSI-ISG-PDL compliant PDL platform MAY include one or more of Optional Services required by the applications using such platform.

[R2] An ETSI-ISG-PDL compliant PDL platform SHALL include registry service(s) to manage the registered participant specific data such as DID, DID documents and VC Data.

[O2] An ETSI-ISG-PDL compliant PDL platform MAY use a unified registry service for storing DID, Documents and VC data specific to the DID Holder.

[O3] An ETSI-ISG-PDL compliant PDL platform MAY use dedicated registry service for storing different data types such as DID with DID Documents and VC data specific to the DID Holder.

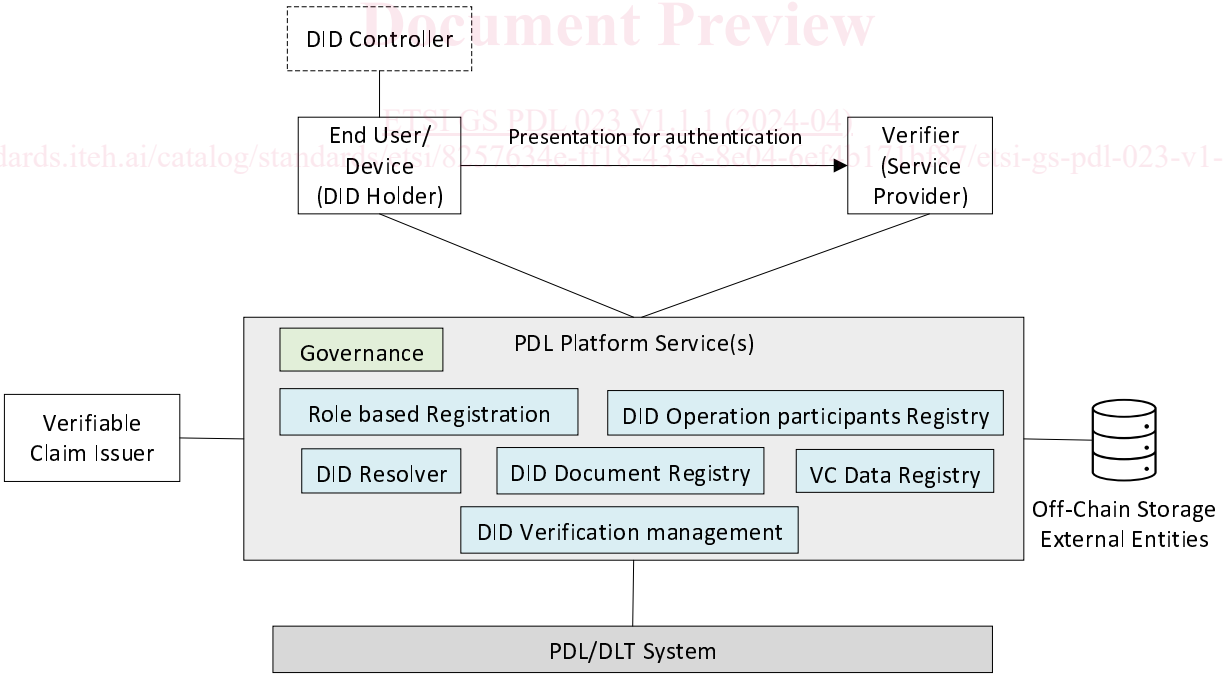

Figure 5.2.1-1: PDL based Decentralized Identification and Trust management framework

5.2.2 PDL services for decentralized identification and trust management

5.2.2.1 Ledger Role-based registration management service

The Ledger role-based Registration Management Service (L-RMS) considers the following different roles for the participants who are the integral users of the decentralized identification and trust management framework. It provides registration service (along with authorization for fine grained access control) specific to the corresponding roles of the participants and their allowed operations in the PDL platform. The role-based registration management service offers registration and de-registration (e.g. revocation of registration) related services for different participants:

- Identity Holder (i.e. a DID Holder);
- Identity Controller (i.e. a DID Controller);
- VC Issuer; and
- DID Verifier.

[O2] An ETSI-ISG-PDL compliant PDL platform MAY include Decentralized Identification and Trust management framework related functionalities.

If the PDL platform supports Decentralized identification and Trust Management Framework (DTMF) related functionalities and operations, then further requirement(s) described in this clause are applicable.

[R2] An ETSI-ISG-PDL compliant PDL platform SHALL include Ledger Role-based registration management service to manage the registration and operation of different participants (entities) utilizing such a framework.

5.2.2.2 DID Operational participants Registry service

The DID operational Participants Registry Service (DPRS) records and keeps track of the registered and de-registered participants from the PDL platform based DTMF by considering the instructions from the L-RMS.

[R3] An ETSI-ISG-PDL compliant PDL platform SHALL include a registry service to record the registration and operational details of different participants (entities) utilizing such a framework.

5.2.2.3 DID Resolver service

The DID Resolver Service (DRS) stores the DIDs in a DID registry, keeps track of the DID(s) and its associated DID document location information (e.g. address) to enable DID document fetching and verification by the authorized services and entities (i.e. DID Verifiers e.g. service providers).

5.2.2.4 DID Document Registry service

The DID Document Registry Service (DDRS) allows to store and manage the DID documents associated to the DID to facilitate DID verification. Whereas each DID Document can contain at least three things: proof purposes, service specific information for which the DID document can be used, verification methods, and service endpoints. Proof purposes are combined with verification methods to provide mechanisms for proving things.

EXAMPLE: A DID Document can specify that a particular verification method, such as a cryptographic public key or pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication.

Service endpoints enable trusted interactions with the DID holder as well as authorized verifier. The DID Document Registry service offers Create (i.e. to store), Update, Revoke DID documents (i.e. deletion) related service operations.

5.2.2.5 VC Data Registry service

The VC Data Registry Service (VDRS) allows to store and manage the VCs associated to the DID to facilitate VC based DID verification and validation related to a service request. The VC Data Registry service offers Create, Update, and Revoke VCs related service operations.