ETSI GS PDL 012 V1.2.1 (2023-06)

Permissioned Distributed Ledger (PDL); Reference Architecture

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
RGS/PDL-0012v121 Ref Arch

Keywords
architecture, distributed ledger

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

Contents

List of figures

List of tables

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.

Executive summary

The present document is a revision of ETSI GS PDL 012 (V1.1.1) that defines an ETSI-ISG-PDL Reference Architecture (RA) for a permissioned Distributed Ledger Technology (PDL) platform. The present document also describes the characteristics and behaviour of such a platform, along with the services that it can provide and solutions that can be built using it. It includes improved definitions, additional clauses and tables resulting from feedback received from stakeholders using the previous version since its release.

Introduction

The present document defines an ETSI-ISG-PDL Reference Architecture (RA) for a permissioned Distributed Ledger Technology (PDL) platform. The present document also describes the characteristics and behaviour of such a platform, along with the services that it can provide and solutions that can be built using it.

The ETSI-ISG-PDL RA is a template for defining a solution to a particular problem domain (in this case, a PDL platform). The ETSI-ISG-PDL RA describes abstract functional components that support specific sets of functionalities and reference points that describe standard interactions between different parts of the platform and users of that platform (refer to Figure1). The present document uses a Functional Block architecture to define three key aspects of a PDL Platform:

- Standardized platform services, which are services and functionality provided by the PDL platform that conform with pre-defined requirements so they can interoperate with other components of the platform.
- Abstraction layers, which are Data Model Brokers allowing different and diverse applications on one side and different PDL chain types on the other side to interface with the PDL platform.
- Modularity, which allows evolution and adaptation of PDL platforms to changing requirements.

The objectives of using the RA are to:

- Maximize the choice of technology solutions available to entities using ETSI-ISG-PDL-endorsed technologies, Services, and applications.
- Maximize ETSI-ISG-PDL endorsed PDL platforms' scalability in terms of the applications supported and the number of entities able to use them.

The ETSI-ISG-PDL RA also provides standardized terminology to simplify the interaction between objects such as PDL Platforms, Services, and applications (as defined in clause 3.1) developed by ETSI-ISG-PDL members including operators and technology vendors/developers.

This approach enables operators and technology vendors/developers to focus on their respective areas of expertise and market leadership by providing solutions for one or more Reference Architecture functional components and/or services. It also allows users to choose appropriate vendors and solutions for their specific environment and product portfolio.

The architecture aims to be independent of specific implementations to accommodate a wide range of technology solutions that comply with both the requirements of the supported applications and ensures adherence to critical architectural requirements such as interoperability, security, privacy, etc.

The ETSI-ISG-PDL RA comprises two categories of architectural components - those components mandated in all platforms (i.e. PDL Mandatory Platform Services), and those components that are optional and may be included or excluded depending on the applications implemented on the Platform (i.e. PDL Optional Platform Services). This approach facilitates the introduction and support of new applications in a structured manner without changing the common, mandatory, parts. The RA also supports the concept of a distributed lifecycle for applications, where different parties take different roles and responsibilities (for example Buyer versus Seller). This expands the vendor-operator space, by allowing vendors to focus on, and operators to choose from, specific architectural components in the stacks and focus their offerings on the different PDL Platforms, Services, and applications.

Intended Audience

All ETSI members, any technical, commercial and operations experts working in the ICT industry, software vendors, standards organizations, other service providers, and industry bodies.

1 Scope

1.1 Definition

The present document defines a RA for a Permissioned Distributed Ledger platform. Following the terminology and general architectural requirements, the present document discusses the architectural components listed below:

a) Orchestration, governance, process management, and eco-system coordination in a complex environment (for example node and PDL management in an environment involving multiple competing parties or supply chains).

b) External and internal information exchange (for example through Oracles, APIs, micro services, webhooks, or external data sources).

c) Off-chain Storage (another chain, local/cloud node that is not part of the PDL, PDL node but not sharing with other nodes of said PDL, trusted by a single node or trusted by all nodes based on governance, etc.).

d) Smart Contracts (including commonalities between Smart Contracts, interoperability of Smart Contracts across chains, PDL agnosticism).

1.2 In scope

a) Definition of functionalities, interfaces, reference points (for example Identity services such as PDL identity, Node identity, and User identity).

b) Functional capabilities of commercial applications using PDL to create/trade value (for example wholesale settlement, cryptocurrency or stable coins-based payments, tokenization, and asset/inventory management).

c) Non-functional capabilities of commercial applications using PDL to create/trade value (for example network design, security, privacy, and access control).

d) Capabilities of different PDL protocols (common aspects of PDL protocols that can be use case, platform, application, and service agnostic amplified through inter-ledger interoperability).

1.3 Out of scope

a) Architecture design and implementation details.

b) PDL network design and implementation details.

c) Design and implementation details of platforms built on PDL network.

d) Specific application/ service implementation details of application platforms built on PDL network (for example implementation of identity using a specific method).

NOTE: Any platform, application, or network specific implementation details will be added at a later phase through dedicated ETSI-ISG-PDL PRD documents (Including Functional, Privacy and Security related services and requirements) or an annex to the present document (for other services) on need basis.

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.

Not applicable.

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] MEF 55.1: "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", January 2021.

[i.2] NIST Special Publication 800-162, January 2014: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations".

[i.3] Gamma E., Helm R., Johnson R., Vlissides J.: "Design Patterns: -Elements of Reusable Object-Oriented Software", Addison-Wesley, Nov 1994.-ISBN 978-0201633610.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

abstraction layer: functionality that serves as an intermediator between subsystems that may be using different protocols, vocabulary, and methods that serves their respective purposes

access control policy: privileges and permissions of a subject entity to perform operations on a set of target entities

addressable storage: content/data that can be accessed through a web link (URL)

API Broker: software that mediates between two systems with different Data Models implemented as APIs

NOTE: Also referred to as API Gateway.

API Gateway: See API Broker.

application: software, program or group of programs designed to perform specific tasks for end users

application abstraction layer: APIs and interfaces, including API Brokers, enabling applications to communicate with a Platform

Application Programming Interface (API): system of tools and resources in an operating system, enabling developers to create software applications

asynchronized data: data that does not require synchronization with other data

Attribute Based Access Control (ABAC): access control method where the subject requests for performing an operation on objects are granted/denied based on:

- Assigned attributes of the subject.
- Assigned attribute of the object.
- Environmental conditions.
- Set of policies.

blockchain: censorship and tamper-proof growing list of records, called blocks, that are linked using cryptography

NOTE: Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

business service: service delivered to business customers by business units

category alpha application: application that is developed and delivered to all users of said application by a single vendor/developer using a Category Alpha Platform developed by that same vendor/developer

NOTE: Can only use a single PDL type prescribed by the developer.

category alpha platform: PDL platform that is designed, developed, delivered, and integrated to all users of said platform by a single vendor using a single PDL technology

NOTE: Broken down to sub-categories "Alpha-1" and "Alpha-2".

category bravo application: application developed and delivered to all users of said application by a single vendor/developer using a Category Bravo Platform developed by that same vendor/developer

NOTE: Can only use PDL types prescribed by the developer.

category bravo platform: PDL platform designed, developed, delivered, and integrated to all users of said platform by a single vendor, but can operate using two or more underlying PDL technologies

NOTE: Broken down to sub-categories "Bravo-1" and "Bravo-2".

category charlie application: application developed towards a specification of an Application so that any user of an application supporting such specifications can fully interoperate with other users of other applications built towards the same Application specifications

category charlie platform: PDL platform that can operate using two or more underlying PDL technologies and is designed and developed towards a specification of an Application Abstraction Layer so that any Application that supports such an abstraction layer can interface with said platform

NOTE: Broken down to sub-categories "Charlie-1", "Charlie-2", "Charlie-3" and "Charlie-4".

category delta platform: category charlie platform that only supports a single PDL type

NOTE: Broken down to sub-categories "Delta-1", "Delta-2", "Delta-3" and "Delta-4".

Certificate Authority (CA): entity that issues digital certificates

NOTE: A digital certificate certifies the ownership of a public key by the named subject of the certificate.

composite application: application using the PDL platform that are made up of other applications that use the PDL platform

composition: act of creating a new object or a new functionality through combination of two or more existing objects or functionalities

concurrency: occurrence of and/or execution at the same time of different programmatic units

consumer: PDL Platform entity that consumes data produced by another entity

data model: concepts of interest to an environment in a form that is dependent on data repository, data definition language, query language, implementation language, and/or protocol

NOTE: Data Models are derived from the Information Model.

data model broker: software that mediates between two systems with different data models

NOTE: also referred to as data model gateway.

data model gateway: same as data model broker

directly connected storage: storage that is local to the node and is either physically connected to the node or is external storage connected using a shared communication channel that is managed by the owner of that node

NOTE: Examples of physically connected storage: internal drive, external thunderbolt drive. Examples of external storage: NAS, Cloud.

Discretionary Access Control (DAC): Access Control Policy where the owner of a resource/object defines the Access Control Policy for the users

distributed addressable storage: Addressable Storage that is distributed across multiple storage devices

Distributed Ledger Technology (PDL): technology implementing a distributed ledger which is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions

NOTE: Unlike with a distributed database, there is no central administrator.

Domain Name System (DNS): hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network

NOTE: It associates various information with domain names assigned to each of the participating entities.

external data: data obtained from resources or systems external to the PDL platform

external IRP: IRP used to communicate between a PDL Functional Block and an external object

fork: split of a PDL chain into two chains that share the history up to the point where the fork occurred, and then each part is headed in its own direction

functional block: abstraction that defines the external structural representation of the capabilities and functionality of a component or module, and its relationships with other Functional Blocks

NOTE: Functionalities such as capabilities, behaviour, and relationships, as well as their inputs, outputs, and optionally, transfer functions. The internal structure of a Functional Block is not revealed.

functional capability: capability of a system to manage resource in each functional area of operations

governance: collection of rules and tools that control the behaviour and function of a PDL platform

hardware interface: point across which electrical, mechanical, and/or optical signals are conveyed from a sender to one or more receivers using one or more protocols

implementation agreement: rules and agreements that describe how a Platform Service is implemented

information model: representation of concepts of interest to an environment in a form that is independent of data repository, data definition language, query language, implementation language, and protocol

insignificant event: event that does not affect any node other than the node where it occurred and does not affect the chain or consensus mechanism

Interface Reference Point (IRP): communication channels through which Functional Blocks communicate with each other

NOTE: IRPs are given names for reference purposes (for example "Debka").

internal data: data generated by a node either through computation or through a directly connected sensor that feeds data to that node

internal IRP: IRP used to communicate between two or more PDL Functional Blocks

NOTE: This communication stays within the PDL Platform and is not seen by objects that are external to the PDL

Internet Corporation for Assigned Names and Numbers (ICANN): American multi-stakeholder group and non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation

Internet Engineering Task Force (IETF): open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite

InterPlanetary File System (IPFS): protocol and peer-to-peer network for storing and sharing data in a distributed file system that uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices

loosely coupled: functionality that has little or no dependency on other functionalities

Mandatory Access Control (MAC): Access Control Policy defined by system administrators

Minimum Viable Product (MVP): version of a product with just enough features to satisfy early customers and provide feedback for future product development

network: In the context of the present document, technical infrastructure that allows applications to access PDLs through use of Platform Services.

NOTE: This term is interchangeable with Platform in the context of the present document.

non-addressable storage: content/data that cannot be addressed and accessed by any other entity except for the entity that directly manages this data

orchestration: automated (and/or manual) configuration and management of systems and their Functional Blocks

NOTE: Orchestrated objects may be Resources, Platform Services, Applications. Orchestration emphasizes coordinated actions; one form of this coordination is service function chaining.

PDL abstraction layer: APIs and interfaces, including API Brokers, enabling Platform services to communicate with ETSI-ISG-PDL endorsed PDL types

platform: in the context of the present document, network environment in which one or more applications and services are implemented and executed

platform atomic service: platform service that does not use any other Platform Service to perform its functionality

NOTE: May use external applications or functions.

platform composite service: platform service that uses one or more other platform services to perform its functionality

platform mandatory service: platform service mandated to be included in a platform

platform optional service: platform Service that does not need to be included in a platform for it to be considered ETSI-ISG-PDL compliant

platform service: service implemented within the Platform Services layer that is compliant with the ETSI-ISG-PDL requirements and definitions

policy: set of rules used to manage and control the changing and/or maintaining of the state of one or more managed objects, defined by the Governance

Policy Based Access Control (PBAC): Access Control method that uses Policies to determine the appropriate type of access control based on the needs of the PDL Platform

producer: PDL Platform entity that generates data that other entities may consume

RAM swap space: portion of a computing device's hard drive used for virtual memory in the event that there is insufficient physical RAM installed on the device

Random Access Memory (RAM): hardware in a computing device where the operating system, application programs and data in current use are kept so they can be quickly reached by the device's processor

Reference Architecture (RA): template for defining a solution to a particular problem domain

Remote Procedure Call (RPC): computer program that causes a procedure to execute in a different address space, which is coded as if it were a normal procedure call, without the programmer explicitly coding the details for the remote interaction

Role Based Access Control (RBAC): access control approach based on the roles the user assumes in a system, rather than the user's identity

service: instance of a technology product implemented using a platform

NOTE: For example, a communication circuit connection between two offices.

significant event: event occurred on any node that may affect the behaviour of the node, the chain, or the consensus mechanism

smart contract: program stored on a Blockchain that executes when predetermined conditions are met

software interface: point through which communication with a set of resources of a set of objects is performed

NOTE: Resources such as memory, CPU, Location, User roles or Smart Contracts.

software reference model: set of architectural patterns and other supporting artifacts that presents a set of unifying terminology, concepts, axioms, and Functional Blocks within a particular problem domain

synchronized data: data that requires sequencing and has dependency on timing or content of other data being collected

tightly coupled: functionality that has a high degree of dependency on other functionalities

trusted third parties: in cryptography, entity which facilitates interactions between two parties who both trust the third party

NOTE: The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content.

Universal Resource Locator (URL): reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it

NOTE: A URL is a specific type of Uniform Resource Identifier, although many people use the two terms interchangeably.

use case: specific situation in which a product or service could potentially be used

virtual service: service that uses one or more virtual objects

NOTE: Objects such as Resources, Services.

3.2 Symbols

Void.