ETSI GR PDL 017 V1.1.1 (2024-07)

GROUP REPORT

Permissioned Distributed Ledger (PDL); Application of PDL to Amended Regulation 910/2014 (eIDAS 2) Qualified Trust Services

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

DGR/PDL-0017_eIDAS App

Keywords

data, PDL, security, time-stamping, trust services

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

Modal verbs terminology

In the present document "**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.

Introduction

Distributed ledgers have become the intrinsic foundation of secure decentralized transaction-based applications, including (but not limited to) decentralized cryptocurrencies. They are often referred to as blockchain, given the use of cryptographic techniques to link a growing list of blocks (records). While blockchain is a specific implementation of a distributed ledger, the industry has conformed with use of a more generic term:

- Distributed Ledger Technology (DLT).

Distributed ledgers can be considered as permissioned or permission-less, referring to the requirements for a node to be approved to validate transactions and record them on the ledger.

The present document is one of a series of reports and specifications developed by the ETSI Industry Specification Group on Permissioned Distributed Ledger (ISG PDL) (see https://www.etsi.org/technologies/permissioned-distributed-ledgers).

Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 [i.12] as regards establishing a framework for a European Digital Identity [i.1], commonly referred to as eIDAS 2, provides a framework for use of digital signatures and electronic identities based on an EU Digital Identity Wallet for a pan-European infrastructure supporting electronic identities, authentication and signatures. The amended regulation includes requirements for an commercially provided infrastructure of "trust services" which supports the European Digital Identity Framework. One of the supporting trust services identified in eIDAS 2 [i.1] is an electronic ledger which may be provided by a single body, or distributed access several providers which are permissioned to provide a distributed ledger in the form of a Permissioned Distributed Ledger.

A set of reports and specification primarily at supporting digital signatures under the current Regulation (EU) No 910/2014 [i.12] have been developed by ETSI Technical Committee on electronic Signatures and Trust Infrastructure (see ETSI TC ESI activities). ETSI TC ESI is currently developing a further set of specifications in support of Regulation (EU) 2024/1183 [i.1] the amending Regulation (EU) No 910/2014 including support for the EU Digital Identity Wallet and additional trust services such as electronic ledgers (see ETSI portal TC ESI). eIDAS 2 defines specific requirements for "Qualified Trust Service" which are overseen by national regulatory bodies and are given a form of legal presumption.

The present document considers the application of PDL to qualified trust services under Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (eIDAS 2) [i.1].

1 Scope

The present document describes the features of a PDL to be applicable as a qualified electronic ledger and in support for eIDAS 2 [i.1] trust services. The present document analyses the properties that a PDL can have to be an enabler for eIDAS 2 [i.1] regulation for electronic identification, authentication and signatures, and also for using eIDAS 2 [i.1] in other areas of the Digital Economy.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2).

[i.2] ISO/TS 23635:2022: "Blockchain and distributed ledger technologies Guidelines for governance".

[i.3] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.4] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[i.5] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.6] ETSI DTS/ESI-0019472-1 Work item on "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestations of Attributes; Part 1: General requirements".

[i.7] ETSI EN 319 522 (all parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services".

[i.8] ETSI GS PDL 012: "Permissioned Distributed Ledger (PDL); Reference Architecture".

[i.9] ETSI GS PDL 015: "Permissioned Distributed Ledger (PDL); Reputation management".

[i.10] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.11] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.12] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.14] ETSI TR 103 684: "Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services".

[i.15] Pilot for the International Compatibility of Trust Services.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in eIDAS 2 [i.1] and the following apply:

eIDAS 2: Regulation (EU) 2024/1183 [i.1] amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity [i.1]

GDPR: EU General Data Protection Regulation [i.13]

NIS2: EU Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [i.10]

3.2 Symbols

Void.

3.3 Abbreviations

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

DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure
LOTL	List of Trusted Lists
PDL	Permissioned Distributed Ledger
QTSP	Qualified Trust Service Provider

NOTE: Under eIDAS 2 [i.1].

TC ESI	Technical Committee on Electronic Signatures and Trust Infrastructures
TSP	Trust Service Provider

4 Features of PDL

4.1 Common Context

PDL, in nature, is a permissioned electronic ledger which is distributed. The capabilities to configure automated process which are permissioned fit into more possibilities for regulatory frameworks to provide legal certainty with distributed ledgers which usually are not single-jurisdictional governance model instead of multi-jurisdictional governance model. The European Union and the efforts for the Digital Single Market in the European space represent per se a multi-jurisdictional governance model which can be harmonised for specific requirements when a distributed ledger is being used like European Blockchain Services Infrastructure (EBSI).

The present document does not consider the alternative approaches to identification and authentication commonly associated with distributed ledgers such as use of decentralised identifiers, and the electronic identification, authentication and signature services of eIDAS 2 [i.1].

A reference architecture for PDL is given in ETSI GS PDL 012 [i.8].

4.2 Properties

The main properties of a PDL are:

- Immutably: The content of the ledger cannot be changed.
- Integrity: Any change to an individual record once placed in the ledger can be detected.
- Sequence: Any change to the sequence of records in a ledger can be detected.
- Persistent: The above properties are not time-limited.
- Verifiable/auditable: The above properties can be checked independent of any provider of ledger services.
- Accountable: Each members of a PDL can be held to account for the provision of its services.
- Redundancy: The properties of the PDL do not depend on a single point of failure in the functionality or security of a ledger service provider.

Non-essential properties of a PDL which may be provided using services external to the PDL:

- The identity of the originator of a record.
- The time at which a record was added to the ledger.

PDL is based upon multi-party provision of a distributed ledger with consensus and synchronization protocols between the parties ensuring an agreed content of the ledger.

PDL is also based on governance regime with permission granted to the ledger providers.

4.3 Governance

4.3.1 Principles

Principles of governance of a distributed ledger, including a PDL, based on ISO/TS 23635 [i.2] are as follows in Table 1.

Table 1

ISO/TS 23635 [i.2]	PDL
Principle 1: Define identifiers of entities involved	Through PDL governance, the entities providing ledgers are identifiable within the community. In addition, the identity of the node originating data record is identifiable.
Principle 2: Enable decentralized decision-making	Decentralised within scope of governance domain as distributed across several nodes. Collective decisions recorded explicitly on ledger.
Principle 3: Ensure explicit accountability	Through the PDL governance the responsibilities and liabilities of the identified PDL providers can be clearly defined.
Principle 4: Support transparency and openness	The governance regime needs to be able to detect if rules for the operation of PDL are not applied. Entities can participate in a PDL provided that they meet the governance criteria provided rule. The transparency and openness needs to be within the limits of GDPR [i.13].
Principle 5: Align incentive mechanisms with system objectives	A PDL governance regime can define equitable alignment for scalable solutions and services based on incentives from a wide range of options. Also it represents a beneficial participatory with the objectives of the PDL itself.

ISO/TS 23635 [i.2]	PDL
Principle 6: Provide performance and scalability	Monitoring tools and services allow to practice performance and scalable perspective, as well as surveillance mechanism that can anticipate mal-functional or risky areas of performance.
Principle 7: Make risk-based decisions and address compliance obligations	The nodes participating in the chain together enforce the rules for the chain though the protocol exchanges. Further governance rules on nodes participating in the chain for a particular business need are applied through the process of grating permission.
Principle 8: Ensure security and privacy	A PDL governance regime may stablish policy requirements for various purposes and have to secure automated scenarios to avoid breaches of privacy based on the operations of the different products and services within the PDL and from the PDL with the real world.
Principle 9: Consider interoperability requirements	Due to the facts that permission requires different paths for interoperate in due conditions, it represents as well, weather direct or indirect tools for interoperability with other governance regimes. A PDL can accommodate also unidirectional interoperability requirements which it does not affect to both PDL interaction but allow the interoperability.

4.3.2 Other Factors to be considered in a Governance Regime

A PDL may apply across jurisdictions provided they apply the requirements of the governance regime enforced through a form of legally recognized agreement such as a contract or multi-national agreement.

A specification on PDL reputation management is given in ETSI GS PDL 015 [i.9] which can be taken into account by a governance regime.

5 Features of eIDAS 2 Qualified Trust Services

5.1 eIDAS 2 trust services

Regulation (EU) 2024/1183 amending Regulation 910/2014 (commonly referred to as eIDAS 2) [i.1] provides a regulatory framework for the provision of electronic identities and trust services. This defines specific types of third party "trust services" supporting the security of electronic transactions. This is primarily aimed at the European internal market but can be applied internationally. Within eIDAS 2 [i.1] trust services are limited to those services which are provided commercially. Government provided services, which are generally funded through taxation, are not considered trust services under eIDAS 2 [i.1].

The concept of trust service was initially applied to services issuing public key certificates in support digital signatures, legally referred to in eIDAS 2 [i.1] as advanced electronic signatures or seals. Issuance of certificates in support of digital signatures remains the main type of trust service used within Europe and this type of trust service is becoming recognized internationally. Currently, 9 trust services types are recognized in the current eIDAS 2 [i.1] regulation, all of which have been implemented by a number of trust service providers. Trust services were previously defined in Regulation (EU) 910/2014 [i.12] are services for:

a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

b) the creation, verification and validation of certificates for website authentication; or

c) the preservation of electronic signatures, seals or certificates related to those services.

This is extended in eIDAS 2 [i.1] for recognized trust services also to include:

a) the electronic archiving of electronic documents;

b) the management of remote electronic signature and seal creation devices;

c) the recording of electronic data into an electronic ledger.

5.2 Qualified Trust Service Providers

eIDAS 2 [i.1] gives specific recognition for the provision of trust services which meet particular requirements as identified in the eIDAS 2 regulation [i.1]. A trust service provider which meet these requirements are referred to as a Qualified Trust Service Provider (QTSP). The requirements for being a QTSP include:

a) requirements to take appropriate technical and organizational measures (applicable to both qualified and non-qualified trust service providers);

b) requirements for notification of security breaches (applicable to both qualified and non-qualified trust service providers);

c) requirements for the cybersecurity of essential services under NIS 2 [i.10];

d) requirements for personal data protection such as in General Data Protection Regulation [i.13];

e) requirements for the provision of Qualified trust services;

f) requirements for the particular type of Qualified trust service.

The QTSPs which are recognized as meeting the requirements of trust service.

eIDAS 2 [i.1] Article 14 cross recognition of qualified trust service providers can be requires recognition either under an implementing act issued by the EU or through legal agreement.

5.3 Specific Requirements of EU Qualified Electronic Ledgers

The specific legal requirements on electronic ledgers as given in the eIDAS 2 regulation [i.1] are as follows:

1) Article 3 (53) 'electronic ledger' means a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological ordering;
Article 45i: Requirements for qualified electronic ledgers.

   It is also required for Qualified electronic ledgers that:

   a) they are created and managed by one or more qualified trust service provider or providers;

   b) they establish the origin of data records in the ledger;

   c) they ensure the unique sequential chronological ordering of data records in the ledger;

   d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.

2) Implementing acts are required 12 months after eIDAS 2 [i.1] comes into force establishing a list of reference standards and when necessary, establish specifications and procedures for the requirements laid down in point 1).

5.4 Governance and Audit Requirements

Qualified Trust Service Providers (QTSPs), including providers of Qualified Electronic Ledgers, are supervised by a national authority to ensure that they meet the functional and security requirements of the eIDAS 2 regulation [i.1]. The acceptance of a Qualified Trust Service as meeting the regulatory requirements is based on an audit by a "Conformity Assessment Body" accredited under EU regulations. It is common for the audit to be based on assessment of Policy and Security Requirements for the provision of particular trust service defined by ETSI.QTSPs who are recognized under the eIDAS 2 [i.1] supervisory scheme are included in Trusted List which identifies the trust services supported and a public key certificate which identifies the provider of the trust service.

Requirements on measures for a high common level of cybersecurity across the Union is specified in regulation Directive (EU) 2022/2555 [i.10], commonly referred to as NIS2 [i.10], applies to Qualified Trust Service thereby assuring that the security of such essential services. ETSI EN 319 401 [i.11] defines general policy requirements for Trust Service Providers and is currently being updated to incorporate all the requirements of NIS2 [i.10].

6 PDL and eIDAS 2 Trust Services

6.1 PDL as an eIDAS Trust Service

6.1.1 Requirements for Qualified Electronic Ledgers vs Features of PDL

Table 2: Ledger Specific Requirements

eIDAS 2 [i.1] Article 45i Requirements on Qualified Electronic Ledgers	PDL Properties	Assessment
(a) they are created and managed by one or more qualified trust service provider or providers;	Multi-party: Based on consensus between multiple ledger providers	PDL is always multiparty. Whereas eIDAS 2 [i.1] only addresses requirements of one QTSP
(b) they establish the origin of data records in the ledger;	Identity of origins not essential	PDL identifies the node originating data record included in chain. May use pseudonym within the PDL
(c) they ensure the unique sequential chronological ordering of data records in the ledger;	Sequence: The sequence of records in a ledger cannot be changed	May be difficult to assure precise chronological order of records entered into different ledger providers. However, chronological order within ledger maintained
(d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.	Immutably: The content of the ledger cannot be changed Integrity: Any change to an individual record once placed in the ledger can be detected Persistent: The above properties are not time-limited	PDL meets eIDAS 2 [i.1] requirements

Generally, eIDAS 2 [i.1] requirements are in common for the basic immutability and integrity of PDL. However, the requirements for supporting the multi-party properties of PDL need to be added to those of eIDAS 2 [i.1].

In terms of electronic records management, EU requirements for qualified electronic ledgers provide some legal certainty that assures the uniqueness, authenticity and correct sequencing of the records entry in a tamper proof manner. From the point of view of the PDL and its governance it fulfils the essential for suitable multiparty co-operations, the main challenge is for those more decentralized or multi-jurisdictional governance models with which the cross-border protection may require additional auditing and reporting mechanisms, although digital single market like the pan-European legal framework recognizes trust services for the recording of data which are able to be qualified by providing legal certainty for its use cases and accountability.

6.1.2 Governance & Audit

Table 3: Governance requirements

eIDAS 2 [i.1] requirements	ISO /TS 23635 [i.2] principles	Assessment
EU Trusted lists	Principle 1: Define identifiers of entities involved	The trusted list identifies whether a QTSP provides qualified electronic ledgers. But it does not identify the PDL community (or communities) for which the QTSP provides services.
	Principle 2: Enable decentralized decision-making	Decentralised decisions not addressed by eIDAS 2 [i.1].
Article 46b: eIDAS 2 [i.1] supervision	Principle 3: Ensure explicit accountability	Provides accountability under eIDAS 2 [i.1] requirements, but not against PDL governance requirements.

eIDAS 2 [i.1] requirements	ISO /TS 23635 [i.2] principles	Assessment
Article 46b: audit requirements	Principle 4: Support transparency and openness	eIDAS 2 [i.1] depends on accredited auditor. The details of the audit are generally not available to all stakeholders.
Article 3 (16) trust service' means an electronic service normally provided for remuneration	Principle 5: Align incentive mechanisms with system objectives	eIDAS 2 [i.1] trust services are generally incentivised through remuneration.
	Principle 6: Provide performance and scalability	Performance and scalability not addressed by eIDAS 2 [i.1].
Compliance required with: • NIS 2 [i.10] cybersecurity • GDPR [i.13]	Principle 7: Make risk-based decisions and address compliance obligations Principle 8: Ensure security and privacy	Risk management and cyber security are essential to NIS2 [i.10]. GDPR [i.13] requires privacy.
Interoperability is a requirement for both digital identities and electronic signatures and seals	Principle 9: Consider interoperability requirements	Common concern of eIDAS 2 [i.1] and PDL.

In general eIDAS 2 [i.1] governance requirements provides a foundation for the governance of a PDL However, there are aspects of PDL which are outside the scope of eIDAS 2 [i.1] relating to the multi-party nature of PDL and governance of a community of ledger providers that support PDL.

Thus, the governance of a PDL based on eIDAS 2 [i.1] should be addressed as two layers:

1) Basic governance requirements of a Qualified Electronic Ledger Provider following the regulatory requirements of eIDAS 2 [i.1].

2) Additional requirements for governance of a community of Qualified Electronic Ledger Providers.

The second PDL specific governance layer would address:

- Application: The applicability of the PDL in terms of usage and community.
- Consensus: The protocol mechanisms used to achieve consensus between PDL node provider.
- Synchronization: The protocol mechanisms used to ensure that ledgers are synchronized over time.
- PDL Community identification: The mechanisms used for identification and authentication of electronic ledger providers that are members of a particular community.
- Additional policy requirements: The requirements on the procedures and practices of electronic ledger providers based on eIDAS 2 [i.1] requirements.
- User requirements: Requirement on the PDL user for providing data to be placed in a ledger.
- Audit: Requirements on the audit of PDL node provider.
- Permissioned: Rules for acceptance under PDL governance regime.

6.1.3 Policy and Security Requirements

In line with 2 layer approach described above policy and security requirements specifications:

- Layer 1: policy and security requirements on individual ledger providers in line with the requirements of eIDAS 2 [i.1].
- Layer 2: policy and security requirements on for governance of a PDL community operating under the same governance regime.

6.1.4 Trust Management

The EU Trusted List [i.10] provides the basis for identifying whether members of a PDL meet the basic requirements for qualified electronic ledgers under eIDAS 2.

The governance regime for specific eIDAS 2 compliant PDL establishes the list of qualified electronic ledgers that meet the requirement of that regime.

6.2 PDL in Support of other eIDAS 2 Trust Services

6.2.1 PDL in support of Time Stamping

A TSP issuing time-stamps may register the time-stamp (as specified in ETSI EN 319 422 [i.3]) in a distributed ledger. This provides added assurance of:

- The existence of a timestamp within the sequential chronological ordering of events.
- The persistence of the time-stamps over extended periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.2.2 PDL in support of Signature Validation

A TSP providing signature validation may register the validation report (as specified in ETSI TS 119 102-2 [i.4]) in a distributed ledger. This provides added assurance of:

- The validation of the signature within the sequential chronological ordering of events.
- The persistence of the validation reports over extended periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.2.3 PDL in support of Certificate Issuance and Revocation

A TSP issuing certificates and managing their revocation status may register the certificate issuance and revocation report (as specified in ETSI EN 319 411-1 [i.5]) in a distributed ledger. This provides added assurance of:

- The status of a certificate within the sequential chronological ordering of events.
- The persistence of the certificate issuance and revocation reports over extended assurance periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.2.4 PDL in support of Electronic Attestation of Attributes Services

A TSP supporting electronic attestation of attributes may register the issuance and change of status (as to be specified under work item ETSI DTS/ESI-0019472-1 [i.6]) in a distributed ledger. This provides added assurance of:

- Reports on the issuance and status change of a of an electronic attestation of attributes within the sequential chronological ordering of events.
- The persistence of reports on issuance and status change of an electronic attestation of attributes over extended periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.2.5 PDL in support of Electronic Archive Services

A TSP supporting electronic archive services may register the existence of an archived data in a distributed ledger. This provides added assurance of:

- The existence of an archived data within the sequential chronological ordering of events.
- The persistence of archived data over extended periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.2.6 PDL in support of Electronic Registered Delivery Services

A TSP supporting electronic registered e-delivery service, including its derivative register electronic mail, may register the proofs (as specified in ETSI EN 319 522 [i.7], parts 1 to 4) in a distributed ledger. This provides added assurance of:

- Existence of registered electronic delivery proofs within the sequential chronological ordering of events.
- The persistence of proofs over extended periods.

Furthermore the redundancy of a PDL adds to assurance of the services provided by this service.

6.3 Application to 3rd (non-EU) countries

eIDAS contemplates an internationalization area with which third (non-EU) countries are able to be subject under eiDAS 2 regulation [i.1] in article14 "*it establishes that "trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country or from an international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 Treaty on the Functioning of the European Union*".

This internationalization aspects reflects the possibility once a Mutual Recognition Agreement is countersigned in this purpose. Hence a List Of Trusted Lists (LOTL) whereby 3rd country trusted list may result of mutual recognition.

NOTE: This is the subject of a Pilot for the International Compatibility of Trust Services [i.15].

There are four pillars for the assessment check-list which are described in ETSI TR 103 684 [i.14] for 3rd countries to perform a self-assessment on how compliance achieve those minimal legal requirements:

- legal context;
- supervision and auditing;
- best practice;
- trust representation.

7 Consideration of benefits and challenges

7.1 Benefits

The benefits of a PDL based on eIDAS 2 are:

a) The property of PDL in assuring persistence of proofs, once entered into the electronic ledger, over extended periods, without depending the limited lifetime of public key algorithms, will significantly enhance the evidence available in support of any application.

b) The property of PDL in providing chronological sequencing of records, with immutability and integrity of the records will significantly enhance the evidence available in support of any application.

c) The distributed nature of PDL avoids dependence on the security and functionality of a trust service.

d) eIDAS 2 adds legal presumption to the services of PDL.

e) The identity assurance, linked to a natural or legal person, provided by eIDAS 2 adds to the legal accountability of a PDL.

f) The regulatory oversight of eIDAS 2 and the cybersecurity regulation NIS2 [i.10] provides a high level of assurance of the functionally correct and security operation of a PDL.

g) The property of PDL combined with another eIDAS trust service provides a new level of security for the other trust services.

h) The provision of a single PDL based ledger supporting information from multiple trust services service can further significantly enhance the security of those trust service. In particular, when applied to trust services supporting digital signatures (time stamping, signature validation, certificate issuance and certificate revocation), the ability of PDL to ensure the chronological sequencing of events, persisting over a long time, in a single ledger, can significantly enhance the security of digital signatures.

EXAMPLE: Events relating to the revocation of certificates can be easily related signature validation at a particular point in time.

7.2 Challenges and Risks

The main challenges and risks of a PDL based on eIDAS 2 are:

Added complexity and costs:

a) Privacy of information held in a PDL where information is shared between multiple ledger providers.

NOTE 1: Use of hashing and encryption techniques and "off chain" storage of sensitive information may be used to reduce this risk.

b) The extra overhead on PDL necessary to meeting regulatory requirements of eIDAS 2 would significantly add extra overhead costs to the operation of a PDL.

c) The accuracy of chronologically sequencing events is limited in a PDL to the time taken to achieve consensus across the nodes that form the PDL. If two events occur within the consensus time it cannot be assured that the events are correctly sequenced.

NOTE 2: This could be reduced by the originator of a resource adding time from a trusted time source to a record. Generally, it is expected that due to the potential involvement of human intervention and the delays that exist across open networks such as the Internet this level of uncertainty should not be significant, provided this uncertainty is taken into account when using the proofs available through the ledger.

7.3 General Conclusions

There are significant benefits in combining the properties of PDL with eIDAS 2. Whilst there may be additional costs, and issues of privacy to address, this is likely to be of significant benefit to the user community. This is particularly so in the case of using a single PDL based ledger in for multiple trust services supporting digital signatures.

Annex A: Bibliography

- For a list information on ETSI activities supporting PDL see:
  - https://www.etsi.org/technologies/permissioned-distributed-ledgers.
- For a list of ETSI specifications and reports supporting current eIDAS regulation see:
  - https://portal.etsi.org/TB-SiteMap/esi/esi-activities.
- For a list of ETSI ongoing work items supporting eIDAS 2, see:
  - https://portal.etsi.org//tb.aspx?tbid=607&SubTB=607#/5068-home.

History

Document history		
V1.1.1	July 2024	Publication