***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.

ETSI GR PDL 017 V0.0.5 (2023-09)

**Group REPORT**

Permissioned Distributed Ledger (PDL);

Application of PDL to Regulation 910/2014 (eIDAS) Qualified 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:
<http://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](http://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***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.

All rights reserved.

Reference

DGR/PDL-0017

Keywords

Data, PDL, Time-Stamping, Security, Trust Service

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

Executive summary 4

Introduction 4

1 Scope 5

2 References 5

2.1 Normative references 5

2.2 Informative references 5

3 Definition of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 5

4 Features of PDL 6

4.1 Common Context 6

4.2 Properties 6

5 Features of eIDAS Qualified Trust Services 6

5.1 Policy and Security Best Practices 6

5.2 Audit and Supervision 6

5.3 Trusted List 6

6 PDL and eIDAS Trust Services 6

6.1 Introduction 6

6.2 PDL as stand alone Trust Service 6

6.3 PDL in support of Time Stamping 6

6.4 PDL in support of Signature Validation 6

6.3 PDL in support of Certificate Validation 7

6.4 PDL in support of Identity Attribute Validation 7

6.5 PDL in support of Preservation Services 7

6.6 PDL in in support of Electronic Registered Delivery Services 7

7 General Conclusions 7

7.1 Benefits 7

7.2 Challenges and Risks 7

8 Benefits and Recommendations 7

8.1 Introduction 7

9. Bibliography 7

Annex A: Title of annex 8

Annex B: Title of annex 9

B.1 First clause of the annex 9

B.1.1 First subdivided clause of the annex 9

Annex: Bibliography 10

Annex : Change History 11

History 12

# 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](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 <long ISGname> (<short ISGname>).

# 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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (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

# Introduction

# 1 Scope

The present document describes the features of a PDL to be applicable as a qualified electronic ledger and in support for eIDAS trust services. The document analyses the properties that a PDL can have to be an enabler for eIDAS, for authentication and identification, and also for using eIDAS 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] <Standard Organization acronym> <document number><version number/date of publication>: "<Title>".

[i.2] etc.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

## Trust Service tbc3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

## 3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

eIDAS tbc

# 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 EBSI (European Blockchain Services Infrastructure).

## 4.2 Properties

* Integrity of record
* Immutability
* Sequence
* Some have identity of originator
* Time is not inherent in PDL
* Permissioning within governance domain For example:
	+ Horizonal, or
	+ Vertical, or
	+ Transversal, or
	+ Combination
* consensus between members of governance domain
* automated synchronisation of ledgers over time
* verifiable,
* auditable
* accountable (non-reudiation)
* persistent over time

## 4.3 Governance

* Principles of governance in PDL based on ISO/TS 23635:2022

|  |  |
| --- | --- |
| ISO /TS 23635:2022 | PDL |
| Define identifiers of entities involved | Through permisioning the identities of the entities involved are resolvableOff layer or psedonomimous |
| Enable decentralized decision-making | Decentralised within scope of governance domain as distributed across several nodes. Collective decisions recorded explicitly on ledger. |
| Ensure explicit accountability |  |
| Support transparency and openness |  |
| Align incentive mechanisms with system objectives |  |
| Provide performance and scalability |  |
| Make risk-based decisions and address compliance obligations |  |
| Ensure security and privacy |  |
| Consider interoperability requirements |  |

## Identification and Authentication Management

* Include concept whether a TAO Trusted Accreditation Organisation (cf: regulatory “competent authority”) authorises for particular “subject matter” / “activity. May need to include “Passporting” in multi-jurisdiction scenario.
	+ Authorises issuers of credentials
	+ Verifiers of credentials

Identification of Nodes

* Managed through EBSI under governance of EBP
* Muti-juresdiction

# 5 Features of eIDAS Qualified Trust Services

## 5.1 eIDAS trust services

Regulation 910/2014 (commonly referred to as eIDAS) 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 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.

The concept of trust service was initially applied to services issuing public key certificates in support digital signatures, legally referred to in eIDAS 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 recognised internationally. Currently, 9 trust services types are recognised in the current eIDAS regulation, all of which have been implemented by a number of trust service providers. Trust services are defined are defined in eIDAS regulations as services for:

1. 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
2. the creation, verification and validation of certificates for website authentication; or
3. the preservation of electronic signatures, seals or certificates related to those services.

This is being extended in proposed revisions to eIDAS regulation for recognised trust services also to include:

1. the electronic archiving of electronic documents;
2. the management of remote electronic signature and seal creation devices;
3. the recording of electronic data into an electronic ledger

## 5.2 Qualified Trust Service Providers

eIDAS give specific recognition for the provision of trust services which meet particular requirements as identified in the eIDAS regulation. 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:

1. requirements to take appropriate technical and organisational measures (applicable to both qualified and non-qualified trust service providers),
2. requirements for notification of security breaches (applicable to both qualified and non-qualified trust service providers),
3. requirements for the cybersecurity of essential services under NIS 2 [ref]
4. requirements for personal data protection such as in GDPR [ref]
5. requirements for the provision of Qualified trust services
6. requirements for the particular type of Qualified trust service.

## 5.3 Requirements of EU Qualified Electronic Ledgers

[For Qualified Electronic Ledgers the specific technical requirements have yet to be established. May include requirements in EU Council version]

## 5.4 Audit & Supervision

A national regulatory body is assigned in to oversee the operations of qualified and non-qualified trust service providers established in its nation. A QTSP is required to provide an audit report to the supervisory body every 2 years to confirm that it meets the requirements of eIDAS. This audit report has to be produced by an accredited “conformity assessment body” which is recognised under EU Regulation (EC) No 765/2008. ETSI EN 319 403-1 defines specific “conformity assessment” requirements for QTSPs which is generally accepted by EU national supervisory bodies as the basis for eIDAS conformant audits.

ETSI publish policy and security standards for trust service providers, including QTSPs, which are commonly used as the basis for the QTSP audit checks.

## 5.5 EU Trusted List

National supervisory bodies publish a list of QTSPs which are recognised as meeting the requirements for given types of trust service called a Trusted List. The EU publish a List of Trust Lists (LOTL) from each EU nation. Parties relying on certificates and other information provided by QTSPs use the LOTL, and national Trusted Lists, to verify that this information can be considered trusted under the eIDAS regulation.

## 5.6 Trust Service Components

A trust service provider may use several independent components for the provision of a trust service. Such trust service components may be provided by the QTSP as an integral part of its operations, or sub-contracted to external parties. For example, when issuing a certificate, a QTSP may subcontract the checking of the identity of the subject to external parties. Such external trust service component can be independently audited. The QTSP however remains responsible to the overall provision of its services, and provides an overall audit report to its supervisory body. A QTSP’s audit report can build on the audit report for an external trust service component,

An electronic ledger can be a trust service component of a QTSP providing another type of trust service. For example, a ledger may be used in support of Qualified signature validation service maintaining a record of signatures with validation information based on checks made by the QTSP at a given time.

## 5.7 eIDAS Qualification and permission

eIDAS Qualification can apply to a provider of an electronic ledger based on the results of the QTSP audit. This can be either as an stand alone QTSP providing an electronic ledger trust service, or as a trust service component supporting a QTSP providing another type of trust service.

A community of Qualified electronic ledger providers can cooperate together, using a consensus protocol, to support a PDL for specific type of Qualified trust service. The EU Trusted List will identify the provider and the trust services it supports. The EU Trusted List can be used as the basis of “Permissioning” the electronic ledger providers as being part of the community.

This is illustrated in the following diagrams

1. For a stand alone electronic ledger:



1. For electronic ledger (e-ledger) as a trust service component



## 5.8 Mutual Recognition with Third Countries outside the EU

[Pilot for the International Compatibility of Trust Services (europa.eu)](https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Pilot%2Bfor%2Bthe%2BInternational%2BCompatibility%2Bof%2BTrust%2BServices)

https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Pilot+for+the+International+Compatibility+of+Trust+Services

# 6 PDL and eIDAS Trust Services

## 6.1 Introduction

Combining PDL community governance and eIDAS audit & supervision

(use concepts in PDL 15 & PDL 12 as relevant)

## 6.2 PDL as stand alone Trust Service

### 6.2.1 Requirements for Qualified Electronic Ledgers vsFeatures of PDL

*[Block chain does not inherently include time of recording (as in Commission original text). However, sequencing is definitive (as in later Council version).*

*It is not mandated in all block chains that the ledger establish the origin of data records in the ledger (as in council version).*

*Need to review when final draft of regulation available.]*

### 6.2.2 Governance & Audit

[Being in Trusted List is necessary for eIDAS but is not sufficient for entering PDL. May need to include additional requirements for governance as in clause 4.]

### 6.2.3 Policy and Security Requirements

Include PDL specific

* Needs to include requirements on consensus mechanism, statement of consensus mechanisms supported by QTSP

Include EN 319 401

Other requirements

## 6.3 PDL in support of Time Stamping

## 6.4 PDL in support of Signature Validation

## 6.3 PDL in support of Certificate Validation

## 6.4 PDL in support of Identity Attribute Validation

## 6.5 PDL in support of Preservation Services

Applied to electronic signatures, seals or certificates

## 6.6 PDL in support of Electronic Registered Delivery Services

## 6.x Application to 3rd (non-EU) countries

# 7 General Conclusions

## 7.1 Benefits

- Application of eIDAS trust controls to permissioning

- Immutable history of timed events (e.g. validity update of certificates, signatures, attributes)

- Distributed trust through consensus mechanisms

## 7.2 Challenges and Risks

# 8 Benefits and Recommendations

## 8.1 Introduction

# 9. Bibliography

Annex A:
Title of annex

Annex B:
Title of annex

# B.1 First clause of the annex

## B.1.1 First subdivided clause of the annex

Annex:
Bibliography

Annex :
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| <Month year> | <#> | <Changes made are listed in this cell> |
|  |  |  |
|  |  |  |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Latest changes made on 2022-03-14*