ETSI GR PDL 002 V1.1.1 (2020-11)

Permissioned Distributed Ledger (PDL); Applicability and compliance to data processing requirements

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger 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-002_CDPR

Keywords

conformity, regulation, trust

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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.

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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

Member States in Europe are responsible for ensuring the health and safety on their territory of workers, consumers, animals and goods in relation to the risks arising out of the use of connected machinery.

The present document captures the impact that the use of connected machinery has upon health and safety compliance. This will specify security requirements for electronic control units, telematics gateway, computational portion of smart sensors, computational portion of smart actuators, and computational portion of other devices. The introduction of connectivity will specify security for on-machine communications between electronic control units and sensors in order to allow the remote reading of a machine's state: both static properties (e.g. manufacturer, equipment identifier, etc.) fixed for the lifespan of the machine, and dynamic properties (e.g. operating temperature, last service date, firmware version, etc.) of varying lifespans. Secure programming will request that a fault in the hardware or the software of the control system does not lead to hazardous situations.

The example given in the present document took a tractor, but an autonomous robot in the field cannot be strictly a tractor but rather an equipment capable to be any self-propelled autonomous machine. This could be any kind of machinery falling under the Regulation No 167/2013 [i.5] and the Directive 2006/42/EC [i.1]. The use case to illustrate the compliance case for the Mobile Machinery is any self-propelled machine (see note) covered by Machinery Directive 2006/42/EC [i.1] Article 1 Clause 1a and defined by Machinery Directive 2006/42/EC [i.1] Article 2 (a) Indent 1 to 4.

NOTE: 'Self-propelled machine' means a mobile machine whose prime purpose is intended to perform work but not to transport passengers or goods having at least two axles and wheels, or endless tracks, or a combination of wheels and endless tracks, which, according to its design and the permanently mounted devices, provides its own means of tractive movement.

The owner of a machine will be properly identified and verifiable, and data shared to and from the machine would require verification to show it has not been corrupted or hacked in transit. Smart sensors and ECU will have cryptographically strong evidence that the source of a message is a manufacturer approved node. Such verifications may need to persist over time (for example, for an audit later), and to be shared across national boundaries in the case of machine roaming. Hence, the present document also describes the use of PDL technologies to assert the health and safety compliance of connected machines, and how to verify these assertions to meet applicable data-processing requirements.

The process described in the present document has the purpose to manage the eco-system around a connected machinery. This is one proposal for a revised content of the Directive 2006/42/EC [i.1], while the directive is under assessment to evaluate if it fits for purposes. These technologies are available today, and manufacturers need to make sure of the safety assessment proposed will provide new solutions complying to Essential Health Safety Requirements. Performance levels for safety and security could be described into harmonised standards or Annexes of the Machinery Directive. Finally, the General Product Safety Directive (GPSD) (2001/95/EC) [i.7] will complement sector specific legislation

The example of a "single registry" is the way in which such requirements could be implemented for all interoperable IoT devices being connected to any networked product on the market including tractors, self-propelled machinery and earth moving equipment. A networked machinery can use the "single registry" based on a Permissioned Distributed Ledger as a technology.

Ensuring the health and safety on their territory of workers, consumers, animals and goods in relation to the risks arising out of the use of connected machinery deals with the horizontal legislation where several DGs are involved like DG GROWTH and DG CNECT. In order to address all technology relevant sectors, the present document cross-cuts several pieces of legislation, the GPSD [i.7], the LVD [i.9], the RED [i.10] and the EMC [i.11]. The pretention is not to align all these legislations, but rather to establish some "bridges" between them.

1 Scope

The present document will analyse the essential data processing prerequisites in terms of trust, security and effective conformity assessment, and make recommendations on how PDL can be used by organizations, operations, deployment, hardware, and software to be trusted.

The present document will reference use-cases work by other standards-developing organizations and material in the public domain. The essential prerequisites for the PDL technology to ensure compliance to existing regulatory aspects will also be analysed.

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] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC.

[i.2] IEC 62351-9: "Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment".

[i.3] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).

NOTE: Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf.

[i.4] Regulation (EU) No 2016/679-GDPR 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.5] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles.

[i.6] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive).

[i.7] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (General Product Safety Directive).

[i.8] Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).

[i.9] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (Low Voltage Directive).

[i.10] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive).

[i.11] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive).

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

AEF	Agricultural-industry Electronics Foundation
AI	Artificial Intelligence
AN	Access Network
CE	Certified Equipment
CNECT	Connect
DG	Directorate General
EC	European Commission
ECDH	Elliptic Curve Diffie Hellman
ECU	Electronic Control Unit
EMC	Electro Magnetic Compatibility
GPSD	General Product Safety Directive
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IoT	Internet of Things
LAN	Local Area Network
LVD	Low Voltage Directive
OBD	On Board Diagnostic
OEM	Original Equipment Manufacturer
OMA	Object Management Architecture
PC	Personal Computer
PKI	Public Key Infrastructure
RED	Radio Equipment Directive
SCEP	Service Creation Environment Point
SLA	Service Level Agreement
TLS	Transport Layer Security
VDMA	Verband Deutscher Maschinen- und Anlagenbau
WAN	Wide Area Network

4 General Overview

4.1 General principles

The present document provides the data processing prerequisites relevant to trust, security, and safety set out in light of the general principles listed as below.

By a way of certification and defined standard, manufacturers can make interoperable machineries, IoT devices between each other.

The data processing will ensure that a risk assessment is carried out in order to determine the trust, security, and safety prerequisites, which apply to the device equipped with sensors. The device will then be designed and calibrated taking into account the results of the risk assessment.

By the iterative process of risk assessment and risk reduction referred to above, the device supplier would need to consider:

1) determine the limits of the trusted environment, which include the intended use and any reasonably foreseeable misuse thereof;

2) identify the risks that can be generated going through all the layers constituting the distributed ledger and the associated unreliable situations;

3) estimate the lack of trust, considering the value that stakeholders can have in the data, that the end-user will use through organizations, operations, hardware, and software;

4) evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of the actuation of the device based on the data generated or received;

5) eliminate the risk of corruption or reduce the risks associated with a distributed database by application of protective measures;

6) perform compliance testing, secure message categories, encrypted communication prerequisite principles, and authentic conformance testing.

4.2 Assessments

The communication layer in PDL is supposed to give the unconditional trust in the safety, security. However, there is a need to assess the safety and security to access sensor data in a way that is not dependent on a single third party. Access to the communication is based on Internet Service Providers who act as a central hub for connected machineries. If there is no communication possible, then the essential health and safety prerequisites have still to be insured.

In the case of lack of communication to the main ledger, a trusted communication between the two peers can be established in such a way that it will be later possible to synchronize the full chain of events in the main ledger.

The local copy of the distributed ledger allows peer to peer connection allowing this decentralized communication in the blockchain ecosystem as a backup in case of unconnected areas where the machinery is used. The PDL could be used not only as a service but also as a decentralization of the services covering at the same time privacy, safety, and security without central hub for the sensor management.

If the product meets the safety prerequisites and for example for the machinery directive, that affects the liability of the manufacturers under the Product Liability Directive (85/374/EEC) [i.6], the General Product Safety Directive (2001/95/EC) [i.7] and the Directive for the minimum safety and health requirements for the use of work equipment by workers at work (2009/104/EC) [i.8], then the technical prerequisites described into the present document are important to consider for the liability of the manufacturers. Indeed, improvements in the safety and health of workers at work are important and the proper use of the equipment will be supported by the presumption of conformity, provided by the unique registry. Additionally, transparent safety instructions should be provided to end users.

The lack of safety will be due to the non-assessment of connected device to the connected machinery where essential requirements are not met. The performances that this IoT device needs to fulfil will be described into the annex of the standards listed for the safety of the machinery. ETSI standards would need however to be referenced under the Machinery Regulation. An agreement between CEN (ISO TC23 under Vienna agreement) and ETSI will be required. This has been the case recently for the subject linked to the wind turbines. This machinery involved CEN, CENELEC and ETSI.

The Original Equipment Manufacturer runs the PDL in compliance with the harmonised standards applicable for the certification of the IoT device or the connected Machinery.

4.3 Example of a potential process to market a connected machinery on the EU market

Besides the existing European legislations as RED [i.10], LVD [i.9], EMC [i.11], etc. here are the steps toward placing a connected machinery on the EU Market or putting a connected machinery into service in the EU would expect implementing the following assessments (2006/42/EC [i.1]):

- **STEP 1:** Identify relevant Essential Health and Safety Requirements for the connected machinery.
- **STEP 2:** Apply technical standards to the connected machinery.
- **STEP 3:** Assemble the technical assessment/certification file.
- **STEP 4:** Certify conformance to the certification scheme.
- **STEP 5:** Create the EC Declaration of Conformity.
- **STEP 6:** Place the CE mark on the machinery.

Compliance to the standards means that the design meets or exceeds the requirements of all relevant and applicable Essential Health and Safety Requirements.

4.4 Layer model to assess security, safety and privacy

4.4.1 Layer model for security, safety and privacy

The following model for the layers would allow the implementation of security, safety and privacy see Table 4.4.1-1.

Table 4.4.1-1: Layer model for security, safety and privacy

COMMUNICATIONLAYER	**Application Layer**
	Machinery parameters
	Management Layer
	Data management
	PDL Layer
	Consensus management
	Network Layer
	LAN, WAN, Routers
	IoT Layer
	Security, safety at the sensor level
	Physical Object
	Analog data

This will provide immutably and securely data, which allows auditability, integrity, and transparency of the data and parameters associated with the machinery.

4.4.2 Use case applied to Mobility

Machinery presenting hazards due to its connectivity should meet all the essential health and safety prerequisites.

4.4.3 Considerations on the model posed by the machinery world

This clause is inspired from Ethical Guidelines for the Use of Automated Machinery in Agriculture/VDMA.

The purpose of these considerations is indicative and falls within the anticipated scope of the Machinery Directive 2006/42/EC [i.1], which is under revision and is expected to be updated in the future and become a regulation. It is without prejudice to the applicable laws by the EU, the Member States, and other countries.

a) 'Connected machinery presenting hazards due to its mobility' means:

- machinery which requires either remote control for the mobility while working, or continuous or semi-continuous remote-control movement between a succession of fixed working locations; or
- machinery which is operated without being moved, but which may be equipped with sensors as to enable it to move more easily from one place to another.

b) 'Driverless' means remote operator responsible for the movement of a machine. The remote operator may be connected to the machinery through the six layers supporting the transfer of the order to the connected machinery by remote control.

c) Data:

i) The generation, storage, processing and evaluation of data are integral components of the work activity of the machinery and are essential for sustainable management. The data are characteristic of the machinery management and have a direct influence on the safety of the work activity (operator and environmental safety). Therefore, they require special measures to protect against unauthorized access.

ii) In the case of data that do not allow conclusions to be drawn concerning persons or individual machinery operations, transparency with respect to data collection and use will be ensured (e.g. via statements in the machinery operating instructions concerning which data are used for what purpose).

iii) Personal and operational data will be subject to legal provisions (e.g. the EU General Data Protection Regulation [i.4]).

d) Liability within the scope of the revision of the Machinery Directive:

i) Those who are particularly involved in the use of automated machinery are the manufacturer, the owner/employer, the operator and the provider of telecommunications services (subject to SLA); all will fulfil their respective roles and responsibilities.

ii) In order for machinery owners and operators to be able to fulfil their responsibilities, appropriate information will be available to them (e.g. information concerning the intended use & limits of the machinery, training/instruction of operators, etc.).

iii) Legal provisions concerning the manufacturer's product liability (e.g. relating to product defects, information defects, etc.) will remain unaffected.

e) Operations:

1) In order for the employer/operator to be able to fulfil his responsibility, the manufacturer will clearly define and communicate the application possibilities and limits for partially and fully automated machine use (e.g. sales literature, operator's manual).

2) Operators - on the machinery or at a control station - will have the possibility of "overruling", so as to be able to fulfil their responsibility for the use of the machinery at all times.

3) It will be clearly apparent at all times whether the system or the operator has direct control over the use of the machinery; the operating condition and thus the responsibility for the machine operation will be traceable; the (re)transfer of control from the system to the operator will not occur abruptly; i.e. the operator will have the opportunity to react.

4) Restriction of the automated use of machinery to particular use cases can be an option for avoiding situations that are not completely controllable (e.g. use in the immediate vicinity of residential areas).