Draft ETSI GR PDL 002 V0.0.6 (2020-03)

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

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 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.

1 Scope

The present document will analyse the essential data processing requirements 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 report will reference use-cases work by other standards-developing organizations and material in the public domain. The essential requirements 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.

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:

AN	Access Network
AR	Aknowledment Receipt
CE	Certified Equipment
ECDH	Elliptic Curve Diffie Hellman
ECU	Electronic Control Unit
GP	Group Product
IEC	International Electromechanical Committee
IOT	Internet Of Things
LAN	Local Area Network
MSP	Membership Service provider
OBD	On Board Diagnostic
OEM	Original Equipment Manufacturer
OMA	Object Management Architecture
PC	Personal Computer
PKI	Public Key Infrastructure
SC	Smart Contract
SCEP	Service Creation Environment Point
TLS	Transport Layer Security
WAN	Wide Area Network

4 User defined clause(s) from here onwards

4.1 General principles

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

The data processing will ensure that a risk assessment is carried out in order to determine the trust, security, and safety requirements, 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 is recommended to:

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 you 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 requirement 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 requirements 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.

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

Steps toward placing a connected machinery on the EU Market or putting a connected machinery into service in the EU would require 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 pricacy

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.

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 has to meet all the essential health and safety requirements.

4.4.3 Considerations on the model posed by the machinery world

(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), which is under revision and is expected to be updated in the future and become a revision. 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).

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).

5) System safety and protection against manipulation will be designed so that the safety of machinery utilization is ensured under normal conditions; targeted attacks on systems cannot always be avoided due to complexity, open interfaces (data transmission from/to machinery to/from PC/mobile equipment/cloud) and the large number of parties involved (manufacturers of hardware and software, owners/operators, telecommunications service providers); but targeted attacks will not lead to a destruction of confidence in technology.

6) The communication between system and operator will be adapted to the capabilities of the person who is authorized to operate the machinery.

7) Self-learning systems are permissible if they increase the sustainability of processes, and if the operator retains the power to make decisions (overrule).

8) In emergency situations the machinery will automatically enter a safe state (e.g. shutdown of the power/energy supply, retransfer of control to the operator, etc.).

9) Fully automated machines will be able to detect and respond to 'obstacles' (persons, animals, objects) in the driving and working area of the machine. The performance of detection systems will be equivalent to that of an average operator under normal operating conditions.

4.4.4 Example of safety component

A braking, a steering system, or the detection of bystanders are critical for the proper operation of a mobile machinery in safe conditions. The example given has the purpose to offer presumption of conformity based on the real status of the safety component, which has been previously qualified against safety assessments.

The purpose of braking, steering, bystander detection performances is to establish defined levels of security for use in the development of other specific safety standards for connected functions of machinery. Due to the potential number of different safety functions of machinery, it is necessary to establish at a high level, the primary management of the safety functions, where the presumption of conformity. It resides on the status of the component and/or perception systems for the specific safety functions. The mitigation of risk of injury to operator and bystander is the primary focus of safety standards. Defining the presumption of conformity in the environment of a Permissioned Distributed Ledger will guide for the development of specific function safety standards.

The status of the machinery is calculated based on the accumulated data received from the IoT device installed in the mobile machinery. This can be described with the safety component and the status associated with:

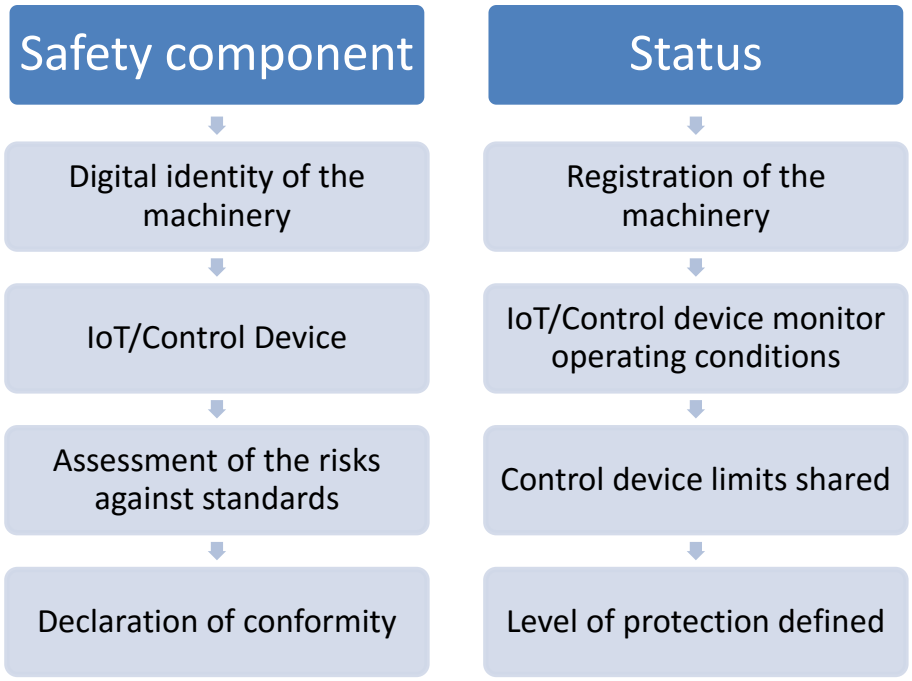

Figure 4.4.4-1: Safety component and status associated with

The integration of the PDL into the overall eco-system of the machinery helps to address the challenges raised by the regulatory environment and the manufacturer infrastructure. This integration provides a safe environment, reliable, and secure data exchange between multiple enterprise applications.

This approach should handle the challenges raised by:

1) Controlled access to (machinery) data.

2) Design of interfaces (for communication/data access).

3) Provide input for additional or revision of current legislations and third-party certification.

4) Revision/modification of basic legal requirements (product safety, product liability, etc.).

The various clouds provided by the Original Equipment Manufacturers or other platforms can provide such infrastructures where the PDL will be the catalyst for the link with the protocols, infrastructure, applications, status.

IoT is about connecting devices and applications. One of its key benefits is automation, but also about new compliance to conformity achieved through enabling applications, services and compliance related data.

The technical specifications to be accepted by all the OEMs as standards would allow off-the shelf connections with standardized APIs. This would include integrated safety and security requirements, which can be then integrated into any blockchain networks.

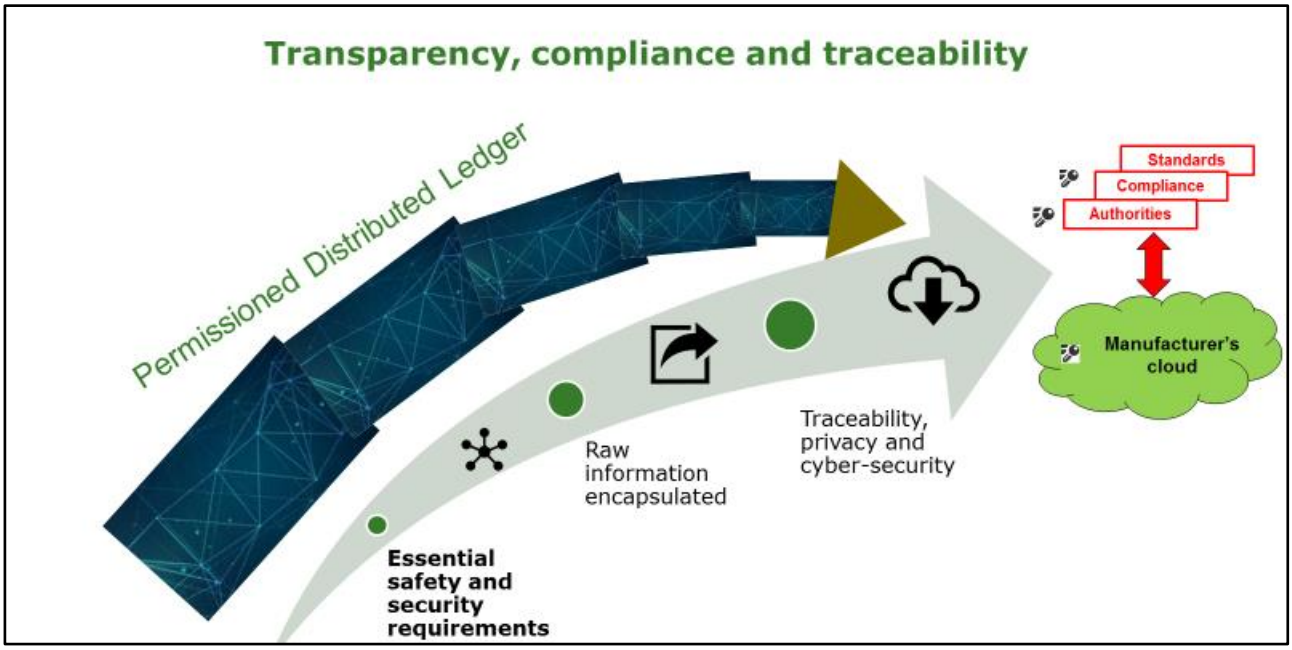

Figure 4.4.4-2: Transparency, compliance and traceability

The ledger to ledger connectivity will be provided by the standardization process in the different standard bodies in a secured and high performant manner.

This principle keeps the presumption of conformity based on the status provided back to the OEM platform where you preserve compliance to privacy, etc. and enables at the same time integration partner public of private. There is convergence of the constraints, which can be solved through the the PDL. However, there is a need to fill the gap regarding the transfer of data between the sensor and the Electronic Control Unit, which is the first element of the IoT backbone for the transfer of data to this IoT infrastructure.

5 Interaction scenario

A simplified interaction scenario for the machinery domain is presented in figure 5-1.

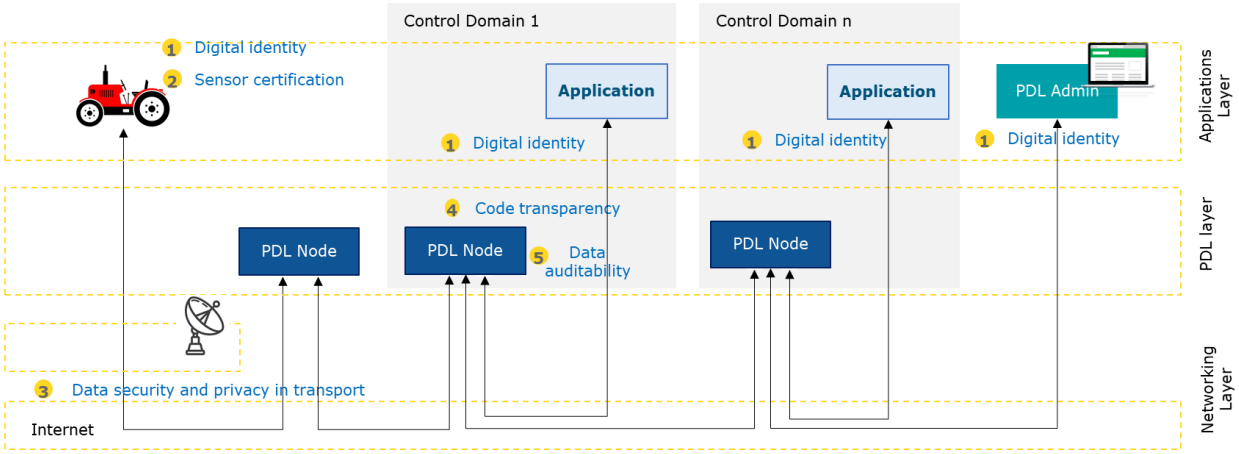

Figure 5-1: machinery based on multiple domains

The schema only shows a single PDL, while multiple connected PDLs may be in place in more complex settings.

The networking layer falls outside the scope of the present document. It covers 3. data privacy and security in transport, using well known technologies and standards.

The PDL layer forms the core of the architecture, granting features like:

- 5. Data integrity and auditability.
- 4. Code transparency (when distributed code is required, in the form of smart contracts/chain code).

NOTE: Both 4. and 5. are native features of PDL.

The applications layer follows traditional security practices. It is however affected in that:

- There is need to establish with certainty the identity of the application acting on the data.
- Possibly, application code may be certified (code review) and signed (code signing).

The devices are affected in that:

- There is need to certify the digital identity of the machinery and/or of the individual micro-sensors.
- There is need for sensor factory tuning and certification.

Propose tbe engine example as a use case to demonstrate the use of the PDL

6 Identity

6.1 Identity of sensors/devices

While this is largely independent from the communication infrastructure (networking/PDL), the presence of a PDL is only justified when there is a proper mean for identifying the authors of the transactions. Having accurate and persistent audit logs for transactions created by uncertain actors would provide little value.

Identity for devices and micro-devices is largely in the scope of IOT standardization initiatives; it is however essential to include them in an overall model of applicability to remote machinery. Identity is not associated to the “role” that a device is playing in a IOT context, but to the specific device, since it is the single device (and not the role) which may be subject to certifications or liabile for possible faults.

Traditional Identity systems leverage on PKI (Private Key Infrastructure) models. They have been widely used in the last 30 years for the secure identification of people and devices (web server using TLS certificates).

Each vertical involved in the digitization of its sector (energy, home, health care, mechanical industry etc.) has already chosen the type of keys and cryptography that will be utilized. The cryptography algorithms and key materials chosen will be mandated by an organization’s own local security policies and by the need to be compliant with other international standards.

Current ongoing effort for the identification of devices follow some main lines:

- Extension of the PKI paradigm to a wider IoT setting (e.g. in the energy domain, IEC 62351-9 [i.2]). It includes the simplification of the enrolment process (e.g. through Simple Certificate Enrollment Protocol - SCEP) and a more complex key lifecycle process (see [i.3]).
- New lightweight key management models (OMA, https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/)
- Distributed PKI (e.g. Iota? https://www.iota.org/)

A major issue to be considered for device identity is the possible impact of quantum attacks. Considering that the replacement of keys on the filed may be problematic or even unfeasible, it may be necessary to endow them with crypto material which is resistant for a long-time window (10 - 15 years or more), by when it is expected that quantum attacks will be a reality. Quantum-safe cryptographic schema is recommended based on a risk assessment.

6.2 Identity of applications

Machine identities are less controversial, since traditional PKI schemas fits appropriately.

The machine will include:

- the name and address of the manufacturer and, where appropriate, his authorized representative;
- a written declaration that the application has not been submitted to another notified body;
- the technical file where it demonstrates the compliance to the PDL requirements defined:
  - Participants to the PDL are already known and trusted.
  - Permissioned ledgers don't need to use a distributed consensus mechanism.
  - An agreement protocol is used to maintain the consensus of the trust about the state of the records on the blockchain.
  - All verifiers are already preselected by a central authority and there is no need for a mining mechanism.
  - Tokens are not required.

Moreover, the applicant will place at the disposal of the notified body a simple state machine replication and an agreement protocol approved by the notified body.

6.3 Identity of operators/administrators

Human identities are out of the scope of the document, traditional authentication schemes fit appropriately.

7 Privacy - Access – Data Value – Compliance associated with the PDL

7.1 Consent

The OEM will enable third parties to access the unique registry reflecting the configuration of the connected machine at the level of each node, but only with machine owner consent. The OEM through the transfer of encrypted data (both in transit and in storage), will ensure the machine owner has the encryption key (the machine owner can then provide the key to authorized third parties accessing the data from any node).

In addition, third parties will remain able to access the unique registry configuration of the machine stored in the replicated node with the consent of the machine owner through APIs. The administrator of the PDL won’t be able to make non-registered configuration data accessible through replication for third parties to access.

To be completed based on the use case for the liability case or the traceability for bio food.

7.2 Fee or subscription

Access to the PDL is conditioned in some way – i.e., on customer consent and / or certification/homologation of the hardware or software, but no fee or subscription will be required to join.

7.3 Data value

The shared distributed ledger is used to store the configuration of the machine where the setting parameters are immutable, secured, and consensus driven. There is no value associated with a specific asset except the status of the machine, which is

7.4 Compliance

A PDL can provide a single shared view through a unique registry of all hardware and software implemented on the connected machine that are cryptographically secure, authentic, and auditable. This will reduce the costs and complexity associated with the current employed regulatory legislative framework. This unique registry reflecting the status of the connected machine will provide compliance to the legacy from the New Legislative Framework relying on such text like the Low Voltage Directive, the Radio Equipment Directive, The Electro Magnetic Compatibility directive and the Machinery Directive for example in Europe.

8 Certifications

8.1 Introduction to Certifications

Compliance to the specific requirements of each sector will be difficult unless there are general principles with harmonised standards or certifications provided. A layer between different clouds through standardized APIs and relying on the architecture from various providers can provide easy solutions without middle man in between.

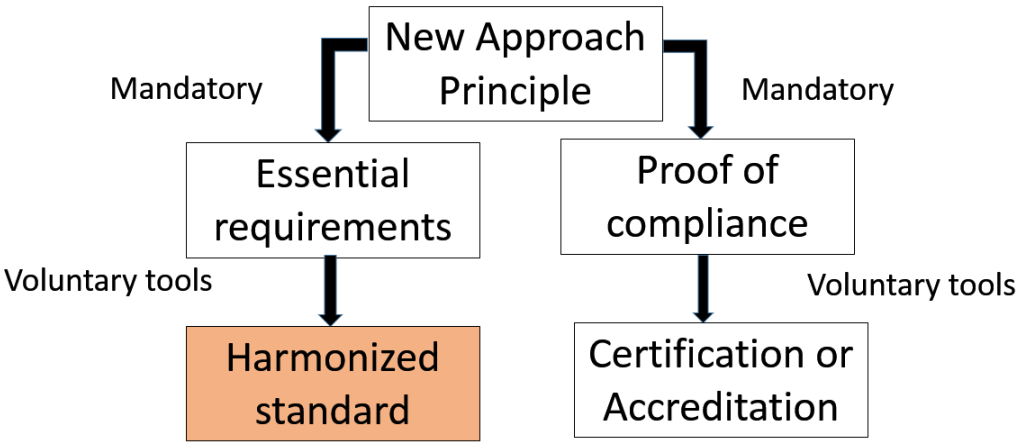

Figure 8-1: New Approach for compliance

The New Approach, as in figure 8-1 [i.YYY], should help with harmonised standards or with certification or accreditation process. As for the Machinery Directive depending on the safety-related functions, a technical file could be requested based on PDL data. This audit could be triggered to perform the assessment of the logic put in place by the OEM against performance levels required into the harmonised standards. Several milestones would need to be carried out to comply with the safety/security test plan:

- Identification of the safety-related components and application characteristics:
  1) Production and testing.
  2) Process capability.
  3) Documentation/traceability.
  4) Modifications.

8.2 Sensor/device certification

The purpose of the sensor/device certification is to guarantee that all complex systems integrated are compliant with common shared safety rules, secure communication and standardized software control, for example machinery. This output of the certification process will be some digital certificate used during the authentication process. This conformance test and authentication generates a strong connection between the certification and the use of a complex system integrating connected devices.

The purpose of the sensor/device certification is to allow compliant products to mutually proof their reliability and functional capability exchanging the certificates through a dedicated cryptographic library. The necessity of a cryptographic library is mandatory to avoid dangerous use of some fraudulent parts or devices in the system, without approval from the OEM.

8.3 Application certification

The base of the complex system authentication structure and the application certification is a PKI that sets the roles for the digital certificates and public-key encryption management. The authentication process will take place at each coupling of an IoT device between the application server and each application client or IoT device present in the application. This means that each connection of a new IoT device to an existing application will trigger a new authentication process.

Both the application server and the application client can generate common secret data owning a private key and counterpart certificate. A key exchange algorithm can extract the common secret without a dedicated data exchange.

Once the authentication process is over, the application can start its functional operations. Several steps constitute the authentication algorithm:

1) Machinery and IoT device will use root certificate, device certificate and the private key connected to that certificate.

2) Machinery and IoT device mutually exchange their certificates.

3) Machinery and IoT device verify the exchanged certificates using the root certificate.

4) Machinery and IoT device generate common secret by their private key and counterpart certificate using the already mentioned key exchange algorithm.

5) Machinery and IoT device authenticate themselves by common secret key and challenge-response mechanism.

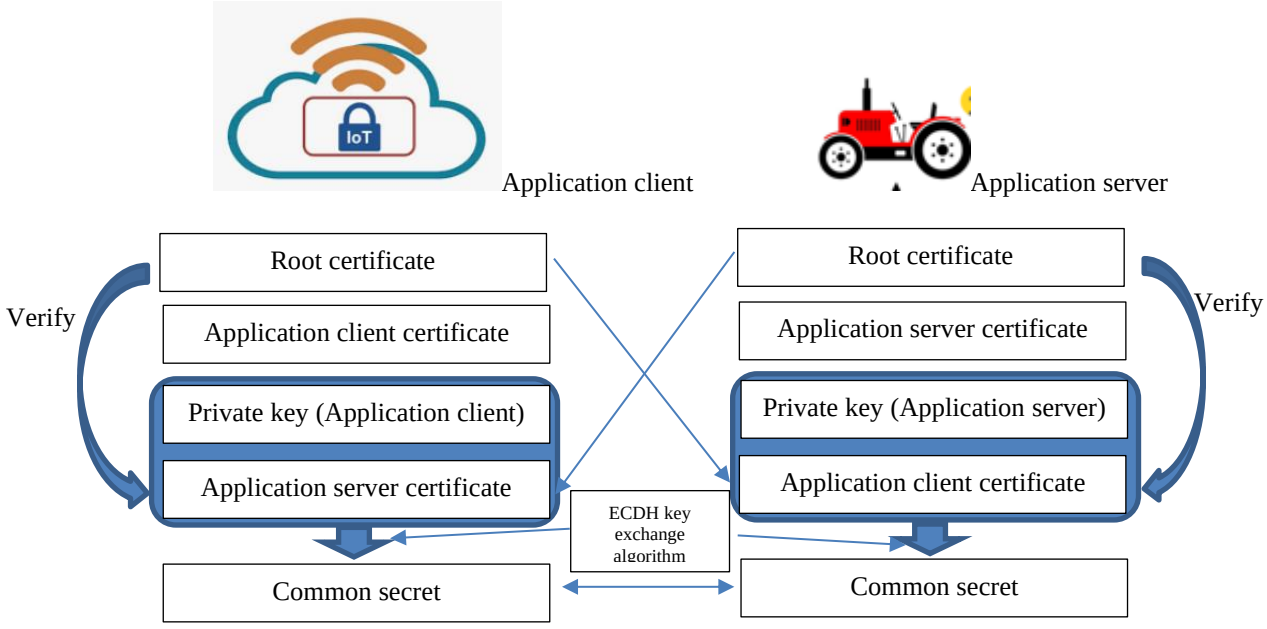

Figure 8.3-1: Example of message authentication by common secret

All IoT device integrated on the machinery need to pass the application conformance test for application functionality since only the OEM that passed conformance test can get a production certificate for the machinery. Applications need to pass through a development certificate to test and tune the complex system before the IoT device integrated on the machinery pass the application conformance test to get a production certificate.

Note: ECDH anonymous key agreement protocol that allows two parties to establish a shared secret over an insecure channel. When the conformance certificate is granted, this implies that the root certificate provides a key to the device certificate.

If a manufacturer needs to test its own IoT device for development or maintenance purposes, it can formally request a compliance test certificate for the notified body with a proper self-declaration in addition to some software/system information.

Once the application (application server or application client) is ready for an official test, the manufacturer can require to perform a application conformance test to the notified body. To obtain a manufacturer certificate, which is a production certificate to sell the application, the manufacturer needs to pass the conformance test.

8.4 Requirement of application authentication

1) Private Key and common shared secret key are the application authentication process trust anchor and their storage is one of the main application system challenges: a tamper resistant area like a Hardware Secure Module in microcomputer to store them is an important feature. In addition, a good source of not foreseeable numbers, that is a pseudo random number generator will avoid security leaks adding additional security to the authentication process.

2) The nature of implementing an IoT device on an application suggest a regular updating process and, in addition, also a private key update could be required. In the case of a regular or an emergency update by the OBD port could result of not being easy. An update through On-The-Air update is a desirable option, but should be under strict definition (Part Improvement Program, etc.) where the safety and the security of the use are at risk.

3) The hacking of wireless system is a threat and root certificates and private key will be installed in a safe area of the ECU application. Cloud systems, key pair generator station and End of Line process for the application are all elements that will be secured by safe key management system.

4) Part of the secure key management system will be also a tamper resistant area in a Hardware Secured Module computer where the keys are generated and stored. A secure server and a safe area in the facilities of the OEM could be stored.

5) A secure path for On-The-Air updates from cloud to the application server and application client ECU will optimize the previous safety precautions.

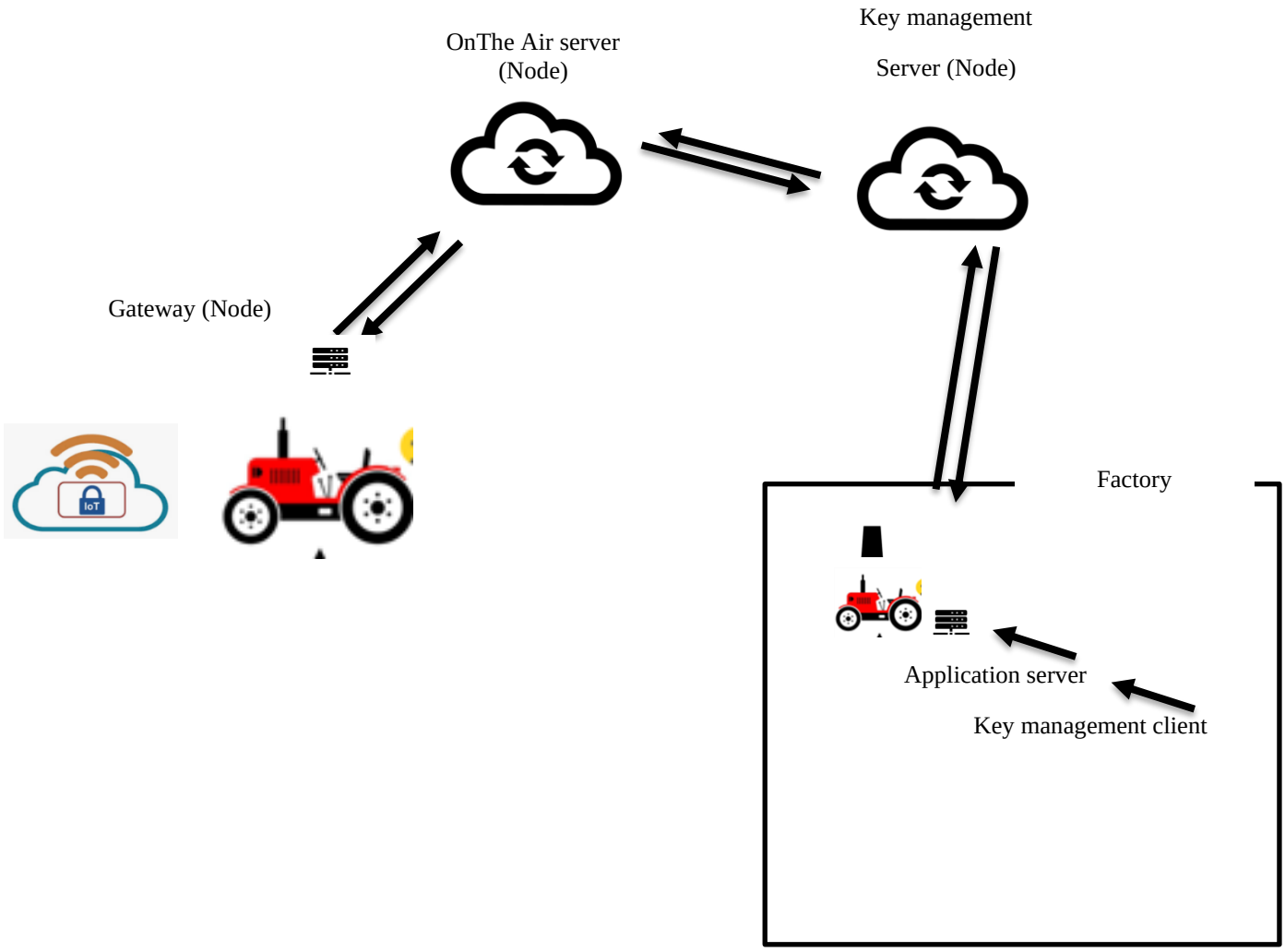

Figure 8.4-1: Example of system requirement of application authentification

This overall process has been inspired by the AEF guidelines for TIM.

9 Conclusion

The mechanism described here targets scenarios such as “connected machines” where a unique registry managed through a PDL will provide presumption of conformity according to performance levels decribed into harmonized standards, which still need to be explained for each sector.

The components described do exist and can provide tools to ensure compliance to the regulation, where cerification/homologation or self-certification based on harmonized standards will be the cornerstones to build a safe and secure environment for users.

The system requirements might be more suitable to autonomous vehicles or machine modified by some IoT devices or AI with validated Machine Learning models. The integration into a existing architecture such as the ISOBUS one used in the agriculture sector for the tractors and the implements, could be a way to find some consensus between the ICT world and the mechanical world to make these connected machines work in this new environment through this unique registry reflecting the status of a machine.

This provides however the foundation to ensure that such connected machines are safe and will behave in a way complying to the minimum risk to match the functional safety expected by a connected machinery put on the market.

Finally, a PDL available and run by the OEM will be the basis to lower costs for the customer and qualify these equipment to comply with the regulatory requiments.

Annex A:
Change History

Date	Version	Information about changes
21/01/2020	5	Cleaning and alignment according to ETSI edit rules
06/02/2020	5 b	Completion of missing paragraphs, and review of the
04/03/2020	5 c	Final version before publication

History

Document history		
005	22/05/2019	Consolidated input covering PDL and Machinery requirements
V0.0.5	December 2019	Clean-up done by ***editHelp!*** E-mail: mailto:edithelp@etsi.org
V0.0.5b	January 2020	Mistakes corrected and deletion of multiple PDL definition to comply with neutrality required
V0.0.5c	Februar 2020	Integration of the mechanism for the server and the client to maintain the registry of the machine, and final version before publication
V0.0.5c	March 2020	Final version