ETSI GR PDL 014 V1.1.1 (2022-10)

Permissioned Distributed Ledger (PDL); Study on non-repudiation techniques

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-0014_non_repud_tech

Keywords
interoperability, scalability, security, smart contract

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

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.

1 Scope

The present document covers the non-repudiation challenges in Permissioned Distributed Ledgers (PDLs), the non-repudiation strategies/technologies, and their viability in PDLs. It also defines the limitations in non-repudiation strategies in PDLs and possible future directions.

The present document discusses PDL based end-to-end architecture that provides non-repudiation. This includes non-repudiation for input and output data for a PDL, such as external PDLs and smart contracts.

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] IETF RFC 4270: "Attacks on Cryptographic Hashes in Internet Protocols".

NOTE: Available at https://datatracker.ietf.org/doc/html/rfc4270.

[i.2] David Chaum: "Blind Signatures for untraceable Payments".

NOTE: Available at http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF.

[i.3] Masahiro Mambo, Keisuke Usuda, Eiji Okamoto: "Proxy Signatures for Delegating Signing Operation".

NOTE: Available at https://dl.acm.org/doi/pdf/10.1145/238168.238185.

[i.4] ETSI GS PDL 012: "Permissioned Distributed Ledger (PDL); Reference Architecture".

NOTE: Available at https://www.etsi.org/deliver/etsi_gs/PDL/001_099/012/.

[i.5] D. Boneh: "Aggregate Signatures", in Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, p. 27.

[i.6] ETSI TS 133 303 (V14.1.0): "Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects (3GPP TS 33.303 version 14.1.0 Release 14)".

[i.7] D. He, J. Chen, and R. Zhang: "An efficient identity-based blind signature scheme without bilinear pairings", Comput. Electr. Eng., vol. 37, no. 4, pp. 444-450, Jul. 2011, doi: 10.1016/j.compeleceng.2011.05.009.

[i.8] T. Peacock, P. Y. A. Ryan, S. Schneider, and Z. Xia: "Verifiable Voting Systems", Comput. Inf. Secur. Handb., pp. e293-e315, 2013, doi: 10.1016/B978-0-12-803843-7.00090-9.

[i.9] D. A. Wijaya, J. Liu, R. Steinfeld and D. Liu: "Monero Ring Attack: Recreating Zero Mixin Transaction Effect", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1196-1201, doi: 10.1109/TrustCom/BigDataSE.2018.00165.

[i.10] Goldreich, Oded, and Yair Oren: "Definitions and properties of zero-knowledge proof systems". Journal of Cryptology 7.1 (1994): 1-32.

NOTE: Available at https://www.wisdom.weizmann.ac.il/~oded/PSX/oren.pdf.

[i.11] Manoj Kumar Chande, Cheng-Chi Lee & Chun-Ta Li (2018): "Cryptanalysis and improvement of a ECDLP based proxy blind signature scheme", Journal of Discrete Mathematical Sciences and Cryptography, 21:1, 23-34, DOI: 10.1080/09720529.2017.1390845.

[i.12] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab: "Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks", in European conference on Wireless Sensor Networks. Springer, 2008, pp. 305-320.

[i.13] ETSI GS PDL 011: "Permissioned Distributed Ledger (PDL); Specification of Requirements for Smart Contracts' architecture and security".

NOTE: Available at https://www.etsi.org/deliver/etsi_gs/PDL/001_099/011/01.01.01_60/gs_PDL011v010101p.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

auditability: ability of an object to undergo a thorough examination and evaluation

NOTE: Generally, auditability is measured against criteria defined by certain authority, such as the PDL governance.

governance: collection of rules and tools that control the behaviour and function of a PDL Platform (see ETSI GS PDL 012 [i.4]).

identifiable natural person: one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

mainchain: primary non-dependent chain which forms the PDL network

PDL participants: nodes which form the PDL network

personal data: any information relating to an identified or identifiable natural person

sidechain: sub-chain which is dependent on a mainchain

3.2 Symbols

Void.

3.3 Abbreviations

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

API Application Programmable Interface

BP	Bilinear Pairing
CA	Certificate Authority
CRC	Cyclic Redundancy Check
ECDSA	Elliptic Curve Digital Signature Algorithm
GDPR	General Data Protection Regulation
I/O	Input/Output
IoT	Internet of Things
MD5	Message Digest 5
NFT	Non-Fungible Token
NR	Non-Repudiation
NRD	Non-Repudiation of Delivery
NRE	Non-Repudiation of Emission
NRO	Non-Repudiation of Origin
NRR	Non-Repudiation of Receipt
NRS	Non-Repudiation of Submission
NRT	Non-Repudiation of Transport
PKI	Public Key Infrastructure
RSA	Rivest-Shamir Adleman
SHA	Secure Hashing Algorithm
TCP	Transmission Control Protocol
TTP	Trusted Third Party
ZKP	Zero Knowledge Proof

4 Introduction to Non-Repudiation Techniques

4.1 Definition

IETF RFC 4270 [i.1] defines non-repudiation as:

> *"A Security service that provides protection against false denial of involvement in a communication."*

Distributed ledges inherently implement non-repudiation through strategies such as digital signatures. Also, every node in the network keeps a record copy; therefore, it is theoretically unrealistic to deny a digitally signed transaction. However, in some situations, it is required to verify data integrity. For example, in the cases of smart contract offloading [i.2].

Therefore, non-repudiation, particularly in PDLs, can be defined as:

> *"Verification techniques and strategies that can provide secure proof that the data entered to/from the PDL are from a valid source and is unaltered, that is, same as entered by the source."*

For example, when capturing temperature data, it can be confirmed that the data captured from the thermometer is unaltered, but it cannot be guaranteed that the thermometer is accurate. In such a case, strategies such as device identity will play a key role.

EXAMPLE: Laboratory calibration confirmation and data, will be associated with the device (e.g. thermometer) identity.

Permissioned Distributed Ledgers (PDLs) provide accountability to the transactions through their inherent properties such as transparency. Historic transactions provide an audit trail for a future audit and produces undeniable records. However, in an end-to-end scenario, a PDL will not be a solitary entity and will include other functional components such as oracles and external data storage.

4.2 Types of Non-Repudiation

4.2.1 Introduction

In distributed ledgers, the role of non-repudiation is to collect evidence, verify and authenticate the source of data. In this clause, the types of non-repudiation relevant to PDLs are discussed.

4.2.2 Non-Repudiation of Origin (NRO)

Non-Repudiation of Origin (NRO) is an application layer consideration and proves that the data is from the source claimed by the message.

PDLs often take data inputs from various data sources, for instance, via oracles or in/directly from the devices. In such a situation, the authenticity of the data source will need to be verified.

4.2.3 Non-Repudiation of Emission (NRE)

Non-Repudiation of Emission (NRE) is a network layer consideration. It provides proof that the data sent is accurate and unaltered while being sent to and stored on the PDL.

In PDLs, this problem may occur when a user sends a valid message and a malicious party in the middle tampers with the message.

EXAMPLE: A user sends a bid through smart contract execution, a malicious user changes the bid as per latter's advantage.

4.2.4 Non-Repudiation of Receipt (NRR)

Non-Repudiation of Receipt (NRR) is the false denial of the receipt of a message. Typically, Permissioned Distributed Ledgers are inherently resilient to NRR because of their distributed nature. As long as the majority (as required by the consensus mechanism) of nodes receive the message correctly, it will be distributed to all the other nodes even if they maliciously deny the receipt from the sender.

4.2.5 Non-Repudiation of Submission (NRS)

Generally Non-Repudiation of Submission (NRS) provides proof that the sender submitted the data for delivery.

Since Permissioned Distributed Ledgers are implemented on the public Internet they are prone to transaction delay and network layer congestion. For example, a remote device sends data to a PDL node, and the transaction is delayed due to network conditions. In certain cases, such delay may render the data invalid. Non-Repudiation of Submission offers a set of tools that can prove that a transaction is valid.

Additionally, NRS may resolve some security vulnerabilities for the PDLs related to receipt of data from external resources. For instance, when the data or a smart contract is sent by an external storage or oracle, it is prone to malicious activity (e.g. virus) in the PDL. NRS provides the sender and the recipient the ability to verify the integrity of the data and the proof of submission.

4.2.6 Non-Repudiation of Delivery (NRD)

NRD provides the sender a set of tools that can prove that data was submitted and delivered to the recipient even if the recipient denies the receipt and/or fails to act upon the data received.

In PDLs, typically NRD is addressed in the context of Trusted Third Party (TTP) and provides the proof that the data was handed to the TTP or a Delivery Agent for delivery. Yet, distributed ledgers, in particular, PDLs advocate distributed trust and there is no TTP by the definition of PDL. Despite the distributed trust, PDLs should still offer NRD to enable data and smart contract efficiency and distribution. Specifically, in situations where the smart contracts are stored on third-party managed external storage.

4.2.7 Non-Repudiation of Transport (NRT)

Non-Repudiation of Transport (NRT) provides the proof that the data was sent by the sender and transported by the delivery agent (e.g. transport channel). NRT is different from NRD, due to the fact that there may be several transport entities involved in one end-to-end message delivery.

4.3 Generalized Non-Repudiation Scenarios

Unreliable Communication Channel: The sender sends a transaction that is dropped/delayed due to poor connectivity conditions or malicious activities on the transmission channel such as Man-in-The-Middle Attack. This may affect both the sender and the recipient because it may cause delay or non-approval of transactions and consequently may result in monetary losses for the parties.

Malicious Sender: The device user or sender is malicious and sends wrong, late or no data. In the example of smart contract external storage, it may include both the owner and the user of the device [i.2].

Malicious Receiver: The receiver of the data is being malicious and denies the receipt of the data. In a PDL scenario, the receiver is expected to be PDL nodes. However, this problem may arise when data traverses an intermediate object/entity such as an API.

4.4 Non-Repudiation Process

By definition, the non-repudiation, is a technique to generate proof that, at a later date, both the service and receiver can use to ensure proper operation of the PDL. Four phase processes for non-Repudiation are defined in [i.3] as follows:

Evidence Generation

The evidence of the message is generated by the respective participants of the system, for example, a sender or receiver. This evidence will later be used by the parties to verify that the data was transmitted/received by the other participant and prevent them denying generation/receipt of the data.

Evidence Transfer and Storage

The evidence generated by the sender/receiver are expected to be stored securely in local/governance-controlled storage.

Evidence Verification

The evidence of the transfer (of assets or an entity) is expected to be verifiable.

Dispute Resolution

In the case of PDLs, dispute resolution can be handled by the governance.

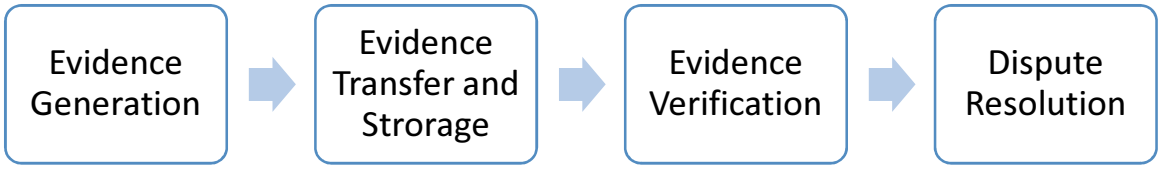

Figure 1: Non-repudiation process

Table 1: Examples of non-repudiation and possible solutions

Challenges/Objects	Example Scenarios where challenges occur	Possible solutions
Mismatched data - sent by the originator and received by the recipient are inconsistent or not the same	NRE, NRD	The sender sent the data and the receiving party received that but the proofs are mismatching, or not same. In this scenarios, the dispute can be launched and governance can step-in to resolve the issue.
Delayed data - data arrived at the destination after the allotted period of time	NRT, NRD, NRE	Timestamps can be recorded in a hashed form together with the data. Sometimes, timestamps can be encrypted part of the data. This problem applies to the *time-critical data.*
Tampered data (both accidental and malicious) - the data sent is tampered by the sender, receiver or a man-in-the-middle	NRE, NRD	Regular device health checks, and monitoring of transmission delays/losses can help the parties to identify the real reason of data tampering. In PDLs, the governance, can also take compliance actions against the parties with poor transmission record and may set standards for connection and security requirements. Multiple transmission ways can also be adopted to ensure the integrity of data.
Erroneous data - the data sent is incorrect or not complying with the agreed/set standards	NRE	Here regular device checks and governance compliance strategies can help.
Missing/incomplete data - the data is not sent at all/or missed by the communication channel	NRE, NRD, NRD	Governance compliance strategies and regular node checks can help.
Data Re-ordering - data arrives in a sequence different than it was sent	NRE, NRD, NRT	Application layer protocols for reordering the packets, at a cost of additional delays.

5 Objects of Non-repudiation

5.1 Introduction

In PDLs, data is written to a ledger by internal and external participants. This includes PDL nodes and oracles; the main objective is that the data integrity is maintained. In this clause, the key properties for a non-repudiation mechanism are highlighted.

5.2 Pre-requisite

5.2.1 Evidence Recovery

In networks, the evidence (e.g. receipt) are sent through a wireless/wired link. These links may suffer from disruption or performance issues that may cause data loss, which may result in delayed or lost evidence. In some applications, such delays in evidence arrival may cause the stakeholders losses such as a delayed bid. Therefore, the evidence generated by either party needs to be recoverable with correct parameters (e.g. time original evidence was sent).

5.2.2 Redact

5.2.2.1 Introduction

In business applications particularly a document may include numerous details such as stakeholders' personal information and previous business dealings. When a number of parties involved in a dealing or business, the whole document cannot be disclosed to all the parties, nor the non-repudiation of a complete document is required. For example, in a loan application, non-repudiation of finances may be required, and stakeholders' personal records may be irrelevant and can be kept hidden through mechanisms such as encryption.