

ETSI GR PDL 030 V1.1.1 (2025-05)



Permissioned Distributed Ledger (PDL); Trust in Telecom System

(<https://standards.iteh.ai>)
Document Preview

[ETSI GR PDL 030 V1.1.1 \(2025-05\)](https://standards.iteh.ai/catalog/standards/etsi/bed1b16e-9f35-47f5-a9ea-1b6b638c86f8/etsi-gr-pdl-030-v1-1-1-2025-05)

<https://standards.iteh.ai/catalog/standards/etsi/bed1b16e-9f35-47f5-a9ea-1b6b638c86f8/etsi-gr-pdl-030-v1-1-1-2025-05>

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-0030_Trust_Telecom

Keywords

PDL, 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 - 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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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 2025.
All rights reserved.

Contents

Intellectual Property Rights	8
Foreword.....	8
Modal verbs terminology.....	8
1 Scope	9
2 References	9
2.1 Normative references	9
2.2 Informative references.....	9
3 Definition of terms, symbols and abbreviations.....	10
3.1 Terms.....	10
3.2 Symbols.....	11
3.3 Abbreviations	11
4 Trust-Related Definitions	12
4.1 Definition of Trust.....	12
4.2 Key Aspects of Trust.....	13
4.2.1 Objective and Subjective Nature	13
4.2.2 Quantifiability.....	13
4.2.3 Multi-faceted Nature	13
4.2.4 Subjective Evaluation	13
4.2.5 Dynamic Nature	13
4.2.6 Context Dependence	14
4.2.7 Asymmetric Relationship	14
4.3 Trust Evaluation Process	15
5 Introduction to Trust in Telecom System.....	15
5.1 3GPP Telecom Networks	15
5.1.1 Components of 3GPP Telecom Networks	15
5.1.2 Functionality of Network Components.....	15
5.1.2.1 Radio Access Network (RAN).....	15
5.1.2.2 Core Network (CN).....	15
5.1.3 Future Trends in 5G-Advanced (5GA) and 6G.....	16
5.1.3.1 Evolution of UE Roles	16
5.1.3.2 Shift Towards Decentralized Architecture	16
5.1.3.3 Increased UE Collaboration	16
5.1.3.4 Distribution of Network Functions	17
5.1.3.5 User-Centric Approach	17
5.1.4 Emerging Trends in 3GPP Development.....	17
5.1.4.1 Network of Service Robots with Ambient Intelligence.....	17
5.1.4.1.1 3GPP SA1.....	17
5.1.4.1.2 Study Objectives.....	17
5.1.4.1.3 Potential Applications	17
5.1.4.1.4 Expected Outcomes	18
5.1.4.2 User-Centric Approach in Telecom Services	18
5.1.4.2.1 3GPP SA2.....	18
5.1.4.2.2 Current Limitations	18
5.1.4.2.3 Future Vision.....	18
5.1.4.2.4 Study Focus	18
5.1.4.2.5 Expected Benefits.....	18
5.1.4.3 Implications for Trust in Telecom Systems	18
5.2 Existing Trust Mechanisms in 3GPP Networks	18
5.2.1 Existing status.....	18
5.2.2 Security Domains in 3GPP 5G	19
5.2.2.1 Network Access Security	19
5.2.2.1.1 Focus	19
5.2.2.1.2 Primary Authentication and Key Agreement.....	19
5.2.2.1.3 Secondary Authentication.....	19

5.2.2.1.4	Security Context Establishment.....	19
5.2.2.1.5	Security Mode Command Procedure.....	20
5.2.2.2	Network Domain Security.....	20
5.2.2.2.1	Focus	20
5.2.2.2.2	Key Components	20
5.2.2.2.3	Security Features	21
5.2.2.3	Service-Based Architecture (SBA) Domain Security	21
5.2.2.3.1	Focus	21
5.2.2.3.2	Key Components	21
5.2.2.3.3	Security Features	22
5.2.2.3.4	Implementation Aspects	22
5.2.3	Zero Trust Architecture in 3GPP	23
5.2.3.1	3GPP TR 33.894	23
5.2.3.2	Key Objectives	23
5.2.3.3	Implementation Considerations.....	23
5.2.4	Ongoing Studies on Zero Trust.....	23
5.2.4.1	3GPP TR 33.794	23
5.2.4.2	Key Issues Under Investigation.....	23
5.2.5	Emerging Trust Concepts in 3GPP	23
5.2.5.1	Distributed Trust	23
5.2.5.2	User-Centric Trust.....	23
5.2.6	Future Directions	23
6	Existing Standards and Trust Mechanisms.....	24
6.1	Trust Computing Group (TCG).....	24
6.1.1	Purpose of TCG	24
6.1.2	TCG's Approach to Trust.....	24
6.1.2.1	Integrity Measurement and Verification	24
6.1.2.1.1	Definition.....	24
6.1.2.1.2	Process.....	24
6.1.2.2	Roots of Trust.....	24
6.1.2.2.1	Root of Trust for Measurement (RTM)	24
6.1.2.2.2	Root of Trust for Storage (RTS).....	24
6.1.2.2.3	Root of Trust for Reporting (RTR).....	24
6.1.2.3	Transitive Trust	25
6.1.2.3.1	Purpose	25
6.1.2.3.2	Process.....	25
6.1.3	TCG Specifications and Implementations	25
6.1.3.1	Trusted Platform Module (TPM)	25
6.1.3.2	Practical Implementation	25
6.1.3.3	TPM Services.....	25
6.1.4	Example: Trust in a Desktop Computer.....	25
6.1.4.1	Aspects of Trustworthiness in a Desktop	25
6.1.4.1.1	Boot-time Integrity	25
6.1.4.1.2	Runtime Integrity.....	25
6.1.4.1.3	Application Monitoring.....	26
6.1.4.2	Trust Chain Establishment Steps.....	26
6.1.4.2.1	BIOS Verification.....	26
6.1.4.2.2	Bootloader Verification	26
6.1.4.2.3	OS Kernel Verification.....	26
6.1.4.2.4	System Components Verification.....	26
6.1.4.2.5	Application Verification	26
6.1.4.3	Continuous Trust Maintenance	26
6.1.4.4	Benefits of This Approach	26
6.2	ITU-T	27
6.2.1	Recommendation ITU-T Y.3052	27
6.2.2	Trust Categorization	27
6.2.3	Direct and Indirect Trust.....	27
6.2.4	Aspects of Trust in ICT	27
6.2.5	Trust Provisioning Process	27
6.3	NIST	27
6.3.1	Special Publication 800-207	27

6.3.2	Core Principles of Zero Trust	28
6.3.2.1	Fundamental Concept.....	28
6.3.2.2	Key Features	28
6.3.3	Zero Trust Architecture (ZTA) Implementation.....	28
6.3.3.1	Adoption Trend.....	28
6.3.3.2	Key Components.....	28
6.3.3.3	Trust Zones	28
6.3.3.4	Design Goal.....	28
6.3.4	Rationale for Zero Trust	28
6.3.4.1	Changing Work Environments.....	28
6.3.4.2	Security Paradigm Shift	28
6.3.5	Key Tenets of Zero Trust Architecture.....	28
6.4	IETF	29
6.4.1	Significant approaches.....	29
6.4.2	Remote Attestation Procedures (RATS).....	29
6.4.2.1	IETF RFC 9334.....	29
6.4.2.2	Key Roles in RATS.....	29
6.4.2.3	RATS Process	29
6.4.2.4	Use Case Example: Network Endpoint Assessment	29
6.4.2.5	Trust Model in RATS.....	29
6.4.3	Trusted Execution Environment Provisioning (TEEP).....	30
6.4.3.1	IETF RFC 9397.....	30
6.4.3.2	Key Concepts	30
6.4.3.3	TEEP Protocol.....	30
6.4.3.3.1	Overview	30
6.4.3.3.2	Process Overview	30
6.4.3.4	Security Measures	30
6.5	ETSI	30
6.5.1	Key Approaches.....	30
6.5.2	Decentralized Identifiers (DIDs) and Trust Management	31
6.5.2.1	Overview.....	31
6.5.2.2	DID-related Operations	31
6.5.3	Self-Sovereign Identity (SSI) in Telecom Networks	31
6.5.3.1	Gap Analysis.....	31
6.5.3.2	Objectives.....	31
6.5.4	Reputation Management in PDL Systems	31
6.5.4.1	Types of Reputation	31
6.5.4.2	Reputation Management Aspects.....	32
6.5.5	Trust in Network Function Virtualisation (NFV)	32
6.5.5.1	Mapping RATS Roles to NFV Entities.....	32
6.6	eIDAS (910-2014).....	32
6.6.1	eIDAS (910-2014) brief.....	32
6.6.2	Key Objectives.....	32
6.6.3	Main Components.....	32
6.6.3.1	Electronic Identification (eID)	32
6.6.3.2	Trust Services.....	32
6.6.4	Key Principles.....	33
6.6.5	Impact	33
6.6.6	Implementation	33
7	Use Cases for Trust in Telecom System	33
7.1	Introduction	33
7.2	Use Case 1 - Decentralized Trust Evaluation	33
7.3	Use Case 2 - Granular and Customized Trust Evaluation	35
7.4	Use Case 3 - Enabling User-centric Trust	36
7.5	Use Case 4 - Trust-aware UE-to-UE Interaction Model (Service Producer & Service Consumer) and Trust Enablement using Smart Contract.....	37
7.6	Use Case 5 - Trust-aware UE-to-UE Interaction Model (Task Initiator & Task Participant)	39
8	Key Issues	40
8.1	Introduction	40
8.2	Key Issue 1 - Trust Evaluation in Different Task Lifecycle Stages	41

8.3	Key Issue 2 - Granular and Customized Trust Evaluation	41
8.4	Key Issue 3 - Trust Data Recording, Discovery and Retrieval.....	42
8.5	Key Issue 4 - TMF Registration and Discovery	42
8.6	Key Issue 5 - Smart Contract-based Trust Enablement.....	42
8.7	Key Issue 6 - Service Access Considering User-Centric Trust	43
8.8	Key Issue 7 - Service Interaction Incorporating Trust Index.....	43
9	Conclusions and Next Steps	44
9.1	Summary	44
9.2	Recommendations for Next Steps	44
	History	45

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI GR PDL 030 V1.1.1 \(2025-05\)](https://standards.iteh.ai/catalog/standards/etsi/bed1b16e-9f35-47f5-a9ea-1b6b638c86f8/etsi-gr-pdl-030-v1-1-1-2025-05)

<https://standards.iteh.ai/catalog/standards/etsi/bed1b16e-9f35-47f5-a9ea-1b6b638c86f8/etsi-gr-pdl-030-v1-1-1-2025-05>