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

GROUP REPORT

Permissioned Distributed Ledger (PDL); Trust in Telecom System

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

Contents

List of figures

List of tables

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 describes scenarios and use cases in telecom system that need trustworthiness among different entities such as users, devices, networks, and applications. Technologies for providing such trustworthiness will be reviewed. Using PDL for realizing trust in telecom system will be discussed and demonstrated. The present document also discusses the key issues or topics related to how to enable PDL-enabled trust in telecom system, such as user trust, distributed trust, trust management, etc. The potential standardization recommendations on those key issues or topics may also be investigated.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] 3GPP TS 23.501 (V18.0.0) (2022-12): "System Architecture for the 5G System (5GS); Stage 2 (Release 18)".

[i.2] 3GPP SP-220447: "Study on Network of Service Robots with Ambient Intelligence". 3GPP TSG Meeting #96e, 2022.

[i.3] 3GPP SP-231804: "New Study on User Identities and Authentication Architecture". TSG SA Meeting #102, 2023.

[i.4] 3GPP TS 33.501 (V18.2.0) (2023-06): "Security Architecture and Procedures for 5G System (Release 18)".

[i.5] 3GPP TR 33.894 (V19.0.0) (2023-09): "Study on Applicability of the Zero Trust Security Principles in Mobile Networks (Release 18)".

[i.6] NIST Special Publication 800-207: "Zero Trust Architecture, National Institute of Standards and Technology", 2020.

[i.7] 3GPP TR 33.794 (V0.3.0) (2024-05): "Study on enablers for Zero Trust Security (Release 19)".

[i.8] 3GPP S1-240238: "Study on distributed device and user-centric trust". 3GPP TSG- SA1 Meeting #105, 2024.

[i.9] Trusted Computing Group: "TCG Specification Architecture Overview", TCG Specification Revision 1.4, The Trusted Computing Group, Portland, OR, USA, August 2007.

[i.10] Recommendation ITU-T Y.3052 (2017): "Overview of trust provisioning in information and communication technology infrastructures and services".

[i.11] IETF RFC 9334 (January 2023): "Remote Attestation Procedures (RATS) Architecture".

[i.12] IETF RFC 9397 (July 2023): "Trusted Execution Environment Provisioning (TEEP) Architecture".

[i.13] ETSI GS PDL 023 (V1.1.1) (2024-04): "PDL service enablers for Decentralized Identification and Trust Management".

[i.14] ETSI GS PDL 027 (V0.0.3) (2024-02): "Permissioned Distributed Ledger (PDL); Self-sovereign identity (SSI) in telecom networks".

[i.15] ETSI GS PDL 015 (V1.1.1) (2023-01): "Permissioned Distributed Ledger (PDL); Reputation management".

[i.16] ETSI GS NFV-SEC 024 (V0.0.8) (2023-09): "Network Functions Virtualisation (NFV) Security; Security Management Specification".

[i.17] eIDAS Made Easy!.

[i.18] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

[i.19] 3GPP TS 23.304 (V19.0.0) (2024-06): "Proximity based Services (ProSe) in the 5G System (5GS)".

[i.20] ETSI TS 133 503 (V18.3.0): "5G; Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS) (3GPP TS 33.503 version 18.3.0 Release 18)".

[i.21] 3GPP TR 23.700-32: "Study on User Identities and Authentication Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

distributed trust: trust relationship built without fully relying on a centralized party

NOTE 1: Such a centralized party may be used to facilitate to build distributed trust relationship.

NOTE 2: Distributed trust can be established among devices, between devices and networks, or between networks.

trust: measurable belief about the quality/behaviour/performance/characteristic of an entity from history and the future expectation on various trust indicators

NOTE: Trust covers many other aspects beyond security.

trust enablement: process to establish trust between entities, including mutual authentication as well as other advanced and decentralized mechanisms, such as smart contract, etc.

trust evaluation: process to collect various data related to an entity and deduce a trust index of an entity.

trust index: aggregated metric of multiple focused trust indicators and can be deduced from a trust evaluation process

trust indicator: trust from a particular aspect, such as security, privacy, resiliency, performance, robustness, scalability, availability, accuracy, reliability, consistency, etc.

trust management: various activities related to trust, such as trust evaluation, trust estimation, trust enablement, etc.

user credential management: activities related to creating, publishing, maintaining, discovery and usage of user credential in the telecom system

NOTE: In order to enable user-centric trust, user credential should be made available in the telecom system.

user identifier management: various activities to manage user identifier (e.g. create, update, delete, etc.) in telecom system

NOTE: In particular, decentralized user identifier manager may be built on top of distributed ledger infrastructure.

user trust: trust relationship relying on user credentials instead of fully relying on or in addition to SIM-based primary authentication in current 5G system

NOTE: User trust also can be established among devices, and between devices and networks. User trust can enable user-centric trustworthiness expanding or beyond existing SIM-based authentication and trust.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	Third Generation Partnership Project
5G	Fifth Generation
5GA	5G-Advanced
5G-AKA	5G Authentication and Key Agreement
5GS	5G System
6G	Sixth Generation
AAA	Authentication, Authorization, and Accounting
AI/ML	Artificial Intelligence / Machine Learning
AKA	Authentication and Key Agreement
AMF	Access and Mobility Function
AR	Augmented Reality
AS	Application Server
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
CN	Core Network
DID	Decentralized IDentifier
EAP-5G	Extensible Authentication Protocol for 5G
eID	electronic IDentification
eIDAS	electronic IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
EU	European Union
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IoT	Internet of Things
KI	Key Issue
NAS	Non-Access Stratum
NF	Network Function
NFV	Network Function Virtualisation
NIST	National Institute of Standards and Technology
NRF	Network Repository Function
NW	NetWork
OS	Operating System
PCR	Platform Configuration Register
PDL	Permissioned Distributed Ledger
PDP	Policy Decision Point
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
ProSe	Proximity-based Services
QoS	Quality-of-Service
RAN	Radio Access Network
RATS	Remote Attestation procedures

REE	Rich Execution Environment
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SA	Service and System Aspect
SBA	Service-Based Architecture
SCP	Service Communication Proxy
SDO	Standards Development Organization
SIM	Subscriber Identity Module
SMF	Session Management Function
SP	Special Publication
SSI	Self-Sovereign Identity
TA	Trusted Application
TAM	Trusted Application Manager
TCG	Trust Computing Group
TEE	Trusted Execution Environment
TEEP	Trusted Execution Environment Provisioning
TI	Task Initiator
TMF	Trust Management Function
TP	Task Participant
TPM	Trusted Platform Module
TR	Technical Report
TS	Technical Specification
UA	Untrusted Application
UE	User Equipment
USIM	Universal Subscriber Identity Module
VC	Verifiable Credential
VNF	Virtual Network Function
ZT	Zero Trust
ZTA	Zero Trust Architecture

4 Trust-Related Definitions

4.1 Definition of Trust

Trust is a measurable confident reliance on the character, ability, strength, or truth of an entity that represents:

1) An accumulated value from history.

2) The expected value for the future.

This accumulated value may relate to the quality, behaviour, performance, and/or characteristic of a logical/physical object or entity. In the context of ICT, the entity could refer to, but is not limited to, a network node (e.g. a 3GPP base station), User Equipment (UE), a device, a network service, or a human role.

4.2 Key Aspects of Trust

4.2.1 Objective and Subjective Nature

Trust operates in both objective and subjective realms, creating a dynamic interplay between measurable behaviours and personal perceptions. Objective trust can be evaluated through concrete actions, reliable patterns, and verifiable outcomes. In the context of security, for example, the use of authentication to validate an entity's identity can increase the level of trust in that entity. However, the subjective dimension of trust may involve personal interpretations, emotional responses, and intuitive judgments that may not align perfectly with objective evidence. This duality makes trust both a rational calculation based on evidence and an emotional investment shaped by individual perspective. Trust may encompass more than a single attribute. When the identity of an entity is successfully authenticated by another entity it only means the identity is successfully proven but other characteristics of that entity may not be fully trusted if not proven separately. E.g. a buyer has authenticated itself on the seller's portal. The seller now trusts that the buyer is who he/she claims to be. That does not mean the seller gives the buyer an unlimited line of credit. The seller may still require additional proof of balance in the banks prior to transacting.

4.2.2 Quantifiability

Trust is an essential input for various decision-making processes in telecom system. It is usually measured or calculated in a quantitative or a qualitative manner, often represented as a Trust Index (e.g. a UE in the telecom system).

4.2.3 Multi-faceted Nature

Trust index is an overall metric, which is often calculated based on the aggregation of one or more Trust Indicators (depending on specific trust evaluation criteria). These indicators may cover various aspects, such as security, privacy, resilience, performance, robustness, scalability, availability, accuracy, reliability, and consistency.

4.2.4 Subjective Evaluation

For the same Entity A, evaluated by two different entities ("B" and "C" for the purpose of this example), Entities B and C may have different and subjective criteria regarding how Entity A's trust should be measured. As a result, Entities B and C may assign different Trust Indices to Entity A based on the same data.

EXAMPLE: Entity B may prioritize Entity A's reliability and availability while Entity C may focus more on Entity A's scalability and privacy.

4.2.5 Dynamic Nature

The dynamic nature of trust means that trust values are not static but evolve and change over time, with any given trust index having temporal validity and requiring regular updates.

Key Aspects:

1) Temporal Validity:

   - Trust assessments have a limited period of applicability
   - Trust values require periodic re-evaluation
   - Historical trust may not reflect current trustworthiness
   - Trust indexes need timestamps for validity tracking

2) Factors Affecting Trust Dynamics:

   - Performance variations over time
   - Changes in operational conditions
   - Evolution of entity behaviour

- Resource availability fluctuations
- Security status changes
- Network conditions variations
- Change of trust evaluation criteria

3) Monitoring Requirements:
   - Continuous monitoring of trust indicators
   - Regular collection of performance metrics and/or behaviour/operation logs
   - Real-time assessment and evaluation of behaviour patterns
   - Periodic trust score updates
   - Automated trust re-evaluation triggers

4.2.6 Context Dependence

Trust levels can vary significantly based on the environmental, operational, or situational context in which an entity operates or interacts.

Key Aspects:

1) Dynamic Environmental Factors:
   - Physical location and network conditions
   - Time of day or specific circumstances
   - Network load and resource availability
   - Security threat levels in different environments
2) Operational Context:
   - Type of service being provided
   - Role being performed (e.g. buyer vs. seller)
   - Performance requirements for specific tasks
   - Resource availability and capabilities
3) Situational Variables:
   - Emergency vs. normal operations
   - Critical vs. non-critical communications
   - Public vs. private network scenarios
   - Regulatory requirements in different regions

4.2.7 Asymmetric Relationship

Trust is an asymmetric relationship. The fact that Entity A trusts Entity B does not imply that Entity B trusts Entity A.

4.3 Trust Evaluation Process

Trust index is often measured and generated via trust evaluation. The process of evaluating trust typically involves:

1) Data collection about an entity.
2) Use collected data as inputs to calculate various trust indicators.
3) Aggregation of trust indicators into an overall metric (Trust index).

This structured definition provides a comprehensive explanation of trust in the context of ICT, highlighting its multi-faceted nature and the process of trust evaluation.

5 Introduction to Trust in Telecom System

5.1 3GPP Telecom Networks

5.1.1 Components of 3GPP Telecom Networks

A telecom system, such as a 3GPP 5G System (5GS), is operated by mobile operators and consists of geographically distributed components, including:

1) Mobile devices (User Equipment (UE)).
2) Radio Access Networks (RANs).
3) Core Network (CN).
4) Application Servers (ASs).

5.1.2 Functionality of Network Components

5.1.2.1 Radio Access Network (RAN)

RAN component (e.g. a base station) allocates radio resources to UEs, providing connectivity for UEs to interact with the CN.

5.1.2.2 Core Network (CN)

The CN contains a variety of Network Functions (NFs) that NFs provide essential services to UEs [i.1], such as:

1) Authentication and authorization.
2) AS access.
3) Mobility management.
4) Policy control.
5) Session management.

EXAMPLE 1: Access and Mobility Management Function (AMF) manages UE access to 5GS and its mobility.

EXAMPLE 2: Session Management Function (SMF) supports session establishment between a UE and the core network.

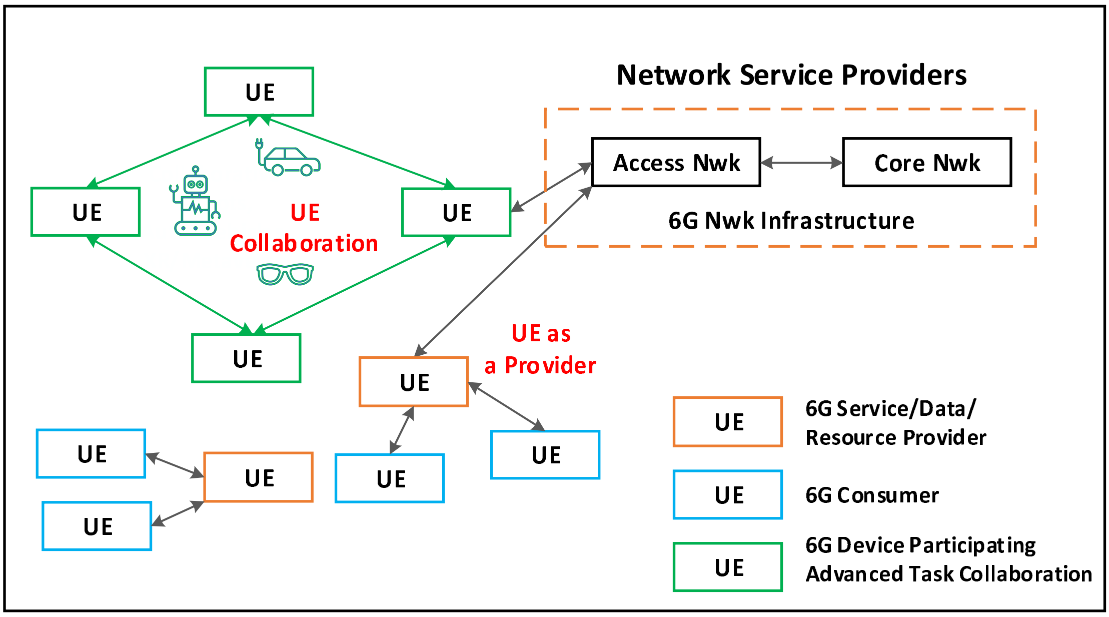
Network Service Providers
Access Nwk
Core Nwk
6G Nwk Infrastructure
UE
UE Collaboration
UE as a Provider
6G Service/Data/ Resource Provider
6G Consumer
6G Device Participating Advanced Task Collaboration

Figure 1: Future Trend: UE Acting as Both Provider and Consumer and Advanced UE Collaboration

5.1.3 Future Trends in 5G-Advanced (5GA) and 6G

5.1.3.1 Evolution of UE Roles

The evolution of telecom systems from 5G-Advanced to 6G brings significant changes in network architecture and device capabilities, fundamentally transforming how network elements interact and collaborate. This is shown in Figure 1. The role of User Equipment (UE) is expanding beyond traditional consumer devices to become active network participants:

- UEs can act as data providers, sharing sensory information and local intelligence.
- UEs can offer computing resources for distributed processing.
- UEs can provide communication resources by acting as relay nodes.
- UEs can participate in collaborative sensing and data collection.
- Advanced UEs can host network functions traditionally reserved for core networks.

5.1.3.2 Shift Towards Decentralized Architecture

The network architecture is evolving from centralized to distributed models:

- Edge computing nodes handle more processing tasks.
- Peer-to-peer communications become more prevalent.
- Network functions are distributed across multiple layers.
- Decision-making becomes more localized.
- Trust establishment moves from centralized to distributed models.

5.1.3.3 Increased UE Collaboration

UEs are becoming collaborative entities in the network:

- Multiple UEs can form dynamic clusters for specific tasks.

- Collaborative computing enables complex applications like AR/VR.
- Shared sensing capabilities enhance environmental awareness.
- Resource pooling allows more efficient utilization.
- Joint collaboration efforts improve coverage and reliability as well as other trust-related performance metrics.

5.1.3.4 Distribution of Network Functions

Network functions are becoming more distributed:

- Core network functions can be deployed at the network edge.
- Some network functions can run directly on capable UEs.
- Dynamic function placement based on needs and resources.
- Hybrid deployment models combining centralized and distributed functions.
- Enhanced security through distributed trust mechanisms.

5.1.3.5 User-Centric Approach

The focus shifts from device-centric to user-centric services:

- Multiple users can share a single UE with personalized services.
- User identity becomes separate from device identity.
- Service customization based on user preferences and context.
- Dynamic trust evaluation based on user behaviour.
- Enhanced privacy through user-controlled data sharing.

5.1.4 Emerging Trends in 3GPP Development

5.1.4.1 Network of Service Robots with Ambient Intelligence

5.1.4.1.1 3GPP SA1

This clause refers to a 3GPP SA1 study item on Network of Service Robots with Ambient Intelligence [i.2].

5.1.4.1.2 Study Objectives

- Explore collaboration among multiple service robots on complex, cross-disciplinary tasks.
- Investigate information sharing mechanisms between robots to optimize coordination.

5.1.4.1.3 Potential Applications

- Goods delivery.
- Hazardous material management.
- Underwater rescue operations.
- Etc.

5.1.4.1.4 Expected Outcomes

- Enhanced daily human life through robotic collaboration.
- Improved efficiency in cross-industry tasks.

5.1.4.2 User-Centric Approach in Telecom Services

5.1.4.2.1 3GPP SA2

This clause refers to a study on User Identities and Authentication Architecture [i.3] for 3GPP Release 19.

5.1.4.2.2 Current Limitations

- Telecom networks use subscription-based identifiers for connections and services.
- Single UE is typically associated with a single user.

5.1.4.2.3 Future Vision

- Multiple users may share a single UE, each with distinct needs.
- Example scenario: A vehicle with an embedded UE providing personalized services to multiple passengers.

5.1.4.2.4 Study Focus

- Creating and utilizing user-specific identifiers in telecom services.
- Enabling differentiated services based on individual user needs.

5.1.4.2.5 Expected Benefits

- Enhanced user experience through personalization.
- More flexible and efficient telecom services.
- Tailored service delivery based on individual user requirements.

5.1.4.3 Implications for Trust in Telecom Systems

These developments have significant implications for trust in future telecom systems:

- Increased need for trust mechanisms in robot-to-robot communications.
- Requirement for more granular trust models to support user-specific services.
- Potential for new trust challenges in multi-user, single-device scenarios.

5.2 Existing Trust Mechanisms in 3GPP Networks

5.2.1 Existing status

While trust encompasses more than security, existing 3GPP 5G security functions, though limited to the context of security, provide a foundation for trust across additional domains. These mechanisms are defined in 3GPP TS 33.501 [i.4].

5.2.2 Security Domains in 3GPP 5G

5.2.2.1 Network Access Security

5.2.2.1.1 Focus

Network Access Security focuses on the security mechanisms between the User Equipment (UE) and the Radio Access Network (RAN)/Core Network (CN).

5.2.2.1.2 Primary Authentication and Key Agreement

5.2.2.1.2.1 Purpose

1) Mutually authenticate the UE and the network.

2) Establish a secure communication channel between UEs on the network.

5.2.2.1.2.2 Key Components

1) 5G Authentication and Key Agreement (5G-AKA) protocol.

2) Extensible Authentication Protocol for 5G (EAP-5G).

5.2.2.1.2.3 Process Overview

1) A UE sends an authentication request to the network.

2) The network challenges the UE with an authentication vector.

3) The UE responds with a calculated authentication response.

4) The network verifies the response and authenticates the UE.

5) Both parties derive session keys for secure communication.

5.2.2.1.3 Secondary Authentication

5.2.2.1.3.1 Purpose

1) Provide an additional layer of security for specific services or network slices.

2) Allow third-party authentication for certain applications.

5.2.2.1.3.2 Key Features

1) Can be initiated after the primary authentication.

2) May involve external authentication servers (e.g. AAA servers).

5.2.2.1.3.3 Use Cases

1) Access to specific network slices with heightened security requirements.

2) Authentication for IoT devices in specialized vertical applications.

5.2.2.1.4 Security Context Establishment

5.2.2.1.4.1 Purpose

Establish a secure environment for data exchange between UE and network.

5.2.2.1.4.2 Key Components

1) Non-Access Stratum (NAS) security context.

2) Access Stratum (AS) security context.

5.2.2.1.4.3 Security Features

1) Confidentiality protection: Encryption of user and signalling data.

2) Integrity protection: Ensuring data has not been tampered with during transmission.

5.2.2.1.5 Security Mode Command Procedure

5.2.2.1.5.1 Purpose

Negotiate and activate security algorithms for NAS and access stratum communications.

5.2.2.1.5.2 Process Overview

1) The network selects the appropriate security algorithms.

2) The network sends a Security Mode Command to the UE.

3) The UE verifies the command and configures the selected algorithms.

4) The UE responds with a Security Mode Complete message.

5.2.2.2 Network Domain Security

5.2.2.2.1 Focus

Network Domain Security focuses on security mechanisms between the Radio Access Network (RAN) and the Core Network (CN).

5.2.2.2.2 Key Components

1) Interface Protection:

   - IPsec tunnelling between RAN and CN elements.
   - Protection of N2 interface between RAN and AMF.
   - Security for F1 interface in disaggregated RAN deployments.
   - Secure communication between distributed RAN functions.

2) Control Plane Security:

   - Integrity protection of signalling messages.
   - Encryption of sensitive control information.
   - Protection against replay attacks.
   - Mutual authentication between network elements.

3) User Plane Security:

   - Data confidentiality between RAN and UPF.
   - Traffic flow security measures.
   - Protection of user data in transit.

- Secure handling of QoS information.

5.2.2.2.3 Security Features

1) Authentication Mechanisms:
    - Mutual authentication between RAN and CN nodes.
    - Certificate-based security.
    - Support for multiple security domains.
    - Dynamic key management.
2) Encryption Capabilities:
    - Support for multiple encryption algorithms.
    - Flexible security policy enforcement.
    - End-to-end encryption options.
    - Key rotation mechanisms.
3) Integrity Protection:
    - Message authentication codes.
    - Digital signatures for critical messages.
    - Sequence number protection.
    - Anti-tampering measures.

This comprehensive security framework ensures reliable and secure communication between RAN and CN elements in the telecom system.

5.2.2.3 Service-Based Architecture (SBA) Domain Security

5.2.2.3.1 Focus

Service-Based Architecture (SBA) Domain Security focuses on secure communication between various Network Functions (NFs) in the Core Network (CN).

5.2.2.3.2 Key Components

1) Service Registration Security:
    - Secure NF registration with NRF.
    - Protection of service discovery information.
    - Authentication of NF service profiles.
    - Validation of NF credentials.
2) Service Authorization:
    - Token-based authorization between NFs.
    - Role-based access control.
    - Dynamic policy enforcement.
    - Service-level authorization.

3) Service Communication Security:
    - TLS protection for HTTP/2 communications.
    - OAuth 2.0 framework implementation.
    - API security measures.
    - Message-level security.

5.2.2.3.3 Security Features

1) NF Authentication:
    - Mutual authentication between NFs.
    - Certificate-based security.
    - Service identity verification.
    - Credential management.
2) Service Access Control:
    - Fine-grained access policies.
    - Context-aware authorization.
    - Dynamic permission management.
    - Security token validation.
3) Communication Protection:
    - End-to-end encryption.
    - Integrity protection.
    - Replay protection.
    - Security association management.

5.2.2.3.4 Implementation Aspects

1) Security Policy Enforcement:
    - Centralized policy management.
    - Distributed policy enforcement.
    - Real-time policy updates.
    - Compliance monitoring.
2) Monitoring and Auditing:
    - Security event logging.
    - Access tracking.
    - Performance monitoring.
    - Security metrics collection.

5.2.3 Zero Trust Architecture in 3GPP

5.2.3.1 3GPP TR 33.894

3GPP TR 33.894 [i.5] has conducted a study on the applicability of zero-trust security principles in mobile networks, such as how to apply zero-trust principles in interactions between network functions. Referencing NIST SP 800-207 [i.6] zero-trust architecture, 3GPP TR 33.894 [i.5] also analysed the seven tenets of zero trust design listed in clause 6.3.5 of the present document.

5.2.3.2 Key Objectives

The key objectives of 3GPP TR 33.894 [i.5] are to:

1) Evaluate existing 5G security design against zero trust tenets.

2) Identify new mechanisms needed to fully implement zero trust.

5.2.3.3 Implementation Considerations

1) Analysis of seven tenets of zero trust design introduced in NIST SP 800-207 [i.6].

2) Assessment of alignment between existing 5G security design and each tenet.

3) Identification of gaps and necessary new mechanisms.

5.2.4 Ongoing Studies on Zero Trust

5.2.4.1 3GPP TR 33.794

3GPP TR 33.794 [i.7] further investigates enablers for zero-trust security in the 5G System.

5.2.4.2 Key Issues Under Investigation

3GPP TR 33.794 [i.7] investigates the following key issues:

1) Necessary data exposure for security evaluation and monitoring.

2) Integration of zero trust principles with existing 5G security architecture.

5.2.5 Emerging Trust Concepts in 3GPP

5.2.5.1 Distributed Trust

- **Needs addressed:** Enable advanced features like decentralized network roaming authentication and subscription-less network service access.

- **Potential approach:** Leverage Permissioned Distributed Ledger (PDL) technology/services.

5.2.5.2 User-Centric Trust

- **Application:** Telecom-enabled vertical applications (see [i.8]).

- **Example:** Providing differentiated services to multiple passengers in a vehicle with a single embedded UE.

5.2.6 Future Directions

The evolution of trust mechanisms in 3GPP networks is moving towards:

1) More flexible and context-aware trust models.

2) Integration of distributed trust concepts.

3) Enhanced focus on user-centric trust approaches.

These developments indicate a shift from traditional security-centric mechanisms to more comprehensive, adaptive, and user-focused trust frameworks in future telecom systems.

6 Existing Standards and Trust Mechanisms

6.1 Trust Computing Group (TCG)

6.1.1 Purpose of TCG

The Trusted Computing Group (TCG) aims to promote trusted computing technology [i.9]. TCG considers an entity trustworthy if it consistently behaves in an expected manner for a specific purpose.

6.1.2 TCG's Approach to Trust

6.1.2.1 Integrity Measurement and Verification

6.1.2.1.1 Definition

Integrity measurement is a systematic process of collecting, storing, and validating critical data that affects the integrity and trustworthiness of a platform.

6.1.2.1.2 Process

1) Measurement data is collected and stored in Platform Configuration Registers (PCRs).

2) Verification compares the measurement data with reference values to assess consistency.

6.1.2.2 Roots of Trust

6.1.2.2.1 Root of Trust for Measurement (RTM)

- A computing engine capable of reliably measuring platform integrity.
- Serves as the starting point of the trust chain.
- Example: BIOS boot block.

6.1.2.2.2 Root of Trust for Storage (RTS)

- A computing engine that performs secure storage.
- Stores integrity measurement data (e.g. in PCRs).
- Uses cryptography to protect data from tampering.

6.1.2.2.3 Root of Trust for Reporting (RTR)

- A computing engine that reliably reports information stored in RTS.
- Provides platform trustworthiness status information to other entities.

6.1.2.3 Transitive Trust

6.1.2.3.1 Purpose

The purpose of Transitive Trust is to systematically extend the trust boundary from a hardware-based root of trust to progressively higher-level components in the system stack, creating a continuous and verifiable chain of trust. This expansion enables trust to propagate from the foundational hardware components through the boot sequence, operating system, and ultimately to application-level software, ensuring that each component in the chain has been verified and can be trusted based on measurements and attestations from the previous trusted component.

6.1.2.3.2 Process

1) Starts from a hardware root of trust.
2) Gradually establishes a chain of trust to the OS and upper-layer software applications.
3) Conducts integrity measurement and verification at each step.

6.1.3 TCG Specifications and Implementations

6.1.3.1 Trusted Platform Module (TPM)

- Latest version: TPM 2.0.
- Often implements the functions of RTS and RTR.

6.1.3.2 Practical Implementation

- RTM: Typically implemented as the boot block of BIOS.
- RTS and RTR: Often implemented by the TPM hardware chip.

6.1.3.3 TPM Services

- TPM can provide various types of encryption services, including:
- Boot encryption.
- Hard disk encryption.
- OS and application software login encryption.

6.1.4 Example: Trust in a Desktop Computer

6.1.4.1 Aspects of Trustworthiness in a Desktop

6.1.4.1.1 Boot-time Integrity

- Detecting the integrity and correctness of the BIOS during power-on.
- Verifying the integrity of the Operating System during boot process.

6.1.4.1.2 Runtime Integrity

- Ensuring the hardware configuration remains untampered during operation.
- Verifying that the OS has not been modified unexpectedly.

6.1.4.1.3 Application Monitoring

- Continuous monitoring of all software applications during use.
- Detecting any unexpected changes or behaviour in running applications.

6.1.4.2 Trust Chain Establishment Steps

6.1.4.2.1 BIOS Verification

1) BIOS boot block (acting as RTM) measures and verifies the rest of the BIOS.
2) If verification succeeds, trust is established in the entire BIOS.

6.1.4.2.2 Bootloader Verification

1) Verified BIOS measures and verifies the bootloader.
2) Trust extends from BIOS to the bootloader upon successful verification.

6.1.4.2.3 OS Kernel Verification

1) Verified bootloader measures and verifies the OS kernel.
2) Trust chain now includes the OS kernel.

6.1.4.2.4 System Components Verification

1) OS kernel measures and verifies device drivers.
2) OS kernel also verifies system services.
3) Trust extends to these critical system components.

6.1.4.2.5 Application Verification

1) Trusted system components can then verify user applications.
2) Trust chain now extends all the way to the application level.

6.1.4.3 Continuous Trust Maintenance

- Runtime Measurements: Periodic re-measurement of critical components during system operation.
- Change Detection: Monitoring for any unexpected changes in system or application files.
- Attestation: Providing proof of the system's trustworthy state to external entities when required.

6.1.4.4 Benefits of This Approach

- Comprehensive Security: Provides security from the hardware level up to the application level.
- Early Detection: Allows for detection of compromises early in the boot process.
- Continuous Protection: Maintains a chain of trust throughout the system's operation.

The approach above ensures a continuous chain of trust from the hardware root to the user applications, providing a robust foundation for trusted computing in a desktop environment.

6.2 ITU-T

6.2.1 Recommendation ITU-T Y.3052

Recommendation ITU-T Y.3052 [i.10] examined trust provisioning in Information and Communication Technology (ICT) infrastructures and services. This study identified potential risks in physical, cyber, and social domains, highlighting how lack of trust can lead to issues such as malicious attacks, data and privacy breaches, and unexpected damages.

6.2.2 Trust Categorization

Recommendation ITU-T Y.3052 [i.10] categorizes trust into three types:

1) **Physical Trust:** Pertains to physical entities such as devices and sensors.

2) **Cyber Trust:** Relates to communication, networking, computing, and control systems.

3) **Social Trust:** Involves stakeholders like humans and organizations.

6.2.3 Direct and Indirect Trust

The study also distinguishes between two forms of trust:

1) **Direct Trust:** Based on a trustor's direct knowledge about a trustee, measured and obtained from available data.

2) **Indirect Trust:** Derived from the trustee's reputation, including personal history experiences and public evidence.

6.2.4 Aspects of Trust in ICT

Trust in ICT infrastructures and services encompasses:

1) **Ability:** Characteristics such as robustness, scalability, and reliability.

2) **Integrity:** Qualities like consistency, accuracy, and completeness.

3) **Benevolence:** Attributes including availability, assurance, and credibility.

6.2.5 Trust Provisioning Process

Recommendation ITU-T Y.3052 [i.10] views trust provisioning as a key capability for enabling trusted ICT infrastructure and services. The process includes:

1) **Data Collection and Management:** Gathering relevant information about entities and their interactions.

2) **Trust Analysis and Evaluation:** Analysing collected data to generate trust information or evaluation results.

3) **Dissemination of Trust Information:** Sharing trust-related data to support trust-aware decision-making.

4) **Trust Information Lifecycle Management:** Recognizing and managing the dynamic nature of trust over time.

6.3 NIST

6.3.1 Special Publication 800-207

The National Institute of Standards and Technology (NIST) Special Publication 800-207 [i.6] introduces the concept of Zero Trust (ZT) architecture, focusing on resource access control in network environments.

6.3.2 Core Principles of Zero Trust

6.3.2.1 Fundamental Concept

Zero Trust operates on the principle that trust is never granted implicitly but needs to be continuously evaluated.

6.3.2.2 Key Features

1) **Granular Access Control:** ZT advocates for granting minimal sufficient access privileges (e.g. read, write, delete) to resources.

2) **Location-Independent Security:** Trust is not based on physical or network location.

3) **Continuous Verification:** The system constantly verifies the trustworthiness of accessing entities.

6.3.3 Zero Trust Architecture (ZTA) Implementation

6.3.3.1 Adoption Trend

Many organizations and companies are incorporating ZTA principles when planning their enterprise network infrastructure.

6.3.3.2 Key Components

1) **Policy Decision Point (PDP):** Evaluates access requests and makes trust decisions.

2) **Policy Enforcement Point (PEP):** Implements the decisions made by the PDP.

6.3.3.3 Trust Zones

1) **Untrusted Zone:** The area between the resource accessor and PDP/PEP.

2) **Implicit Trust Zone:** The area between the resource and PDP/PEP.

6.3.3.4 Design Goal

ZTA aims to minimize the implicit trust zone by positioning PDP/PEP closer to the protected resources.

6.3.4 Rationale for Zero Trust

6.3.4.1 Changing Work Environments

1) **Remote Work:** Increase in employees working from non-corporate locations.

2) **Bring Your Own Device (BYOD):** Growth in personal devices accessing corporate networks.

6.3.4.2 Security Paradigm Shift

1) **Insider Threat Recognition:** Acknowledges that threats can originate from within the corporate network.

2) **Equal Treatment:** Treats corporate-owned environments with the same level of scrutiny as the public internet.

6.3.5 Key Tenets of Zero Trust Architecture

1) All data sources and computing services are considered resources.

2) All communication is secured regardless of network location.

3) Access to individual enterprise resources is granted on a per-session basis.

4) Access to resources is determined by dynamic policy.

5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

7) The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

This comprehensive approach to security in NIST's Zero Trust model provides a framework for organizations to implement more robust and adaptive security measures in increasingly complex and distributed network environments.

6.4 IETF

6.4.1 Significant approaches

The Internet Engineering Task Force (IETF) has developed two significant approaches related to trust in networked systems: Remote Attestation Procedures (RATS) and Trusted Execution Environment Provisioning (TEEP).

6.4.2 Remote Attestation Procedures (RATS)

6.4.2.1 IETF RFC 9334

IETF RFC 9334 [i.11] introduces RATS, addressing how one system can determine the trustworthiness of another system.

6.4.2.2 Key Roles in RATS

1) **Attester:** Provides evidence about its own state.

2) **Relying Party:** Decides whether to trust the Attester based on the evidence.

3) **Verifier:** Appraises the evidence presented by the Attester and generates attestation results.

6.4.2.3 RATS Process

1) Attester generates trust-related measurements.

2) Verifier appraises the evidence based on appraisal policies.

3) Relying Party uses the attestation results to make trust decisions.

6.4.2.4 Use Case Example: Network Endpoint Assessment

1) A device (Attester) generates trust-related measurements using hardware-based root-of-trust components.

2) The device sends signed measurements to a network node (e.g. a router acting as the Relying Party).

3) The measurements create a trustworthy report of the device's status.

4) The operator uses this report to determine appropriate access privileges for the device.

6.4.2.5 Trust Model in RATS

1) The Relying Party trusts the Verifier to accurately appraise the Attester's trustworthiness.

2) The Attester trusts the Verifier with sensitive information provided as evidence.

3) The Verifier trusts the manufacturer (often an endorser) to provide reliable endorsements for appraising the Attester's evidence.

6.4.3 Trusted Execution Environment Provisioning (TEEP)

6.4.3.1 IETF RFC 9397

IETF RFC 9397 [i.12] introduces the TEEP Architecture, addressing security concerns in device software and sensitive data.

6.4.3.2 Key Concepts

1) **Trusted Execution Environment (TEE):** A protected environment where code and data are safeguarded from external tampering.

2) **Trusted Application (TA):** An application component executed inside a TEE.

3) **Untrusted Application (UA):** An application running outside any TEE, in the Rich Execution Environment (REE).

6.4.3.3 TEEP Protocol

6.4.3.3.1 Overview

TA developers may interact with and manage TAs executed in a TEE (e.g. deploying, installing, updating and deleting TAs) using TEEP protocol [i.12]. The key components include:

1) **Trusted Application Manager (TAM):** Responsible for TA lifecycle management.

2) **TEEP Agent:** A processing module running inside the TEE that handles TAM requests.

6.4.3.3.2 Process Overview

1) TAM sends requests (directly or via a TEEP Broker) to the TEEP Agent.

2) TEEP Agent processes requests, potentially forwarding them to other TEE modules.

3) TEEP Agent returns response messages to TAM.

6.4.3.4 Security Measures

1) TEEP Agent evaluates TAM authorization before processing requests.

2) TEEP Agent verifies that TAs are correctly signed by authorized parties (e.g. TA developer or device administrator).

3) The system returns success or error messages based on operation outcomes.

These IETF approaches provide robust frameworks for establishing and maintaining trust in diverse network environments, from remote attestation of device trustworthiness to secure management of trusted applications within protected execution environments.

6.5 ETSI

6.5.1 Key Approaches

The European Telecommunications Standards Institute (ETSI) has developed several key approaches related to trust in digital systems, focusing on Decentralized Identifiers (DIDs), Self-Sovereign Identity (SSI), and reputation management.

6.5.2 Decentralized Identifiers (DIDs) and Trust Management

6.5.2.1 Overview

ETSI GS PDL 023 [i.13] specifies a DID operational framework built upon a Permissioned Distributed Ledger (PDL) platform service layer. The key PDL services for DIDs include:

1) DID resolver service.
2) DID document registry service.
3) Verifiable Credential (VC) data registry service.

6.5.2.2 DID-related Operations

The specification defines procedures for various DID-related operations on the PDL system, including:

1) DID publishing.
2) DID document publishing.
3) Verifiable Credential storage.

6.5.3 Self-Sovereign Identity (SSI) in Telecom Networks

6.5.3.1 Gap Analysis

The study [i.14] analyses existing identity mechanisms in 3GPP systems and identifies potential issues, such as:

- Limited social attributes associated with current identities (e.g. mobile phone numbers).
- Challenges in leveraging 3GPP system's trustworthy information for non-3GPP services.

6.5.3.2 Objectives

1) Build a telecom-native identity solution.
2) Enable flexible and seamless access to various network services across different operators or service providers.
3) Integrate 3GPP mobile operator credibility with third-party credibility.

6.5.4 Reputation Management in PDL Systems

6.5.4.1 Types of Reputation

ETSI GS PDL 015 [i.15] explores reputation management in PDL systems, proposing quantifiable and verifiable reputation as a crucial operational metric for decision-making in digital systems. There are several types of reputation:

1) Quality-of-Service (QoS) Reputation:
   - Indicates an entity's capability to meet performance goals.
   - Attributes: downtime, uptime, system responsiveness, transaction loss rate.
2) Trustworthiness Reputation:
   - Relates to security and involvement in fraudulent activities.
   - Example: Lower reputation for participation in malicious activities like "51 % attacks".

3) Commercial Reputation:

   - Indicates an entity's financial stability.
   - Attributes: payment history, credit score.

6.5.4.2 Reputation Management Aspects

1) Defining actions that influence reputation (positive or negative).
2) Establishing frequency of reputation re-evaluation.
3) Implementing mathematical formulas for reputation calculation.

6.5.5 Trust in Network Function Virtualisation (NFV)

6.5.5.1 Mapping RATS Roles to NFV Entities

ETSI GS NFV-SEC 024 [i.16] defines a security framework for managing NFV-based networks, drawing parallels with the IETF RATS architecture. For example, the mappings between RATS roles and NFV entities could be:

- RATS Attester ≈ NFV Secure Agent (SA).
- RATS Verifier and Relying Party ≈ NFV VNF Bootstrapping Service.

This comprehensive approach by ETSI provides frameworks for establishing and managing trust in various aspects of digital systems, from identity management to reputation systems and virtualized network functions.

6.6 eIDAS (910-2014)

6.6.1 eIDAS (910-2014) brief

eIDAS stands for "electronic IDentification, Authentication and trust Services" [i.17]. It is a Regulation (EU) No 910/2014 of the European Parliament and of the Council, adopted on 23 July 2014.

6.6.2 Key Objectives

1) Enhance trust in electronic transactions within the EU internal market.
2) Provide a common foundation for secure electronic interaction between citizens, businesses, and public authorities.

6.6.3 Main Components

6.6.3.1 Electronic Identification (eID)

- Ensures mutual recognition of eID schemes across EU member states.
- Allows citizens to use their national eIDs to access public services in other EU countries.

6.6.3.2 Trust Services

Regulates and standardizes electronic trust services, including:

- Electronic signatures.
- Electronic seals.
- Time stamping.

- Electronic registered delivery services.
- Website authentication.

6.6.4 Key Principles

1) **Technological Neutrality:** The regulation is designed to be independent of specific technologies.
2) **Non-Discrimination:** Electronic signatures and related trust services cannot be denied legal effect solely because they are in electronic form.
3) **Mutual Recognition:** eID schemes notified by one member state needs to be recognized by others.

6.6.5 Impact

1) **Cross-Border Transactions:** Facilitates secure electronic transactions across EU borders.
2) **Digital Single Market:** Supports the EU's goal of creating a digital single market.
3) **Standardization:** Promotes standardization of trust services across the EU.
4) **Legal Certainty:** Provides a clear legal framework for electronic identification and trust services.

6.6.6 Implementation

- Came into effect on 1 July 2016.
- Replaced the earlier eSignature Directive [i.18].
- Requires ongoing adaptation and implementation by EU member states.

eIDAS plays a crucial role in building trust and security in the digital environment within the European Union, facilitating safer online transactions and supporting the growth of the digital economy.

7 Use Cases for Trust in Telecom System

7.1 Introduction

This clause is to introduce a few user cases related to trust in the telecom system and corresponding key issues will be derived from those use cases in clause 8.

7.2 Use Case 1 - Decentralized Trust Evaluation

Existing cellular wireless systems (e.g. 5G System) provide various security functions as defined in 3GPP TS 33.501 [i.4], such as primary authentication during registration, secondary authentication during Protocol Data Unit (PDU) session establishment, NF service authorization, data plane encryption and integrity protection, etc. For example, Network Function (NF) service authorization in 5GS can be static authorization (in which some local authorization policies are maintained at NF service producer and Network Repository Function, or NRF) or token-based authorization (in which NRF can grant an access token to a NF service consumer).

In general, 3GPP system mainly involves security related mechanisms and has limited considerations of trust evaluation, for example:

- 3GPP TS 23.304 [i.19] specifies Proximity based Services (ProSe) in the 5G System and a number of features have been defined. For example, 5G ProSe UE-to-Network Relay enables indirect communication between the 5G network and UEs which are out of coverage of the network. 5G ProSe UE-to-UE Relay enables indirect communication between two 5G ProSe End UEs who cannot build direct communications between each other and needs a 5G ProSe UE-to-UE Relay to be used as an intermediate node. A related ETSI TS 133 503 [i.20] focuses on the security aspects of ProSe in the 5G System. For example, ETSI TS 133 503 [i.20] specifies how security establishment (e.g. generating security parameters such as key materials, and security policy negotiation) can be conducted between a 5G ProSe UE-to-UE Relay and a Source End UE, by assuming that relaying UE is trustable (but how the relaying UE can be trusted is not addressed in ETSI TS 133 503 [i.20]).

- Trust covers concerns beyond security. Trust enablement is a focused feature for 3GPP Release 19. 3GPP TR 33.794 [i.7] studies enablers for zero-trust security in the 5G System by investigating several key issues, such as what kinds of data exposure is necessary to enable security evaluation and monitoring, etc. In the meantime, 3GPP TR 33.794 [i.7] mainly considers the NF security, which requires collecting various data for dynamically authenticating and authorizing the NF service access requests sent from service consumers. With respect to the solutions, a more centralized trust enablement approach is considered for enabling zero-trust in the core network (e.g. using Policy Decision/Enforcement Point defined by NIST SP 800-207 [i.6]).

- However, telecom systems are becoming more decentralized, e.g. any two UEs may directly interact with each other without being managed/monitored by the network-side NFs. Therefore, future telecom systems may also require decentralized trust management solutions, e.g. trust management among UEs in the field. Overall, the trust management may cover various mechanisms related to trust, such as trust evaluation, trust enablement, trust exposure, etc.

In future telecom systems, UEs (e.g. one 5G ProSe UE-to-UE Relay provides traffic relaying service to two 5G ProSe End UEs) may not only need to conduct basic authentications, but also need to evaluate whether their counterparts can also be trusted on their characteristics/behaviour/performances. When UEs are interacting, various data may be collected from the field for supporting trust evaluation regarding e.g. whether the 5G ProSe UE-to-UE Relay has a sufficient trust for providing excellent relaying service to the 5G ProSe End UEs. Collecting data and sending it back to the core network for trust evaluation may incur additional overhead and decentralized trust evaluation may be desired for future telecom systems. For example, a near-by entity hosting a Trust Management Function (TMF) can be used to support trust evaluation of UEs in the field:

- In a basic scenario, there could be an (pre-)authorized/trustful TMF instance (e.g. TMF-1) deployed by the network operator. A piece of trust evaluation result may also contain various useful information, including but not limited to e.g. whose trust was evaluated (e.g. UE-1), on which aspect (e.g. about the trust of UE-1 acting as a 5G ProSe UE-to-UE Relay), who conducted the trust evaluation (e.g. TMF-1), the latest trust index produced by TMF-1, whether the trust evaluation result is accurate (e.g. which could be ranked by involved stakeholders, e.g. who consumed the result), etc. The above-mentioned useful information may be recorded in a secure and accessible medium (such as distributed ledgers, e.g. in PDL systems) in order to support trust management traceability.

- In an advanced scenario, various UEs (e.g. government vehicles, 3rd-party or a company-owned UE, or even a private UE) could host TMF instances and provide services (such as trust evaluation) to nearby customers. In this scenario, the reputation of a specific TMF instance may be a concern and additional information may also be recorded in the distributed ledger, such as whether a specific TMF instance has a good reputation (which could also be reported/ranked by involved stakeholders), etc. The distributed ledgers may be leveraged for storing historical work records/performances/outputs/ranks of a TMF instance, which can be traced/analysed/referred at any time in order to establish a TMF reputation tracking and maintenance system.

7.3 Use Case 2 - Granular and Customized Trust Evaluation

As defined in clause 4, trust is an essential input for various decision making in telecom systems and it is usually measured or calculated in a quantitative or a qualitative manner, e.g. represented as a Trust Index (generated via trust evaluation). However, trust index is an overall metric, which is often calculated based on the aggregation of one or more Trust Indicators (depending on specific trust evaluation criteria being adopted), which may cover various aspects, including but not limited to security, privacy, resilience, performance, robustness, scalability, reputation, availability, accuracy, reliability, consistency, etc. In future telecom systems, trust evaluation and management need to be enhanced in two folds:

- First, the below example illustrates that a single trust index cannot reflect the full facets of an entity and trust evaluation of a given entity should be more granular. Taking the previous 3GPP ProSe example introduced in clause 7.2, a specific UE-1 may act in two roles and an illustration is shown in Figure 2:

  - as a 5G ProSe UE-to-UE Relay, e.g. UE-1 may provide relaying service to another UE-2, where UE-1 relays traffic between UE-2 and UE-3; and

  - as a 5G ProSe UE-to-NW Relay, e.g. UE-1 may also provide relaying service to UE-2, where UE-1 helps UE-2 in connecting to the network.

  However, UE-1 may have different levels of trust when providing different types of services. For example, UE-1 may achieve sufficient trust level when UE-1 is in the role of 5G ProSe UE-to-UE Relay. However, UE-1's trust level may be low when UE-1 is acting as a 5G ProSe UE-to-NW Relay since UE-1 currently is having a poor connection with the access network. From this example, it can be seen that a single entity (such as UE-1) may have multiple trust indexes, each of them being associated with a specific function/service/aspect/role of the entity.

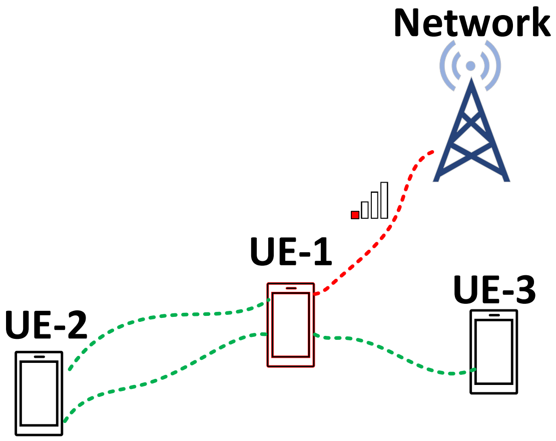

Figure 2: UE-1 Has Two Different Roles For Serving UE-2 and UE-3

- Second, the usefulness of a given trust index may also depend on what trust evaluation criteria has been adopted and different stakeholders may have differentiated trust evaluation criteria when initiating trust evaluations (even on the same entity). In general, a trust index is generated via trust evaluation process, which is often conducted by adopting a certain set of trust evaluation criteria, which may specify the instructions such as:

  - What kinds of trust indicators should be focused?

  - What kinds of algorithms should be adopted for calculating each focused trust indicator and/or the aggregated trust metric, i.e. trust index?

  - During calculation of trust index, the values of certain parameters may be configured, such as the weight of each trust indicator, etc.

Still taking the previous 3GPP ProSe example introduced in clause 7.2, UE-1 may act as a 5G ProSe UE-to-NW Relay and may be serving both UE-2 and UE-3 so that UE-2 and UE-3 could connect to the network when out of coverage and an illustration is shown in Figure 3. UE-2 and UE-3 may have different and/or customized preferences regarding how to evaluate UE-1's trust. For example:

- UE-2 prefers to evaluate UE-1's trust level by focusing on two major trust indicators like reliability and availability, since UE-2 cares more about whether UE-1 can always be available for relaying UE-2's traffic at any time.
- In comparison, UE-3 prefers to evaluate UE-1's trust level by focusing on the other two trust indicators such as scalability and robustness, since UE-3 cares more about whether UE-1 can always manage to relay the burst traffic from UE-3 without dropping any packet.

This example also shows that even if UE-2 and UE-3 are using the same service provided by the same entity (i.e. UE-1), UE-2 and UE-3 may choose to adopt different set of trust evaluation criteria when they want to evaluate UE-1's trust.

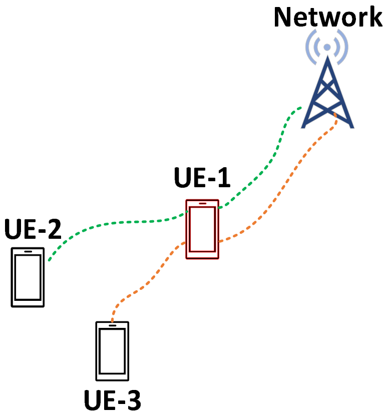

Figure 3: UE-1 Has One Role For Serving UE-2 and UE-3

7.4 Use Case 3 - Enabling User-centric Trust

3GPP TR 23.700-32 [i.21] studies how to enhance the 5G System with the utilization of user-specific identities to enable improved and differentiated user experience. For example, this study focuses on how to support the identification of a human user of a UE's 3GPP subscription when the human user accesses 5G services using a user identifier.

Beyond identifying a user, the trust of the user (e.g. her behaviours/status/context) may also need to be taken into account when future telecom systems provide services to the user. The reason is that a user may access services with highly dynamic behaviour and in a highly dynamic context. Dynamic user behaviours and context means that a user may access services from a new location, or access services via different devices at different times, etc. Such dynamic behaviours and context may lead to changes of the trustworthiness of the user and associated UE/device(s). For example, in the Scenario 1 of Figure 4, UE-1 may move to a new location while it is accessing a network service provided by a NF (via UE-1). Another example, in the Scenario 2 of Figure 4, UE-1 may choose to use a different UE (e.g. UE-2) other than UE-1 while it is accessing a network service provided by a NF.

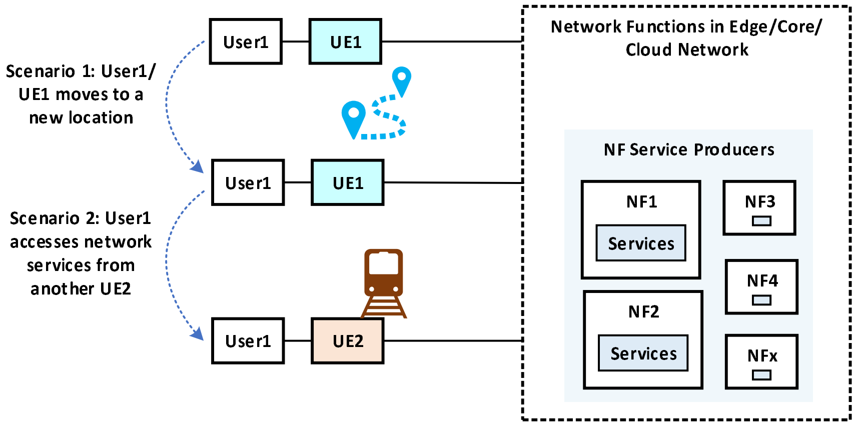
Scenario 1: User1/ UE1 moves to a new location
Scenario 2: User1 accesses network services from another UE2
User1
UE1
User1
UE1
User1
UE2
Network Functions in Edge/Core/ Cloud Network
NF Service Producers
NF1
Services
NF2
Services
NF3
NF4
NFx

Figure 4: Dynamic Context and Behaviour of UE-1 (Leading to Changing Trust)

However, currently 5GS does not consider dynamic user context and does not well support dynamic user authentication. For example, primary authentication in 5GS is based on statically configured information (i.e. the root key in USIM), which cannot reflect or capture the dynamically-changing user context and the resulting user trust index. In token-based authorization in 5GS, an access token cannot reflect or capture the dynamically-changing user context and user trust index either.

User-centric trust should be considered in future telecom systems. For example, when a user requires to access network services, in addition to enabling the basic device-level trust (e.g. supported by existing security mechanisms, such as primary authentication in 5GS), user trust-aware authentication/authorization considering user trust based on the dynamically changing user behaviour and contexts should be enabled and taken into account. To implement user trust-aware mechanisms, the Trust Management Function (TMF) introduced in clause 7.2 can be leveraged. Note that the TMF benefits from leveraging distributed ledgers to calculate trust index. For example, when a service producer receives a service access request sent from a user, the service producer could ask TMF to evaluate the latest trust of the user based on user's runtime context/characteristics/status, etc. The service producer may take into account the latest trust of the user and dynamically determine whether to approve the service access request. In the meantime, the trust index records may be stored in the distributed ledger using PDL platform services (such as Storage Platform Service), which can not only enable trust management traceability, but also may provide reference values for the future. For example, TMF may use PDL Storage Platform Service or Discovery Platform Service to identify and analyse historical trust index records stored in the PDL systems to estimate the trust of the user. Such an estimation could be regarded as a calibration component when there is no sufficient real-time data for calculating the latest trust of the user.

7.5 Use Case 4 - Trust-aware UE-to-UE Interaction Model (Service Producer & Service Consumer) and Trust Enablement using Smart Contract

Existing ProSe services already enables basic type of interactions between UEs on the connectivity level. Future telecom systems may be more decentralized and UEs may collaborate and interact with each other in a more advanced manner for supporting various emerging applications beyond connectivity. This use case introduces a first type of UE-to-UE interaction model (denoted as **Interaction Model-1**), in which trust is an essential aspect to be considered.

In this interaction model, two roles are involved, one is Service Producer and the other is Service Consumer. It is assumed that the service producer has already pre-installed necessary software and is ready to provide services to service consumers. An example of Interaction Model-1 is illustrated in Figure 5. Still taking the previous 3GPP ProSe example introduced in clause 7.2, UE-1 (as a service producer) may act as a ProSe UE-to-NW Relay by providing communication (e.g. relaying) service to another UE-2 (as a service consumer). More than that, UE-1 may also provide other types of services to UE-2:

- UE-1 may provide computing-related services, which may cover various application scenarios.

EXAMPLE 1: UE-2 is running an AR-related applications and may need UE-1 to help in complex AR processing.

- UE-1 may also provide sensing-related services to UE-2. For example, UE-2 may send service access requests to UE-1 in order to ask UE-1 to capture desired sensory information from the real-world using UE-1's sensing capabilities.

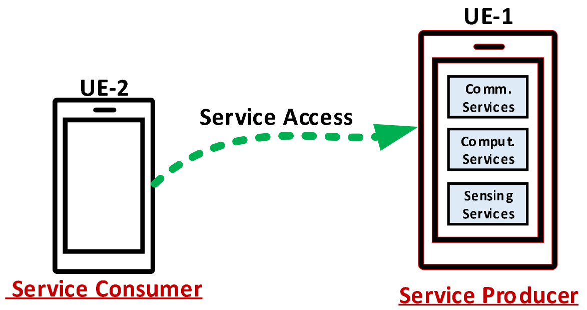

Figure 5: UE-to-UE Interaction Model-1: Service Producer and Service Consumer

In the meantime, UEs (acting as service producers and service consumers) may not be in the same trust domain. It is likely that UEs may not act as commercial service producers with a "pre-assumed" level of trust. Trust evaluation is to evaluate the trust of an entity, but sometimes evaluation is not sufficient and further trust enablement may be needed.

EXAMPLE 2: When a service consumer intends to access the services provided by a service producer, the consumer may specify trust-related requirements for service provisioning.

EXAMPLE 3: The consumer may require the producer to achieve high trust when provisioning the required service(s).

However, the reality is that even if the service producer accepts the service requests sent from the consumer, the service producer may not have an obligation to meet the trust-related requirements specified by the consumer since both producer and consumer may be personal UEs/devices.

Since UE-to-UE interactions in future telecom system becomes more decentralized, a corresponding decentralized trust enablement solution is desired. Distributed ledger technology, and in particular, the smart contract mechanism can help in this case. For example, when a consumer intends to access the services provided by a service producer, they could establish a smart contract, in which various requirements on the trust can be prescribed. Such a smart contract can be deployed into distributed ledgers systems e.g. by leveraging ETSI PDL platform services (For example, smart contract deployment and execution often creates transactions to be recorded in the PDL). If the producer decides to accept the service access request and a smart contract is established, the producer will have an obligation to accomplish its commitments (e.g. what level of the trust needs to be achieved). If failed, certain penalty may be incurred, which can automatically be enforced by the smart contract. Note that, service enablement using smart contract may also be leveraged for supporting UE-to-UE Interaction Model-2 to be introduced in clause 7.6.

7.6 Use Case 5 - Trust-aware UE-to-UE Interaction Model (Task Initiator & Task Participant)

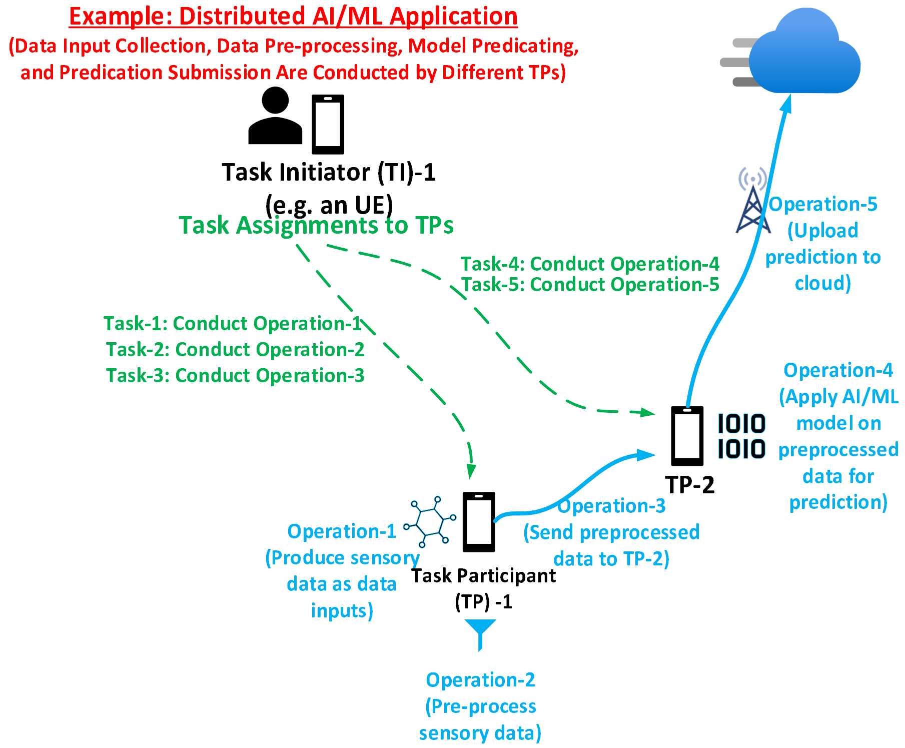
Example: Distributed AI/ML Application
(Data Input Collection, Data Pre-processing, Model Predicating, and Predication Submission Are Conducted by Different TPs)
Task Initiator (TI)-1
(e.g. an UE)
Task Assignments to TPs
Task-4: Conduct Operation-4
Task-5: Conduct Operation-5
Task-1: Conduct Operation-1
Task-2: Conduct Operation-2
Task-3: Conduct Operation-3
Operation-5
(Upload prediction to cloud)
Operation-4
(Apply AI/ML model on preprocessed data for prediction)
1010
1010
TP-2
Operation-3
(Send preprocessed data to TP-2)
Operation-1
(Produce sensory data as data inputs)
Task Participant (TP) -1
Operation-2
(Pre-process sensory data)

Figure 6: UE-to-UE Interaction Model-2: Task Initiator (TI) and Task Participant (TP)

This use case introduces a second type of UE-to-UE interaction model (denoted as **Interaction Model-2**), in which trust is also an essential aspect to be considered.

In this interaction model, two roles are involved: Task Initiator (TI) and Task Participant (TP):

- A TI initiates a task, which could be a human user, a UE/device/gateway, a software application installed on a UE, etc. A TI may assign a task to another entity as a TP.
- A TP receives a task from the TI and conducts the operations required by the task. A TP could also be a UE, a device, etc.

Overall, Interaction Model-2 focuses on task assignment between TIs and TPs. A practical example is shown in Figure 6, which illustrates how to realize a distributed AI/ML application via task assignment to multiple TPs: TI-1 (which could be a UE) intends to deploy an AI/ML model for predictions in a distributed way. In order to realize this application, the following operations are involved:

- The AI/ML model needs to be sent to distributed entities (e.g. multiple TPs).
- The input data needs to be collected.
- The collected input data needs to be fed into the AI/ML model.
- The AI/ML model processes the collected input data and produces prediction results.
- The prediction results may need to be submitted to a remote entity for further processing.

To realize the above distributed AI/ML application, TI-1 could identify multiple TPs to collaboratively conduct the above operations. TI-1 may assign different tasks to multiple TPs for execution, each of them being responsible for conducting one or more task(s). Here, a given Task prescribes what a specific type of operation(s) that TI requests a TP to perform, which could be communication-related, computing-related or sensing-related operations. For example, TI-1 may create five tasks related to the distributed AI/ML application and each task is to ask a particular TP to conduct a certain type of operation:

- TI-1 may assign Tasks 1-3 to TP-1 and assign Tasks 4-5 to TP-2. TP-1 may first use its onboard sensors to generate the needed data (corresponds to Operation-1 required by Task-1, which is a sensing-related operation).
- Then, TP-1 may preprocess the data (corresponds to Operation-2 required by Task-2, which is a computing-related operation) so that the data can be ready for use as input into an AI/ML model.
- After that, TP-1 may deliver the pre-processed data to TP-2 (corresponds to Operation-3 required by Task-3, which is another communication-related operation).
- Once TP-2 obtains the data, it can input the data into an AI/ML model, which will process the data and produce a prediction result (corresponds to Operation-4 required by Task-4, which is a computing-related operation).
- Finally, TP-2 may submit the prediction result to a remote entity (corresponds to Operation-5 required by Task-5, which is a communication-related operation).
- Once those five tasks are assigned to TP-1 and TP-2, they could start performing those tasks, which will realize the distributed AI/ML application.

Trust is an essential aspect to be considered in both UE-to-UE interaction models discussed above since UE acting as a TP may not be a commercial-level device with sufficient resource capability/capabilities. For example:

- A TI may ask TMF to analyse the historical trust evaluation results recorded in distributed ledgers (e.g. using ETSI PDL systems) in order to evaluate or estimate the potential trust of a TP for performing a specific task before the TI makes a formal decision to assign the task to the TP. This may avoid undesired task assignment, which may not only cause unnecessary overhead (e.g. resource waste due to task assignment, deployment and configuration), but also time waste and unsatisfactory task execution results.
- After the TI assigns a task to a TP for execution, the TI may still need to evaluate the practical trust of a TP while TP is performing the task, e.g. whether the TP achieves sufficient trust for performing the task and producing desired results/performance.

8 Key Issues

8.1 Introduction

The following key issues are derived from the use cases as described in the clause 7. A key issue may be applicable to multiple use cases and the corresponding mappings between key issues and uses cases are shown in Table 1:

- Key Issue #1 - Trust Evaluation in Different Task Lifecycle Stages
- Key Issue #2 - Granular and Customized Trust Evaluation
- Key Issue #3 - Trust Data Recording, Discovery and Retrieval
- Key Issue #4 - TMF Registration and Discovery
- Key Issue #5 - Trust Enablement using Smart Contract
- Key Issue #6 - Enabling User-Centric Trust
- Key Issue #7 - Service Interaction Incorporating Trust Index

Table 1: Mapping between Key Issues and Use Cases

Key Issues	Use Case 1: Decentralized Trust Evaluation	Use Case 2: Granular and Customized Trust Evaluation	Use Case 3: Enabling User-centric Trust	Use Case 4: Trust-aware Service Producer & Service Consumer Interaction	Use Case 5: Trust-aware Task Initiator & Task Participant Interaction
KI #1: Trust Evaluation in Different Task Lifecycle Stages	X	X			
KI #2: Granular and Customized Trust Evaluation	X	X			
KI #3: Trust Data Recording, Discovery and Retrieval	X	X			
KI #4: TMF Registration and Discovery	X	X			
KI #5: Trust Enablement using Smart Contract				X	
KI #6: Enabling User-Centric Trust			X		
KI #7: Service Interaction Incorporating Trust Index				X	X

8.2 Key Issue 1 - Trust Evaluation in Different Task Lifecycle Stages

In future decentralized telecom systems, UEs may be assigned with and undertake various tasks (e.g. communication, computing, sensing) and collaborate with each other in order to realize a telecom system function or a vertical application. However, UEs or entities involved in collaboration are unlikely to have pre-assumed trust among each other, which significantly affects the performance and success of the system function to be realized or the vertical application to be supported. This key issue focuses on how to enable decentralized trust evaluation and management in future telecom systems, which could provide trust evaluation support in different task lifecycle stages (e.g. from task deployment stage to task execution stage). Solutions to this key issue will address:

- Task deployment stage involves with various task assignments to different UEs/Devices, in particular, trust estimation is an essential factor to be considered during the decision making regarding whether a task should be assigned to the UE for execution. The question is: How to leverage historical trust-related data (which may be stored in PDL platform), in order to estimate the potential trust level of a UE (acting as a TP) for performing a specific task? A task should not be assigned to a UE/device with low trust potential.

- Task operation stage involves task executions performed by different UEs/devices. How TMF could monitor the practical trust of a UE (acting as a TP) through periodical trust evaluation while the UE is executing the task(s)? What kinds of information should be included in a trust evaluation record to be stored in the PDL?

8.3 Key Issue 2 - Granular and Customized Trust Evaluation

A UE (e.g. acting as a TP) may have differentiated trust potentials for performing different tasks. Another observation is that TMF conducts trust evaluation based on a certain set of trust evaluation criteria, but different stakeholders may have differentiated trust evaluation criteria for the same UE. This key issue focuses on how to enable granular and customized trust evaluation in future telecom system and solutions to this key issue will address:

- How to enable granular trust evaluation by defining e.g. a task-level trust index of a UE (acting as a TP)? For example, a task-level trust index mainly reflects the trust of UE for performing a specific task.

- What kinds of information should be collected for calculating a task-level trust index? For example, detailed information reflects the request processing during the execution of a specific task may be needed.

- To enable customized trust evaluation, how could TMF collect trust evaluation needs (e.g. preferred trust evaluation criteria) from various stakeholders, e.g. using a standard template? Stakeholders may also modify their preferred trust evaluation criteria from time to time, then another issue is how TMF can manage these changes.

8.4 Key Issue 3 - Trust Data Recording, Discovery and Retrieval

Various trust-related data (such as trust evaluation records) can be stored in the PDL platform, which could provide valuable reference. This key issue focuses on how to efficiently enable trust data recording, discovery and retrieval. Solutions to this key issue will address:

- How to leverage distributed ledger technology (such as PDL platform) to support recording/maintaining trust related data, such as trust evaluation records?

- In case granular and customized trust evaluation is adopted, the resulting trust evaluation records may also become more granular, e.g. with more specific applicable scopes and scenarios. How to efficiently identify useful/applicable trust evaluation records stored in PDL? For example, a trust evaluation record contains a trust index of UE-1 for performing a computing task, which was generated based on a specific set of trust evaluation criteria. However, such a record may not be a valuable reference to a stakeholder, e.g.:

    1) who wants to know UE-1's trust for performing a communication task; or

    2) who prefers to evaluate UE-1's trust for performing the same computing task but using a different set of trust evaluation criteria.

- How to organize the PDL storage for facilitating trust records retrieval?

EXAMPLE: Trust evaluation records can be stored in the same ledger if they adopted the same set of trust evaluation criteria, or related to the same entity (e.g. a particular TP), etc.

8.5 Key Issue 4 - TMF Registration and Discovery

To support decentralized trust management in future telecom systems, multiple entities can act as TMFs. This key issue focuses on how to efficiently conduct TMF discovery. Solutions to this key issue will address:

- How to leverage a TMF registration repository to store TMF availability information? For example, entities hosting TMF instances can register themselves at a TMF registration repository.

- Trust evaluation conducted by TMF has certain overhead. How to conduct TMF discovery in the repository for discovering an appropriate TMF instance while minimizing the overhead incurred by trust evaluation?

- When TMF registration repository is unavailable, how can a TMF be discovered directly by other entities in an ad hoc approach (e.g. the TMF could proactively announce its existence)?

8.6 Key Issue 5 - Smart Contract-based Trust Enablement

Trust can be evaluated and measured. However, beyond evaluation, trust may also be proactively enabled in case certain trust-related requirements have to be met during task execution. This key issue focuses on how to realize decentralized trust enablement using smart contract technology (e.g. enabled by PDL system). Solutions to this key issue will address:

- For a given task assigned to a TP by a TI, how to collect trust related requirements, e.g. what kind of trust level should be met by the TP when performing the task?

- How to establish a smart contract between the TI and the TP, and what kinds of information elements should be recorded in the smart contract so that TP will have an obligation to accomplish its commitments to meet the trust requirements?

- How to leverage existing PDL platform services to facilitate smart contract establishment, deployment and enforcement?

- In case TP has difficulties (e.g. short on available resources) in meeting trust requirements specified in a smart contract during a task execution, how TP can take proactive actions on task management (e.g. resource adjustment across different tasks or task migration)?

- In addition to smart contract approach, what other approaches can be used for enabling or improving trust?

8.7 Key Issue 6 - Service Access Considering User-Centric Trust

Existing trust mechanisms for service access in 5G telecom system (such as primary authentication) do not capture dynamically-changing user context, but the trust of the user (i.e. the expectation about user's status/context/behaviour/performance/etc.) also needs to be taken into account in future telecom systems. This key issue focuses on how to realize user-centric trust mechanisms and how service access in future wireless system can leverage such mechanisms so that the service access can be user-aware and trustworthy. Solutions to this key issue will address:

- The first question is to identify what kinds of factors may affect the user's trust?

EXAMPLE: TMF may evaluate the latest trust of the user based on user's runtime context/characteristics/status, etc.

- Existing 5GS only supports USIM-based primary authentication, how to expand it to realize user-centric trust authentication in future telecom system by leveraging dynamically-changing user context/characteristics (e.g. in case where the same UE is shared by multiple users, authentication can be conducted based on user credential/context instead of only based on USIM)?

- What other telecom system features/procedures (e.g. roaming) can benefit from the consideration of user's real-time trust level?

8.8 Key Issue 7 - Service Interaction Incorporating Trust Index

Existing telecom system (e.g. 3GPP 5G system) has defined different communication and interaction models for two or more Network Functions (NF) (e.g. a service producer and a service consumer) to interact with each other, such as Direct Communication, In-Direct Communication via a Service Communication Proxy (SCP), etc. This key issue focuses on how to incorporate or leverage trust information (e.g. the trust indexes of service producers and/or service consumers) during various service interaction models to realize trustworthy service interaction in future telecom systems. Solutions to this key issue will address:

- Service producers and service consumers (which could be UEs in the field or NFs in the core network) may need to be discovered and matched with each other (e.g. via a network repository) before interaction. The first question is how to enable trust-aware registration of service producers to a network repository.

EXAMPLE: A service producer can indicate its trust-related capabilities/scores during registration as well as its trust-related requirements on the potential service consumers that it is willing to serve.

- How can the network repository enable trust-aware service producer discovery to help a service consumer to find desired service producer(s) meeting certain trust requirements, and vice versa?

- How can service access using different communication models leverage dynamic trust information (e.g. the latest trust index of an entity measured by TMF) so that service access can be more trust-aware?

9 Conclusions and Next Steps

9.1 Summary

The present document discussed various trust management use cases and described key issues associated with them in the context of telecom systems. The present document started with a survey on trust mechanisms being developed in various SDOs. Then, it was explained why trust is an essential aspect for the next-generation telecom systems, such as 6G. In particular, the present document presented a number of use cases justifying a few unique challenges when realizing trust management in future telecom systems, including trust evaluation, trust enablement, user-centric trust, etc. A number of key issues were derived based on the presented user cases. Finally, recommendations for next steps are included in the next clause.

9.2 Recommendations for Next Steps

The present document summarized a list of key issues, which could be regarded as a basis for the normative work. It is recommended that the following topics be in the scope of the normative work:

- Next-generation telecom systems feature more decentralized architecture and more diverse distributed computing/communication/sensing tasks to be assigned to UEs/devices for execution. Specifications on trust evaluation mechanisms throughout the task lifecycle and how to support decentralized trust evaluations using PDL capabilities are needed.

- Different stakeholders in next-generation telecom systems may have varied views/choices regarding how trust should be evaluated and what key trust indicators should be focused. Specifications on enabling customized trust evaluation are also needed.

- UEs/devices in future telecom systems may act as service producers. Thus, specifications on enabling trust-aware service interaction to/from UEs/devices are needed.

- User has been included as an identifiable entity in 5G system, which will continue to exist in future telecom systems. Specifications on how to further realize user-centric trust are needed.

- Trust enablement is required for decentralized telecom applications where no pre-assumed trust can be made between UEs (as service producers/consumers). Specifications on supporting decentralized trust enablement using PDL-based smart contracts need to be developed.

- It is also recommended to identify other potential issues related to trust management, which may not be fully covered in the present document.

History

Document history		
V1.1.1	May 2025	Publication