**3GPP TSG SA WG 1 Meeting #111 S1-253038r3**

**25-29 August 2025, Goteborg, Sweden** *(revision of S1-253038 was 3030)*

**Source: InterDigital**

**pCR Title: Trustworthiness assessment**

**Draft Spec: 3GPP TR 22.870 v0.3.1**

**Agenda item: 8.1.3**

**Document for: Approval**

**Contact: Catalina Mladin,** **Catalina.Mladin@Interdigital.com**

*Abstract: This contribution introduces support for Network-assessed Trustworthiness in the TR.*

**1. Introduction**

This contribution introduces clause 5.y with support for Network-assessed Trustworthiness within System and Operation Aspects clause of the TR. In addition, an Annex for the study of the concept of Trustworthiness in SA, in order to ensure that this work is aligned with that of other 3GPP WGs and the ecosystem.

This content is complemented by S1-253039r1 addressing scenarios enabled through Trustworthiness.

**2. Reason for Change**

To provide support for Trustworthiness and related services in 6G

**Notes for S1-253028r3:**

* Simplified PR-1
* Added two ENs

**Notes for S1-253038r2:**

* Added ppt with highlights
* Simplifications of text (deletions, accepted)
* Corrections based on rapporteur feedback, tracked

**Notes for S1-253038 rev 1 and updates relative to S1-253038:**

* Addition of the last two paragraphs in 5.y.1, under the heading “Exposure and additional monetization opportunities”, addressing the value-add of implementing Trustworthiness in the 6G Network.
* Addition of new clause TBD.1.4 which seeks to clarify:
	+ The difference between Network-assessed Trustworthiness and its exposure. Network-assed trustworthiness is clarified as functionality enabling network operations and management, especially in distributed cloud deployments. This is similar to the Trustworthiness assessments for AI/ML Models introduced in TR 28.908, although it is TBD whether the broader concept introduced here is an MnS functionality.
	+ Clarification that there is no direct esposure of Trustworthiness assesemnts outside the 6G Network.
	+ Exposure based on Network-assed trustworthiness is value-add functionality which relies on Third-Party specific policies (termed “Affinity Policies”).
* Note that S1-253039r1 complements this text and provides examples of use of the Trustworthiness assesements and the exposure determined via Affinity policies
* Various editorials, simplifications and changes for text alignement have been also introduced.

**Notes on the use of the new references:**

* 3GPP TR 28.908 Provides information about how Trustworthiness is proposed to be implemented in 3GPP in the context of AI/ML Model assessments.
* [ITU-T-2022][NextG][NGMN] are three independent resources for appreciating how a variety of peer organizations have studied Trustworthiness and are specially calling for implementation of this concept in 6G.
* [ISO/IEC] and [ITU-T-2017] are used first to demonstrate the depth of recognition of the concept of Trustworthiness in the industry. They are also used as references to appreciate how the nomenclature used in this proposal related to the that in the industry.
* [ITU-T-2017] is also used as reference for one example of implementation in clause TBD.1.3.
* [Veith] is used for its analysis of the relationship created between Trust and Trustworthiness by the exiting technologies, since terminology can vary between subfields. In addition, it provides insight into the necessity and value of associating non-security characteristics included in Trustworthiness with Trust Anchor functionality.

**3. Conclusions**

Trustworthiness provides important value to the 6G Network.

**4. Proposal**

It is proposed to agree the following changes to 3GPP TR 22.870 v 0.3.1 .

\* \* \* First Change \* \* \* \*

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[3GPPTR28908] 3GPP TR 28.908 “Study on Artificial Intelligence/Machine Learning (AI/ML) management”

[ISO/IEC] ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary (https://www.iso.org/standard/81608.html)

[ITU-T-2017] ITU-T Technical Report, “Trust in ICT”, 2017 (<http://handle.itu.int/11.1002/pub/80fd6f3d-en>.).

[ITU-T-2022] ITU-T Technical Specification, “Trustworthiness evaluation for autonomous networks including IMT-2020 and beyond”, 2022 (https://www.itu.int/en/ITU-T/focusgroups/an/Documents/Trustworthiness\_AN.pdf)

[NextG] NextG Alliance White Paper Report, “Trust, Security, and Resilience for 6G Systems”, July 2022 (<https://nextgalliance.org/white_papers/trust-security-and-resilience-for-6g-systems/>).

[NGMN] NGMN Publication, “6G Trustworthiness Considerations”, October 2023 (<https://www.ngmn.org/wp-content/uploads/NGMN_6G_Trustworthiness.pdf>).

[Veith] Veith, B., Krummacker, D., & Schotten, H. D. (2023). The road to trustworthy 6G: A survey on trust anchor technologies. IEEE Open Journal of the Communications Society, 4, 581-595.

\* \* \* Next Change \* \* \* \*

5 System and Operational Aspects

Editor's Note: "System and Operational Aspects" facilitates system and network operation features that underpin overall operation, covering aspects that apply across use cases and services, and those that relate to network operations. These aspects include, for example: migration scenarios, interworking with earlier 3GPP systems, interworking with non-3GPP system, roaming and interconnection, network simplification, network sharing, security, privacy, resilience, sustainability and energy efficiency, device diversity, support of legacy services, exposure

Editor’s Note: The proposed sub-clauses are provided as guidance from the rapporteurs based on the previously agreed EN (above). If text is not agreed for any clause or sub-clause, these clauses/sub-clauses will be removed from the document.

Editor’s Note: Annex TBD is used for studying whether and how to capture emerging concepts. For example, the Trustworthiness definition in clause TBD.1.4 is included for discussion and is FFS. If text is not agreed for usecases or for guidance of downstream WG work, the text will be removed from the document.

\* \* \* Next Change \* \* \*

## 5.y Network-assessed Trustworthiness

### 5.y.1 Description

Public telecommunication networks are considered part of critical national infrastructures and the services they deliver are increasingly critical for many daily activities. This is driving a sharper focus on the trustworthiness inherent in network-related services.

**Terminology and relationship with other 3GPP concepts.**

An often-used definition of Trustworthiness from the National Institute of Standards and Technology (NIST) adapted by NGMN for mobile networks includes the following five aspects: security (including confidentiality, integrity, availability), privacy, reliability, resilience, and safety [NGMN]. ISO/IEC clarifies the need for implementing Trustworthiness by defining it as the “ability to meet stakeholders’ expectations in a verifiable way” [ISO/IEC]. In other 6G ecosystem contexts, it is clarified that while the term is certainly about the ability of 6G to fulfil or exceed expectations in terms of user experience, it is rooted in the ability to offer full security and resilience.

NOTE 1: “Network-assessed trustworthiness” in 6G includes aspects additional to security-related Trust (as inherited from the 5G 3GPP security specifications), such as reliability, resilience, etc. In 6G 3GPP “Network-assessed trustworthiness” is a network assessment capability supporting the fulfilment of the customer’s service requirements in distributed (network) environments, as well as for providing additional, value-add services. See Annex TBD for further considerations and analysis.

**Relationship with 3GPP security and decentralization.**

As described in clause 5.5.1.1, 6G deployments in private, public, and hybrid environments require more decision-making functionality to become distributed, autonomous and self-sustainable. This includes but is not limited to security-related assessments, based on the owners’ policy and with few dependencies on a central authority in the home or visited network. The same clause clarifies that minimization of administrative and operational burdens as another imperative, beyond those obtained by employing Isolated Computing (e.g. Federation), Authentication, Privacy Preservation, Audit trails, Service Level Agreement (SLA) automation.

The above results effectively in requirements for a distributed framework: “Envisaged use cases and possibilities to provide services and resources in a distributed manner render an architectural solution for trust establishment a critical component of 6G networks.” [Veith]. Such a decentralized approach to security in 6G can leverage Network-related Trustworthiness assessments to enable distributed decision making.

Consider for example, a network pre-provisioned with Operator policies for determining Network-assessed Trustworthiness. When a user requests an application service, the 6G Network first determines all the entities involved in providing the necessary communication resources and then performs an assessment on Trustworthiness using implementation-specific algorithms and Operator pre-provisioned policies. In addition, dynamic evaluations including various aspects (e.g. reliability, security, privacy, resiliency, reputation) can be leveraged by the 6G Network for new services which are highly distributed, such as AI/ML and sensing.

NOTE 2: 3GPP TR 28.908 [3GPPTR28908] provides an example study of trustworthiness in the context of machine learning and AI/ML management. It includes assessment of trustworthiness for data, training, inference, etc. While the functionality described in this clause is not in the network management domain, it may rely upon similar models, subject to downstream WG decisions.

**Exposure and additional monetization opportunities.**

Network-assessed Trustworthiness can be leveraged for value-add services to users and Third Parties. Such services may rely, for example, on additional parameters and policies (Affinity policies) used to determine how Network-assessed Trustworthiness impacts the fulfilment of service expectations from a user or Third-party perspective.

With Affinity policies based on user or Third-Party preferences, Operator polices, SLAs, etc. the network can derive Affinity indicators for the services being enabled by the 6G Network. Exposure of Affinity indicators by the network can be leveraged for monetization. In addition to preferences for the Affinity policies, user and Third Parties provide dynamic feedback (e.g. regarding the fulfilment of service expectations) to the Affinity indicators. This feedback loop can be used to optimize network resources while maximizing returns.

### 5.y.2 Potential New Requirements needed to support the use case

[PR 5.y.2-1] Based on operator policy, the 6G system shall provide Trustworthiness assessments of individual service components for the purpose of enhancing the services provided to all stakeholders.

Editor’s Note: The PR above is FFS.\* \* \* Next Change \* \* \* \*

## Annex TBD: Trustworthiness assessment by the 6G Network

TBD.1.1 Introduction

This annex provides information regarding the relationships between the existing concept of “Trust” in 3GPP, the 6G ecosystem concept of “Network-assessed Trustworthiness” to increase understanding and provide clarity on how to address the topic of “Trustworthiness” in this study.

TBD.1.2 Ecosystem considerations

Given the variety of stakeholders and deployment models anticipated to be covered by 6G, the ecosystem has issued many calls to make trust building (including but not limited to security-related Trust, therefore encompassing Trustworthiness) an integral part or service of the network [ITU-T-2022][NextG][NGMN].

### TBD.1.3 Network-assessed Trustworthiness Examples

This clause provides, for study purposes, examples of Network-assessed Trustworthiness implementations, without any implications on their 3GPP applicability. Multiple examples are to be included to represent a variety of views, while allowing further development in the downstream groups.

#### TBD.1.3.1 New metric such as ITU-T Trust Index

Similar to the quantitative measurement of quality of service (QoS) and quality of experience (QoE), ITU-T has studied quantitative methods for measuring trustworthiness [ITU-T-2017] as summarized in this clause.

An example of quantitative and/or qualitative assessment and calculation is a weighted combination (or other equations) of multiple trustworthiness metrics, referred to as “Trust Index” (as termed in [ITU-T-2017]). Such metrics can be calculated based on technical attributes related to security, strength, reliability, availability, ability, etc (Figure MTBD.1.3.1-1). The needed attributes for evaluating trustworthiness may vary depending on corresponding services and applications [ITU-T-2017].



**Figure TBD.1.3.1-1 – Example use of quantitative, qualitative and/or measurable information for Network-assessed Trustworthiness (in the form of Trust Index [ITU-T-2017])**

#### TBD.1.3.2 Network-assessed Trustworthiness policy

Another example relies upon definition of new policy types e.g. Network-assessed Trustworthiness Policy.

Using such policies, network functions provide Trustworthiness assessments based on standardized criteria, such as reliability, availability, ability, etc. The assessments are based on non-standardized algorithms and may include additional, non-standardized criteria or context.

In addition to the Trustworthiness assessment criteria, this policy includes Operator’s criteria for exposure or sharing (e.g. to other Operators or Trusted Third Parties) of Trustworthiness assessments.

### TBD.1.4 Exposure Examples

This clause provides examples of information exposure based on Network-assessed Trustworthiness, without implications on 3GPP applicability. Multiple examples are to be included to represent a variety of views, while allowing further development in the downstream groups.

This clause assumes that exposure of information based on Network-assessed Trustworthiness is:

* Subject to Operator policies and SLAs.
* Subject to privacy requirements and regulations
* Abstracted and contextualized (e.g. relative to specific user and/or Third-party service requirements)
* Used for Value-add network services (e.g. via feedback from user and/or Third-party )

#### TBD.1.4.1 Affinity policy

This is an example of Affinity Policy which may be defined to enable exposure of information based on Network-assessed Trustworthiness. In this example, the information derived by the network based on Network-assessed Trustworthiness is in the form of Affinity indexes.

Two Application Service Providers (ASP) provide similar services in the same geographical area. The ASPs provide the network Affinity policy AP1 and AP2, respectively. The network implements Network-assessed Trustworthiness evaluations for its own network management and optimization purposes. Assume two entities (e.g. UE AI Agents) with the same overall Trustworthiness assessment (e.g. Trustworthiness index = TWiA). Based on AP1 and AP2, the ASPs are provided different Affinity assessment.

The exposed information (e.g. affinity assessments) are based on non-standardized algorithms and may include additional, non-standardized criteria or context. Exposure of information (e.g. affinity assessment) allows a dynamic feedback loop between Third Parties and Operators which is unavailable in 5G.

TBD.1.5 Analysis of terminologies and concepts

**Trustworthiness**: quantifiable and coherent belief and/or confidence that a service participant functions and benefits the system. **Network-assessed Trustworthiness** can include (but not be limited to) a multi-dimensional and dynamic parameter which includes aspects of reliability, security, privacy, resiliency, and reputation as they relate to the 6G System. The complex values assigned to this parameter can be based on (but not restricted to) policies, evidence of behavior and implementation-specific algorithms.

Editor’s Note: The definition above is FFS.

\* \* \* End of Changes \* \* \* \*