6G Trustworthiness Considerations

v1.0

www.ngmn.org

WE MAKE BETTER CONNECTIONS

6G TRUSTWORTHINESS CONSIDERATIONS

by NGMN Alliance

Version:	1.0
Date:	04.10.2023
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public
Project:	6G Trustworthiness Considerations
Approved by / Date:	NGMN Board, 14 September 2023

EXECUTIVE SUMMARY

As the mobile industry continues to look at the next generation of mobile networks, NGMN Alliance (NGMN) is firmly established as a leading force driving discussions on the development of 5G and emerging 6G use cases [1]. While attention is often focused on extending exciting applications such as immersive extended reality (XR), digital twin, interacting cobots, and trusted native AI, NGMN firmly believes it is essential to establish the indisputable trustworthiness of the 6G network.

Considering this, NGMN has identified several technology trends that will influence the trustworthiness of a 6G network including network AI, open source, virtualisation and containerization, and quantum computing which might bring new security threats. 6G networks must therefore have an inherent trustworthiness design to promote the effectiveness of security protection and enhance the ability of privacy protection, such as trusted computing and blockchain.

In the subsequent sections of this publication, we pull all these technology trends together, providing the industry with comprehensive guidance to ensure trustworthiness in the 6G network. By embracing a holistic approach to security and privacy, we can not only enable the realisation of future 6G use cases but also safeguard the interests and trust of end-users.

CONTENTS

01 INTRODUCTION

The mobile network is a critical element of both societal and industrial development. 6G telecommunications system developments have already begun in the industry with NGMN having identified that 6G needs to be driven by societal goals, market expectations and operational necessities. 6G will enable and extend both current 5G use cases as well as 6G envisioned uses cases [2]. 6G mobile network infrastructure must support current and envisioned use cases and be able to adapt to new technologies and be resilient to new attack vectors. A 6G mobile network should be trusted to deliver these use cases across several trustworthiness aspects including security, privacy, reliability, resilience, and safety [3].

The term of "trustworthiness" in this publication is composed of the following five aspects by referring to the National Institute of Standards and Technology's [NIST] definition [3] with minor adaptations to the mobile networks:

- **Security:** The ability of the mobile networks to ensure that all its infrastructure, processes, mechanisms, protocols and services, physical or cyber, are afforded internal or external protection from unintended and unauthorised access, change, damage, destruction, or use. Security usually consists of the following three facets:
  - **Confidentiality:** Preserving authorised restrictions on access and disclosure of the information being transferred between parties.
  - **Integrity:** Guarding against improper modification or destruction of information in transit and includes ensuring non-repudiation and authenticity.
  - **Availability:** Ensuring timely and reliable access to and use of the mobile network.
- **Privacy:** The ability of the mobile network to prevent entities (people, machines) from gaining access to personal data stored in, created by, or transiting a mobile network or its components such that individuals or groups can obscure themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.
- **Reliability:** The ability of the mobile network to deliver stable and predictable performance in expected conditions.
- **Resilience:** The ability of the mobile network to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.
- **Safety:** The ability of the mobile networks to ensure the absence of catastrophic consequences on the life, health, property, or data of mobile networks stakeholders and the physical environment. Note that although mobile networks have different mechanisms to protect the data in transmission, there is still no way to guarantee the authenticity of the data origin.

Trustworthiness is related to the ability to mitigate the security risks in the mobile network. Even though the above five aspects are considered in the design phase of the mobile network, the trustworthiness of the mobile network system is mostly dependent on operators' deployment implementation and configuration. When the five dimensions of trustworthiness are applied, a common practice should be followed to ensure the robustness of the mobile network while at the same time, consistent monitoring and assessment is also required to enhance the trustworthiness.

This publication further analyses the key drivers and typical use cases in relation to 6G trustworthiness and delivers the 6G security requirements covering the aspects of security, reliability, privacy, resilience and safety. Section 2 investigates the key drivers of 6G trustworthiness including societal, network evolution, service driven and security technology driven demands. Section 3 details the specific use case analysis with security risks and requirements analysed, followed by a summary of 6G trustworthiness requirements with classification and consolidation in Section 4. NGMN provides guidance to the 6G technology design, described in Section 5, in order to fulfil the trustworthiness needs for the customers and Mobile Network Operators (MNOs).

02 KEY DRIVERS OF 6G TRUSTWORTHINESS

2.1 SOCIETAL DEMANDS

The United Nations Sustainable Development Goals (UN SDGs) have identified access to mobile connectivity as a key driver of sustainable economic growth and associated societal development. Public safety and data privacy protections are the foundation of societal development. 6G is envisaged to further enhance public safety and data privacy while enabling societal development through use cases like smart city, intelligent interactive systems, intelligent medical treatment, smart transportation, education and smart retail. These use cases are important for both the development and growth of the global society. Significant exposure of privacy systems and heavy processing of user data applications (e.g., industrial intelligent control, driverless vehicles, virtual reality and other high-tech related industries) will require fundamental protections be built into 6G. Basically, the higher the impact of data and control systems exposure, the more protections and reliability that needs to be built in. This means 6G trustworthiness requirements must align with societal demand in securing an individual's daily activities and societal challenges.

2.2 NETWORK EVOLUTION DEMANDS

The 6G network is expected to provide coverage in hard-to-reach rural areas, and this may include non-conventional solutions such as non-terrestrial high-altitude-platforms or satellite-based services to deliver mobile services. This convergence will create massive data and resources which will increasingly rely on reliable network operation. Furthermore, mitigation must be provided against vulnerabilities in the network due to component and functionality splits introduced by virtualisation. Sensing network, as a new network feature, will integrate with communication capabilities to achieve service integration, which will demand agile security mechanism negotiation and ultra-fine-grained security scheduling. To continuously improve the user experience, the 6G network will become more distributed and provide unique services centred on users. This will require appropriate adaptation in the 6G security architecture. As computing power becomes the new driver of network evolution, the computing collaboration and intelligent connection will become inherent attributes of the network, with built-in security an essential feature.

2.3 SERVICE DRIVEN DEMANDS

The extensive coverage, connectivity and reliable network capability of 6G will enable its communication infrastructure to develop from the Internet of Everything (IoE) to the intelligent internet. It will not only provide more coverage, but also make the digital world and the physical world deeply integrated, people's lives will increasingly rely on reliable network operation. In the 6G era, immersive experience, telepresence, multimodal interaction, sensing and XR technology may become mainstream applications. From the interconnection of all things to intelligence, the service value of the 6G network in the future will also be enhanced, this will undoubtedly have a great impact on interest driven attackers. Many of those services require high data -rates, low latency as well as precise positioning and sensing, served by different endpoints in the 6G network, e.g., in the edge or in the cloud. For critical services a strict end-to-end isolation and protection of network slices including the Radio Access Network (RAN) may be required. 6G is therefore required to provide stronger security protection capabilities. At the same time, due to the enhanced flexibility and dynamic expansion of the network, the 6G security capabilities are required to be fine-grained and flexible on demand, to ensure the dynamic adaptation of the network, the user demands and business scenarios.

2.4 SECURITY TECHNOLOGIES DRIVEN DEMANDS

The rapid development of new technologies and new ideas will become one of the key driving forces of security evolution. Security technology is moving forwards with more native intelligence and flexibility. The development of these new technologies/principles will promote the effectiveness of security protection and enhance the ability of privacy protection. It is necessary to consider how to introduce and apply these new technologies in 6G to improve the level of security protection, such as trusted computing, blockchain, zero trust, etc.; The development of some technologies will bring some challenges to the security of the existing communication system. For example, quantum computing technology brings risks to the existing cryptosystem. It is necessary to consider how to deal with the impact of such new technologies. AI and ML are expected to be integrated by design in the 6G architecture, though this brings more risks and vulnerabilities to the system, these can be leveraged to automate detection of new threats, anomalies and cyberattacks. Further AI can assist to predict the breach risk of the different assets and network functions in the system, considering the individual threat exposure so that countermeasures to mitigate vulnerabilities can be planned. Another application of AI is endpoint protection, where AI can detect novel malware and ransomware where signature-based detection mechanisms would fail.

03 USE CASES ANALYSIS

3.1 ENHANCED HUMAN COMMUNICATION

From the security perspective, XR immersive holographic telepresence and multimodal communication for tele-operation seems likely to attract more security attacks because of its coexistence with potential adversary entities in an open environment and its increased points of attack with data from multiple sources and sensors. The threats and requirements non-exhaustively include the following:

- **Privacy of human biometric data:** On one hand, in XR applications biometrics-based authentication is more widely used, such as fingerprint, eye scan, face recognition etc. On the other hand, human centric multimodal sensory data including human's audio, video, taste, odour, haptic and emotion information could be transferred in bulk in the overall network. Due to the irrevocable nature of human biometric data, it represents a very important privacy issue to be tackled by 6G.

- **Protection of the interface between the physical and virtual world:** XR immersive holographic telepresence communication enables the digital representation of the physical world in a virtual network (digital twin network). Due to the dense and real-time interaction between the twin network and the physical network, the virtual twin network itself may have various unknown security vulnerabilities, and the interaction interface between the two will be potentially vulnerable to external attacks, resulting in the virtual twin network giving wrong instructions to the physical network, threatening the device security, network security and business security in the physical network. Technologies to ensure the security of the twin network itself and its interaction with the physical network are therefore significant.

- **Prevention of device compromise:** Enhanced human communication relies on the deployment of devices and sensors in an open environment, and hence is more in danger of being compromised through physical contact or visual observation by external attacks. As a result of device compromise, user's credentials can be stolen or directly accessed. It is therefore crucial to prevent an external attack from directly exploiting such a compromise.

- **Privacy and data protection in Metaverse:** In Metaverse an avatar representing a user can smoothly traverse between different "worlds", all of which as a whole comprise a Metaverse. A good design of federation of authentication and identity is expected to allow a smooth traverse of an avatar between "worlds". A Mobile Network Operator (MNO) that offers a system to enter Metaverse, or other business entities, which are sufficiently trusted by users, may be able to assist realisation of Metaverse in this aspect. If a user is led to a malicious "world" by a fake user consent for a prompt-less traverse to the malicious "world", the user might be exposed to malicious activities. User consent needs to be well protected, in particular with regard to integrity. An avatar is to be unique and should not be easily copied for use to represent someone else. Copy and reuse of avatar data needs to be prevented. When giving the user's information to any "world", national and/or regional regulation and user's consent needs to be considered.

3.2 ENHANCED MACHINE COMMUNICATION

The enhanced machine communication can be described with some generic use cases such as robot network fabric where for example autonomous mobile robots, drones, automatic guided vehicles (AGV) will be moving through the smart city and provide parcel delivery services or services for personal use. These robots communicate with both the 6G network and each other and the communication requires a high reliability and low latency to avoid collisions. To avoid accidents and damage to humans, robots as well as their communications must be secured to protect against hijacking and malevolent manipulation. Since the robots move autonomously and rely on the information received from the network to take decisions, the integrity of the relevant data needs to be guaranteed.

Another further enhanced use case will be interacting collaborative robots (cobots), cobots provide a closer interaction between humans and robots and should interpret the human actions in order to assist the humans. Those cobots could be a separate machine or a machine close to the human e.g., exoskeleton or adaptive wheelchair. The detection of the human action may be based on machine

learning and artificial intelligence; thus, the integrity of the machine learning model must ensure any resulting decision of the cobot does not lead to damage or injuries to the humans. Further communication with sensors or the 6G network must be protected to avoid false decisions that lead to wrong actions not intended by the humans. In general, hijacking and malevolent manipulation on robots [4] can include intention modification attacks, where the command messages from a controller to the robot are modified to redirect the messages or to modify the data on the target robot. Intention modification attacks includes Denial of Service attacks (DoS). Robot halting as a result of a DoS attack may cause the robot to stop or perform undesired movements. There can also be a delay in responding to direction commands for robots subject to DoS attacks, thus that the robot at high speed does not react to navigation commands instantly and may therefore cause accidents.

Intention modification attacks are performed by an adversary as a kind of man in the middle attack (MitM) where the messages from the robot to the controller are manipulated and the controller identifies them as legitimate feedback and uses them as input for the next control messages which can lead to wrong control decisions.

The hijacking attack is very crucial since the adversary takes over control of the robot and executes commands not intended by the legitimate controller and can lead to service disruption for the time the hijacking attack is carried out.

For 6G multi domain heterogeneous interconnection, the massive diversity and concurrency of sensors may access the network frequently, lightweight access authentication must be enabled without compromising security.

The evolution of Internet of Vehicles (IoV) will generate a large amount of data which should not be tampered with. The information exchanged includes the intrinsic attributes of entities and dynamic interaction data of entities. Entity intrinsic attributes include vehicle intrinsic information, such as vehicle model, engine parameters, fuel consumption, vehicle condition, etc. User privacy information includes ID card information, phone number, drivers' license information, and bank account; inherent information about roadside facilities, such as sensor type and location. The IoV source tracing system is a control system that can track data in the IoV forward, backward, or directionless. Traditional centralised source tracing systems may be invaded by external hackers, and malicious entities inside the source tracing systems may be tampered with at low cost. Thus, a more decentralised data storage and source tracing system needs to be considered.

3.3 ENABLING SERVICES

Data Security and privacy are the crucial aspects to most of the enabling services which rely on 6G communication such as 3D hyper - accurate positioning, localisation, and tracking, interactive mapping, digital healthcare, automatic detection, recognition and inspection, smart industry, and trusted composition of services.

- **Security and privacy in positioning, localisation, and tracking:** Positioning and tracking services associated to devices used by human and non-human assets are both critical to security and safety as positioning service compromise (e.g., tampering of communication links, gaining of location data and controlling by impersonation) may lead to illegitimate tracking of human users. Similarly for non-human assets such as devices, objects, robots, drones, vehicles, positioning service compromise may lead to various risks such as executing malicious controls, hijack of devices, forcing into accidents to impact the dependent business etc.

- **Data security with interactive mapping and digital twins:** As digital transformation unlocks new value it also brings new threat landscape. In case of interactive mapping and digital twins it is essential to identify and adopt metrics that define an accurate virtual digital model related to a real-time physical representation. Lack of conformance to standard metrics for the virtual digital twin will greatly impact not only the operation analysis and observations but also the security and cyber resilience when the respective physical device or model is utilised. Further a virtual digital model during its testing, feedback driven iterative construction, observation and analysis phase can involve multiple stakeholders to collaborate and operate the virtual digital model. If the virtual digital twin model processing involves any business-critical data or real-time user data, lack of sufficient critical data translations and process hiding will reveal the sensitive data thus impacting the business and privacy requirement.

- **Secure data storage, processing, and exposure control for digital healthcare:** In-body devices and wearables-based data collection, processing and medical inference data exposure are critical operations associated to digital healthcare. If any of the data links are compromised, it may lead to serious risks associated to the healthcare system's reputation. In most of the cases, the data processing associated to healthcare may be processed at the end-device or if advanced medical processing is required, the data may be processed in independent devices/gateways, where if sufficient data processing security and storage security is not adopted, this may lead to data leakage and data manipulation for varied reasons (e.g., personal gains such as insurance benefits). The processing devices should ensure non-repudiation (e.g., with distributed ledgers supporting both on chain and off chain storage) and the communication links should be sufficiently authenticated (i.e., multimodal), authorised and secured.

- **Security for intelligence and automation:** Smart and intelligent devices are expected to be deployed for monitoring services such as to monitor vital signs in healthcare/critical units, to monitor passengers and belongings during safety check-ins (e.g., in airport), crowd screening (e.g., in any mall or sensitive public spots/private sports) etc. If such monitoring devices and associated communication links are compromised, false reporting can impact people with serious legal consequences. Further, malicious control of such monitoring devices due to vulnerabilities in the end-devices or lack of security in the communication link can provide malicious users with access to sensitive data.

- **Security for resilient operations in smart industry:** Smart industry involves automation in product design, factory production lines and supply chain etc. Each phase involves various devices (i.e., operational e.g., manufacturing functional unit, and assistance devices such as AGVs), software, operator (e.g., human) digital communication etc. Each communication link, devices and operational data processes needs to be accountable and auditable in real-time to ensure overall secure operation.

- **Trusted composite services and user-controlled privacy:** Composite services involves convergent networks to offer varied on-demand end-user services with enhanced human and machine communication. As it requires trustworthy relationships to be set-up when a new on-demand service is requested by the end-users/device, it is a huge challenge to offer identity verification control in compliance with all regional regulations. Most service subscription activations require submission of user documents (e.g., passport, national identity card, driving license etc.) and verification of user documents by third parties. Government databases are also used to enable the service provider(s) to perform identity verification. But if the identity documents are forged and misused by the third party or if the identity related document are compromised at the third party's premise, it may lead to serious issues such as service provider fines (if the breach is identified), service provider reputational harm [5], and the end-user may face legal issues, or their safety put at risk if their identity is misused. Blockchain based digital identity such as decentralised identity and self-sovereign identity [6] can enable the end-users to have control over their identity (i.e., service identity) and control over the identity information disclosed (e.g., controlled data disclosure).

Overall, selective application of security by the communication network should be avoided, e.g., relying on 3rd party application security for some services and not mandating communication network security (i.e., signalling and user plane) for the services will end-up with no security being applied for the critical services. In conclusion there needs to be a standardised approach to co-ordinate and apply security and privacy measures, as well as threat mitigation techniques as a common security baseline for the 6G dependent services.

3.4 NETWORK EVOLUTION

To realise the vision of "smart connection" in the 6G era, artificial intelligence technology will be fully integrated into the next generation of mobile communication systems. The deep integration of AI and 6G network will bring new opportunities for the built-in security of 6G networks. Multi-dimensional data perception and learning such as network data, business data and user data, will help the network security intelligence, improve the efficiency, flexibility and security autonomy of the communication system, reduce the network security operation cost, and build a measurable and evolving endogenous security protection system.

Based on big data analysis technology and deep learning algorithm models, the exponential growth of 6G network data can be handled; also features of attack behaviour and threat intelligence can be modelled or extracted. The system will also be able to detect and identify known or unknown malicious software, analyse and trace network attack behaviour, create a self-definition of the security boundary, ensure self-isolation of the risk domain, develop adaptive generation and execution of the security policy optimal set, promote flexible arrangement of the security capability. The system will also be capable of global resource mobilisation and precise risk control, improving the automatic deployment capability and security capability adaptation level of threat intelligence in network security products, and fully adapting to changes in external and internal threats.

6G is expected to provide interoperation between the terrestrial and non-terrestrial networks. It will integrate the network architecture, network functions, radio interface transmission, and wireless resource management and scheduling. Full coverage and network interconnection have become an important direction of 6G development. Because of the complexity of the network and the importance of the services carried on it, it is particularly important to ensure the security of the space-based network.

With the open communication environment, time-varying topology of communication nodes, complex network structure and low processing capacity of space-based nodes, the network risk is increased, and the potential vulnerability is easier to be exploited by attackers. For example, the service link, inter satellite link and feeder link all use wireless communication. The wireless link is open and more vulnerable to human interference, eavesdropping, playback and wireless resource occupation. The data confidentiality, data integrity, network availability and reliability of the wireless link shall be considered in combination with the characteristics of the 6G network wireless link. Another example is with the large number of heterogeneous terminals accessing at any time and satellite nodes operating in exposed space orbits for a long time, attackers are more likely to fake and hijack legitimate terminals or network nodes. Therefore, it is necessary to consider the system access and communication security authentication of terminals and network nodes. At the same time, the satellite node resources are limited, and the existing access authentication mechanism has problems such as high overhead and easy congestion. Hence, 6G authentication mechanisms should consider lightweight and cost-effective mechanisms to ensure that the authentication process uses as few resources as possible.

04 6G TRUSTWORTHINESS REQUIREMENTS

Requirements related to security:

Requirements	Description	Applicable use cases
Credential and authentication	The 6G system should support light-weight authentication mechanisms.	Enhanced machine communication
	The 6G system should support multi-factor access authentication mechanisms with credentials securely stored and protected.	Enhanced human communication
Confidentiality and integrity protection	The communication links should be protected from eavesdropping and tampering.	All
Cryptography enhancement	The 6G system should be quantum robust in face of the introduction of quantum computing.	All
Identification	Digital identities should be protected and securely stored (e.g., decentralisation) to prevent from unauthorised access. The 6G system should support identification of service requestors at the earliest (possible) during authentication to prevent flooding attacks.	All
Interface protection in digital twin	Ensuring the security of the twin network itself and its interaction with the physical network is required.	Interactive mapping, digital twin
All data related to control systems used for industrial process control, should be integrity protected.	Each communication link, devices and operational data processing in the complete industrial process need to be accountable and auditable in real-time to ensure overall secure operation.	Enhanced machine communication

Requirements related to privacy:

Requirements	Data Type	Description	Applicable use cases
Privacy protection of users' data	Sensitive data	Sensitive data need to be controlled by users and protected not only in terms of anonymity and confidentiality, but also integrity and availability, as well as according to the minimality principle.	All
	User consent	User consent should be protected, in particular with regards to integrity, etc.	All
	Identities	Identities should be managed to prevent linkability attacks.	All
	Positioning	Positioning verifications and security should govern local regulatory requirements.	3D hyper-accurate positioning, localisation, and tracking

Requirements related to reliability:

Requirements	Description	Applicable Use Case
Automatic security management and orchestration	An automated management system to detect vulnerability and provide response solutions is required to quickly check and update the vulnerability. The ability to distribute and orchestrate security capabilities intelligently is also required.	Network evolution
Security assurance schemes	The 6G system should support providing security assurance schemes for the whole life cycle of from the products to network deployment and operation.	All
Traceability for critical services	The 6G system should support auditability of network operations (both from the network and UE side) for critical scenarios/services (e.g., digital healthcare, roaming).	All

Requirements related to resilience:

Requirements	Description	Applicable Use Cases
Ability to recover based on AI	The 6G system should ensure availability in the face of varied threats which require mitigation and recovery methods with the help of artificial intelligence in the network.	Network evolution

Requirements related to safety:

Requirements	Description	Applicable Use case
Protection related to human action	All data related to human action should be protected to avoid damage or injuries to the humans.	All

05 DESIGN CONSIDERATIONS OF 6G TRUSTWORTHINESS

To achieve 6G trustworthiness, the whole system should be designed with a holistic and risk-based mindset, taking the following building blocks into consideration.

5.1 DECENTRALISED TRUST FOUNDATION

The 6G network should consider options to address the increasing evolution and integration of different network topologies (e.g., cloud, edge) and business models. The network can be improved with a decentralized trust model in some use cases, using distributed ledger technology in a global context, to more regional hierarchies where the decentralisation is limited to a relevant community of interest (similar models are being tried in other networks [7]). With an updated trust framework, the 6G network would benefit by increased security and trustworthiness.

5.2 DYNAMIC TRUST MODEL

3GPP defines the security architecture of two-way trust. Both UE and the operator share the user root key as the trusted root of two-way trust. When the user equipment accesses the operator network and uses network resources, the user and the operator network perform two-way authentication according to the user's root key. In addition, the user and operator networks derive the key according to the user root key and obtain a series of protection keys to encrypt and protect the two-way transmission of signalling and data.

In the 6G era, when the connection mode and business model continue to change and combine flexibly, such as the connection between the sidelink machine, multi service collaboration, MEC deployment, etc., the trust relationship is based on the three-way trust model of access devices, industry users, and operators, and further evolves into a multi-party trust model that includes multiple terminals, multiple users, and multiple network access nodes. The secure trusted root, required by the multi-party trust model, includes that multiple terminals, multiple users, and multiple network nodes cannot be based on a single user root key, but needs to be built based on the basic components of devices, services, and networks.

In the 6G era, the network should leverage zero trust [8] concepts and could include a dynamic trust model, it will be necessary to perform a trust evaluation in a dynamic manner by carrying out continuous profiling of user identity and analysing user behaviour. Depending on a trust assessment, the trust level of a user could be upgraded or downgraded when accessing resources in real-time.

5.3 INTELLIGENT COLLABORATION

It is not easy to achieve high-efficiency and low-cost security protection in the telecommunications network, due to lack of intelligent analysis and coordination between different security mechanisms. For example, the analysis of current security events is generally based on known security vulnerabilities, which makes it difficult to identify new attacks such as Advanced Persistent Threat (APT).

By delivering ever-present intelligent communication, 6G is expected to comprehensively improve network security mechanisms including threat intelligence, attack detection and security management automation. Collaboration between the security capabilities needs the support of intelligent analysis to analyse security threats using AI, big data and other technologies, and manage the security capability exposure.

5.4 SECURITY AS A SERVICE

As 6G is expected to be a self-evolving flexible network, through software defined and virtualised technology, 6G security mechanisms will also require flexibility, elasticity, and dynamic adjustment and atomic level customisation. By constructing a flexible and convenient resource pool with all security capabilities dynamically organised on demand, a 6G network will be able to support flexible security capability orchestration, thus efficient security implementation could be achieved. This also requires the security capability to be decoupled from the bottom layer, the network function to be software defined

5.5 TRUST AND RISK ASSESSMENT

The fundamental question facing the trustworthiness of the mobile networks is how to know whether the network is trusted or not. To prove the trustworthiness of the system to the stakeholders, measurable or attestable evidence which act as proof points covering all the aspects of standardisation, development, deployment and network operation to assure security is required.

6G should support multi-dimensional network situation awareness, as well as a series of technical proofs, to measure the trust levels of the network, so that the network can perceive the network status, assess network risks, and update security protection strategies in a timely manner.

06 CONCLUSION AND ROADMAP

The emergence of 6G is poised to significantly reshape communication, opening up new avenues to enhance human potential. Through seamless integration of the physical and digital realms, individuals can securely create and engage in immersive digital experiences. To realise the value and benefits brought by 6G trustworthiness between human and machines across every enabled system is essential.

This publication has explored trends, requirements and design considerations related to 6G trustworthiness, in order to provide an enlightening guide for the future technology design on 6G security, privacy, resilience, reliability and safety aspects.

To realise trustful collaboration across industries, the trustworthiness design from the very beginning is vital so that the security and privacy is intrinsically embedded in the 6G system, not only protecting the system from increasing threats, but also providing flexible, sustainable and measurable trust solutions.

07 ABBREVIATIONS

3D	Three Dimensional
3GPP	3rd Generation Partnership Project
5G	5th Generation Mobile Network
6G	6th Generation Mobile Network
AGV	Automatic Guided Vehicles
AI	Artificial Intelligence
APT	Advanced Persistent Threat
DOS	Denial of Service
HE	Home Environment
IoE	Internet of Everything
IoV	Internet of Vehicles
MitM	Man in the Middle
ML	Machine Learning
MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
RAN	Radio Access Network
UN SDG	The United Nations Sustainable Development Goals
UE	User Equipment
XR	eXtended Reality

08 ACKNOWLEDGEMENTS

NGMN would like to thank to the following individuals for their expertise, support, and guidance throughout the entire process of producing this work:

Editor/Lead:
Xiaoting Huang, China Mobile

Contributors:
Andreas Kunz, Lenovo
Atsushi Minokuchi, NTT Docomo
Chitra Javali, Huawei
Fei Liu, Huawei
Haitao Du, China Mobile
Hua Song, China Mobile
Ivy Guo, Apple
Jean Trakinat, T-Mobile US
Javan Erfanian, Bell Canada
Lei Wang, China Mobile
Li Su, China Mobile
Stan Wong, BT
Sheeba Backia Mary Baskaran, Lenovo
Marc Kneppers, Telus

Their contributions have been instrumental in shaping and refining the content in this publication. Their collective efforts have helped to ensure that this guidance is comprehensive, accurate, and insightful.

09 REFERENCES

[1] NGMN, 6G Use Cases and Analysis, February 2022, https://www.ngmn.org/wp-content/uploads/220222-NGMN-6G-Use-Cases-and-Analysis-1.pdf

[2] NGMN, 6G Requirements and Design Considerations, February 2023, https://www.ngmn.org/wp-content/uploads/NGMN_6G_Requirements_and_Design_Considerations.pdf

[3] NIST Framework for Cyber-Physical Systems; Volume 1, Overview

[4] I. Priyadarshini, "Cyber Security Risks in Robotics", May 2018

[5] GSMA, "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid", 2017

[6] Europa Futurium, 'eIDAS Supported Self-Sovereign Identity', 2019

[7] The SCION Internet Architecture, VOL. 60 NO. 6 COMMUNICATIONS OF THE ACM, June 2017

[8] NIST Special Publication 800-207 Zero Trust Architecture

NEXT GENERATION MOBILE NETWORKS ALLIANCE

NGMN, established in 2006, is a global, operator-led alliance of over 80 companies and organisation spanning operators, manufacturers, consultancies and academia.

VISION

The vision of the NGMN Alliance is to provide impactful industry guidance to achieve innovative, sustainable, and affordable mobile telecommunication services for the end user with a particular focus on Mastering the Route to Disaggregation / Operating Disaggregated Networks, Green Future Networks and 6G, whilst continuing to support 5G's full implementation.

MISSION

The mission of the NGMN Alliance is

- to evaluate and drive technology evolution towards 5G's full implementation and the three major priorities for 2021 and beyond:

  Route to Disaggregation: Leading in the development of open, disaggregated, virtualised and cloud native solutions with a focus on the end to end operating model.

  Green Future Networks: Building sustainable and environmentally conscious solutions.

  6G: Emergence of 6G highlighting key trends across technology and societal requirements plus use cases, requirements and design considerations to address.

- to establish clear functional and non-functional requirements for mobile networks of the next generation.

- to provide guidance to equipment developers, standardisation bodies and cooperation partners, leading to the implementation of a cost-effective network evolution.

- to provide an information exchange forum for the industry on critical and immediate concerns and to share experiences and lessons learnt for addressing technology challenges.

- to identify and remove barriers for enabling successful implementations of attractive mobile services.