ITUPublications

International Telecommunication Union

Standardization Sector

ITU-T Technical Report

(09/2024)

TR.5Gsec-bsf

Guidelines for a telecommunication network built-in security framework

Technical Report ITU-T TR.5Gsec-bsf

Guidelines for a telecommunication network built-in security framework

Summary

Technical Report ITU-T TR.5Gsec-bsf analyses security requirements and existing security mechanisms of IMT-2020 systems and identifies security challenges that must be addressed during the operation and management of telecommunication networks. Based on this analysis, a built-in security framework for the evolved telecommunication network is proposed to address said security challenges at the planning and implementation stage of the telecommunication network, to form a reliable, flexible, dynamic and in-depth security protection system.

Keywords

Built-in security framework.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T TR.5Gsec-bsf

Guidelines for a telecommunication network built-in security framework

1 Scope

This Technical Report provides guidelines for a telecommunication network built-in security framework. This Technical Report covers:

– Objectives of the built-in security framework for telecommunication networks.

– Framework design and functionality definition of the built-in security framework.

– Applicable practices of the built-in security framework in the 5G network.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.2 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.3 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g. session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.4 trust [b-ISO/IEC 25010]: Degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AMF	Access and Mobility management Function
APT	Advanced Persistent Threat
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
HSM	Hardware Security Module
IDS	Intrusion Detection System

IPsec	Internet Protocol Security
MANO	Management and Orchestration
PDRR	Protection, Detection, Response, and Recovery
PKI	Trusted Execution Environment
TEE	Trusted Execution Environment
TLS	Transport Level Security
TPM	Trusted Platform Module
WAF	Web Application Firewall

5 Conventions

None.

6 Overview

The 5G evolution in the telecommunication industry not only enables an infrastructure of all-round connectivity, but also drives the digitalization of various industries. This means that the security of 5G networks is of even greater importance. Typical security risks and security requirements of 5G network compared to 4G network include:

– The openness of the 5G network requires the network functions themselves to be more secure.

– The adoption of cloud and virtualization technologies into the 5G network puts more demand on the security of network functions and on internal security detection and monitoring within the mobile network domain.

– Dedicated networks for vertical industries require orchestrated security capabilities to fulfil customized security needs.

Based on the above typical security requirements, the status quo of the design and deployment related to 5G security is analysed, with investigations into the following four aspects:

– Security assurance requirements of 5G network functions have been well specified by 3GPP. The 5G network has more comprehensive data security protection, richer authentication mechanism support, stricter user privacy protection, and more flexible inter network information protection.

– Dedicated security equipment have been deployed at the borders of the security domains.

– Security detection and monitoring capabilities are preliminarily equipped within the mobile operator network.

– Dedicated security equipment and capabilities are capable of being orchestrated due to the involvement of cloud and virtualization technologies.

By analysing the status quo of existing security mechanisms and deployments in the 5G system, it can be seen that although they address the security requirements to some extent, there are significant areas for improvement considering the development and the application of the 5G network, as well as the evolution of the next generation telecommunication network.

This Technical Report first analyses the security challenges that need to be addressed and the issues to be considered in the evolution of the telecommunication security framework. Based on the analysis of the problem, built-in security is proposed as the evolutionary objective and direction of a security framework for the telecommunication system. This Technical Report also lists design principles to establish the built-in security framework for the telecommunication system. Based on said design principles, the detailed framework design and the functionality definition of each component in the framework are described. In addition, the applicable practice of the framework is presented in order to justify the feasibility of the implementation of the framework into the telecommunication network.

7 Problems of the security framework for the telecommunication network

Due to limitations associated with network compatibility and technological maturity, the following problems (P1 to P4) continue to exist and need to be addressed:

P1: Overlapping and duplication of security capabilities from the network functions and the dedicated security equipment

Network functions in the 5G network are gradually being equipped with security capabilities, such as for example the access and mobility management function (AMF) that is required to have anti-DDoS capability according to the 3GPP specifications, this may overlap with dedicated security equipment at the border. On the one hand, it is foreseen that when more and more overlapping and duplication of security capabilities from network functions and dedicated security equipment occurs, the overall efficiency and performance of the 5G system might be impacted, with increased operating costs and inefficient usage of resources. On the other hand, such overlapping may also be utilized to coordinate among heterogeneous entities in order to improve the security protection level.

P2: Lack of internal security detection and monitoring mechanisms

With the virtualization and cloudification of network infrastructure, network devices continue to decouple, increasing internal exposure. Vulnerabilities in third-party open-source libraries will also be introduced as internal hazards, making it difficult for traditional security measures to load on broken security boundaries. Internal attacks within the network operator network are increasingly occurring. With the exception of firewalls and other dedicated security equipment at the border, which are mainly intended for protection against the external risks, internal protection mechanisms including the complete procedures of security protection, detection, response, and recovery (PDRR) capabilities need to be established. Some of these security capabilities need to be carried out through dedicated security equipment or services on the Intranet, such as vulnerability scanning, security situation awareness and centralized analysis and response to security events, etc. In addition, parts of these security capabilities, such as vulnerability scanning and situation awareness can be invoked as a service provided to dedicated networks. Therefore, it is reasonable to build a security capability function in the production domain of the mobile network, which can interact with the core networks and perform intranet security guarantees.

P3: Incomplete operation and management mechanisms for security capability resource pool

According to the needs of vertical industries, the dedicated network resources should be equipped with customized security capabilities, this creates the need for a security capability resource pool (including firewalls, web application firewalls (WAFs), cryptographic devices, and so on) to be built into the core network of the 5G system, which is enabled or loaded through management and orchestration (MANO). The realization of the security capability resource pool and its management not only requires resource reservation in the core network, but also the establishment of a security management centre cooperating with the network management system and the virtual resource orchestration system. The security management function is intended to manage and dispatch the virtualized security functions, and to formulate and issue the security decisions.

P4: Intelligent collaboration between security capabilities from the network functions, dedicated security equipment and the security capability function has to be enhanced

At present, there is no coordination between the security capabilities from network functions, dedicated security equipment and the security capability function, so it is difficult to achieve high-efficiency and low-cost security protection in telecommunication networks. In addition, 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 threats (APTs). On the one hand, in order to avoid overlapping and repeated construction of security capabilities, as well as improve the detection capability of new attacks, the security management function also needs to have stronger intelligent analysis capability. On the other hand, the collaboration between the security capabilities from the network functions and the dedicated security equipment also needs the support of intelligent analysis.

8 Issues and objectives during the evolution of the telecommunication security framework

8.1 Issues to be considered during the evolution of the telecommunication security framework

Facing the significant increase in security requirements and complexity brought by future network evolution, it is necessary to consider the problem from the perspective of the overall network: How to conduct security design to achieve a triangular balance between network quality, capability, and efficiency. In detail then this question can be subdivided into the following three key issues:

1) Key issue 1: New requirements often require the introduction of new security capabilities, and with the evolution of the network, the increase of the network's own business processing chain and the continuous addition of security detection and protection mechanisms will inevitably lead to a decline in overall network performance. Therefore, it is necessary to consider the issue of how to avoid performance degradation caused by the continuous addition of security capabilities, and balance security with network performance and functional requirements?

2) Key issue 2: From 2G to 5G, the tightly coupled security functions are difficult to change, making it difficult to flexibly adapt to dynamic security requirements. Repetitive development of common security functions in different network elements wastes resources. With the evolution of distributed and autonomous network architectures in the future, rigid security capabilities will lead to higher complexity. Therefore, it is necessary to consider how to avoid the design complexity caused by the introduction of security capabilities in differentiated scenarios, and balance security and resource efficiency.

3) Key issue 3: Security design often lags behind, and is limited by, communication network design. Most measures can only protect the network through plug-ins or patches, which affect the performance, efficiency and security of the communication. Firstly, security disposal outside facilities and processes may incur additional communication costs and transmission risks. Some security functions may require invoking internal data of network elements and are more suitable for local execution. Secondly, the centralized security disposal may become a bottleneck point, which may affect the performance of the network flow passing through the disposal point and the robustness of security disposal. Finally, during network evolution, due to the limitations of existing network designs, the evolution of security function scans only be carried out in a patched manner, making it difficult to implement overall and active protection measures which limit the security protection effect. Furthermore, it is also not possible to fully utilize the security potential of the network itself. Therefore, it is necessary to consider how to avoid the separation of security architecture and network architecture, and achieve an integrated architecture.

Facing with the above problems, a systematic security framework built inside the operator network in order to form a reliable, flexible, dynamic and in-depth security protection system while providing the security capabilities to vertical industry customers as services, needs to be established. Additionally, the given framework is aimed at providing guidance concerning the security design for future evolutions of telecommunication networks, as well as to guide operators to manage and coordinate security capabilities in either the planning stage or implementation stage.

8.2 Evolution objectives of the telecommunication security framework

By analysing the issues to be considered during the evolution of the telecommunication security framework, an evolution path and objectives can be proposed:

1) Regarding key issue 1: Looking back at the security design of mobile communication networks, it can be seen that the communication network initially achieved high reliability of the system by building trust between different entities. But with the continuous opening from 2G to 5G, the original trust foundation based on closeness has been constantly challenged. The continuously built security detection and protection capabilities not only maintain the high reliability level of telecommunication networks but also pose a huge challenge to the performance and resources efficiency of the entire network. Therefore, the essence of issue one is the imbalance between the development of trust technology and of security technology. It should be based on the principle of moderate security and should integrate trust and security concepts in communication technology (CT) and information technology (IT). In more detail, on the one hand, security risk detection, response, and disposal are essential when facing evolving attack capabilities. In the process of transforming the network from data connectivity to information service capabilities, it is necessary to strengthen communication network security capabilities from infrastructure, information networks, and other levels. On the other hand, trust can effectively improve performance. As a proactive security measure, it will significantly reduce the need for security detection and analysis in trusted business processes. Building a new security system based on trust can also fully utilize the advantages of CT's accumulated identity and trust, along with other trust establishment and protection technologies, to achieve trusted infrastructure, network connections, business applications, and data services, and build a trustworthy network space. Effective complementarity is necessary between security and trust to achieve a combination of confrontation and cooperation, and a balance between capability and efficiency.

2) The essence of key issue 2 is the uneven development of the pace of security and the flexible transformation of network architecture. Inspiration can be drawn from the 5G service-based architecture, in which flexible adaptation is considered as the principle and service-oriented architecture as the means. On the one hand, service-based security functions can be flexibly scheduled and adapted to differentiated security needs, and provided as external services. On the other hand, effectively atomized security functions can be arranged and scheduled according to changes in network and security risks, and then on-demand deployment and growth of security capabilities is achieved. Establishment of security mechanisms in uncertain environments such as network security, user sources, and business types can ensure that the system is not compromised and assets are not damaged, achieving deterministic security protection for the network.

3) The essence of key issue 3 is the insufficient integration of security into the overall network architecture. For some considerable time, security, as a necessary capability of the network, has not been fully integrated into the design of the network ontology. It is possible to consider designing security and network architecture in an endogenous and integrated manner, with more security capabilities embedded in network facilities, processes, and architectures. The potential of the network itself can be transformed into security protection capabilities that adapt to network characteristics. Specifically, based on the principle of simplicity and efficiency, with an endogenous design, security can be achieved through network element built-in security, process embedded security, and network architecture driven security, which construct a built-in security protection system for network "point – line – plane" endogeneity. Point endogeneity refers to the transfer of security disposal capabilities from the boundary to

the interior of network elements, which can enhance the security protection of each network element itself, and reduce the communication cost of security disposal outside the facility. Line endogeneity security refers to the integration of security mechanisms as steps or elements into network functional processes, in order to achieve consistency and low latency in process security. Plane endogeneity refers to network architecture that can empower security, build a collection of security functional processes, and support overall, active and passive system protection.

In summary, the goal and direction of the evolution of the telecommunication network security system is to 1) Achieve moderate security through the integration of trust and security; 2) Implement flexible adaptation through atomization and service-based methods. 3) Use "point – line – surface" integrated endogenous design as a means to achieve simplicity and efficiency. The security system that meets the above requirements is the built-in security framework of the telecommunication network.

9 Built-in security framework for the telecommunication network

9.1 Design principles of the built-in security framework for the telecommunication network

This clause will provide the design principles of the built-in security framework, based on the recommended solutions given in clause 7.

Principle 1: Built-in security capabilities for the telecommunication network

1) By establishing security measures within or based on network elements and networks, security capabilities can be developed with network capabilities and provide closer and more targeted protection which can also be seen as foundations for more sophisticated protection.
2) In open and autonomous networks, it is necessary to refer to the zero trust principle and to require network facilities (including physical devices and virtual network elements) to have independent high security capabilities to ensure their own security. The necessary security mechanisms to resist internal attacks (such as authentication, security configuration, alarm, log, etc.) are implemented by the network function itself.
3) End-to-end security capabilities can be realized by the network function itself (e.g. security protocols).
4) The common security capabilities required for the network/subnet are prioritized by dedicated security equipment e.g. firewall, Internet protocol security (IPSec), and the security capability centre.
5) Special equipment are used for intranet security (e.g. scanning, monitoring, baseline verification, and so on) in a centralized way which is more conducive to consistency and operation and maintenance management.
6) The network/subnet boundary can adopt special security equipment in order to take advantage of the function and performance and so lower the security and management cost by using centralized protection of regional boundaries.
7) When a security capability can be realized in multiple ways, prioritize the implementation method based on cost, efficiency, and so on.
8) Security capabilities can be derived based on network capabilities.

Principle 2: Capabilities cooperation and orchestration for security of the telecommunication network

1) Collaborate various security capabilities to form security elasticity and schedulability which can improve security protection and operational efficiency, and reduce redundant construction and deployment of network security capabilities for operators.

2) Security capabilities within the network can cooperate with each other and with network capabilities to achieve security targets.

3) Security devices can cooperate to achieve security targets. For example, intrusion detection system (IDS) detects attacks and then firewalls filter out messages with attack source Internet protocol (IP).

4) Security devices and security capabilities within network functions can cooperate with each other to achieve security targets.

5) All security capabilities, security configurations and security decisions should be managed and orchestrated together to improve the efficiency and reduce cost.

6) Existing orchestration related technologies such as MANO, software defined networking (SDN), and software defined security (SDS) can be utilized.

7) A scalable security architecture is needed which supports vertical and horizontal expansion of security capabilities as needed, ensuring the robustness and flexibility of the security architecture, including scalable security capabilities and flexible management of security capabilities.

Principle 3: Active security of the telecommunication network

1) Adjust and optimize security decisions on operation and maintenance to build active security capabilities, which can enable the network to proactively discover risks like unknown vulnerabilities, and intelligently deduce policies, perceive security status and optimize security measures. AI/ML algorithms can be used to describe the status of the network, to predict the network performance trends and potential network faults, and to make optimization decisions.

2) Establish security mechanisms in uncertain environments such as network security, user sources, and business types to ensure that the system is not compromised and that assets are not lost which can achieve deterministic security guarantees for the network. Digital twin for network which provides real digital representation of a physical network could be constructed. With the profound and full-scale understanding of the historical, real-time and static network related data in a digital twin for the network and with the twin network as a test bed, various network situations can be sensed; security risks or security devices could be simulated; and different security strategies could be generated, tested, optimized and decided.

Principle 4: Adaptive security of the telecommunication network

1) Adaptive security refers to security considering trust and resilience. Dynamic evaluation on credibility and the need for trust can be conducted based on trust criteria such as asset value, impact scale and impact severity [b-ITU-T X.1812]. The trust evaluation result can be used to make decisions on applying temperate security measures in order to achieve adaptive security. The network can also have intelligent resilience capabilities which means the network can analyse risks and threats, take appropriate measures to avoid risks, and mitigate the impact of attacks. If risks cannot be avoided, the network can control the impact of risks to the lowest level and quickly recover after damage.

2) A trusted telecommunication network can prove itself to perform as expected and provide confidence to the customers by relying on the built-in trust-enabling technologies. The built-in trust-enabling technologies enable root of trust, trusted computing environment, trusted network, trusted applications and trusted service and data.

3) The trust-enabling technologies of the telecommunication network can be built on trust infrastructure which can form a verifiable technical chain of trust. The trust infrastructure could be decentralized to avoid single point failure of the centralized infrastructure.

4) Trust-enabling technologies can rely on certain fundamental factors such as certifications, level of assurance, and qualifications, which offer confidence in the telecommunication system to potential customers.

9.2 Framework and functionality of the built-in security framework for the telecommunication network

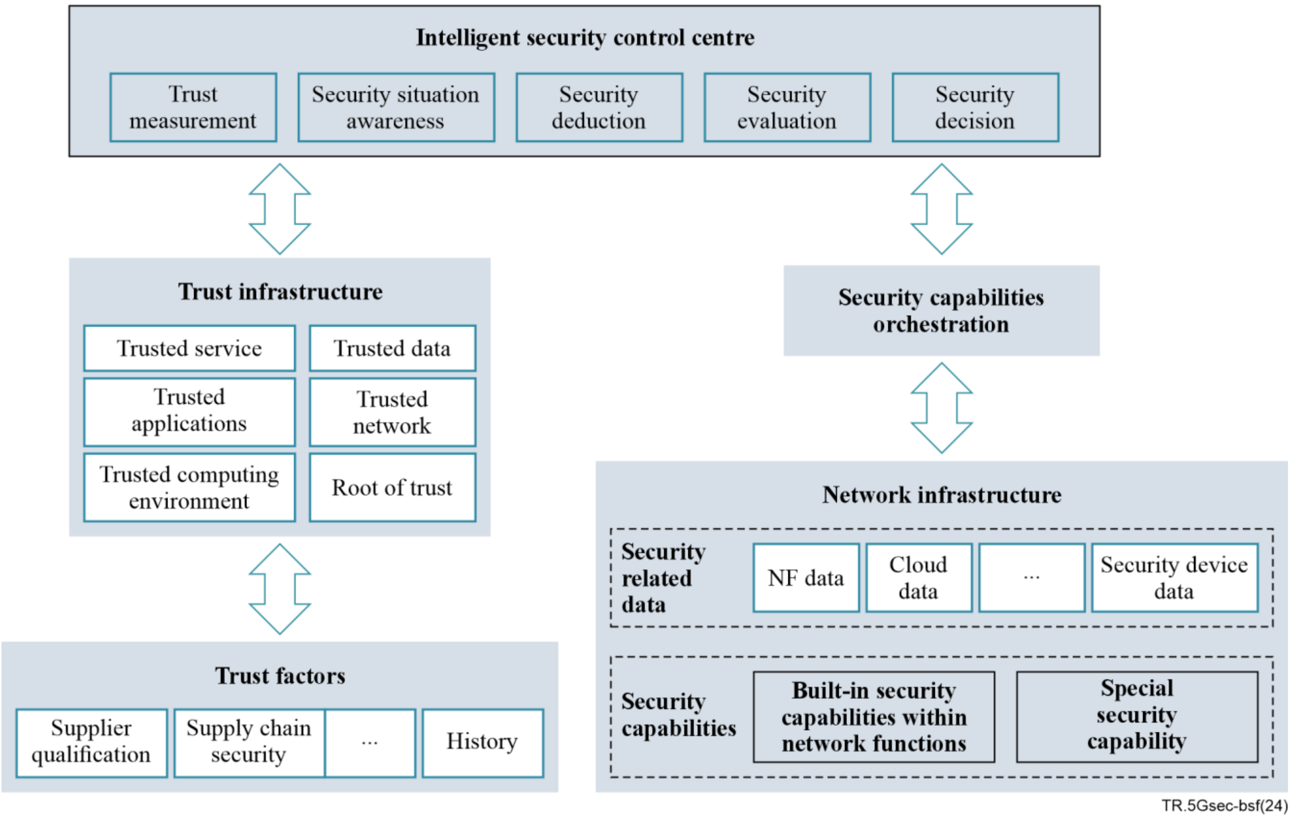

Figure 1 – Example of the built-in security framework for the telecommunication network

A built-in security framework based on the design principles listed in clause 8, is shown as Figure 1. The functional descriptions of the built-in security framework are as follows:

- **Network infrastructure**: Network infrastructure provides security related data for security analysis and implements security capabilities to support the protection of the network, services, and users.

  1) **Built-in security capabilities within network functions**: Network functions are processing functions in a network, which has functional behaviour and interfaces. A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure. The functional behaviours implemented inside a network function to achieve security are called the built-in security capabilities of the network function. There are many kinds of built-in security capabilities: 1) self-security protection capabilities, such as access control, identity authentication, and security baseline configuration, device intrusion detection, software integrity verification, logs, etc.; 2) End-to-end security capabilities, such as transport level security (TLS) and Internet protocol security (IPSec) based on digital certificates; 3) Personalized security capabilities, such as black-and-white lists, service license lists, etc.

2) **Special security capabilities and resources**: There are many kinds of special security capabilities and resources: 1) physical security equipment mainly used for boundary protection, 2) the instance of virtualized security function provided by a security capability resource pool like security vulnerability scanning, security configuration verification, security status monitoring, etc., 3) and the resources reserved for the activation of a virtualized security function to realize security flexibility.

3) **Security related data**: Security related data can include network functions (NF) data, cloud data and security devices data, attack information and so on which are collected from the network to support security analysis.

4) The security devices or virtualized security functions or built-in security capabilities within network functions are subject to the unified management of the security capability orchestration and the intelligent security centre, including reporting security events and security logs to the intelligent security centre, and implementing the security decisions directly issued by the security capability orchestration or the intelligent security centre.

- **Security capability orchestration functions**: They accept the decisions issued by the intelligent security control centre, and unified control is implemented over the security capabilities based on resource allocation, scheduling capabilities and SDN technologies. When the network environment or security status changes, the intelligent security control centre provides response instructions, and the security capability orchestration function schedules the security capabilities to make decision adjustments or to respond to and dispose of them. Through the joint action of various security layers, an adaptive security mechanism that integrates "detection, response, prediction, and prevention" is formed. Security capability orchestration functions include network function security orchestration and security device orchestration. They can usually be located on the network side, manifested as physical or virtual independent network functions, and the two can be independent of each other or combined.

  1) **Network function security orchestration** supports the analysis of the attack information reported by the network functions and reports the analysis results of the network function attack and the trusted status information of the network function to the intelligent security centre. At the same time, it can link the network functions based on security decisions issued by the intelligent security centre;

  2) **Special security capability orchestration** supports the analysis of security events and security logs reported by special securities implemented by physical security devices and virtualized security functions and reports the analysis results to the intelligent security centre. At the same time, it can link the special security capabilities based on security decisions issued by the intelligent security centre.

- **Intelligent security control centre**: This is the brain of the built-in security framework and mainly comprises the functions presented below. It can usually be located on the network side, manifested as physical or virtual independent network functions. The security capability orchestration functions can be independent of each other or combined.

  1) **Security analysis**: Centralized and intelligent analysis of the security related data reported by the infrastructure using artificial intelligence (AI) and big data technology to output threat intelligence, security strategies, and security situation.

  2) **Security deduction**: Supports deduction of potential security risks and security decisions based on technology like AI and digital twin network. It supports generating security decisions on countermeasures and required trust levels.

  3) **Trust assessment**: Supports the analysis of the required trust levels and the assessment of the trust state which includes either quantitative measurement or qualitative measurement, or both. The quantitative measurement assigns a numeric value as level of

trust, whereas the qualitative approach assigns a rating based on the possible consequences. Trust measurement considers the trust factors and all the fundamental components of trust establishment.

4) **Security services**: Achieves the integration and output of security capabilities as services.

5) **Security management**: Includes, but is not limited to, system management, audit management, centralized control, and security situation warning for the security administrators.

- **Trust infrastructure**: Includes the establishment of trust related capabilities like trust roots and trust chain to support the construction of trusted objects such as trusted network, trusted computing environment, trusted data, trusted application, trusted services, and so on. The construction of these trusted objects can be conducted during delivery and running. Possible trust anchors which are trusted a priori include digital identity system, public key infrastructure and root of trust such as trusted execution environment (TEE), hardware security module (HSM), and trusted platform module (TPM), etc. It also includes an infrastructure of chain of trust such as distributed ledger technology (DLT), blockchain, etc. The units of the trust infrastructure can be flexibly implemented as needed, such as on the network side, terminal side, and application side, accepting the configuration and management from the intelligent security control units, and executing specific trusted functions. The capabilities supported by trust enabling units can vary in order to meet the different needs of different nodes for trustworthiness,
- **Trust factors**: Subjective or objective factors which influence the measurement of level of trust, such as enterprise background, service qualifications, organizational structure, reputation evaluation, development process, operation management, etc.

10 Applicable practices of the framework in the 5G network

This clause provides applicable practices of how the designed built-in security framework can be used in the 5G network, based on existing 5G deployment cases.

In 5G network, some security capabilities, according to the design principles of the built-in security for the telecommunication network, have been recommended to be implemented or supported. These security capabilities include: [b-3GPP TS33.501], [b-3GPP SCAS] [b-GSMA FS.13], [b-GSMA FS.14], [b-GSMA FS.15], [b-GSMA FS.16].

These security capabilities and their associated Specifications are presented in Table 1.

Table 1 – Security capabilities and associated Specifications

Specifications	Security capabilities
Authentication and authorization [b-3GPP SCAS-gNB] [b-3GPP SCAS-AUSF] [b-3GPP SCAS-UDM] [b-3GPP SCAS-UPF] [b-3GPP SCAS-AMF] [b-3GPP SCAS-NRF] [b-3GPP SCAS-NWDAF] [b-3GPP SCAS-NEF]	1) 3GPP primary authentication supports 5G-AKA and other authentication mechanisms to authenticate terminal access. 2) Access authentication of non 3GPP terminals 3) Core NE authentication function. 4) Core network element authorization function. 5) When network capabilities are provided as services for vertical industries, its interface adopt authentication and authentication mechanism.

Table 1 – Security capabilities and associated Specifications

Specifications	Security capabilities
Encryption [b-3GPP SCAS-gNB] [b-3GPP SCAS-AUSF] [b-3GPP SCAS-UDM] [b-3GPP SCAS-UPF] [b-3GPP SCAS-AMF] [b-3GPP SCAS-NEF]	1) Data encryption of user plane data in air interface. 2) Data encryption of control plane data in air interface. 3) Encryption of communication traffic between core network elements. 4) Set up security transmission channel from access network to the core network to realize data encryption. 5) Encryption of communication between network exposure functions and vertical industries. 6) Establish a secure transmission channel (such as IPSec tunnel) between the UPF and the data network.
Security service exposure [b-3GPP SCAS-AUSF] [b-3GPP SCAS-NEF] [b-3GPP SCAS-AAnF]	1) Provide terminal abnormal behaviour analysis capability, abnormal event alarm and other capabilities to the vertical industry. 2) Provide terminal authentication and key derivation capability for vertical industries.
Integrity [b-3GPP SCAS-gNB] [b-3GPP SCAS-UPF] [b-3GPP SCAS-AMF] [b-3GPP SCAS-NEF]	1) User plane data integrity protection. 2) Data integrity protection of control plane. 3) Communication traffic integrity protection between core network elements. 4) Integrity protection of communication data between network and vertical industries.
Cryptographic algorithms [b-3GPP SCAS-gNB] [b-3GPP SCAS-AUSF] [b-3GPP SCAS-UDM] [b-3GPP SCAS-UPF] [b-3GPP SCAS-AMF] [b-3GPP SCAS-N3IWF]	1) Encryption algorithm 2) Integrity protection algorithm 3) Algorithm negotiation 4) Key management
Security context management [b-3GPP SCAS-gNB] [b-3GPP SCAS-AMF]	1) State transition 2) Mobility security context management 3) Security context coordination under 3GPP/non 3GPP access
Privacy protection [b-3GPP SCAS-AUSF] [b-3GPP SCAS-UDM] [b-3GPP SCAS-AMF]	1) Prevent leakage of Subscription Permanent Identifier 2) Ensure that users are informed and consent when using user related information. 3) Prevent users from using slice information disclosure
Non cellular access security + interoperability security [b-3GPP SCAS-AUSF] [b-3GPP SCAS-N3IWF] [b-3GPP SCAS-AMF]	1) Non 3GPP UE access authentication 2) Interoperability security between networks of different generations 3) Wired access security

Table 1 – Security capabilities and associated Specifications

Specifications	Security capabilities
Interconnection security [b-3GPP SCAS-SEPP]	1) Ensure the security of network interfaces between different operators. 2) Defend attacks from one operator's network to another.
Abnormal traffic analyzation [b-GSMA Micro-seg] [b-3GPP SCAS-NWDAF]	Analyse the traffic of terminal abnormal behaviours and the traffic of network element abnormal behaviours. Provide security access control for host, virtual machine or container and visualization management of the east-west traffic.
Active security – security deduction based on digital twin network [b-ITU-T Y.3090]	Digital twin of network which can provide a twin environment with high simulation, high flexibility and low cost can support the deduction of the security risks and security strategies for scenarios such as signal storm attacks, network functions de-registration attacks, distributed denial-of-service (DDoS) attacks, and so on.

Bibliography

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1812] Recommendation ITU-T X.1812 (2022), *Security framework based on trust relationships for the IMT-2020 ecosystem*.

[b-ITU-T Y.3090] Recommendation ITU-T Y.3090 (2022), *Digital twin network – Requirements and architecture*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-3GPP SCAS] 3GPP TS 33.117 V18.0.0 (2023), *Catalogue of General Security Assurance Requirements (Release 18)*.

[b-3GPP SCAS-AAnF] 3GPP TS 33.537 V18.1.0 (2023), *Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF) (Release 18)*.

[b-3GPP SCAS-AMF] 3GPP TS 33.512 V18.0.0 (2023), *5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF) (Release 18)*.

[b-3GPP SCAS-AUSF] 3GPP TS 33.516 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class (Release 18)*.

[b-3GPP SCAS-gNB] 3GPP TS 33.511 V18.0.0 (2023), *Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (Release 18)*.

[b-3GPP SCAS-N3IWF] 3GPP TS 33.520 V18.0.0 (2023), *5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF) (Release 18)*.

[b-3GPP SCAS-NEF] 3GPP TS 33.519 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class (Release 18)*.

[b-3GPP SCAS-NRF] 3GPP TS 33.518 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class (Release 18)*.

[b-3GPP SCAS-NWDAF] 3GPP TS 33.521 V18.0.0 (2023), *5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF) (Release 18)*

[b-3GPP SCAS-SEPP] 3GPP TS 33.517 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class (Release 18)*.

[b-3GPP SCAS-SMF] 3GPP TS 33.515 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class (Release 18)*.

[b-3GPP SCAS-UDM] 3GPP TS 33.514 V18.0.0 (2023), *5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class (Release 18)*.

[b-3GPP SCAS-UPF] 3GPP TS 33.513 V18.0.0 (2023), *5G Security Assurance Specification (SCAS); User Plane Function (UPF) (Release 18).*

[b-3GPP TS33.501] 3GPP TS 33.501 V18.2.0 (2023), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 18)*.

[b-GSMA FS.13] GSMA FS.13 (2019), *Network Equipment Security Assurance Scheme – Overview*.

[b-GSMA FS.14] GSMA FS.14 (2019), *Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process*.

[b-GSMA FS.15] GSMA FS.15 (2019), *Network Equipment Security Assurance Scheme – Product Development and Lifecycle Accreditation Methodology*.

[b-GSMA FS.16] GSMA FS.16 (2019), *Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements*.

[b-GSMA Micro-seg] GSMA, *Guideline of Micro-segmentation in 5G core network resource pool (version 0.6).*

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*.

____