Review Paper about NESAS

by

Nepal Telecommunications Authority (NTA)

Contents

1. Evolution of 5G

5G is an evolution of 3G and 4G technology that will enable new kinds of services. From 2016 to the present, the selected candidate technologies have been evaluated in detail in three 5G target application scenarios: eMBB (Enhanced Mobile Broadband), uRLLC (ultra-Reliable-Low-Latency Communications), and mMTC (massive Machine-Type Communications). eMBB will enhance the user experience with AR/VR, UHD and 360-degree streaming videos, uRLLC will make self-driving cars possible, and mMTC will underpin smart manufacturing. The core networks and radio access networks (RAN) are still separated in 5G, similar to 4G. However, 5G evolves across a broad technological environment which includes virtualization, disaggregation, cloud, AI, IoT and Industry 4.0. Moreover, 5G offers stronger guarantees regarding privacy and security protection than either 3G or 4G.

The Mobile Broadband Standard Partnership Project (3GPP, originally 3rd Generation Partnership Project) unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). It provides with a stable environment to produce the Reports and Specifications that define 3GPP technologies (cellular telecommunications technologies, including radio access, core network and service capabilities).[1]

The Radiocommunication Sector of ITU (ITU-R) Working Party 5D (WP 5D) is responsible for the overall radio system aspects of International Mobile Telecommunications (IMT) systems, comprising IMT-2000, IMT-Advanced, IMT-2020 and IMT for 2030 and beyond.[2] The IMT-2020 technical standard is the name given by the ITU to the 5G standard, that is, the next-generation mobile communication technology to be used after 2020. In July of 2020,

[1] https://www.3gpp.org/about-us/introducing-3gpp

[2] https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx

ITU-R Working Party 5D (WP5D) #35 meeting (teleconference) announced that the 3GPP 5G technology (including NB-IoT) meets the requirements of the IMT-2020 5G technical standard and is officially accepted as the ITU IMT-2020 5G technical standard.[3] The Recommendation ITU-R M.2150-1 of ITU-R includes the **"Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020 (IMT-2020)"[4].** The ITU Radiocommunication Assembly recommends that the terrestrial radio interfaces for IMT-2020 should be:

- **"3GPP 5G-SRIT"**: Developed by 3GPP Proponent as "5G, Release 15 and beyond − LTE+NR SRIT"
- **"3GPP 5G-RIT"**: Developed by 3GPP Proponent as "5G, Release 15 and beyond − NR RIT"
- **"5Gi"**: Developed by TSDSI as "5Gi RIT"
- **"DECT 5G-SRIT"**: Developed by ETSI as DECT-2020 and 3GPP 5G radio interface technology − SRIT

The ITU Radiocommunication Assembly considers that IMT-2020 systems include the new capabilities of IMT that go beyond those of IMT-2000 and IMT-Advanced, and will interwork with and complement existing IMT-systems and their enhancements. The 3GPP 5G technology meets the requirements of the IMT-2020 technical standard in terms of services, spectrum, and technical performance indicators, and has advanced technical capabilities such as a peak rate exceeding 20 Gbit/s, a communication delay of less than 1 ms, and support for 1 million devices per square kilometer.

In Nepal, the 4G ecosystem in the Country is gradually maturing, and Service Providers are planning 5G trial. It is the obligation of the service providers to make sure that all installed 4G

[3] https://www.3gpp.org/news-events/3gpp-news/3gpp-meets-imt-2020

[4] https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-1-202202-I!!PDF-E.pdf

sites shall be of LTE advance standard. This criterion is expected to make the process of migration towards 5G easier. As of now, 60 MHz in 2600 MHz Band (TDD) has been assigned, free of cost, for 5G trial purpose and test network is being assembled. Primary use case is expected to be eMBB for the time being, while the demand for mMTC will be generated imminently and uRLLC is anticipated to grow gradually.

Digital Nepal Framework recognizes Internet as the backbone of Digital Nepal initiative and connectivity for all is critical for the success of Digital Nepal program. It has recommended to take a lead in 5G, rather than be a follower to put Nepal at the forefront of ongoing digital transformation. It is expected that 5G technology will provide the opportunity to reduce the digital divide in Nepal. The technology infrastructure and features of 5G will help Nepal to rapidly materialize the concept of smart cities and digital transformation. “Master Action Plan for Implementation and Promotion of 5G in Vertical Sectors” is also being prepared by NTA.

2. Security Challenges in 5G

5G faces security challenges and opportunities brought by new services, architectures, and technologies, as well as higher user privacy and protection requirements. The industry needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks. The industry as a whole is working together to address new security risks faced by 5G architectures, technologies, and services, and address potential security challenges through unified 5G security standards, common 5G security concepts, and an agreed 5G security framework.

Within the 3GPP Technical Specification Group Service and System Aspects (TSG SA), the main objectives of 3GPP TSG SA WG3 (SA3) includes defining the requirements and specifying the architectures and protocols for security and privacy in 3GPP systems. During 2020, 111 companies (including their subsidiaries) from around the world sent technical experts to six SA3 meetings for the development of 5G security standards. The 3GPP SA3

Working Group has established 42 projects to analyze security threats and risks in various 5G scenarios.[5]

3GPP 5G standards have inherited existing 4G security standards and improved upon these standards. In terms of 5G, new security mechanisms and measures have been designed for cloud, mobile edge computing (MEC), and network slicing.

To address the security challenges in 5G, the security mechanisms in the Release 15 and beyond developed by 3GPP Proponent have evolved in following manner:

- **Release 15 (5G Phase I)[6]**

  Basic Security Architecture and eMBB Security Functions

  - Integrity protection for air interface user plane
  - Subscriber-level security policies (finer granularity)
  - Enhanced air interface encryption protection for user IDs
  - SEPP Protection Inter-PLMN Roaming Messages
  - SBA Security
  - Unified authentication

- **Release 16 (5G Phase II)[7]**

  Vertical industry security enhancement

  - uRLLC security: dual-path transmission security

[5] https://www-file.huawei.com/-/media/corp2020/pdf/trust-center/huawei-5g-security-white-paper-2021-en.pdf

[6] https://www.3gpp.org/specifications-technologies/releases/release-15

[7] https://www.3gpp.org/specifications-technologies/releases/release-16

- mMTC (cIoT) Security: Lightweight Small Packet Transmission Security
- Slice security: defines NSSAAF slice authentication NEs and supports slice secondary authentication
- Non-public Network (NPN) security: EAP based non-public network authentication

Security Authentication

- SCAS 1.0

- **Release 17 (5G Enhancement)[8]**

Continuous evolution of security functions

- Security Capability Exposure: AKMA Authentication and Key Management Based on 3GPP Credentials
- Enhanced slice security: ID broadcast privacy protection
- MEC security (Support for Edge Computing in 5GC): interface security, client authentication and authorization

Security Authentication

- SCAS 2.0/ 3.0

- **Release 18 (5G Advanced)[9]**

Future-oriented security evolution

- 256-bit key algorithm (anti-quantum attack and higher security)

[8] https://www.3gpp.org/specifications-technologies/releases/release-17

[9] https://www.3gpp.org/specifications-technologies/releases/release-18

- Fake base station (FBS) detection
- Automatic 5GC virtual NE certificate management

Security Authentication

- SCAS Evolution

3. NESAS (Network Equipment Security Assurance Scheme)

The GSMA is a worldwide company unifying the mobile ecosystem to explore, develop and deliver an innovation foundation for positive business environments and societal changes. This company brings for its members three main pillars: industry services and solutions, connectivity for good, and outreach.[10]

NESAS, a scheme defined by industry experts through GSMA and 3GPP, is a security assurance framework for the mobile industry. NESAS defines security requirements and an assessment framework for Secure Product Development and Product Lifecycle Processes, as well as security test cases for the security evaluation of network equipment. NESAS is of value to both operators and vendors, and is intended to be used alongside other mechanisms to ensure a network is secure.[11]

The 3GPP specifications define the security scheme while the scheme's processes and requirements are from the GSMA. The 3GPP specifications about network security are as follows:

Table 1: 3GPP Specification about network security

Document Title[12]	**Description**

[10] https://www.gsma.com/aboutus/

[11] https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf

[12] https://www.3gpp.org/specifications-technologies/specifications-by-series

3GPP TS 33.916 Assurance Methodology for 3GPP network products	Network Equipment Evaluation Process and Creation of SCAS
3GPP TS 33.117 Catalogue of general security assurance requirements	Generic SCAS for all Network Functions
SCAS specific to 3GPP-defined Network Functions are published by 3GPP	Reference: https://www.3gpp.org/DynaReport/33-series.htm

GSMA has published following documents regarding NESAS processes and requirements:

Table 2: NESAS documents (processes and requirements)

Document Title	**Description**
FS.13 – NESAS Overview[13]	High level explanation of NESAS
FS.14 – NESAS Security Test Laboratory Accreditation[14]	Test laboratory accreditation process and requirements
FS.15 – NESAS Development and Lifecycle[15]	Methodology for vendor development and lifecycle processes assessment

[13] https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview/

[14] https://www.gsma.com/security/resources/fs-14-network-equipment-security-assurance-scheme-security-test-laboratory-accreditation/

[15] https://www.gsma.com/security/resources/fs-15-network-equipment-security-assurance-scheme-vendor-development-and-product-lifecycle-requirements-and-accreditation-process/

FS.16 – NESAS Development and Lifecycle Security Requirements[16]	Requirement for vendor development and lifecycle processes assessment
FS.46 – NESAS Audit Guidelines[17]	Guidelines to Auditors and Equipment Vendors on how to conduct the vendor assessment
FS.47 – NESAS Product and Evidence Evaluation Methodology[18]	Methodology of product and evidence evaluation

Cyber security assessment mechanisms shall follow globally accepted uniform standards to ensure that their operations are cost-effective and sustainable for the ecosystem. NESAS is used to assess the security of mobile network equipment. It provides an industry-wide security assurance framework to improve the security level across the mobile industry. NESAS uses security test cases in the Security Assurance Specifications (SCAS) defined by 3GPP to assess the security of network equipment. Currently, 3GPP has initiated security evaluation of multiple 5G network equipment, and major equipment vendors and operators are actively participating in the NESAS standard formulation.

[16] https://www.gsma.com/security/resources/fs-16-network-equipment-security-assurance-scheme-development-and-lifecycle-security-requirements/

[17] https://www.gsma.com/security/resources/fs-46-nesas-audit-guidelines-v-1-0/

[18] https://www.gsma.com/security/resources/fs-47-nesas-product-and-evidence-evaluation-methodology-v-1-0/

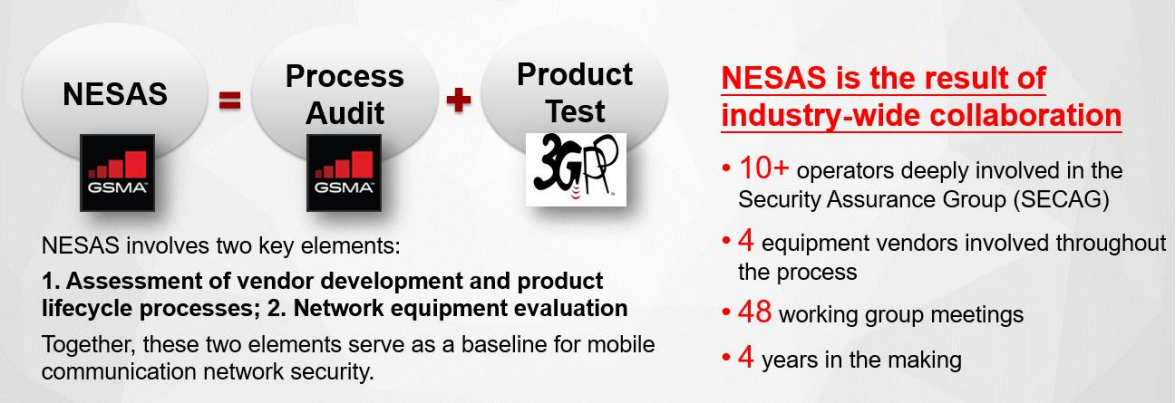


Figure 1: Key Elements of NESAS

The GSMA released NESAS 1.0 in October 2019, continued to evolve NESAS based on industry requirements, and released NESAS 2.1 in January 2022. Currently, the NESAS ecosystem has been established. Mainstream equipment vendors actively participate in NESAS evaluation. The world's top audit bodies and well-known testing labs have been qualified for evaluation.

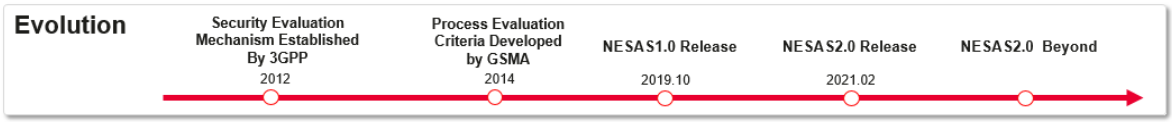
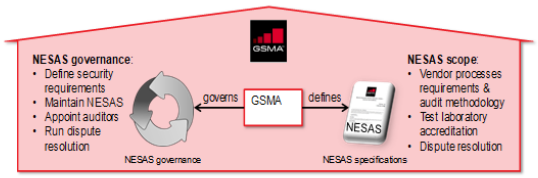
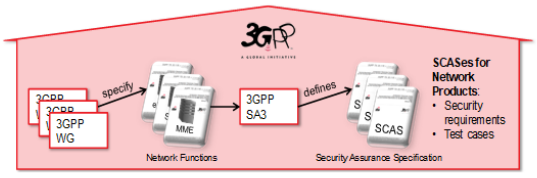


Figure 2: Evolution of NESAS

NESAS promotes security cooperation and mutual trust in the global mobile communications industry, and enables operators, equipment vendors, and other stakeholders to jointly promote 5G security construction. It provides customized, authoritative, efficient, unified, open, and constantly evolving cyber security assessment standards for the communications industry, and is a positive reference for stakeholders such as operators, equipment vendors, and government regulators.





Part 1 (NESAS)	Part 2 (SCAS)
(FS.xx series) Standards developed by GSMA SECAG	(TS 33.xx series) Standards developed by 3GPP SA3
Audit vendor's security development process & product lifecycle management process to ensure the product is securely developed	***Evaluate*** vendor's specific product (like eNB, gNB, AMF, UPF, etc.) to ensure the equipment is secure
By ***Independent Audit Team*** accredited by GSMA	By ***ISO17025 accredited lab***
21 requirements contained	100+ cases depend on products (being extended)
Output audit report	Output evaluation report

Figure 3: Roles of GSMA and 3GPP in NESAS

NESAS brings the following benefits to equipment vendors:

- Provides accreditation from the world's leading mobile industry representative body
- Delivers a world-class security review of security related processes
- Offers a uniform approach to security audits
- Avoids fragmentation and potentially conflicting security assurance requirements in different markets

NESAS brings the following benefits to mobile operators:

- Sets a rigorous security standard requiring a high level of vendor commitment
- Offers assurance that vendors have implemented appropriate security measures and practices
- No need to spend money and time conducting individual vendor audits

NESAS brings the following benefits to regulators:

- Developed by the mobile communications industry as a whole to prevent standards fragmentation
- Open; maintained by the industry; continuously evolving and enhanced

Figure 4: Ecosystem of NESAS

For 5G network, NESAS provides the right kind of standards: customized, authoritative, global, efficient, unified, open, and constantly evolving.

So far, a four-in-one (Carriers, Vendors, Audit Institutions and Labs, Regulator) ecosystem has been formed.

The industry is supposed to work together to make positive contributions to the sustainable development of the global unified security assessment for 5G.

4. NESAS in Global Scenario

The 3GPP not only formulated 5G technical standards, it also defined NESAS, jointly with GSMA, to assess the security of mobile network equipment. NESAS is becoming the basis and reference for 5G schemes developed by different countries and organizations.

The status of recognition and adoption of NESAS in different communities and countries is tabulated below:

Table 3: NESAS in International scenario

Range	Achievement

European Union (EU)	European Union (EU) is preparing European cybersecurity certification scheme for 5G network which needs to comply with the EU Cyber Security Act. In the process of preparation, elements from current industry schemes GSMA's NESAS, the relevant eUICC protection profile and ETSI/3GPP's 5G standards are planned to be re-used.[19]
Germany	In Germany, the Federal Office for Information Security (BSI) has started a new certification program for components of 5G telecommunications networks. The certification program is planned to be based on the "Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation" scheme (NESAS CCS GI) and is aimed primarily at manufacturers of 5G mobile communications components.[20]
Netherlands	Regulation of the Minister of Economic Affairs and Climate of 1 October 2021, no. WJZ/20056324, containing further rules regarding the security and integrity of public electronic communications networks and services (Telecommunications Security and Integrity Regulations) mentions NESAS Scheme as an example of security evaluation measure that can be completed for mobile network equipment.[21]

[19] https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification/ad-hoc-working-group-on-5g-cybersecurity-certification

[20] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220705_Zertifizierung_5G-Komponenten.html

[21] https://zoek.officielebekendmakingen.nl/stcrt-2021-42618.html

Brazil	Item 2 of <ATO Nº 77, DE 5 DE JANEIRO DE 2021> Cyber Security Requirements for Telecommunications Equipment, released by Anatel in 2020 and effective in 2021, lists NESAS/SCAS as the reference standard for telecommunications equipment.[22]
China	NESAS has been approved as the basic standard for 5G security assessment and has been implemented by China's IMT 2020 promotion team. All 5G equipment suppliers in the Chinese market comply with the NESAS standard system. Approximately 1.5 million 5G sites in China's 5G networks (as of December 2021) were expected to be NESAS compliant and certified.[23]
Singapore	Singapore government has acknowledged NESAS (IMDA 21 GHz Public Consultation Document) on 26 July 2021.[24]
Malaysia	CyberSecurity Malaysia is the national cyber security specialist agency under the purview of the Ministry of Communications and Multimedia.[25] CyberSecurity Malaysia, Celcom and Huawei Malaysia jointly kick off cyber security lab with the objective of understanding, learning, managing, mitigating, and reducing 5G-related cyber threats while introducing the Network Equipment Security Assurance Scheme (NESAS), to help build a safe, resilient, and inclusive digital ecosystem in Malaysia.[26]

[22] https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302

[23] http://www.caict.ac.cn/kxyj/qwfb/bps/202002/t20200204_274118.htm

[24] https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Consultations/2021/Next-Wave-of-5G-Growth-and-Deployment-in-Singapore/21-GHz-Public-Consultation-Document.pdf?la=en&hash=871CDE093D95FA731129030985E8DECD

[25] https://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html

[26] https://www.cybersecurity.my/data/content_files/44/2224.pdf

Sri Lanka	Sri Lanka CERT and multi-stakeholder discussed about NESAS scheme in 8th Annual Cyber Security Summit held on 30th Nov 2021.[27], [28]
Thailand	The Office of the National Broadcasting and Telecommunications Commission (NBTC) released the national 5G security guideline, which acknowledges NESAS standards.[29]
Philippines	Philippines Department of Information and Communications Technology（DICT）officially released the national 5G security guideline, recognized which recognized NESAS.[30]
Laos	Laos Ministry of Technology and Communications（MTC） officially released the national 5G security guideline, and recognized NESAS on 1st July 2022.[31]
Organization of The Islamic Cooperation	The Organization of The Islamic Cooperation (OIC) is an intergovernmental organization founded in 1969, consisting of 57 member states including Malaysia, Tunisia, Nigeria, Pakistan, Saudi Arabia and United Arab Emirates[32]. It has approved and accepted the Resolution on "Collaboration of

[27] https://www.ft.lk/it-telecom-tech/5G-roll-out-challenges--Governance--legislation--awareness--capacity-and-NESAS-standards/50-726824

[28] https://www.mpt.gov.la/index.php?r=site/downloadfile&file=pjRvXRtljQT-h2kVFmOQaZ/ece66ff64da4a2ed72fd20c072abd846.pdf

[29] https://www.nbtc.go.th/News/govnewspartner/51190.aspx

[30] https://dict.gov.ph/wp-content/uploads/2022/07/The-Need-for-Philippines-Security-Standards-and-Framework-in-5G-Equipment-2022-07-01.pdf

[31] https://mtc.gov.la/index.php?r=site%2Fdetail&id=897

[32] https://www.oic-cert.org/en/history.html#.Y0rqtHZBxD8

(OIC)	Computer Emergency Response Team (CERT) Among the OIC Member Countries". The OIC-CERT 5G Security Framework specifies that 5G equipment layer's cybersecurity is confirmed to apply network equipment security assurance scheme (NESAS) and security assurance specification (SCAS) for network products, which are developed by GSMA and 3GPP, respectively.[33]

5. Network Security Schemes in Nepal

NTA has framed Cyber Security Bylaw, 2020 for the implementation of cyber security standards and best practices so as to protect ICT Infrastructure and Information Systems of Telecommunication Service Providers of Nepal from various malicious attacks and threats; and build trust and confidence of users towards using ICT technology and services. Following Provisions are included in the Bylaw[34]:

- Provisions Relating to General Security Standards and Practices
- Provisions Relating to Infrastructure/Network Security
- Provisions Relating to Core System Security
- Provisions Relating to Application Security
- Provisions Relating to Data Security/Privacy
- Provisions Relating to Information System (IS) Audit
- Provisions Relating to Cloud Security

[33] https://www.oic-cert.org/en/journal/pdf/4/1/2.pdf

[34] https://nta.gov.np/wp-content/uploads/2020/08/Cyber-Security-Bylaw-2077-2020.pdf

- Provisions Relating to CERT/Incident Response
- Provisions Relating to Security Operations Centre (SOC)
- Provisions Relating to Cyber Security Awareness & Capacity Building

The provisions related to infrastructure/network security in the bylaw are of generic nature. No specific schemes are formulated or recommended regarding minimum security measures for 5G networks. As the 4G sites in Nepal are required to be of LTE advance standard, it can be said that the regulator is already envisaging upgrade of the current mobile network to the 5G ecosystem. Therefore, it is also necessary to formulate 5G security schemes to address the security challenges imposed by 5G.

6. Conclusion

NESAS, the Network Equipment Security Assurance Scheme, is a security advancement aimed at 5G communication. The NESAS framework covers security standard requirements and assessment of the quality and characteristics of telecommunication equipment from the planning, design and development phase to the manufacturing and testing that benefits both telecom equipment manufacturers and telecom operators. This framework can be used by manufacturers to develop and manufacture equipment of high quality and safety features. Telecom operators, regulators and relevant agencies can also take advantage from this framework to develop policies and measures to provide the more secured telecommunication services. NESAS introduces a security baseline, which participating equipment vendors are requested to achieve by fulfilling the security requirements. The NESAS framework are used to create a nationally neutral and transparent security standard in some countries.

Unified cybersecurity standards and compliance methods that include standardized verification and testing helps in the development of a greater level of confidence and a more competitive, transparent playing field. In contrast to a world with various standards and diverse supply chains, a cyberspace enabled by unified standards is more likely to stimulate vigorous competition, resulting in higher quality, cheaper costs, improved security, and increased resilience.

Nepal Telecommunications Authority (NTA) should recognize the importance of adopting security standard framework such as NESAS SCAS for regulatory basis to standardize telecommunication services that are effective and provide the enhanced level of security for subscribers. The most

important benefit is the process by which all sectors play a role in driving modern and secure telecommunication services, particularly by collaborating to develop more secure telecommunication services using security framework like NESAS, SCAS framework as a key guideline.