SZTFH Decree No

…../2025 (… …) of the President of Supervisory Authority for Regulatory Affairs

on a national cybersecurity certification scheme for 5G network devices

[1] The purpose of this regulation, issued by the President of the Supervisory Authority for Regulatory Affairs (hereinafter: SZTFH), is to support the decisions of citizens, business entities and public authorities in the procurement of 5G network devices by assessing the security, resilience and availability of 5G networks based on international standards, and to ensure the comparability of the devices based on the assurance levels specified in the certification scheme.
[2] On the basis of the authorisation granted under Section 81(6)(m) of Act LXIX of 2024 on cybersecurity in Hungary,
with regard to Section 9(3) and (4), on the basis of the authorisation granted under Section 81(6)(k) of Act LXIX of 2024 on cybersecurity in Hungary,
and acting within the scope of my duties as defined in Section 13*(n)* and *(q)* of Act XXXII of 2021 on the Supervisory Authority for Regulatory Affairs, I hereby order the following:

Section 1

(1) For the purposes of this Decree, a 5G network device is defined as an ICT product within the meaning of Act LXIX of 2024 on cybersecurity in Hungary (hereinafter: Cybersecurity Act) which meets the requirements of paragraph 2 and is part of the infrastructure of a 5th generation mobile network (hereinafter: 5G networks), including base stations.

(2) A 5G network device as referred to in paragraph 1 consists of:
a) hardware - in particular chip, processor, RAM, network card,
b) firmware or software - in particular operating system, drivers, applications, services, protocols, and
c) interfaces - in particular console and operational interfaces;
which achieves the functionality of one or more network product classes according to Annex 1.

Section 2

The National Cybersecurity Certification Scheme for 5G network devices (hereinafter referred to as the ‘certification scheme’) shall apply to the conformity assessment (hereinafter referred to as the ‘conformity assessment’) and certification of 5G network devices.

Section 3

For the purposes of this Decree:
1. *assessment evidence:* any evidence which should be submitted to the conformity assessment body by the manufacturer of a 5G network device pursuant to the Cybersecurity Act (hereinafter referred to as the ‘manufacturer’) or by the customer of the conformity assessment (hereinafter referred to as the ‘client’), demonstrating that the requirements for the development and product life cycle process and the security expectations for the 5G network device have been correctly applied in the manufacturer’s and the supplier’s processes;

2. *development and product lifecycle process:* stages in the development of a 5G network device, including design, implementation, testing, release, manufacturing and delivery, and end-of-life stages, including maintenance and updates;
3. *network function*: a processing function defined in a network with specific functional behaviour and specific interfaces;
4. *manufacturer's declaration:* a written declaration from the 5G network device manufacturer confirming that the 5G network device complies with the requirements of the certification scheme in terms of the development and product life cycle processes (which are subject to assessment) and the security expectations for the 5G network device.

Section 4

(1) The certification scheme contains requirements for a 'high' assurance level in accordance with Section 40(1) of the Cybersecurity Act.

(2) Unless otherwise provided for in EU or Hungarian legislation, the marketing or use of a 5G network device is not subject to the condition that the 5G network device has a national cybersecurity certificate issued under the certification scheme.

(3) Conformity self-assessments under the certification scheme cannot be performed. Verification by the manufacturer of whether the requirements have been met does not constitute a conformity self-assessment within the meaning of the Cybersecurity Act.

(4) Conformity assessment may be carried out, at the request of the manufacturer or the client, by a conformity assessment body which was registered with 'high' assurance level by SZTFH as the national cybersecurity certification authority designated in Section 45(1)(a) of the Cybersecurity Act (hereinafter referred to as the 'certification authority').

Section 5

(1) The certification scheme is based on the "Network Equipment Security Assurance Specification" cybersecurity assessment framework (hereinafter: NESAS), jointly developed by the Groupe Speciale Mobile Association (hereinafter: GSMA) and the Third Generation Partnership Project (hereinafter: 3GPP), and the German "Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation" (NESAS CCS-GI).

(2) The purpose of the certification scheme is to lay down basic security requirements for 5G network devices, ensuring that manufacturers comply with the specified security requirements during their development and life cycle and that the security properties of 5G network devices can be assessed.

Section 6

(1) The NESAS documents defining the certification scheme are listed in point 2 of Annex 2, with the provision that the documents shall be applied with the derogations set out in Annex 3.

(2) Conformity assessment shall be carried out on the basis of that version of the documents referred to in point 2 of Annex 2, which was valid at the time when the conformity assessment agreement was concluded. Modifications to the versions may be made during the ongoing

conformity assessment procedure at the express request of an entity which is party to the conformity assessment and with the consent of all contracting parties.

(3) The documentation requirements that should be submitted for conformity assessment are set out in Annex 4. The manufacturer or client shall provide the conformity assessment body with the documents and assessment evidence necessary for the conformity assessment in Hungarian or in English.

(4) In the conformity assessment of a 5G network device, the conformity assessment body shall assess all the development and product lifecycle processes (as set out in Annex 5) which are relevant for the network product class for the 5G network device or 5G network devices under assessment, according to Annex 1.

(5) Where the assessment referred to in paragraph 4 has been successfully completed, the conformity assessment body shall carry out an assessment of the technical properties of every functional unit of the 5G network device or of the ones covered by the conformity assessment agreement, based on the requirements laid down in Annex 1 and in point 3 of Annex 2.

Section 7

(1) The requirements for the development and product life cycle processes are set out in the document mentioned in row 7 of the table in point 2 of Annex 2, which shall apply with the derogations set out in Annex 3.

(2) The assessment process for development and product life cycle processes is set out in the document referred to in row 6 of the table in point 2 of Annex 2, which shall apply with the derogations set out in this Decree.

(3) Before initiating a conformity assessment, the manufacturer shall carry out a preliminary assessment of compliance with the requirements set out in row 7 of the table referred to in point 2 of Annex 2. The manufacturer shall provide the conformity assessment body with the manufacturer’s declaration, the document supporting the assessment, and the assessment evidence accompanying the manufacturer’s declaration.

(4) Conformity assessment may be carried out on the basis of the documents provided in accordance with paragraph 3, if the documents have been issued within two years prior to the start of the assessment.

(5) In relation to the assessment referred to in Section 6(4), the conformity assessment body shall draw up an assessment report with the content referred to in point 1 of Annex 6, documenting the results of the evidence assessment and the assessment of the 5G network device from the point of view of development and life-cycle safety requirements.

Section 8

(1) For the assessment of the 5G network device, the manufacturer shall define the scope of the assessment under Section 6(5) by specifying the network function or network functions provided by the 5G network device. The 5G network device must provide one or more network functions. Each network function includes specific procedures and interfaces, which must be defined in a technical specification. Where the network device consists of more network functions than those covered by the assessment, the device manufacturer shall also identify them

and declare them as functions outside the scope of assessment. The conformity assessment body shall document the scope of the assessment in the assessment report and also list the network functions of the 5G network device that are not covered by the assessment.

(2) The certification scheme shall use the assessment methodology set out in row 9 of the table in point 2 of Annex 2 and the documents set out in point 3 of Annex 2 for the assessment of the security of 5G network devices, the versions of which shall be continuously updated by the NESAS scheme management working group. The documents referred to in point 3 of Annex 2 shall apply in the version in force on the date when the conformity assessment agreement was concluded. Amendments to the versions applicable in the ongoing conformity assessment procedure may only be made in accordance with Section 6(2).

(3) The Conformity Assessment Agreement specifies
- a) the scope of the assessment pursuant to paragraph (1), and
- b) in accordance with the network functions provided by the 5G network device subject to evaluation, the applicable security specifications called Security Assurance Specification (hereinafter: SCAS), against which the assessment is carried out by the conformity assessment body.

(4) Two types of SCAS may be applied to a 5G network device:
- a) generic SCAS, applicable to any network product and all its functions, and
- b) specific SCAS, which concerns only certain network functions.

(5) The following guidelines shall be used to identify the types of SCAS that are to be used:
- a) all network products under assessment are, in any case, covered by the document referred to in row 2 of the table in point 3 of Annex 2, and it cannot be excluded,
- b) for network functions specified by 3GPP, the corresponding specific SCAS types shall be used, with the provision that
- (ba) if there are specific types of SCAS for the network functions that are part of the product which is to be evaluated, these are also the subject of the evaluation, or
- (bb) if no specific SCAS exists for the product subject to assessment, only the generic SCAS may be used, and
- c) each type of SCAS applies only to a particular network function.

(6) The manufacturer shall carry out a preliminary assessment before initiating the assessment referred to in Section 6(5). The completed document and the related assessment evidence shall be made available to the conformity assessment body carrying out the assessment.

(7) The detailed rules for the evaluation process referred to in Section 6(5) shall be laid down in the document referred to in row 9 of the table set out in point 2 of Annex 2.

(8) The conformity assessment body shall draw up an assessment report on the assessment pursuant to Section 6(5), with the content set out in point 2 of Annex 6, documenting the results of the assessment of the evidence and the assessment of the 5G network device. The conformity assessment body shall hand over the assessment report to the manufacturer or the client.

Section 9

(1) The conformity assessment body may issue a national cybersecurity certificate in accordance with Annex 7 if the assessment of the 5G network device pursuant to Section 6(4) and (5) has resulted in a ‘pass’ mark in accordance with points 1.3.1 and 2.2.1 of Annex 6.

(2) The language of the assessment report and the certificate prepared in the course of the assessments pursuant to paragraphs (4) and (5) of Section 6 shall be Hungarian, from which the client and the conformity assessment body may derogate in the conformity assessment agreement.

(3) Once the national cybersecurity certificate has been issued, the conformity assessment body shall submit the completed assessment documents to the certification authority for registration, for which it shall use an electronic form created for this purpose by the certification authority, and shall inform the manufacturer or client at the same time.

(4) The administrative time limit for registration pursuant to paragraph 3 shall be 45 days.

(5) The validity period of the national certificate (hereinafter referred to as ‘period of validity’) is maximum 5 years from the date of issue.

(6) The manufacturer is obliged to affix, as a conformity marking, a label provided for in the Decree of the President of the Supervisory Authority for Regulatory Affairs on the cybersecurity certification of information and communication technologies. This shall be affixed to 5G network devices which have been produced until the expiry of the validity period and that have a national certificate, with the content specified in the decision of the certification authority.

Section 10

(1) Except as provided for in paragraph 2, changes to the documents referred to in points 2 and 3 of Annex 2 shall not affect the validity of an existing national cybersecurity certificate.

(2) It is the manufacturer’s responsibility to monitor the security of the certified 5G network device it manufactures. If the manufacturer becomes aware of threats to the security of a certified 5G network device that have not been addressed by the manufacturer, or that a change to the documents referred to in points 2 and 3 of Annex 2 is motivated by the emergence of new threats presenting a serious risk to the security of the 5G network device, it shall inform the conformity assessment body thereof.

(3) The conformity assessment body shall inform the certification authority of the requirements set out in paragraph 2 and of any new relevant threat to the security of the certified 5G network device not addressed by the manufacturer. In its decision, the certification authority will set a deadline for the modification of the 5G network device to eliminate the risk and for the conformity assessment of this modification. In case of failure to comply with the decision within the deadline, the conformity assessment body shall withdraw the national cybersecurity certificate.

Section 11

(1) During the period of validity, the manufacturer shall continuously and consecutively conduct safety impact assessments for each change that may affect a certified 5G network device, stating:

a) the date of change,
b) the reason for the change,
c) whether the change affects the certified 5G network devices manufactured prior to the change,
d) a detailed description of the elements of the change,
e) what risks are affected by the change, and
f) whether the change addresses a vulnerability or introduces a new security control.

(2) For the purposes of paragraph 1, any change that affects the security status of the 5G network device, including the emergence of new threats and vulnerabilities, shall be considered as a change.

(3) Any incident affecting the development and product life cycle processes of a 5G network device registered on the basis of a national cybersecurity certificate shall be reported by the manufacturer to the conformity assessment body that issued the national cybersecurity certificate and to the certification authority.

(4) The national cybersecurity certificate shall, subject to the conditions set out in paragraph 6, cover those changes that the manufacturer disclosed concerning the certified 5G network device during the validity period and that are considered minor updates. Changes to the security functions covered by the assessment or to the nature of the 5G network device that are intended to maintain or restore the validity of the manufacturer's declaration or the assessment evidence submitted, or that are not relevant for such assessment evidence, should be considered to be minor updates, including the elimination of functional failures or changes made to avoid inappropriate use of the 5G network device. Minor updates to the 5G network device shall be clearly identified by the manufacturer in the product version in accordance with paragraph 1.

(5) A change to a security patch which modifies a security function or introduces a new function is not considered a minor update.

(6) A minor update shall be covered by a national cybersecurity certificate if the manufacturer sends the information on the update, together with the security impact assessment referred to in paragraph 1 (hereinafter jointly referred to as 'change documents'), to the conformity assessment body before the 5G network device is made available on the market with the update, and the conformity assessment body does not raise objections within 40 days of receipt. A product with a minor update shall be considered certified during the 40-day period. If, on the basis of the change documents, the conformity assessment body accepts the change as a minor update, the conformity assessment body shall make a statement on extending the validity to the new version and shall inform the certification authority accordingly.

(7) If the conformity assessment body concludes that the update cannot be considered a minor update, the conformity assessment body shall inform the client of its objections, setting a deadline of 15 days for a response. The deadline for reply may be extended once by 5 days in justified cases. If the consultation with the client fails, the National Cybersecurity Certificate shall apply to the last authenticated version of the 5G network device and its minor updates.

If the manufacturer provides the change documents for minor updates under the certification scheme for the assessment under paragraph 6, additional costs may be incurred for the assessment, which shall be provided for in the conformity assessment agreement.

Section 12

(1) In order to renew the national cybersecurity certificate, the manufacturer or the client shall inform the conformity assessment body that issued the national cybersecurity certificate if:

a) five years have elapsed since the previous audit and the manufacturer wishes to renew the validity of the certificate after reassessment;
b) a significant safety incident has occurred in the manufacturer's environment during the manufacturer's development process of the product life cycle process, which is likely to have had an impact on the processes being assessed;
c) significant changes have been made to the 5G network device which affect the validity of the national cybersecurity certificate, and which are classified as non-minor updates.

(2) In the case referred to in paragraph 1, the conformity assessment shall be carried out again. In the case referred to in paragraph 1(c), the rules on conformity assessment shall apply to the conformity re-assessment of the modified 5G network device, with the provision that the assessment referred to in Section 6(4) does not need to be carried out again if it was performed not more than a year ago.

Section 13

The period of validity cannot be extended for any certificate issued under the certification scheme.

Section 14

This Decree shall enter into force on the third day following its publication.

Section 15

The requirement for the prior notification of this draft decree, as stipulated in Articles 5 to 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, has been met.

Annex 1 to SZTFH Decree No …/2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Network product classes and requirements

1.1 Generic Network Product (GNP) Class

Overview

The 3GPP generic network product class defines devices that implement a common set of functions defined by a common 3GPP. This includes the components of the hardware, software and operating system, as well as the interfaces that allow the product to be managed and configured locally and remotely. The objective of the GNP classes is to lay down security requirements and test cases for products to ensure the reliability and security of telecommunications networks.

Related SCAS: 3GPP TS 33.117 Catalogue of general security assurance requirements

Applicable release: Release 16.6 or higher

1.2 Mobility Management Entity (MME)

Overview

MME belongs to the network product classes which implement functions related to mobility management. This includes the management of user identities, authentication parameters and the data needed to manage network traffic. MMEs must comply with the security requirements laid down by the 3GPP to ensure the protection of network resources and the continuity of service.

Related SCAS: 3GPP TS 33.116 Security Assurance Specification (SCAS) for the MME network product class

Applicable release: Release 17 or higher

1.3 Evolved Node B (eNB)

Overview

eNB is the radio access point for 4G networks, which plays a key role in the LTE network. The eNB is responsible for providing the radio interface to the subscribers and for forwarding traffic to the core network. eNBs must also comply with the 3GPP security standards to protect network data and ensure the security of the service.

Related SCAS: 3GPP TS 33.216 Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

Applicable release: Release 17 or higher

1.4 Packet Gateway (PGW)

Overview

The Packet Gateway (PGW) networking product class is a critical component of mobile networks, playing a central role in managing data traffic on 4G/LTE and 5G networks. PGW is responsible for the management of data packets, traffic management and the provision of user data and services on the mobile network. In addition, the PGW integrates network security functions such as firewalls and intrusion detection systems to protect the network from external attacks

Related SCAS: 3GPP TS 33.250 Security assurance specification for the PGW network product class

Applicable release: Release 17 or higher

1.5 Network Slice Selection Assistance and Authorisation Function (NSSAAF)

Overview

The NSSAAF (Network Slice Selection Assistance and Authorisation Function) network product class plays a key role in the management and optimization of network slices in 5G networks. NSSAAF shall facilitate the selection and allocation of network slices based on different services and user needs, thereby ensuring the efficient and dynamic allocation of resources. This functionality is particularly important in 5G networks where different applications and services (e.g. IoT, eMBB, URLLC) have different network requirements.

Related SCAS: 3GPP TS 33.326 Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class

Applicable release: Release 17 or higher

1.6 Next generation Node B (gNodeB)

Overview

The gNodeB (gNB) networking product class is a core component of 5G networks that performs the functions of a radio access network (RAN). gNodeB is responsible for managing radio frequency signals, ensuring communication between user devices and the mobile network, and forwarding data traffic to the 5G core network. In addition, gNodeB supports high-speed data transmission, low latency and high connection density which are essential for the various 5G applications such as real-time IoT, self-driving vehicles and augmented reality.

Related SCAS: 3GPP TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

Applicable release: Release 17 or higher

1.7 Access and Mobility Management Function (AMF)

Overview

AMF is responsible for access and mobility management functions in 5G networks. This includes user login, identity management, and mobility management between network slices. AMF ensures that subscribers have access to the appropriate services while moving within the network.

Related SCAS: 3GPP TS 33.512 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)

Applicable release: Release 17 or higher

1.8 User Plant Function (UPF)

Overview

The UPF network product class is a key component of 5G networks, playing a central role in the management and transmission of data traffic. UPF is responsible for processing and routing data packets between user devices and the 5G core network, as well as optimising network traffic and minimising latency.

Related SCAS: 3GPP TS 33.513 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

Applicable release: Release 17 or higher

1.9 User Data Management (UDM)

Overview

UDM is responsible for managing subscriber data in 5G networks. This includes user profiles, authentication data and information necessary to access the services. UDM ensures that subscriber data is secure and that only authorised network elements have access to it.

Related SCAS: 3GPP TS 33.514 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

Applicable release: Release 16 or higher

1.10 Session Management Function (SMF)

Overview

SMF is responsible for managing network slices and data traffic in 5G networks. This includes the creation, modification and deletion of PDU sessions. SMF ensures that data traffic in the network is managed efficiently and safely.

Related SCAS: 3GPP TS 33.515 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

Applicable release: Release 17 or higher

1.11 Authentication Server Function (AUSF)

Overview

AUSF is responsible for the authentication of users in 5G networks. This includes the management of authentication vectors and the authorisation of access to services. AUSF shall ensure that users have secure access to network services.

Related SCAS: 3GPP TS 33.516 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

Applicable release: Release 17 or higher

1.12 Security Edge Protection Proxy (SEPP)

Overview

SEPP is responsible for managing the security links between networks in 5G networks. This includes the encryption and authentication of messages to protect traffic between networks. SEPP ensures that network connections are secure and reliable.

Related SCAS: 3GPP TS 33.517 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

Applicable release: Release 17 or higher

1.13 Network Repository Function (NRF)

Overview

NRF is responsible for the registration and discovery of network functions in 5G networks. This enables network elements to find each other and communicate with each other. NRF shall ensure that the services in the network are available and up-to-date.

Related SCAS: 3GPP TS 33.518 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

Applicable release: Release 17 or higher

1.14 Network Exposure Function (NEF)

Overview

NEF is responsible for the exposure of network services to external applications in 5G networks. This allows third-party applications to access network services in a controlled and secure manner. NEF shall ensure that network services are securely and reliably accessible to external partners.

Related SCAS: 3GPP TS 33.519 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

Applicable release: Release 17 or higher

1.15 Network Data Analytics Function (NWDAF)

Overview

NWDAF is a key network product class in the 5G architecture, providing data analysis and network intelligence. NWDAF supports the networks' automated decision-making capabilities by analysing large amounts of network data in real time, thereby helping network management and improving service quality. This feature enables service providers to better understand network traffic and user behaviour, optimise network resources, and proactively manage network performance and security issues.
Related SCAS: 3GPP TS 33.521 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)
Applicable release: Release 16 or higher

1.16 Service Communication Proxy (SCP)
Overview
The SCP is an important network product class in the 5G architecture, which plays a key role in mediating communication between different network functions. The SCP is responsible for the relationship between the different network services and applications, helping to facilitate the efficient flow of network messages and data. In addition, SCP supports the modular and flexible architecture of the 5G network, allowing providers to respond quickly and effectively to changing user needs and network conditions.
Related SCAS: 3GPP TS 33.522 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)
Applicable release: Release 17 or higher

1.17 Split gNB product classes
Overview
Split gNB, i.e. the Shared Generation Node B, is a special network product class in 5G network infrastructure, which makes it possible to distribute the functions of a base station among several different entities. This distributed architecture helps to increase network flexibility and scalability, allowing service providers to manage network resources more efficiently and better adapt to changing user needs. In a split gNB model, the control functions (CU - Control Unit) and data functions (DU - Data Unit) can be separated, which optimises network performance and improves network security.
Related SCAS: 3GPP TS 33.523 5G Security Assurance Specification (SCAS); split gNB product classes
Applicable release: Release 18 or higher

1.18 Management and Orchestration Function (MnF)
Overview
MnF is a vital network product class in 5G networks that performs network resource management and orchestration. This function assists in the efficient allocation and management of network resources, supporting the smooth and dynamic provision of network services. MnF plays a key role in the automated deployment, configuration and maintenance of network functions, increasing the efficiency of network operations and reducing the potential for errors.
Related SCAS: 3GPP TS 33.526 Security assurance specification for the Management Function (MnF)
Applicable release: Release 18 or higher

1.19 3gpp virtualized network products
Overview
The class of network products virtualised by 3GPP includes the network functions and components that are implemented in software, thus enabling a more flexible and cost-effective management of resources. These virtualised products play a critical role in modern 5G

networks, supporting dynamic scalability and the rapid deployment of new services. By means of virtualised network functions (VNNF) and infrastructures for the virtualisation of network functions (NFVI), service providers are able to optimise network resources according to needs in real time. 3GPP standards also specify the security requirements for such virtualised products, ensuring the protection of network integrity and user data.

Related SCAS: 3GPP TS 33.527 Security Assurance Specification (SCAS) for 3GPP virtualized network products

Applicable release: Release 18 or higher

Annex 2 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Documents that define the certification scheme

1. The certification scheme, pursuant to NESAS, includes both process and product assessments, with a particular focus on the security of 5G network devices.

2. The documents to be used in the conformity assessment under the certification scheme are as follows:

	A	B
1.	**Document ID**	**Title**
2.	FS.13 – NESAS Overview	Network Equipment Security Assurance Scheme – Overview
3.	3GPP TR33.926	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
4.	GSMA FS.13	Network Security Assurance Scheme - Overview
5.	GSMA FS.14	Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation
6.	GSMA FS.15	The audit assessment for network equipment vendors' processes. Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology
7.	GSMA FS.16	Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements
8.	GSMA FS.46	Network Equipment Security Assurance Scheme – Audit Guidelines
9.	GSMA FS.47	Network Equipment Security Assurance Scheme – Product and Evidence Evaluation Methodology
10.	GSMA FS.50	Network Equipment Security Assurance Scheme – Security Assurance Specification Development Guidelines
11.	List of Security Assurance Specifications	NESAS Documents

3. The applicable SCAS requirements and tests are set out in the following documents:

	A	B	C
1.	**Document Number**	**Document Title**	**Technology Parameter**
2.	33.117	Generic Network class Catalogue of general security assurance requirements	LTE, 5G
3.	33.116	Security Assurance Specification (SCAS) for the MME network product class	LTE
4.	33.216	Evolved Node B (eNB) network product class	LTE
5.	33.250	Security assurance specification for the PGW network product class	LTE
6.	33.326	Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class	5G
7.	33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class	5G
8.	33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)	5G
9.	33.513	User Plane Function (UPF) 5G SCAS	5G
10.	33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class	5G
11.	33.515	Session Management Function (SMF) network product class. 5G SCAS	5G
12.	33.516	Authentication Server Function (AUSF) network product class. 5G SCAS	5G
13.	33.517	Security Edge Protection Proxy (SEPP) network product class. 5G SCAS	5G
14.	33.518	Network Repository Function (NRF) network product class. 5G SCAS	5G
15.	33.519	Network Exposure Function (NEF) network product class. 5G SCAS	5G
16.	33.521	Network Data Analytics Function (NWDAF). 5G SCAS	5G
17.	33.522	Service Communication Proxy (SCP). 5G SCAS	5G
18.	33.523	Split gNB product classes 5G SCAS	5G
19.	33.526	Management Function (MnF) 5GSCAS	5G
20.	33.527	3GPP virtualized network products 5G SCAS	5G

Annex 3 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Differences between NESAS and the national cybersecurity certification scheme for 5G network devices

1. NESAS documents shall be used in the certification scheme with the following derogations.

1.1. Where notification to GSMA is required by NESAS, the manufacturer and the conformity assessment body shall notify the certification authority with the same content.

1.2. The assessment processes pursuant to Sections 7 and 8, as mentioned in the documents referred to in rows 6 and 9 of the table in point 2 of Annex 2, shall be defined uniformly in the certification system as an assessment process, with the same content.

1.3. Where NESAS Security Test Laboratory is mentioned in the documents, it should be understood as a conformity assessment body that meets the requirements for testing laboratories, and also holds ISO/IEC 17025 accreditation.

1.4. In the assessment of a 5G network device, only SCASs defined in this certification scheme may be used.

Annex 4 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Documents to be submitted for conformity assessment, evidence of assessment

1. When assessing the development and product life cycle processes, the assessment evidence shall demonstrate that the manufacturers' preliminary assessments and safety measures meet the safety objectives underlying the requirements set out in Chapter 6 of the document referred to in row 7 of the table in point 2 of Annex 2 and those in Annex 5.

1.1. The manufacturer shall present two types of assessment evidence to demonstrate compliance with the certification scheme for each of the requirements:
1.1.1. Audit Evidence Category 1: Evidence related to product development or product lifecycle processes at the enterprise or product family level, including process evidence related to version control, vulnerability management, testing procedures, design guidelines or principles, testing principles and practices, threat modelling methodologies, which must be adhered to by the entire enterprise or product family concerned.
1.1.2. Audit evidence Category 2: Evidence which demonstrates that the security measures described in Category 1 of the audit evidence have been implemented in the product family subject to audit, including design documentation, test reports, IT platforms, tools, completed checklists, review records, certificates, logs, which the conformity assessment body checks to ensure compliance.

1.2. In the assessment, the audit evidence referred to in points 1.1.1 and 1.1.2 shall be evaluated against the following criteria to determine whether the requirements of the certification scheme have been implemented:
1.2.1. Coverage: whether the implemented measures are documented for the business groups or organisations covered by the scope of the assessment, e.g. whether the relevant process descriptions are available for all NESAS requirements.
1.2.2. Effectiveness: the effectiveness of the implemented measures, such as whether the manufacturer has trained professionals, whether information is managed by IT systems, whether there are review and problem-solving mechanisms, continuous improvement processes.
1.2.3. Efficiency: the efficiency of the implemented measures, such as whether the manufacturer is able to perform automatic code scanning, source code inspection, testing, the testing of components based on a common knowledge base, tool pools, or checklist generation.
1.2.4. Application: application of the implemented measures, such as the submission of evidence demonstrating that the manufacturer is training its professionals, applies automatic code reading and tests its network products.

1.3. In the case of the evaluation of 5G network devices, it is necessary to provide the evidence referred to in row 9 of the table in point 2 of Annex 2.

Annex 5 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Development and life cycle safety requirements

1. Definition of the manufacturer's development and product life cycle

Within NESAS, the manufacturer's development and product lifecycle shall cover all aspects affecting the lifecycle of a 5G network device (for the purpose of this Annex, hereinafter referred to as 'network product'), including planning, implementation, delivery, upgrade and decommissioning.

1.1. Network product development process

Network product development has the following phases:

	A	B
1.	**Phase**	**Description**
2.	Design	Planning the requirements of the first release in the case of a new network product.
3.	Design	In the case of a new version of an existing network product, planning the requirements for the changes that are to be introduced with the next release, on the basis of the updated functional requirements and, where appropriate, the error and vulnerability reports received in relation to the previous versions.
4.	Design	The implementation of the requirements envisaged for the release under rows 2 and 3 has been planned in detail.
5.	Implementation and software build-up	The planned requirements will be implemented in accordance with the plan and the network product will be constructed.
6.	Testing and audit	Compliance with the requirements will be checked during implementation according to row 5. This section also includes security-related testing and audit activities. If the audit fails, the relevant requirement is returned to the 'Implementation and software build-up' phase.
7.	Release creation	Decision to release a specific review of a tested and verified implementation.
8.	Production	Transformation of a development release into a transportable network product. In the case of pure software delivery, the production phase in the delivery process corresponds to the delivery of the release.
9.	Delivery	Delivery of the manufactured network product.

1.1.1. For new network products and modifications to network products, the product development phases are cyclical, starting over from the beginning after the previous network product release has been completed.

1.2. Network Product Life Cycle Processes
The life cycle of a network product within NESAS covers all activities from the initial idea of the network product to the end of the life cycle. The lifecycle of a network product consists of the following processes:

	A	B
1.	**Process**	**Description**
2.	Product development process	As described in subsection 1.1.
3.	First commercial introduction	The commercial life cycle of the network product starts with a first release, which is approved for use in live commercial networks. Prior to this, previous releases could be tested in sandboxes.
1.	Update	Updates to the network product take place with a minor or larger release. This phase is usually a cycle of such communications.
2.	Minor release	Minor release corrects vulnerabilities and other errors found in previous versions. It usually introduces only minor functional improvements and architectural changes.
3.	Main release	The main release corrects vulnerabilities and other errors found in previous versions. It could introduce significant functional improvements and architectural changes.
4.	End-of-life	The network product will no longer receive updates. Since this process takes place after the expiry of the contractual and regulatory requirements which apply to the maintenance of the network product, this usually indicates the end of the service life of the network product.

2. Values to protect

2.1. Source code (SRC)
2.1.1. The source code is used to create the binary software of the network product. The source code also includes scripts that are not necessarily translated into binary but are included in the software of the network product. The source code includes application software as well as software and hardware platforms and integrated APIs, if any. Software platforms include operating systems and virtualisation management software.

2.1.2. The main types of source code are:

2.1.2.1. created by the equipment manufacturer for use in one or more specific network products **[SRC_VND]**
2.1.2.2. created by a subcontracting third party on behalf of the equipment supplier for use in one or more specific network products **[SRC_SUB]**
2.1.2.3. generic software components (e.g. directories) created by a third party supplier and made available to the equipment supplier in binary form **[SRC_TRB]**

2.1.2.4. generic software components (e.g. directories) created by a third party supplier and made available as a source to the equipment supplier **[SRC_TRS]**
2.1.2.5. free and open-source, created by a third party, without support **[SRC_FOS]**

2.2. Software packages (SPK)
Software packages are usually generated from the source code (SRC) during the active development and maintenance phase, using a build process. They are then subjected to testing and audit and release decisions, and are potentially used for production.
Each network product contains a combination of several software packages after production.
Common types of software packages are:

2.2.1. Created by the equipment supplier **[SPK_VND]**
2.2.2. Created by a subcontracting third party on behalf of the equipment supplier **[SPK_SUB]**
2.2.3. Created by a third-party supplier **[SPK_TRD]**

2.3. Finished products (FIN)
Finished products are typically:

2.3.1. Software images to be installed on network products **[FIN_SWR]**, typically coming from one or more software packages (SPK).
2.3.2. Hardware components integrating the complete network product **[FIN_HWR]**, typically with a certain release of FIN_SWR after the manufacturing process.

2.4. Security documentation (DOC)
The security documentation is used to guide the planning of the network product and the development of the source code, and is a document to be handed over during the design and development process of the network product.
The main types of security documents include those that are created by the equipment supplier during the design and development process of the network product, such as schematic designs or architecture design documents. **[DOC_DES]**

2.5. Operational products (OPP)
Operated network products are products that are actively used by a mobile network operator. These are FIN_HWRs that can be updated with new FIN_SWRs after the first delivery by the equipment manufacturer, and this may have already been done.

2.5.1. Network products operated in live networks **[OPP_LVE]**

2.6. Product development support system (SUP)
Support systems are used to manage activities, the documentation and the source code throughout the entire life cycle in the network product development process.
Common types of support systems:

2.6.1. Product build environment, including the translation environment and tools used in the process of building the network product, such as operating system, translation scripts, build tools. **[SUP_BUI]**

3. Threats and risks

A risk analysis shall be carried out in order to identify the main hazards for the network products. The threats referred to in subsection 3.1 shall include the identification of the hazards

presenting the highest risk.

3.1. Description of threats

Risks should be mitigated through derived objectives where this is reasonably feasible and where this results in requirements with high returns. The main threats are described in the following table:

	A	B	C
1.	**Threats**	**Values to protect**	**Description**
2.	T_ROGUE_DEV	SRC_VND SRC_SUB	The developer secretly places a vulnerability in the source code that is intended for use in the network product.
3.	T_VULN_SRC_OWN	SRC_VND SRC_SUB	The source code used in the network product leads to vulnerabilities.
4.	T_VULN_SRC_OTHER	SRC_TRB SRC_TRS SRC_FOS	Third-party generic source code leads to vulnerabilities.
5.	T_POOR_DES	FIN_SWR FIN_HWR OPP_LVE	A design error of a network product leads to vulnerability. Security considerations are deficient in the architecture or design of the network product. Attackers can bypass or destroy the security system to launch attacks due to inadequate security planning or failure to plan.
6.	T_UNTRUSTED_SWR	OPP_LVE	The recipient of the software image file which is to be installed on the network product receives a non-original release, which may contain a vulnerability.
7.	T_VULN_SWR	OPP_LVE	The recipient of the software image file which is to be installed on the network product receives an old version containing old vulnerabilities.
8.	T_FIX_UNAWARE	OPP_LVE	The operator is not aware of the software updates available for the operated network product. This expands vulnerabilities and reduces defensive measures against a hostile environment.
9.	T_VULN_UNAWARE	SPK_TRD FIN_SWR	The manufacturer of the equipment is not aware of vulnerabilities caused by third-party components.
10.	T_VULN_NOHANDL	SPK_VND SPK_SUB FIN_SWR	The equipment manufacturer does not adequately address vulnerabilities brought to its attention by equipment suppliers, operators or other third parties.
11.	T_SENSITIVE_DOC_LEAK	DOC_DES	Security documents containing sensitive information related to the network product have been leaked. This can be used by malicious attackers to detect vulnerabilities and launch related attacks.

12.	T_BLD_TAMPER	SUP_BUI	A malicious attacker can cause damage to the system by replacing appropriate tools, modifying related parameters or implanting malicious programs.
13.	T_WRONG_DOC	FIN_SWR FIN_HWR OPP_LVE	The network product customer documentation does not cover the actual functions and properties of the network product.
14.	T_NO_CONTACT	OPP_LVE	The customer's operator does not have the right to contact the organisation of the equipment supplier in connection with safety issues or incidents.
15.	T_VULN_SWR2	FIN_SWR	Vulnerability that can be identified multiple times in the software but is not corrected everywhere.
16.	T_TPC_EOL	FIN_SWR FIN_HWR	Third-party system components (including directories, operating systems and tools) that may be discontinued or have their support structure significantly changed so that they do not receive updates to address vulnerabilities.

4. Safety targets

All objectives need to be addressed, but different levels of assurance are required depending on the classification of the tools and the returns of the actual security level in the network product. The description of the safety objectives for the supplier's development and product life cycle shall consist of the following:

	A	B	C	D
1.	**ID**	**Objective**	**Threats**	**Description**
2.	O_CONTROL	All source code changes have been checked. It is possible to reconstruct the reason for the code changes.	T_ROGUE_DEV	Reducing the risk that vulnerabilities are deliberately installed.
3.	O_VUL_INT	Software dedicated to the network product does not contain vulnerabilities.	T_VULN_SRC_OWN	Reducing the risk of the accidental occurrence of vulnerabilities.
4.	O_VUL_PAT	Any vulnerabilities discovered are addressed in an appropriate and timely manner.	T_VULN_SRC_OWN T_VULN_SRC_OTHER T_VULN_NOHANDL T_VULN_SWR2 T_TPC_EOL	Reducing the potential to exploit an opportunity arising from a known vulnerability.

5.	O_PROT_DOC	Sensitive documents do not leak.	T_SENSITIVE_DOC_LEAK	Protecting sensitive information from potential attackers.
6.	O_PROT_BLD	The translation and software building environment is protected from manipulation.	T_BLD_TAMPER T_TPC_EOL	Reducing the risk that the replaced IT elements or manipulated parameters represent a vulnerability.
7.	O_VULN_AWARE	Newly discovered vulnerabilities, originating from components used by a third party, can be identified as soon as possible.	T_VULN_UNAWARE	Ensuring that known vulnerabilities can be mitigated within a reasonable timeframe for operated network products, and that they do not go unnoticed.
8.	O_GENUINE_SWR	The integrity of the software can be verified by appropriate means before it is installed in the network product.	T_UNTRUSTED_SWR	Preventing the accidental installation of malicious manipulated software overloads.
9.	O_IDENT_SWR	The software overload variants can be identified by appropriate means.	T_VULN_SWR	Preventing old versions of the software from being accidentally installed in the operated network products and old vulnerabilities from being re-introduced into the networks.
10.	O_INFORM_FIX	Operators will be informed in a timely manner of available safety-related improvements for the network product.	T_FIX_UNAWARE	Ensuring that operators are informed of available repairs and are able to apply them so that they do not unnecessarily extend the exploitability of the vulnerability period within their networks.
11.	O_TRA_ANALYSE	Safety was built into the design from the start.	T_POOR_DES	Design security ensures that vulnerabilities can be mitigated by the

				secure design of the network product.
12.	O_SEC_TEST	The testing shall demonstrate the safe and reliable implementation of the network product.	T_ROGUE_DEV T_POOR_DES	When testing a network product, security is tested to determine vulnerabilities, unexpected behaviour, unspecified behaviour and resistance to unspecified inputs.
13.	O_STAFF_EDU	Staff involved in the design, development, implementation and maintenance are well informed about IT/network security issues.	T_VULN_SRC_OWN	Ensuring that the personnel involved in the creation of the network product and its upgrades are trained and knowledgeable in relevant network and IT security issues.
14.	O_ACCURATE_DOC	Accurate and up-to-date customer documentation is available for the network product, describing all the details concerning the safety of the network product. The documentation corresponds to the development status of the network product (HW, SW, functionality, configuration).	T_WRONG_DOC	Customer documentation related to safety issues is accurate and describes the actual operation and properties of the network product in the way it is delivered to the operator.
15.	O_SEC_POC	For each safety issue, the operator knows whom he should contact within the equipment manufacturer’s organisation.	T_NO_CONTACT	The equipment supplier shall clearly inform the operator’s customers so that operators know whom to contact in the event of a safety issue or incident.
16.	O_CONT_IMP	The likelihood of reoccurrence of vulnerabilities should be reduced through continuous improvement.	T_POOR_DES	The identified security problems are analysed to determine how to prevent their recurrence.
17.	O_SPC_SEC	The quality and	T_VULN_SRC_OTHER	Reducing the risk of

		availability of system components made available by third parties must be ensured.	T_VULN_UNAWARE T_VULN_NOHANDL	vulnerable, unsupported, third-party system components being integrated into network products.

5. Safety requirements

The requirements have been chosen on the basis of the effectiveness of the achievement of the safety objectives and the return on investment. Each requirement fulfils one or more safety objectives, and there may be one or more requirements to fulfil the same safety objective.
The requirements of this standard must be met by established processes or controls, for which there is evidence of their correct operation.
It is possible that mechanisms or tools other than those described in this section can be used to achieve the same security objective.

5.1. Planning

5.1.1.[REQ-DES-01] Intended safety

The network product shall achieve safety by design throughout the development and product life cycle. Therefore, architecture and design decisions should be based on security principles that are monitored throughout the development and product life cycle. **[O_TRA_ANALYSE]**
The purpose of design safety is to limit the impact of safety risks through robust and consistently applied principles, in particular:
5.1.1.1. Security architecture principles (domain separation, stratification, encapsulation);
5.1.1.2 Security design principles (default security, least privilege, minimisation of attack surface, centralised parameter enforcement and centralised security functions, preparation for error and exception management, data protection with design).

The principles of design safety must be taken into account and, where appropriate, applied.

In the design phases, a threat analysis process shall be carried out for the network product in order to identify the potential threats and associated mitigation measures, taking into account the interaction with other network equipment and units as well as the impact of the network product on the network in terms of security.

5.2. Implementation

5.2.1. [REQ-IMP-01] Source code review

The equipment supplier shall ensure that the new and amended source code dedicated to the network product is reviewed in accordance with an appropriate coding standard. Where feasible, the review shall also be carried out by means of a source code analysis tool and, where appropriate, automation. **[O_VUL_INT]**
The aim is to reduce the risk of software problems that could cause vulnerabilities in the network product.

5.2.2. [REQ-IMP-02]: Source code management

The supplier of the equipment shall ensure that no modification is made to the network product without proper guidance. **[O_CONTROL]**
The aim is to prevent unauthorised changes and reduce the likelihood of unintentional or

unauthorised changes, and to ensure that changes have independent audit trails.

5.3. Production of executables

5.3.1. [REQ-BUI-01] Automated software build process
The equipment supplier shall use an automated software build process with minimal manual intervention to build the software for the finished product and to store the software build logs. **[O_PROT_BLD]**
The aim is to ensure that the software build is reproducible and deterministic, and that it covers the safety procedures specified by the equipment supplier.

5.3.2. [REQ-BUI-02] Management of software build processes
All the data in the software build process, including the source code, software build scripts, software build tools and software build environment, must come directly from a version control system. **[O_PROT_BLD]**
The aim is to ensure that the same binaries can be reproduced and that any modification has a clear audit trail.

5.4. Testing

5.4.1. [REQ-TES-01] Security testing
Security testing shall include the validation of security functions, both positive and negative testing, as well as the vulnerability testing of the network product.

Network products should be tested for security within a realistic representation of the operating environment.
The principles applied in the design security requirement shall be tested to ensure that the principles and functions are properly implemented.
Vulnerability testing shall test the reliability of the network product against unspecified or unexpected input data. **[O_VUL_INT], [O_SEC_TEST]**
The aim is to ensure that security functions are validated and weaknesses that could lead to potential vulnerabilities are identified and mitigated before the network product is delivered.

5.5. Release creation

5.5.1. [REQ-REL-01] Software integrity protection
The equipment supplier shall establish and maintain methods to ensure that the network products are delivered under controlled conditions. The mobile network operator shall be provided with adequate means to determine whether the received software package is genuine. **[O_GENUINE_SWR]**
The aim is for mobile network operators to be able to verify the integrity of the software package and the related documentation.

5.5.2. [REQ-REL-02] Unique software release identifier
Each software package version released must have a unique identifier associated with a particular build version. **[O_IDENT_SWR]**
The aim is to ensure that all software is identifiable and that exactly the same software uses the same unique identifier.

5.5.3. [REQ-REL-03] Accuracy of the documentation
The documentation shall be up-to-date from all safety aspects and shall reflect the current

functionality of the network product at the time when both the network product or its software updates and the customer documentation are delivered to the customer. **[O_ACCURATE_DOC]**
The aim is to ensure that the documentation of the network product reflects the delivered version of the network product.

5.5.4. [REQ-REL-04] Security documentation

The documentation delivered with the network products must contain all up-to-date information necessary for the secure configuration and running of the network product. The default configuration of the product shall be explicitly described in the security documentation. **[O_ACCURATE_DOC]**
The aim is to ensure that operators can configure network products in a secure manner, including clarification of whether the default configuration is secure.

5.6. SW version release

5.6.1. [REQ-OPE-01] Security contact point

The equipment supplier shall provide a point of contact for safety issues or problems and communicate this point of contact to its customers and third parties who disclose the vulnerability to the public. This point of contact should be able to identify the appropriate person or department within the equipment manufacturer's organisation to deal with the safety concerns raised by the third party customer. **[O_SEC_POC]**
The aim is to ensure that the equipment supplier forwards incoming requests to the competent department in a timely and safe manner, and that the requesting or informing party receives a timely and appropriate response.

5.6.2. [REQ-OPE-02] Managing vulnerability information

The equipment supplier shall have robust processes in place to ensure that it is aware of the newly discovered potential vulnerabilities of the components provided by the third party and assess whether they result in a vulnerability of the network product. **[O_VULN_AWARE]** **[O_VULN_AWARE]**
The aim is to reduce the impact on the network product of any third-party system component becoming unsupported, unavailable or vulnerable.

5.6.3. [REQ-OPE-03] The vulnerability mitigation process

The equipment supplier shall establish a procedure to handle any vulnerabilities found in or in connection with the released network products, including third-party system components. Vulnerabilities should be properly addressed and corrections and software updates, where appropriate, should be delivered to all relevant mobile network operators in order to comply with existing maintenance contracts, according to the agreed schedule. **[O_VUL_PAT]**
The aim is to reduce the impact of network product vulnerabilities and to prevent third-party system components from becoming unsupported, unavailable or vulnerable.

5.6.4. [REQ-OPE-04] Independence in vulnerability mitigation

In order to allow easy installation, the equipment supplier shall have the possibility to provide corrections or software updates that eliminate security gaps, independently of any independent corrections or software updates that modify the functionality of the network product. **[O_VUL_PAT]**
The aim is to ensure that security patches can be executed quickly and independently of the functional delivery schedule.

5.6.5. [REQ-OPE-05] Security patch communication

The process should ensure that information on available security-related patches is communicated to mobile network operators that have a maintenance contract at the time the patch is released. **[O_INFORM_FIX]**

The aim is to ensure that mobile network operators are informed of the application of security patches in a timely manner.

5.7. General requirements

5.7.1. [REQ-GEN-01] Version control system

Throughout the lifetime of a network product, the equipment supplier shall apply a version management system for hardware, source code, software build tools and environment, binary software, third-party system components and client documentation that ensures the accountability, authorisation and integrity of all changes. **[O_CONTROL]**

The aim is to trace the above elements in the finished network product.

5.7.2. [REQ-GEN-02] Change tracking

The equipment supplier shall establish a comprehensive, documented process that spans over network product lines to ensure that requirements and design changes affecting the network product(s) at any time during the development and product life cycle, including all aspects of REQ-GEN- 01, are systematically addressed and monitored in a timely manner, appropriate to the life cycle of all relevant product components, throughout the life cycle stages of every network product. **[O_CONTROL]**

The aim is to ensure that all changes are made in a consistent manner across all network products through the development of all network product components concerned.

5.7.3. [REQ-GEN-03] Staff training

All staff involved in the design, development, implementation, testing and maintenance of network products should be provided with ongoing training to ensure that their knowledge and awareness of security issues is up-to-date in relation to their role. **[O_STAFF_EDU]**

The aim is to ensure that all personnel have a consistently high level of knowledge and awareness of the safety issues related to their duties.

5.7.4. [REQ-GEN-04] Classification and management of information

Throughout the life-cycle, the equipment supplier must use an information classification and management system that prevents sensitive information such as security flaws, signature keys, etc. from leaking out. **[O_PROT_DOC]**

The aim is to ensure that sensitive information is identified, classified and handled appropriately.

5.7.5. [REQ-GEN-05] Continuous improvement

The equipment manufacturer should have a continuous improvement process throughout the development and product life cycle, and this process should include an analysis of the root causes of security flaws. The resulting improvements should be incorporated into the relevant planning or processes. **[O_CONT_IMP]**

The aim is to improve processes and reduce the likelihood of the reoccurrence of vulnerabilities through continuous improvement.

5.7.6. [REQ-GEN-06] Procurement of third-party components and their life cycle management

The equipment supplier shall have procedures in place to ensure the quality of third-party components throughout the life cycle of the product. The supplier of the equipment should select supported third-party components and avoid the use of components that have reached the end of their service life. **[O_SPC_SEC]**

The aim is to reduce the possibility of the equipment supplier sourcing and using vulnerable, unsupported third-party components within its supply chain.

Annex 6 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Content of the conformity assessment report

1. Evaluation report on development and product life-cycle processes according to GSMA FS.15

1.1. In the audit, the conformity assessment body shall summarise the results in a conformity assessment report about the 5G network device, which shall include:

1.1.1. the audit ID, which is unique within the certification scheme,
1.1.2. reference to those versions of the documents referred to in rows 6 and 7 of the table in point 2 of Annex 2 on the basis of which the audit was carried out,
1.1.3. the process identifiers specified by the manufacturer and the list of audited development and product life cycle processes, -
1.1.4. the date of completion of the audit,
1.1.5. the conformity assessment body and the persons involved in the assessment on behalf of the manufacturer or the client,
1.1.6. summary and overall evaluation of the audit,
1.1.7. identification of the necessary measures,
1.1.8. the observations of the conformity assessment body,
1.1.9. details of the 5G network devices developed in accordance with the assessed processes, as known at the time of the conformity assessment,
1.1.10. details of the assessment of each requirement and its outcome, with a list of the audit steps performed,
1.1.11. for each of the requirements, details of the conformity evidence that the conformity assessment body considers sufficient,
1.1.12. reference to all the manufacturer's verified input documentation and materials, including the hexadecimal representation of the SHA-512 hash code,
1.1.13.a declaration that the completed and signed Manufacturer's Declaration is available to the conformity assessment body.

1.2. The details of the assessment results shall be provided according to the classification shown in the following model table:

	A	**B**	**C**	**D**	**E**
1.	**Requirement code**	**Requirement**	**Result (M/NF/NA)**	**Comments from the conformity assessment body**	**The audit steps that have been performed**
2.	REQ-GEN-02	Change tracking		note	audits, document reference
3.	REQ-GEN-03	Staff training		note	audits, document reference
4.	...				

1.3. Assessment results can be of the following types:
1.3.1. M: ‘pass’; evidence, examination and test results that have been provided to the conformity assessment body demonstrate compliance with the requirement,
1.3.2. NF: ‘fail’; evaluation with a pass mark cannot be issued,
1.3.3. NA: ‘not applicable’, the requirement is not relevant.

1.4. A reference shall be given to all the manufacturer’s verified input documentation and material, and a SHA-512 hash hexadecimal representation of all evidence shall be provided for each.

1.5. It shall be confirmed that the completed and signed manufacturer’s declaration has been made available to the conformity assessment body and a summary shall be made of the results thereof, upon their approval.

2. Evaluation report on the evaluation of network devices according to Section 6(5) (A GSMA FS.47)

2.1. On completion of the assessment, the conformity assessment body shall draw up an assessment report containing the results of the security tests carried out on the 5G network device, including the results of the vulnerability analysis and evidence assessment.

2.2. The assessment report shall contain the following:
2.2.1. the company name and contact details of the conformity assessment body, the testing laboratory and the manufacturer,
2.2.2. a full description of the 5G network device subject to evaluation, e.g. software, hardware, interfaces, data, services and scope of application,
2.2.3. the name, version of the 5G network device and the description of the product configuration,
2.2.4. the followed version of the document referred to in row 9 of the table in point 2 of Annex 2,
2.2.5. details of the location(s) where the assessment was carried out,
2.2.6. a description of the implementation of the test, with on-site or remote testing,
2.2.7. a description of the test environment,
2.2.8. the schedule of evaluation activities,
2.2.9. the list of documents and versions used for the assessment and the mapping of SCASs to network functions within the assessed 5G network device, as set out in point 3 of Annex 2,
2.2.10. details of product or system components or network functions that may not have been tested,
2.2.11. details of the product and operating documentation provided by the manufacturer,
2.2.12. list of all executed test cases, test names and test results,
2.2.13. a description of the executed test cases and the documentation used by the conformity assessment body,
2.2.14. a list of the test cases for the applied SCASs that are not applicable, in whole or in part, to the 5G network device (Product under Evaluation) and the reasons why these test cases are not applicable,
2.2.15. a list of test cases that could not be performed in full or in part and an explanation of why the tests could not be carried out,
2.2.16. all the evidence required for each SCAS test case to support the test result,
2.2.17. details of the completed basic vulnerability testing and the tools used,
2.2.18. details of the vulnerability analysis for all identified vulnerabilities,
2.2.19. documentation of all tools used for testing, with their unique name, version and

configuration, and a reference to the tools used in each test case,
2.2.20. version of the audit report and a list of the evidence examined to assess the adequacy of the product development process for the 5G network device under assessment.

2.3. Assessment results can be of the following types:
2.3.1. M: ‘pass’; evidence, examination and test results that have been provided to the conformity assessment body demonstrate compliance with the requirement,
2.3.2. NF: ‘fail’; evaluation with a pass mark cannot be issued,
2.3.3. NA: ‘not applicable’, the requirement is not relevant.

National cybersecurity certificate model for the national cybersecurity certification scheme for 5G network devices

CERTIFICATE

<Name of the conformity assessment body> (registered address), registered by the Supervisory Authority for Regulatory Affairs (hereinafter: SZTFH) under registration number <registration number> as a conformity assessment body fulfilling the criteria to issue cybersecurity certificates at <assurance level> assurance level pursuant to the SZTFH Decree on the cybersecurity certification of information and communication technologies, and acting within its competence as a product certification organisation accredited by NAH (Hungarian National Accreditation Authority), **certifies** that the following 5G device, which was produced by

<name of manufacturer>,
namely
exact name of 5G device, HW, SW version number

fulfils the requirements laid down for the
<assurance level>
assurance level in the SZTFH Decree concerning the national cybersecurity certification scheme for 5G network devices.

This certificate has been issued based on Conformity Assessment Report Nr **<number>**.

This certificate only applies to the given version and release of the product, in its assessed configuration, and to its subsequent versions and configurations with minor updates, which have been approved by the conformity assessment body.

Created on behalf of the <client's name> (*registered office*).
Certificate registration number **<Certificate unique number>**
Start of validity for the Certificate: <start date>
End of validity for the Certificate: <end date>

stamp

…… ……..
professional certifier of the conformity assessment conformity assessment body authorised signature

To be filled in by SZTFH:

Date of registration:	
Registration ID:	

SZTFH Szabályozott Tevékenységek Felügyeleti Hatósága

Annex 8 to SZTFH Decree No …../2025 (... ...) of the Supervisory Authority for Regulatory Affairs

Main abbreviations used in the certification scheme and in its source documentation

Term	**Description**
3GPP	3rd Generation Partnership Project
3GPP TS	3GPP Technical Specification
NF	Network Function
NESAS	Network Equipment Security Assurance Scheme
PRD	Permanent Reference Document
SCAS	Security Assurance Specification
SHA-512	Secure Hash Algorithms – 512
TR	Technical Report
TS	Technical Specification

EXPLANATORY NOTES

These explanatory notes will not be published according to Section 21(2)*(b)* of IM Decree No 5/2019 of 13 March of the Ministry of Justice on the publishing of the Hungarian Gazette and its referencing during the publication of a law and during the publication of a public body regulating instrument, because the regulation set forth in the draft has a technical nature.

Pursuant to Section 81(6)*(m)* of Act LXIX of 2024 on cybersecurity in Hungary (hereinafter: Cybersecurity Act), the President of the Supervisory Authority for Regulatory Affairs shall be authorised to define and specify by decree the national cybersecurity certification systems, with the exception of research, development, production and trade in the military industry.

The purpose of the National Cybersecurity Certification Scheme for 5G network devices (hereinafter referred to as the 'certification scheme') is to lay down basic security requirements for 5G network devices, ensuring that manufacturers comply with the specified security requirements during their development and life cycle, and that based on that it is possible to assess the security properties of 5G network devices.

The certification scheme contains requirements for the 'high' assurance level pursuant to the Cybersecurity Act, therefore conformity self-assessments under the scheme cannot be performed.

The use of the certification scheme is voluntary; unless otherwise provided for in EU or Hungarian legislation, the marketing or use of the 5G network device is not subject to the possession of a national cybersecurity certificate issued under the certification scheme.

Conformity assessment under the certification scheme may be carried out on behalf of the manufacturer or the customer of the conformity assessment by a conformity assessment body registered with 'high' assurance level by SZTFH, the certification authority (hereinafter referred to as 'certification authority').

The conformity assessment was carried out with due regard to the "Network Equipment Security Assurance Specification" cybersecurity assessment framework (hereinafter referred to as "NESAS"), which was jointly developed by the Groupe Speciale Mobile Association (hereinafter: GSMA) and the Third Generation Partnership Project (hereinafter: 3GPP), and the German national scheme "Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation" (NESAS CCS-GI). The certification scheme, according to NESAS, includes both process and product evaluations.

The NESAS documents defining the certification scheme are listed in point 2 of Annex 2 to the draft, with the provision that these documents are to be applied with the derogations set out in Annex 3.

According to Section 6(4) of the draft, in the conformity assessment of the 5G network device, the conformity assessment body first assesses all the development and product life cycle processes which are referred to in Annex 5 to the draft and that are involved in the creation of the network product class of the 5G network device to be assessed as the subject of the assessment.

Pursuant to Article 6(5) of the draft, if this assessment has been completed with a satisfactory result (a ‘pass’ mark), the conformity assessment body shall, as a second phase of the assessment, carry out an assessment of the technical properties of every functional unit of the 5G network device or of the ones covered by the conformity assessment agreement, based on the requirements set out in Annex 1 and point 3 of Annex 2 of the draft.

The conformity assessment body shall draw up an assessment report on these assessment processes. A national cybersecurity certificate may be issued if the assessment of the 5G network device pursuant to Section 6(4) and (5) of the draft has been completed with a satisfactory result (a ‘pass’ mark).

The national cybersecurity certificate shall be valid for a maximum period of five years from the date of issue. The validity period cannot be extended pursuant to the draft.

The draft sets out rules for the registration of the cybersecurity certificate by the certification authority as well as rules for affixing the label as a conformity marking.

The draft also provides for the obligation of the manufacturer to monitor the security of the certified 5G network device.

The national cybersecurity certificate shall cover those changes that the manufacturer disclosed concerning the certified 5G network device during the validity period and that are considered minor updates. Changes to the security features or the nature of the 5G network device that are covered by the assessment and that are intended to maintain or restore the validity of the submitted manufacturer’s declaration or of the assessment evidence, or that are not relevant to such assessment evidence, shall be considered as minor updates.

Minor updates are covered by the national cybersecurity certificate if the manufacturer sends the update information and the security impact assessment report to the conformity assessment body before marketing the 5G network device with the updates, and the conformity assessment body does not raise objections within 40 calendar days of receipt. If the conformity assessment body accepts the change as a minor update, the conformity assessment body shall make a public statement about extending the validity to the new version and shall inform the certification authority accordingly.