EU-wide 5G Certification Scheme

Information from NIS CG 5G Security Standardization Sub Group

- 5G Sub-Group

Robert Kosla, Bernd Kowalski

Co-Chairs

5G Security Standardization Sub-Group

Background

Cybersecurity of 5G networks
EU Toolbox of risk mitigating measures

NIS COOPERATION GROUP

- **5G Toolbox agreed** and presented by Member States, EC, ENISA – 29th January 2020
- 5G Security **Standardisation and Certification are included in Supporting Actions – SA03, SA04, SA05**
- **5G Security Standardisation Sub-Group** of the NIS Cooperation Group Work Stream on 5G Cybersecurity (NIS 5G WS) works within the framework of 5G Toolbox, with a **special emphasis on facilitating coordination between Member States regarding standardisation to achieve specific security objectives and developing relevant EU-wide certification scheme(s)** in order to **promote more secure products and processes** as it is laid down in the conclusions and way forward of the 5G Toolbox.
- **5G Security Standardisation Sub-Group focuses on strengthening the cybersecurity standardisation of 5G with the EU and developing relevant EU-wide certification scheme(s)**
  - Its aim is **not to duplicate the current EU process on 5G**, but to **support this process on a deeper technical level**

EU Toolbox – Supporting Actions - Standardisation

SUPPORTING ACTIONS				
Id	**Supporting action**	**Description**	**Relevant actors**	**Related measure(s)**
b) Standardisation				
SA03	**Supporting and shaping 5G standardisation**	Increase engagement in relevant standardisation bodies, in particular through reinforced coordination at EU level in order to increase ability to shape standardisation according to identified needs, by setting up a forum or group of national regulatory authorities and other relevant competent authorities of Member states, reporting to the NIS Cooperation Group and the EECG[41], in particular tasked to: - Contribute to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification, in line with existing legislation, such as but not limited to the Cybersecurity Act; - Promote standardisation of interfaces to facilitate diversity of suppliers; - ensure liaison between the NIS Cooperation Group and relevant European and/or international standardisation bodies; - Ensure full participation by EU industry and improve the dialogue between the industry and the MS.	▪ Relevant authorities ▪ EC ▪ Operators ▪ Suppliers ▪ ENISA	SM05, SM06, TM02, TM09, TM10
SA04	**Developing guidance on implementation of security measures in existing 5G standards**	Develop specific EU guidance on the implementation of security measures under the existing 5G standards (e.g. 3GPP), and in particular: - Provide recommendations on the optional elements of standardisation and on aspects that are not covered by a specific standard;[42] - Identify existing gaps in telecommunications standardisation of architectures/functionalities for mitigating identified risks.	▪ Relevant authorities ▪ ENISA	SM01, TM02
SA05	**Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme**	Consider developing an EU-wide certification scheme under the EU certification framework for information security management systems (ISMS) for telecommunication providers.	▪ Relevant authorities ▪ ENISA ▪ Stakeholders	TM01 to 06

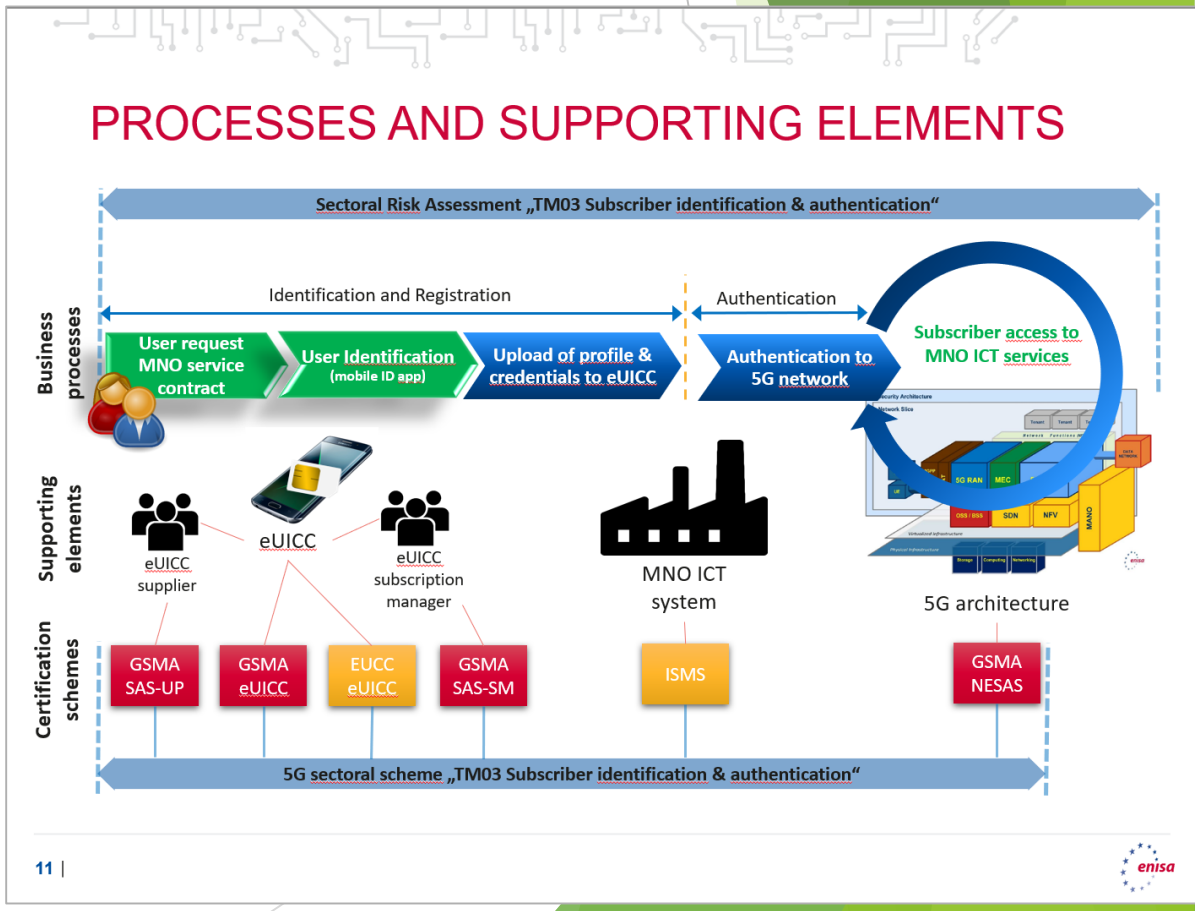
EU Toolbox – Supporting Actions - Standardisation

Main categories of elements and functions (*)	Risks (*) according to EU Toolbox (2), Page 5: Table 1 - Risk categories and scenarios	Criticality (**)	Examples of key elements (**) according to EU Risk Assessment (1), Page 16-17, Number 2.21, Table, except items formatted in italic according to TM09 of (2)	Available standards, technical specifications and certification schemes for products			Available standards, technical specifications and certification schemes for (management) systems		
Core network functions	R1 - Misconfiguration of networks R2 - Lack of access controls R3 - Low product quality R4 - Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis R5 - State interference through 5G supply chain R6 - Exploitation of 5G networks by organised crime or organised crime group targeting end-users R7 - Significant disruption of critical infrastructures or services R8 - Massive failure of networks due to interruption of electricity supply or other support systems R9 - Exploitation of IoT (Internet of Things), handsets or smart devices	Critical	User Equipment Authentication, roaming and Session Management Functions User Equipment data transport functions Access policy management Registration and authorization of network services Storage of end-user and network data Link with third-party mobile networks Exposure of core network functions to external applications Attribution of end-user devices to network slices *Subscriber registration* *User authentication (subscriber and application user level)*	3GPP SCAS	TS 33.116 - Security Assurance Specification (SCAS) for the MME network product class TS 33.117 - Catalogue of general security assurance requirements TS 33.250 - Security assurance specification for the PGW network product class TS 33.401 - 3GPP System Architecture Evolution (SAE); Security architecture TS 33.402 - 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses TS 33.501 - Security architecture and procedures for 5G System TS 33.512 - 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF) TS 33.513 - 5G Security Assurance Specification (SCAS); User Plane Function (UPF) TS 33.514 - 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class TS 33.515 - 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class TS 33.516 - 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class TS 33.517 - 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class TS 33.518 - 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class TS 33.519 - 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class	required for basic assurance: NESAS (Network Equipment Security Assurance Scheme) under governance by EU-COM (CSA) required for substantial: Penetration based on CEN/CENELC JTC13 WG3	IEC/ISO	ISO/IEC 27001 ISO/IEC 27011	ISO/IEC 27001
				GSMA	SGP.25 - Embedded UICC for Consumer Devices Protection Profile SGP.05 - Embedded UICC Protection Profile (for m2m-devices)	SOGIS Common Criteria (transferred to EU, migration ongoing)	GSMA	FF.02 Fraud Management Systems - Guidelines for Mobile Operators FF.15 Advice on Internal Fraud Risks FF.19 NRTRDE Commercial Implementation Handbook FF.21 Fraud Manual FS.01 Use of SIM Boxes to bypass interconnect communications FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines FS.13-16 NESAS FS.20 GTP Security FS.21 Interconnect Signalling Security Recommendations FS.22 VoLTE Security Analysis and Recommendations FS.24 CAMEL Roaming Fraud Management Handbook FS.26 Guidelines for Independent Remote Interconnect Security Testing FS.30 Security Manual FS.31 Baseline Security Controls FS.34 Key Management for 4G and 5G inter-PLMN security FS.35 Security Algorithm Implementation Roadmap FS.36 5G Interconnect Security FS.37 GTP-U Security FS.38 SIP Network Security FS.50 5G Security IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers SGP.21 - RSP Architecture SGP.22 - Technical Specification TS.26 - NFC Handset Requirements TS.27 - NFC Handset Test Book FS.27 Security Guidelines for UICC profiles FS.28 Security Guidelines for UICC credential protection	additional guidance and test requirements for management system certification based on ISO/IEC 27001
				Other	BSI-CC-PP-0104-2019 - CC-PP Cryptographic Service Provider				
NFV management and network orchestration (MANO)	R1 - Misconfiguration of networks R2 - Lack of access controls R3 - Low product quality R4 - Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis R5 - State interference through 5G supply chain R6 - Exploitation of 5G networks by organised crime or organised crime group targeting end-users R7 - Significant disruption of critical infrastructures or services R8 - Massive failure of networks due to interruption of electricity supply or other support systems	Critical		3GPP SCAS	TR 33.818 Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products	required for basic assurance: NESAS (Network Equipment Security Assurance Scheme) under governance by EU-COM (CSA) required for substantial: Penetration based on CEN/CENELC JTC13 WG3	IEC/ISO	ISO/IEC 27001 ISO/IEC 27011	ISO/IEC 27001
							GSMA	FS.33 NFV Threats Analysis	additional guidance and test requirements for management system certification based on ISO/IEC 27001
Management systems and supporting	R1 - Misconfiguration of networks R2 - Lack of access controls R7 - Significant disruption of critical infrastructures or services R8 - Massive failure of networks due to interruption of electricity supply or other support systems	Moderate/	Security management systems Billing and other support systems such as network performance				IEC/ISO	ISO/IEC 27001 ISO/IEC 27011	ISO/IEC 27001
								FF.02 Fraud Management Systems - Guidelines for Mobile Operators FF.15 Advice on Internal Fraud Risks	additional guidance and test

Member states initiatives – input for EU process

- **Discussions of PL and DE with GSMA** (with CSA presentation by ENISA) and MNOs provided **promising feedback concerning the scope of a 5G scheme** and the potential implementation approach discussed in the 3rd meeting of the SubGroup

- A way forward should be a **5G Candidate Scheme (under CSA)** covering cybersecurity certification of:
  1. **critical network components and functions** used in 5G networks
  2. **corresponding supplier's design, development, delivery and maintenance processes**, as indicated by ENISA presentation



Proposals discussed at NIS CG 5G SubGroup

For the future work on 5G cybersecurity **it is important that MSs mutually understand the individual directions they are moving on standardisation and certification** and become aware about the resulting different options on how to proceed with the further work.

The co-chairs identified the following options to be considered:

- **Option 1:** The Commission shall be encouraged **to ask ENISA to accompany Member States in their cooperation with GSMA/3GPP**. Participating MSs and ENISA will report frequently about the results at the 5G SubGroup meetings
- **Option 2:** The Commission will proceed according to Option 1 and shall additionally be encouraged **to request ENISA to establish an Ad-hoc Group for the development of a 5G certification candidate scheme in accordance with the art. 48 of CSA:**

Article 48

Request for a European cybersecurity certification scheme

1. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.

2. In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.

- **Option 3:** The Commission will proceed according to Option 2 but shall additionally be encouraged to **start a communication with GSMA/3GPP to clarify formal aspects, like licensing of standards etc. including an analysis about possible differences between the needs of a future European Certification Scheme and the status available from GSMA to date**

Next step – NIS CG encouraged Commission to proceed with request to ENISA and join discussion with GSMA

- Member States indicated a **preference for the proposed options 2 and 3**:

Option 2: The Commission will proceed according to Option 1 and shall additionally be encouraged **to request ENISA to establish an ad-hoc group for the development of a 5G certification candidate scheme in accordance with the art. 48 of CSA**.

  - ENISA Vision for Preparatory Activities presented at 5G Sub-Group and ECCG (Cord Bartels presentation)

Option 3: The Commission will proceed according to Option 2 but shall additionally be encouraged to **start a communication with GSMA/3GPP to clarify formal aspects, like licensing of standards etc. including an analysis about possible differences between the needs of a future European Certification Scheme and the status available from GSMA to date**

Policy Context for 5G certification scheme

- **European Commission Recommendation on 5G cybersecurity from March 2019**, as well as the 5G Toolbox from the NIS Cooperation Group of January 2020, and the Commission Communication adopted on the same date, **foresee various means to improve 5G cybersecurity, including European certification in line with the Cybersecurity Act**

- **Certification at EU level can bring value** in relation to certain risks as identified in the 5G Toolbox

- **A certification scheme should at least cover the list of components and functions provided in Annex II of the EU Toolbox** of risk mitigating measures for cybersecurity of 5G networks

- **Certification at EU Level addresses technical measures TM09 and TM10 of 5G Toolbox** and raises the technical assurance of the networks.

- **Certification is a technical tool and <u>does not address strategic measures</u>**, for example strategic measure SM03 related to the risk profiles of suppliers

Possible scope for EU 5G certification scheme

Objectives

- Comply with **public authorities' objectives**
- Take into account **existing and relevant schemes and standards**
- Generate **benefits for stakeholders and customers of the 5G ecosystem**
- To be **based on ENISA scheme proposal outline**
- Address the need of some MS for rapid deployment of a first, interim solution under the CSA and the **final goal of a EU cybersecurity certification scheme under CSA** in compliance with above objectives
- **Harmonization between national and European scheme** activities - **Member States encouraged to fully cooperate in EU wide capabilities development** – e.g. testing, evaluation, threats analysis, CABs cooperation establishment

References

- The 5G cybersecurity scheme definition shall build on the existing documents:
  - **EU coordinated risk assessment** on cybersecurity 5G networks
  - **ENISA's threat landscape** for 5G networks
  - **5G Toolbox**
- Taking into account **binding national requirements**

Phased implementation

- Include 2 consecutive steps of implementation as illustrated by ENISA presentation:
  1. **A transfer of current schemes** (GSMA's NESAS, eUICC and SAS) **under the governance of the CSA**
  2. **Analyse gaps and improve schemes** towards **full coverage for the business process "Identification and authentication of subscribers"** by **CSA-conformant cybersecurity certification schemes**

Daily News 03 / 02 / 2021

- **Cybersecurity of 5G networks: Commission requests the EU cybersecurity agency to develop a certification scheme**
- The Commission has tasked the European Union Agency for Cybersecurity, ENISA, to prepare the EU's cybersecurity certification scheme for 5G networks that will help address risks related to technical vulnerabilities of the networks and further enhance their cybersecurity. Certification plays a critical role in increasing trust and security in digital products and services – however, at the moment, there are various security certification schemes for IT products, including 5G networks, in Europe. A single common scheme for certification would make it easier for businesses to trade across borders and for customers to understand the security features of a given product or service.
- Thierry **Breton**, Commissioner for the Internal Market, said: *"Security is at the core of 5G technology roll-out. EU-wide certification, in combination with other types of measures in the EU 5G Toolbox, supports our efforts to optimise 5G security and patch technical vulnerabilities. This is why it is important that Member States make further progress in implementing the Toolbox."* Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity, said: "*The certification of 5G networks emerges as the logical next step in the EU cybersecurity strategy for the Digital Decade. The new initiative builds on the actions already engaged in to mitigate the cybersecurity risks of the 5G technology."*
- The request for the development of the scheme is in accordance with the Cybersecurity Act, which establishes the European cybersecurity certification framework, and it was also announced in the new EU Cybersecurity Strategy for the Digital Decade. The Commission will soon adopt its first Union Rolling Programme for cybersecurity certification

EUROPEAN UNION AGENCY FOR CYBERSECURITY

PRESS RELEASE

Securing EU's Vision on 5G: Cybersecurity Certification

The European Union Agency for Cybersecurity welcomes the European Commission request for a candidate cybersecurity certification scheme on 5G networks.

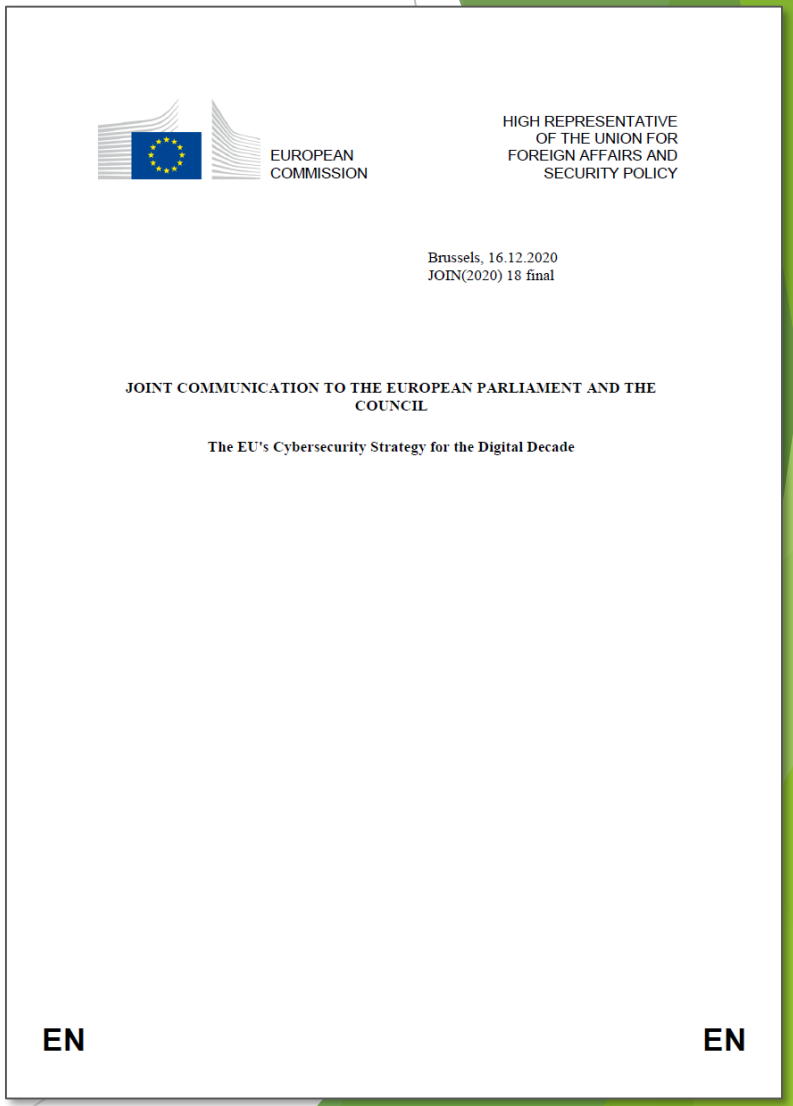
Published on February 03, 2021

Following a request by the European Commission, ENISA will proceed with the preparation of the new candidate cybersecurity certification scheme on 5G. This step follows on from the EU toolbox for 5G security and it is expected to further enhance the cybersecurity of 5G networks as it contributes to addressing certain risks, as part of a broader risk mitigation strategy.
To this effect, a cybersecurity certification scheme on 5G will be based on provisions already available by means of existing cybersecurity certification schemes as well as experience already acquired since the Agency started engaging in cybersecurity certification

This request meets the requirements of the Cybersecurity Act, which allows the European Commission to issue a request for a cybersecurity certification scheme to ENISA outside the scope of the Union Rolling Work Programme, if duly justified.
ENISA is looking forward to contributing and supporting the Commission in the development and realisation of a cybersecurity certification scheme for 5G and will cooperate with and take due account of the inputs of relevant stakeholders. The European Cybersecurity Certification Group (ECCG), the NIS Cooperation Group Work Stream and its subgroup on 5G standardisation and certification will be informed of the planning and progress continuously and will be given many opportunities to participate. Experts in 5G will be invited to be involved via the ad hoc working group work that ENISA will establish for the scheme development. The call will be published on ENISA's website.

5G Standardization – Joint Communication to the European Parliament and the Council

The EU's Cybersecurity Strategy for the Digital Decade


EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 16.12.2020
JOIN(2020) 18 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU's Cybersecurity Strategy for the Digital Decade

EN EN

5G Standardization – Joint Communication to the European Parliament and the Council

Appendix: Next steps on cybersecurity of 5G networks

Key objective 3: Promote supply chain resilience, and other EU strategic security objectives		
Areas	**Main short- and mid-term actions**	**Lead actors**
Standardisation	Define and implement a concrete action plan to enhance EU representation in standard setting bodies as part of the next steps of the work of the NIS sub-group on standardisation, in order to achieve specific security objectives, including the promotion of interoperable interfaces to facilitate diversification of suppliers.	Member States authorities

Thank you

Robert Kosla – robert.kosla@mc.gov.pl