ETSI Security Week 2020 goes virtual!

Cybersecurity Act – one year on: 5G Network

Presented by: **Colin Whorlow, NCSC**
Domenico Ferrara, European Commission
Goran Milenkovic, ENISA
Sven Lachmund, Deutsche Telekom
Marcus Wong, Futurewei

ETSI Security Week

- Deploying 5G Securely
- Cybersecurity Act – one year on
- Smart Secure Platform
- Even more advanced Cryptography

scheduled in CEST

Monday 8 June			3pm 5G Deployment
Tuesday 9 June		3pm SSP: The New Smart Secure Platform - A High Level Introduction	4.45pm SSP: The New Smart Secure Platform - The Technical Realisation
Wednesday 10 June	10.30am Insight into the First Steps of the Cybersecurity Act Reality		3pm 5G Security for Verticals
Thursday 11 June	10.00am Consumer IoT Security Standards	11.30am Consumer IoT Security – Certification Schemes	3pm ETSI Standardization in Advanced Cryptography
Monday 15 June			3pm SKINNY LATTE: Scalable Hierarchical Identity Based Encryption over Lattices
Tuesday 16 June			3pm 5G Security Evolution
Wednesday 17 June	10.30am **5G Network Certification**		
Thursday 18 June	10.00am Security Challenges and Regulatory Aspects		3pm Fully Homomorphic Encryption
Friday 19 June	10.30am Industry Applications and Use Cases for Advance Cryptography		

5G Network Certification

Moderated by Colin Whorlow, NCSC

- Policy actions at EC and EU member states level regarding 5G networks security
  Domenico Ferrara, European Commission
- Role of ENISA in the Coordinated EU Approach for Securing 5G Networks
  Goran Milenkovic, ENISA
- Network Equipment Security Assurance Scheme (NESAS)
  Sven Lachmund, Deutsche Telekom
- 3GPP SCAS
  Marcus Wong, Futurewei, 3GPP SA3 rapporteur

EU TOOLBOX FOR 5G CYBERSECURITY

ETSI Security Week 2020

Domenico Ferrara, DG CNECT H1, Cybersecurity Technology and Capacity Building

European Commission

COMMISSION RECOMMENDATION ON CYBERSECURITY OF 5G NETWORKS – (March 2019)

12 March 2019 Report by the **European Parliament**

22 March 2019 Conclusions by the **European Council**

26 March 2019 Commission **Recommendation** on the cybersecurity of 5G networks

July 2019 Member States national risk assessments

9 October 2019 EU coordinated risk assessment of 5G networks security

21 November 2019 ENISA report on threats relating to 5G networks

29 January 2020 EU **toolbox of mitigation measures** and Commission Communication on the implementation of the EU toolbox

European Commission

EU COORDINATED RISK ASSESSMENT (OCTOBER 2019) (1/2)

Joint assessment by all Member States: 9 risk categories and scenarios identified

I - Risk scenarios related to insufficient security measures	R1-Misconfiguration of networks R2-Lack of access controls
II - Risk scenarios related to 5G supply chain	R3-Low product quality R4-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
III - Risk scenarios related to modus operandi of main threat actors	R5- State interference through 5G supply chain R6- Exploitation of 5G networks by organised crime or organised crime group targeting end-users
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	R7- Significant disruption of critical infrastructures or services R8-Massive failure of networks due to interruption of electricity supply or other support systems
V - Risk scenarios related to end user devices	R9-Exploitation of IoT (Internet of Things), handsets or smart devices

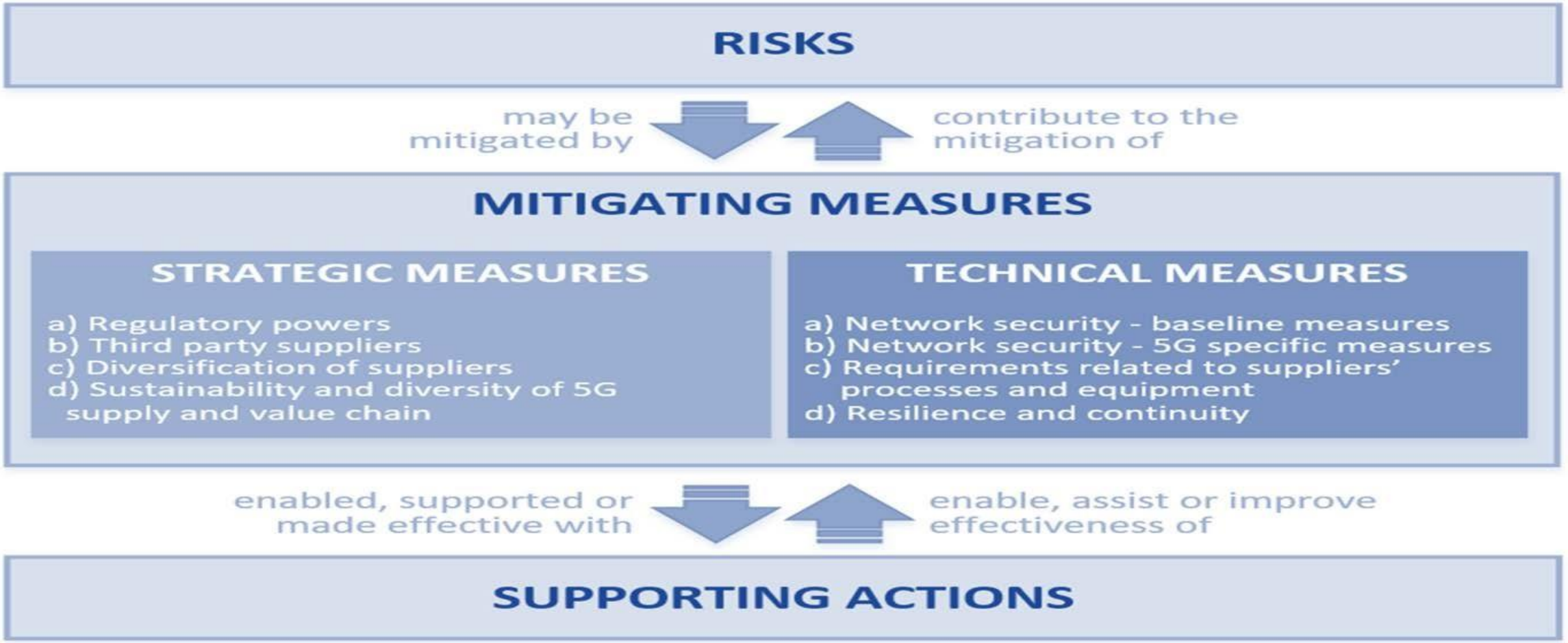
EU COORDINATED RISK ASSESSMENT (2/2)

Main findings:

- ✓ **Increase of the overall attack surface** and **potential entry points** for attackers
- ✓ Certain pieces of equipment will become more **sensitive**
- ✓ Increased exposure to risks related to **reliance on suppliers**
- ✓ Importance of the **risk profile of individual suppliers**
- ✓ **Availability** and **integrity** of networks will become major concerns
- ✓ **State and state-backed actors** are the most serious and most likely to target 5G networks

EU TOOLBOX- MEASURES & SUPPORTING ACTIONS

Identifies **8 strategic and 11 technical measures** to mitigate the risks, and 10 corresponding supporting actions to reinforce their effectiveness.



EU TOOLBOX – MEASURES ON CERTIFICATION

- ✓ TM09: Using EU certification for 5G network components, customer equipment and/or suppliers' processes.
- ✓ TM10: Using EU certification for non 5G-specific ICT products and services.
- ✓ SA02: Reinforcing testing and auditing capabilities at national and EU level.
- ✓ SM02: Performing audits on operators and requiring information.
- ✓ The Commission should consider including 5G-related schemes into the URWP.

European Commission

EU TOOLBOX – MEASURES ON STANDARDISATION

- ✓ TM02: Ensuring and evaluating the implementation of security measures included in existing 5G standards.
- ✓ SA 04: Developing guidance on implementation of security measures in existing 5G standards.
- ✓ SA 05: Ensuring application of technical standards and organisational security measures through EU-wide certification scheme.
- ✓ SA 03: Supporting and shaping 5G standardization.
  - ✓ Increase and coordinate European participation in the standardization bodies, in order to achieve Europe's security and interoperability objectives.

European Commission

EU TOOLBOX – REINFORING EU COOPERATION

- ✓ A subgroup on standardization and certification has been recently set up under the Work Stream on 5G security.
- ✓ Germany and Poland are co-chairs; participants from national authorities.
- ✓ Subgroup reports to the NIS Cooperation Group and the ECCG.
- ✓ Ongoing discussions/activities:
  - ✓ mapping of available standards and certification schemes
  - ✓ prioritisation of 5G-relevant schemes
  - ✓ definition of the scope
  - ✓ alignment with URWP.

European Commission

COMMISSION COMMUNICATION ON SECURE DEPLOYMENT OF 5G IN THE EU – IMPLEMENTING THE EU TOOLBOX

29 January 2020 Publication of EU **toolbox of mitigation measures** and Commission Communication on the implementation of the EU toolbox

30 April 2020 The Commission calls on Member States to **start** implemention of key measures.

30 June 2020 The Commission calls on Member States to prepare a report on **implementation of key measures by Member States**

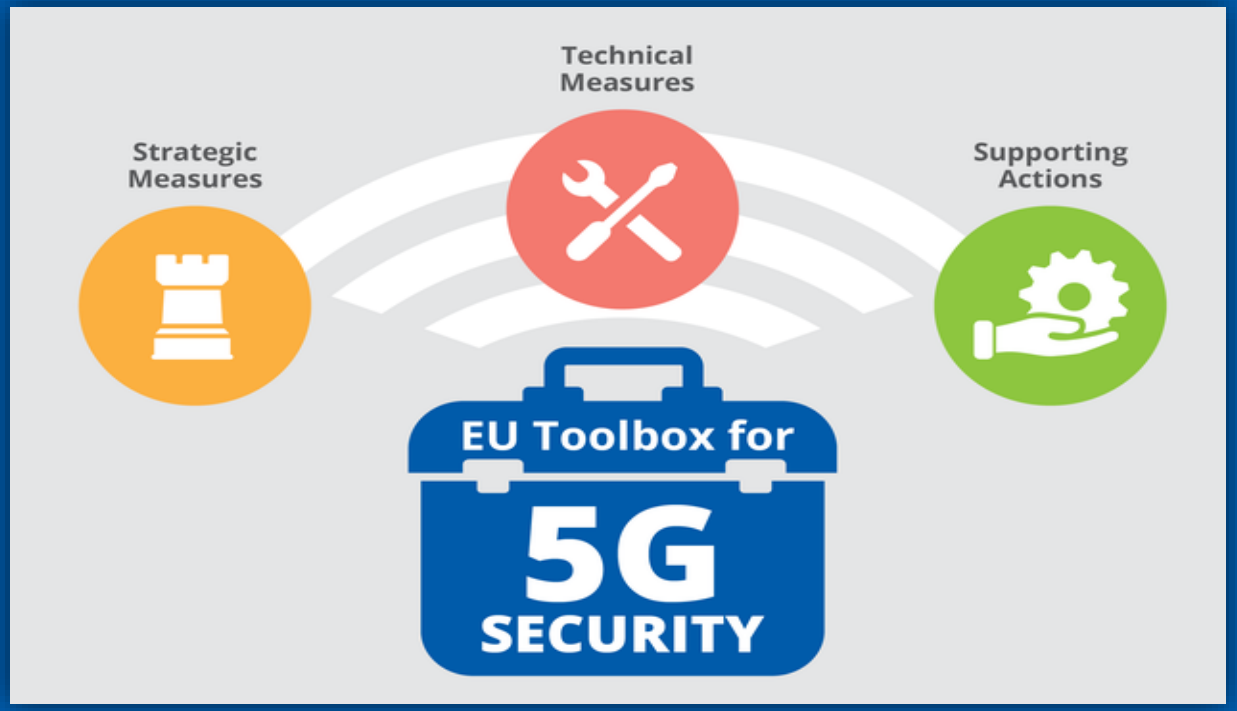
By October 2020 Review of the Commission Recommendation adopted 26 March 2019

European Commission

THANK YOU!

European Commission

THE EU CYBERSECURITY AGENCY



ROLE OF ENISA IN THE COORDINATED EU APPROACH FOR SECURING 5G NETWORKS

GORAN MILENKOVIC, ENISA

POSITIONING ENISA'S ACTIVITIES

1

RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2

SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3

'HANDS-ON' WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE

SUPPORT IN DEVELOPMENT OF EU CYBERSECURITY CERTIFICATION SCHEMES

MARCH 2019

EU Council calls for a **concerted approach** to EU 5G cybersecurity Commission issues a **recommendation:**

Action plan:

a) MS do **national risk assessments**

b) MS develop jointly a **coordinated Union risk assessment** that builds on the national risk assessment.

c) The Cooperation Group identifies a set of measures to mitigate risks (the **EU toolbox**)

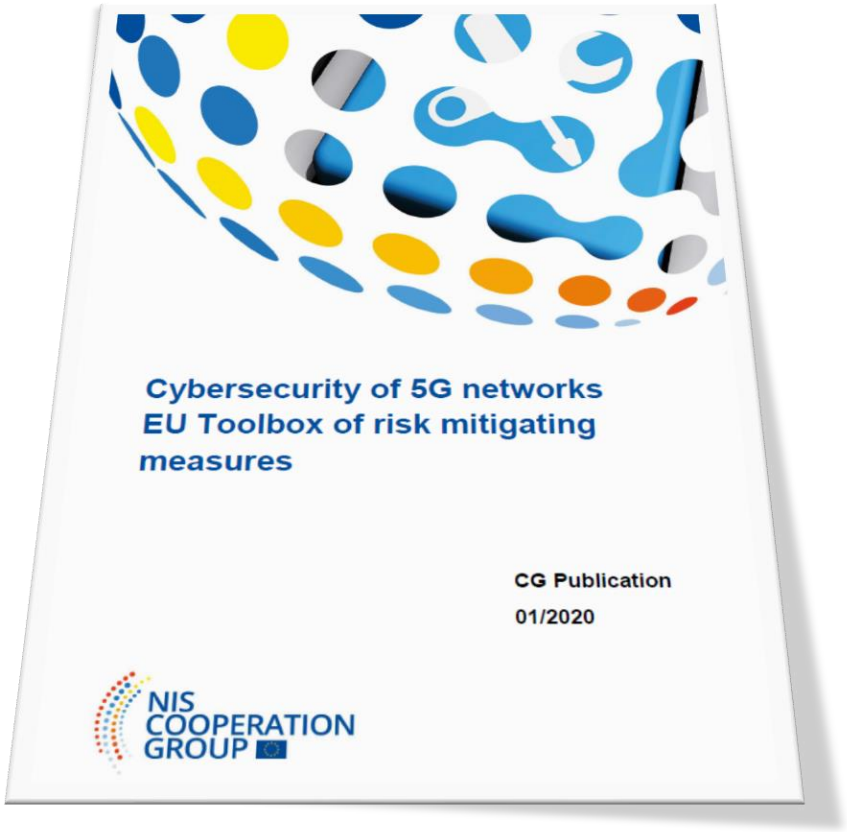
OCTOBER 2019

NIS CG publishes the EU **coordinated risk assessment** report

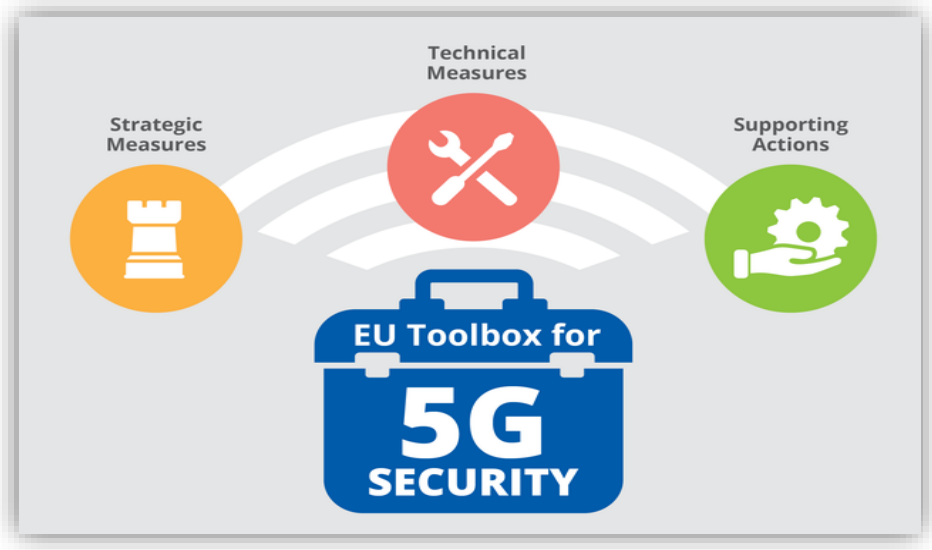
I - Risk scenarios related to insufficient security measures	R1-Misconfiguration of networks R2-Lack of access controls
II - Risk scenarios related to 5G supply chain	R3-Low product quality R4-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
III - Risk scenarios related to modus operandi of main threat actors	R5- State interference through 5G supply chain R6- Exploitation of 5G networks by organised crime or organised crime group targeting end-users
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	R7- Significant disruption of critical infrastructures or services R8-Massive failure of networks due to interruption of electricity supply or other support systems
V - Risk scenarios related to end user devices	R9-Exploitation of IoT (Internet of Things), handsets or smart devices

29 JANUARY 2020

NIS CG published the EU **Toolbox** on 5G Security



A set of appropriate, effective and proportionate possible risk management measures to mitigate the cybersecurity risks identified in the EU coordinated risk assessment



TOOLBOX MEASURES

MEASURES	Indicative timeframe[1]			Potential impact factors				SPECIFIC MEASURES	RISKS									
	Short-term	Medium-term	Long-term	Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation	
STRATEGIC MEASURES																		
Regulatory powers	✓			✓	✓	✓	✓	SM01										
								SM02										
Third party suppliers	✓			✓	✓	✓	✓	SM03										
								SM04										
Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM05										
								SM06										
5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM07										
								SM08										
TECHNICAL MEASURES																		
Baseline network security	✓			✓	✓			TM01										
								TM02										
5G specific network security	✓			✓	✓			TM03										
								TM04										
								TM05										
								TM06										
								TM07										
Requirements related to suppliers' processes and equipment		✓	✓	✓	✓	✓		TM08										
								TM09										
								TM10										
Resilience, continuity	✓			✓	✓			TM11										

Expected effectiveness:
Very low — Very high

TOOLBOX – KEY MEASURES

EU Toolbox conclusions: key measures

Member States: they should have measures in place and powers to mitigate risks. In particular they should address these aspects:

- strengthen **security requirements** for **mobile network operators**;
- assess the risk profile of suppliers; apply relevant restrictions for suppliers considered as high risk, including necessary exclusions for key assets;
- ensure that each operator has an appropriate **multi-vendor strategy** to **avoid** or **limit** any **major dependency** on a single supplier and avoid dependency on suppliers considered to be high risk.

The **European Commission** together with Member States should take measure to:

- maintain a **diverse** and **sustainable 5G supply chain** in order to avoid long-term dependency, including by:
  - making full use of the existing EU tools and instruments (FDI screening, Trade defense instruments, competition);
  - further strengthening EU capacities in the 5G and post-5G technologies, by using relevant EU programmes and funding;
- facilitate coordination between Member States regarding **standardisation** to achieve specific security objectives and developing relevant EU-wide **certification schemes**.

In addition, the mandate of the **NIS Cooperation Group Work Stream** should be extended to support, monitor and evaluate the implementation of the toolbox.

GENERAL SUPPORT

- **Support to toolbox implementation**
  - Implementation of supporting actions
  - Technical advice and expert support to MS
  - Capacity building
- **Monitoring and reporting**
  - Mechanism for monitoring of the toolbox implementation progress
  - Data analysis of input from MS on implementation progress
  - Preparation of the MS implementation report

SECURITY MEASURES

- **Update of ENISA technical guidance on security measures for telecom sector (Article 13a)**
  - General updates (EECC)
  - Security profile for (5G) MNOs

STANDARDISATION AND CERTIFICATION

- **Guideline on implementation of measures in existing 5G standardization**
- **Active support to MS in standardization activities**
- **Development of relevant certification schemes in line with Cybersecurity Act**
  - Cloud certification (ongoing)
  - Network equipment (expected)

ENISA 5G THREAT LANDSCAPE

November 2019: ENISA published a **Threat Landscape** report for 5G networks

- A detailed architecture outlining the most important/critical 5G infrastructure components.
- Detailed threat assessments for the 5G infrastructure components.
- Planned updates for the next version:
  - Update on 5G Architecture and assets
  - Asset vulnerabilities and updated threats
  - Threat mitigation options
  - Update of impact statements
  - Threat scenarios for different 5G deployment options

THANK YOU!

QUESTIONS?

Goran Milenkovic

goran.milenkovic@enisa.europa.eu

www.enisa.europe.eu

NESAS

Network Equipment Security Assurance Scheme

Sven Lachmund, Deutsche Telekom

17 June 2020 | ETSI Security Week

Why NESAS?

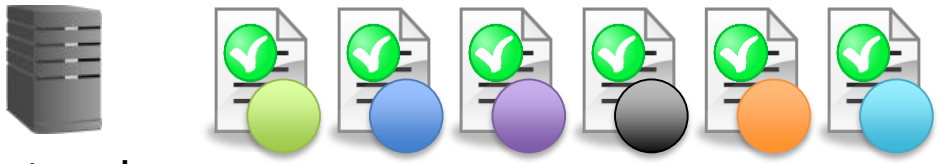
- Mobile networks are critical infrastructure and need to be robust and reliable

- Individual nations started regulating mobile network equipment

- Security requirements and conformance fragmentation globally was suspected

Why NESAS?

- Equipment vendor would have to meet all the requirements

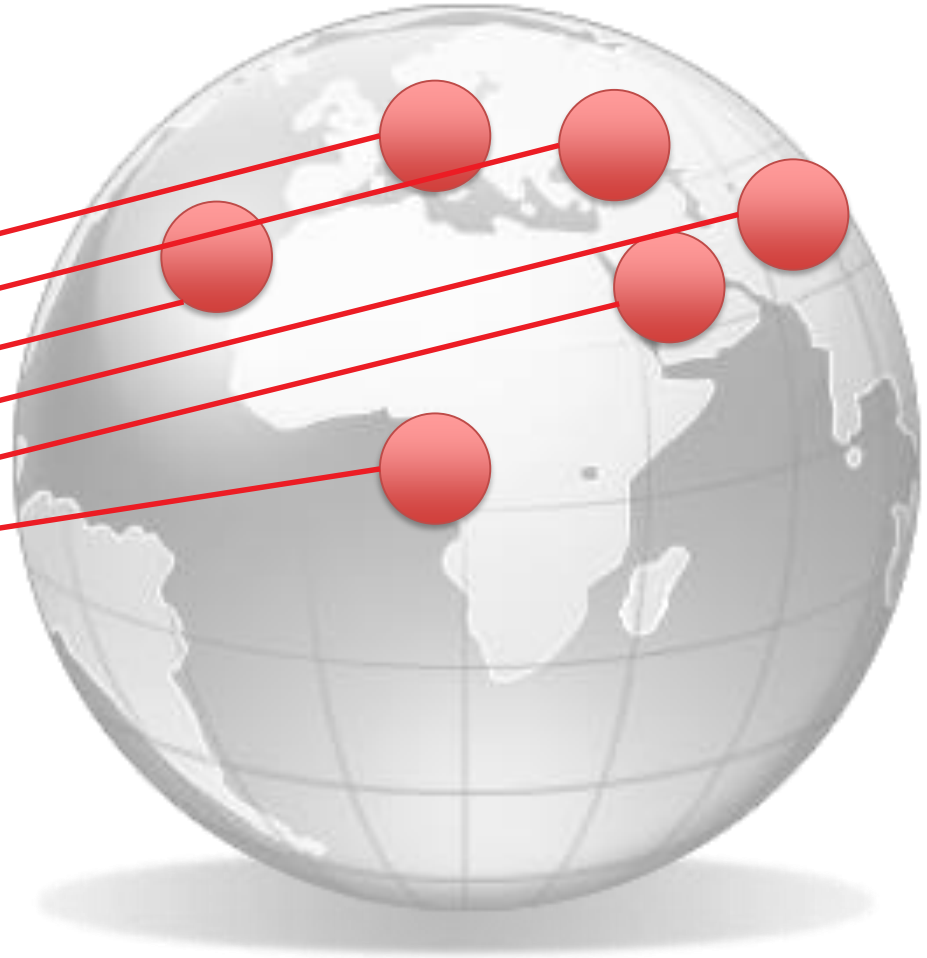


Network equipment

- Does not necessarily improve security

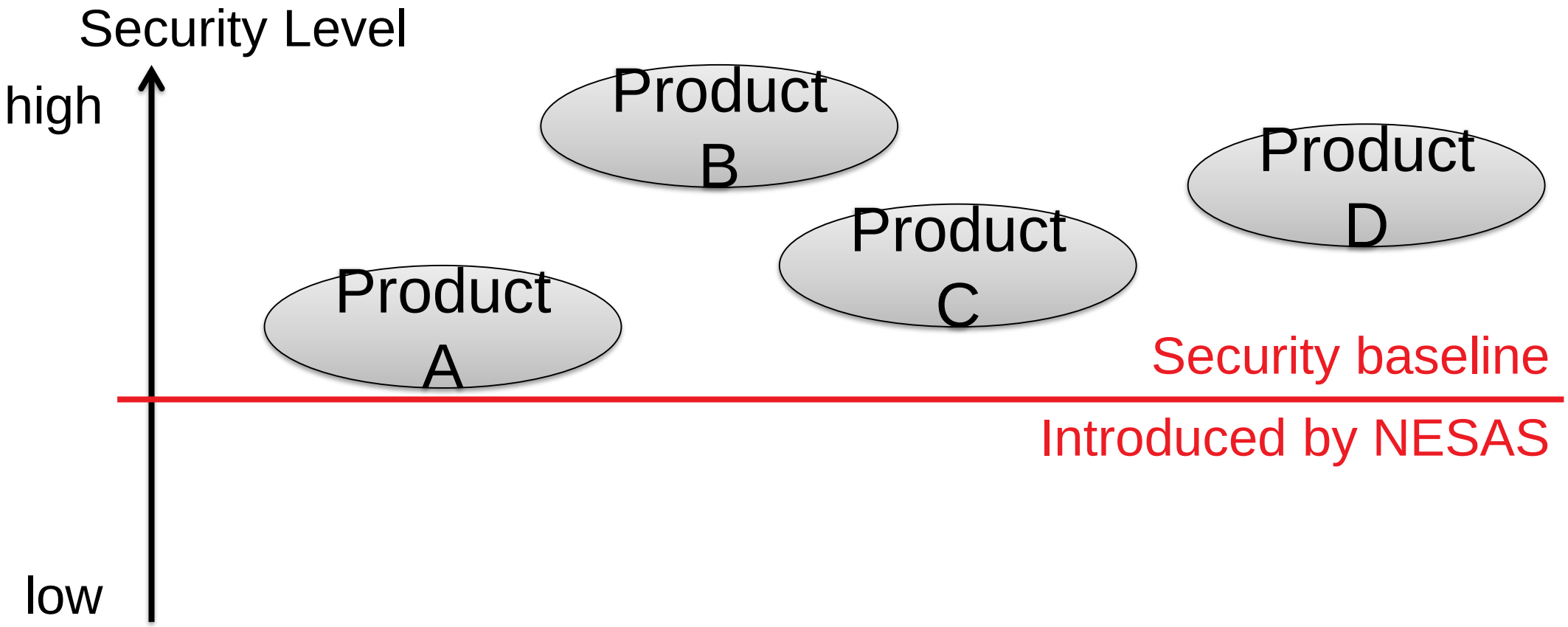
Why NESAS?

Common set of security assurance requirements



Network equipment

Why NESAS?


Security Level
high
low
Product A
Product B
Product C
Product D
Security baseline
Introduced by NESAS

What NESAS is

A security baseline to evidence that:

- Network equipment has been developed according to standard guidelines
- Network equipment satisfies a list of security requirements;

Achieved by:

Assessment of equipment vendors + Security evaluation of network equipment

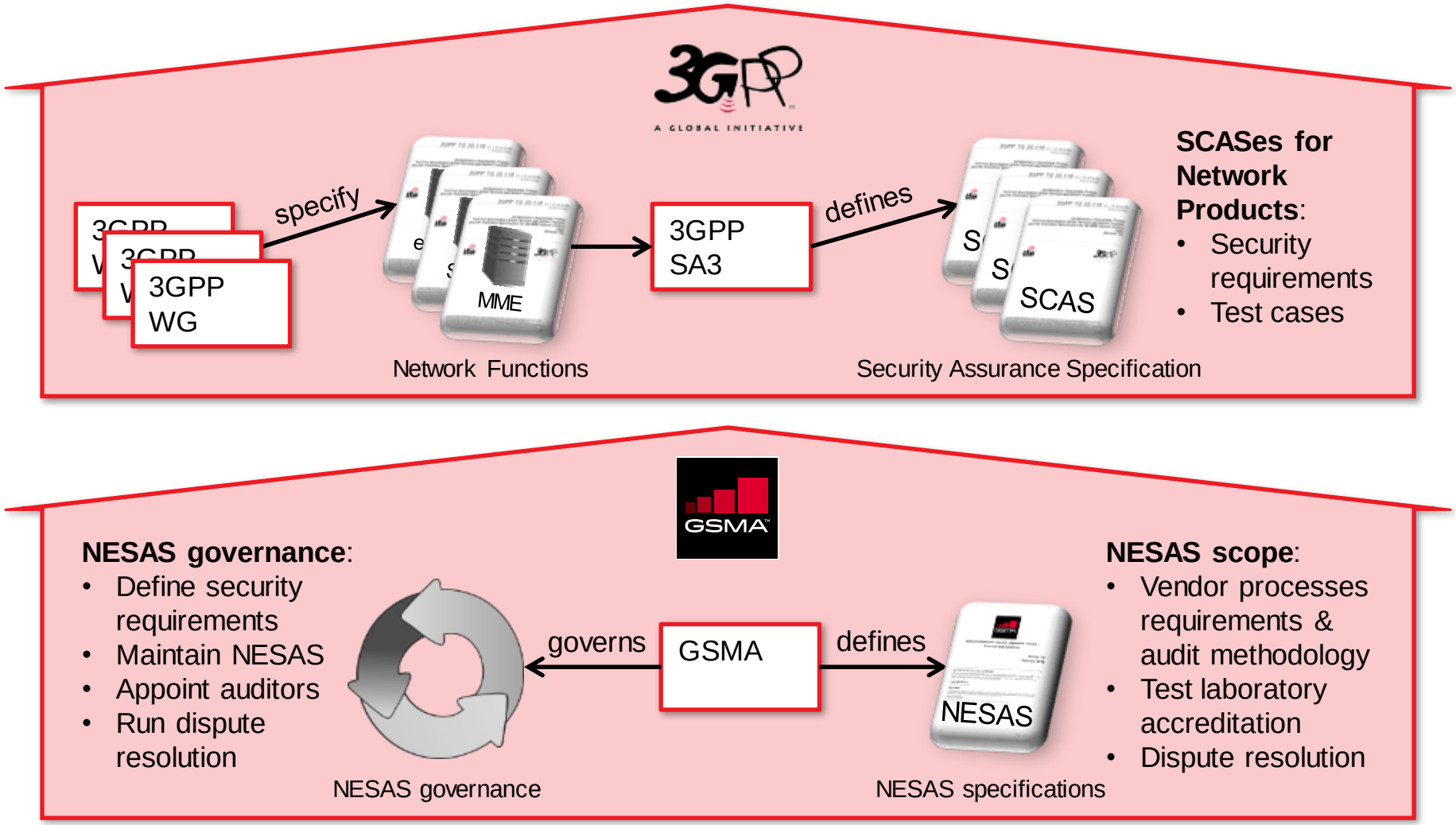
NESAS Approach

Security assessment of equipment vendors'
- product development processes and
- product lifecycle processes

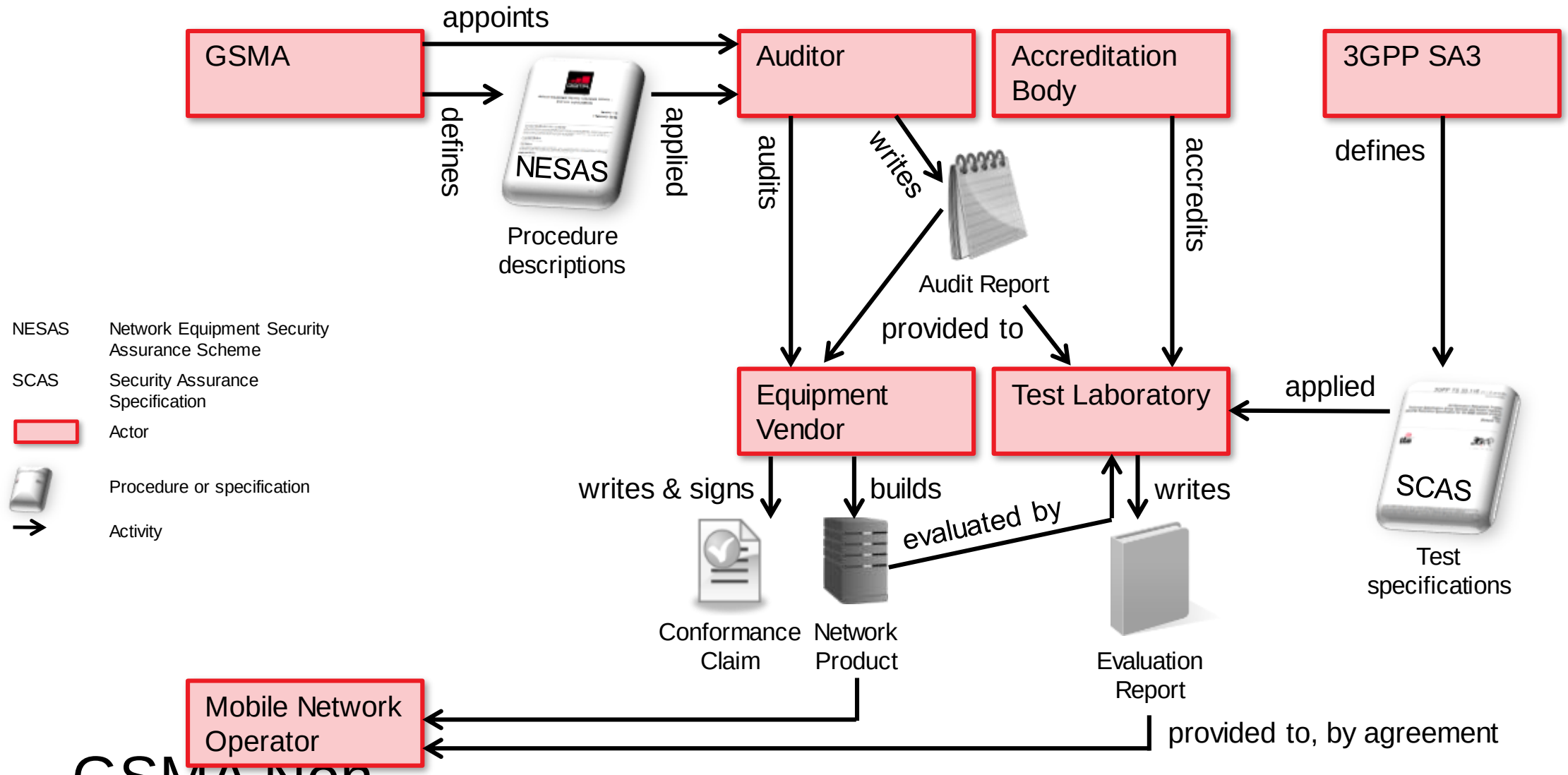
Product evaluation by competent test labs with jointly defined and standardised security tests

Accreditation of test labs

Roles of GSMA and 3GPP in NESAS

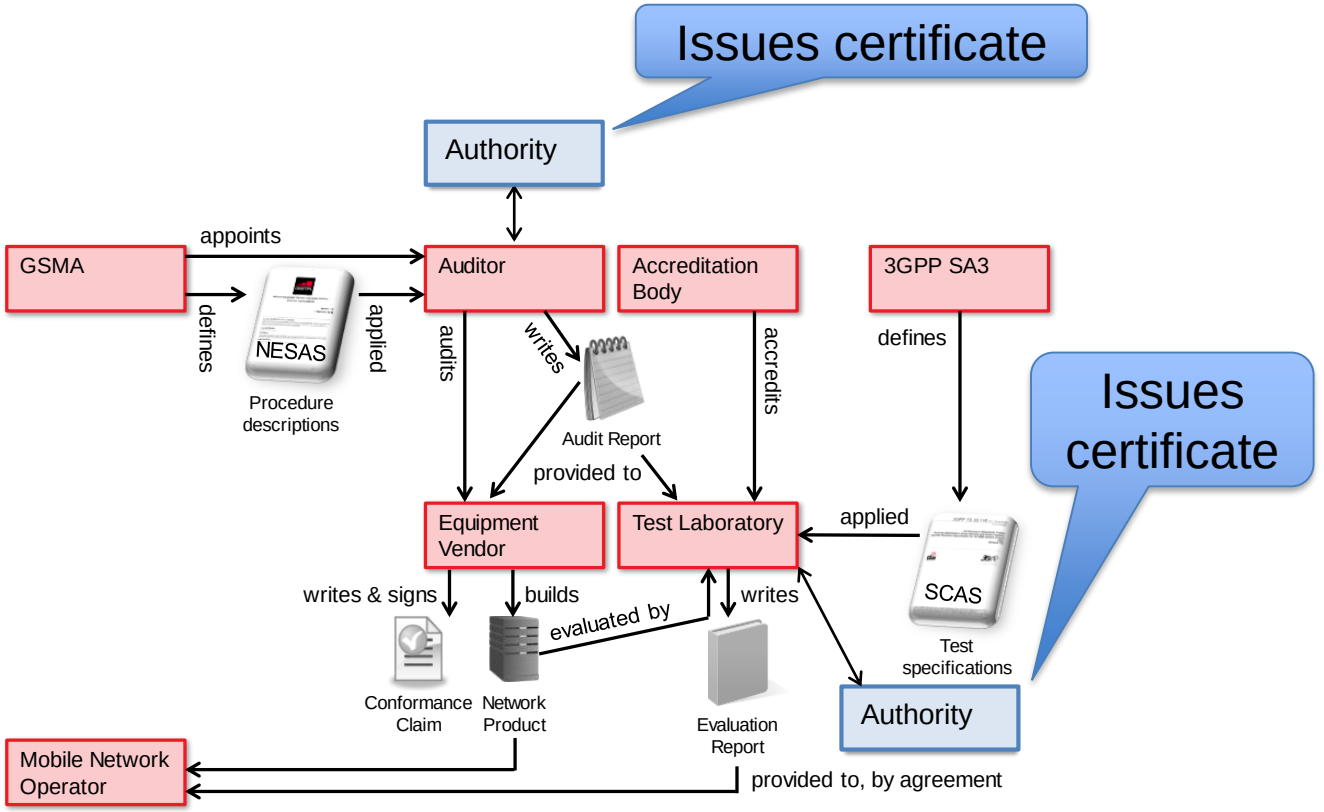


NESAS High Level Overview



Key Aspects about NESAS

- Tailored to industry needs and practicable
- NESAS is designed to evolve over time
- Voluntary participation, driven by market demand
- NESAS interfaces well with certification
  - Requirements and procedures by NESAS
  - Certification by an official authority



NESAS Benefits for Equipment Vendors

- Common set of security assurance requirements for all customers and markets
- Remove duplication of work in having to respond to inquiries regarding equipment security
- Highlights vendor ability to achieve/maintain security levels
- Encourages security by design culture across the entire vendor community

NESAS Benefits for Operators

- Level of security assurance of network equipment is visible and understood
- Industry defined requirements decreases the need for individual security requirements
- Provides reference requirements for use in procurement RFPs
- Shared cost of security among vendors and across all operators
- Managed by GSMA at no cost to network operators

NESAS Benefits for Nation States

- Security requirements commensurate with national security requirements (regulation of critical infrastructure)
- Security assurance scheme accepted and funded by industry
- Single assurance scheme that is universally applicable
- No barrier for innovation and entering markets
- Cost effective scheme that delivers security gains
- NESAS interfaces well with certification
- NESAS is designed to be enhanced as needed

Status of NESAS and Activities (June 2020)

Status

NESAS Release 1 launched in October 2019

NESAS Documentation

Available publicly at https://gsma.com/nesas

Current Activities

- Proposal for NESAS integration into EU CSA is being written
- Enhancements are being prepared → next release

Conclusions

- NESAS covers vendor processes assessment and product evaluation to reach baseline of security
- Voluntary global scheme, created and supported by the industry
- NESAS interfaces well with certification
- NESAS is designed to be enhanced as needed
- Avoiding global security requirements and conformance fragmentation is key
- Nation states are invited to embed NESAS into their certification/regulation of mobile networks

Questions?

Network Equipment Security Assurance Scheme

Web-Site: https://gsma.com/nesas

Contact: nesas@gsma.com

Sven Lachmund
Deutsche Telekom &
Chairman of GSMA's
Security Assurance Group

3GPP SCAS Update

Marcus Wong

ETSI Security Week 2020

FUTUREWEI

www.futurewei.com

SCAS in 3GPP and NESAS in GSMA recap

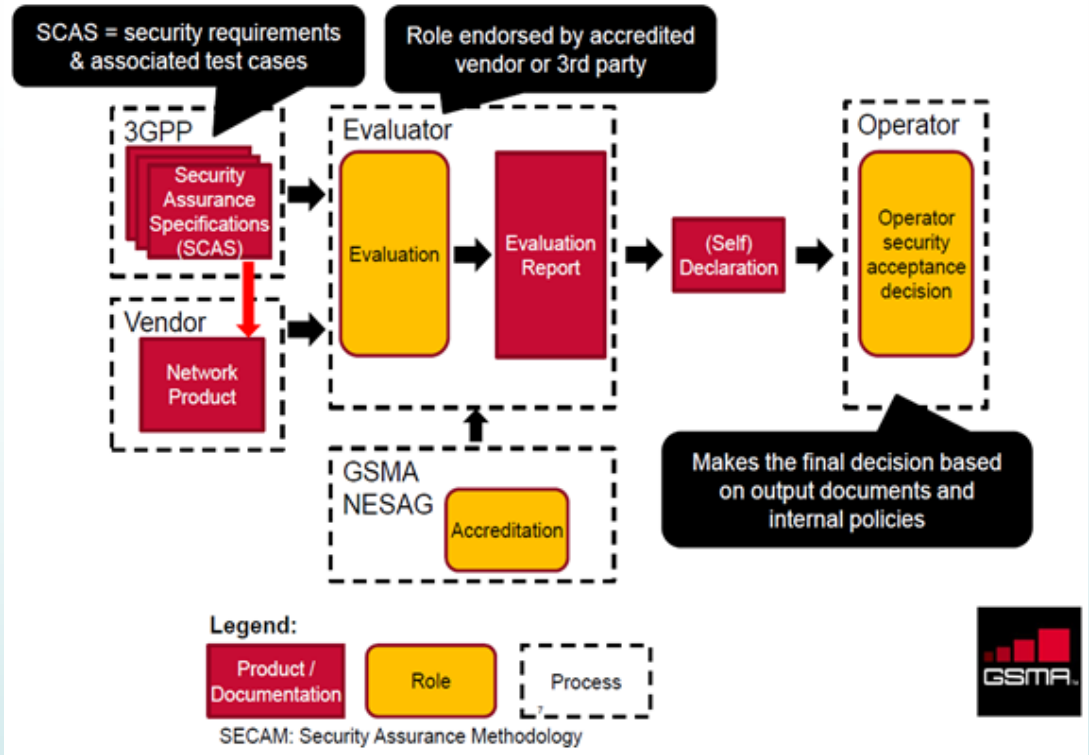
3GPP started with 4G security assurance specifications process

- TR 33.916 Security Assurance Methodology for 3GPP network products
- TS 33.117 Catalogue of general security assurance requirements
- TS 33.116 SCAS for the MME network product class
- TS 33.216 SCAS for the evolved Node B (eNB) network product class
- TS 33.250 SCAS for the PGW network product class
- TR 33.926 threats and critical assets in 3GPP network product classes

GSMA took over NESAS, testing, lifecycle, and assessment

Network Equipment Security Assurance Scheme (NESAS)

- Defined by GSMA and 3GPP
- Provides a security baseline for
  - Network equipment security requirements
  - Vendor development and product lifecycle process
- FS.13: NESAS Overview
- FS.14: NESAS Security Test Laboratory Accreditation
- FS.15: NESAS Development and Lifecycle Assessment Methodology
- FS.16: NESAS Development and Lifecycle Security Requirements



https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme

Work Item(s) on 5G Security Assurance Specs

Objective:

identify threats and critical assets to the gNB, AMF, SMF, UDM, UPF, AUSF, SEPP, NRF, NEF, N3IWF, NWDAF, and SECOP not already identified in TR 33.926
identify threats to the interfaces to the network functions as introduced by service-based architecture
develop and/or adapt gNB, AMF, SMF, UDM, UPF, AUSF, SEPP, NRF, NEF, N3IWF, NWDAF, and SECOP specific security functional requirements and related test cases
Additional network elements to be covered as they are introduced to the 5G architecture

Expected Output:

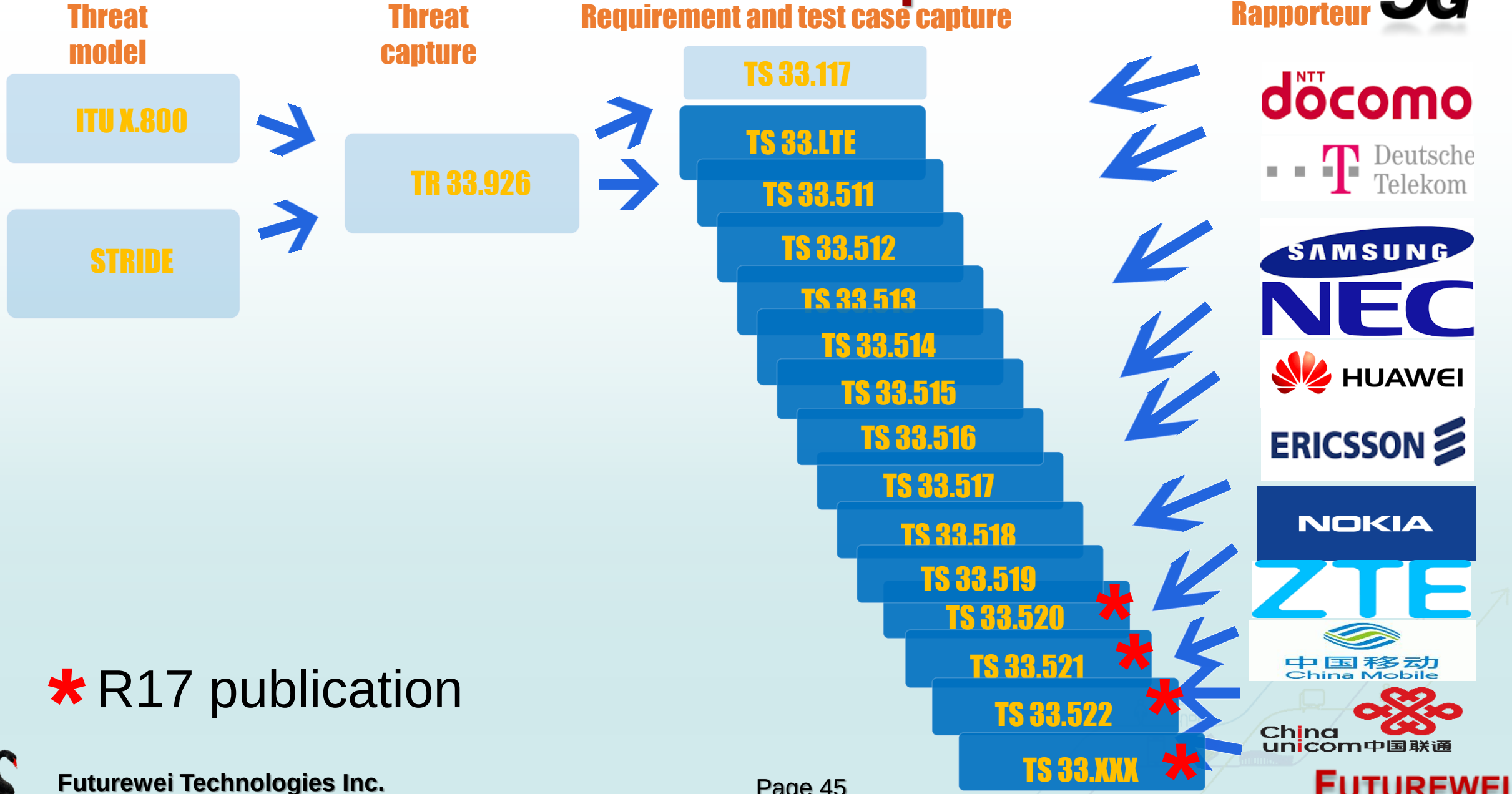
New R16 TS for gNB, AMF, UPF, UDM, AUSF, SMF, SEPP, NRF, NEF
New R17 TS for N3IWF, NWDAF, IPUPS, and SECOP, R18 TS for MEC
CR to eNB SCAS (33.216) for supporting NSA
CRs to TS 33.117
CRs to TR 33.926R 33.926

18Q1	18Q2	18Q3	18Q4	19Q3	20Q4

CR to eNB for supporting NSA

New TS for gNB, AMF, UPF, UDM, SMF, AUSF, SEPP, NRF, NEF, N3IWF, NWDAF SECOP,* IPUPS*, and MEC*

3GPP SCAS standards development



* R17 publication

Completed 5G SCAS Specifications

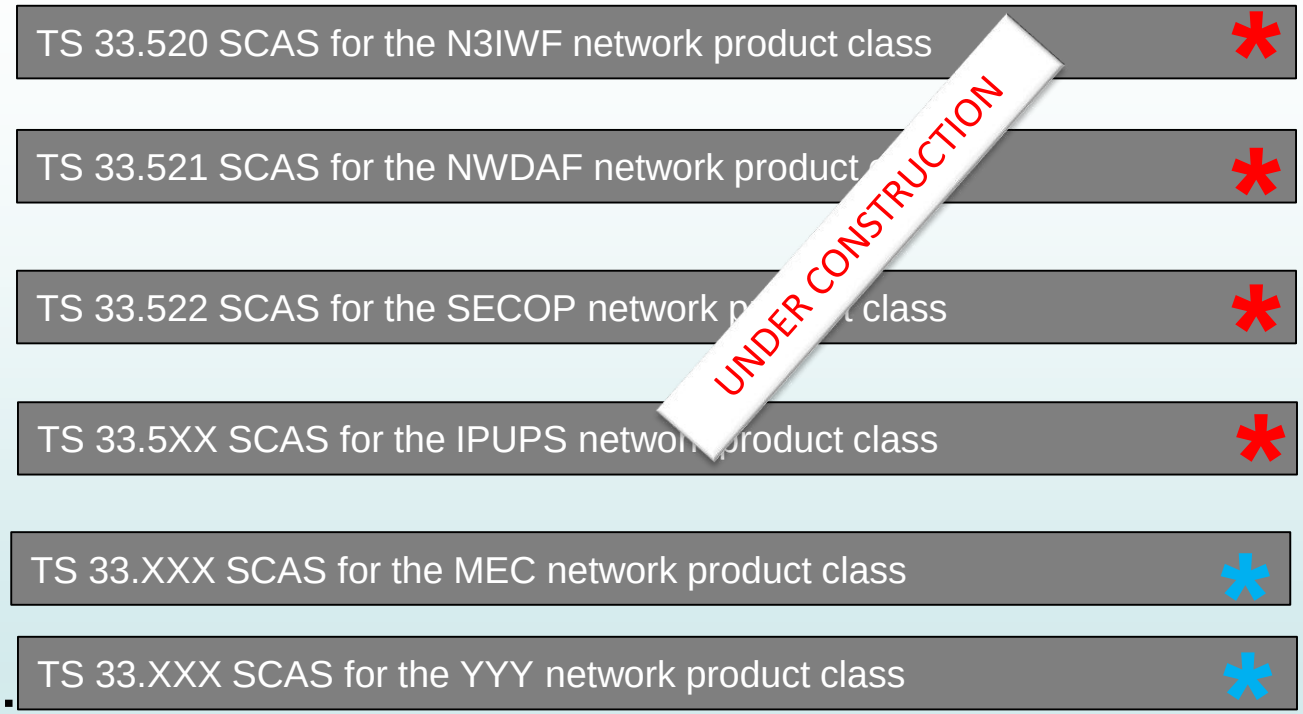
Current 5G SCAS specifications completed

- TS 33.511 SCAS for the gNB network product class
- TS 33.512 SCAS for the AMF network product class
- TS 33.513 SCAS for the UPF network product class
- TS 33.514 SCAS for the UDM network product class
- TS 33.515 SCAS for the SMF network product class
- TS 33.516 SCAS for the AUSF network product class
- TS 33.517 SCAS for the SEPP network product class
- TS 33.518 SCAS for the NRF network product class
- TS 33.519 SCAS for the NEF network product class

impacted current specs

- TR 33.916* Security Assurance Methodology for 3GPP Network Products
- TS 33.117 Catalogue of general security assurance requirements
- TS 33.216 SCAS for eNB network product class
- TR 33.926 threats and critical assets in 3GPP network product classes

Extending SCAS to additional network entities



* R17 publication
* R18 publication

R17 Study Items on SCAS

Security Assurance Methodology (SECAM) and Security Assurance Specification for 3GPP Virtualized network product

Gap analysis between current SECAM/SCAS work and SECAM/SCAS work for 3GPP virtualized network products.
Identify and determine the actors/roles involved in SECAM for 3GPP virtualized network products.
Identify and determine the ToE (Target of Evaluation) of SCAS for 3GPP virtualized network products and needed change or addition work to current security assurance methodology

- ## Security Assurance Specification for IMS

Develop the SCAS for the IMS network product classes (Release 15):
identify threats and critical assets of IMS network elements (e.g. CSCF, ATCF, ATGW, HSS, I-BCF, MRFC and MRFP)

Security Assurance Specification enhancement

Update 5G SCAS with new 5G R16 features.
Identify any additional threats, critical assets, requirements and test cases for 5G R16 features not covered
Adopt corrections or potential new security assurance requirements identified during testing in R16;
Align with GSMA NESAS specifications on some aspects when the NESAS documents are developing;

Thank You !

Questions & Answers

This was the last webinar in the thread on Cybersecurity Act – one year on

You may also listen to all past webinars available from

www.etsi.org/etsisecurityweek

10 June: Insight into the First Steps of the Cybersecurity Act Reality

11 June: Consumer IoT Security Standards

11 June: Consumer IoT Security – Certification Schemes

17 June: 5G Network Certification

Thank you for joining this webinar !

Find the full
'ETSI Security Week 2020 goes virtual'
programme at

www.etsi.org/etsisecurityweek