A year (and a bit) in the life of NESAS

James Moran, GSMA

The GSMA in numbers

1987
The GSMA was founded

5.2bn+
unique mobile subscribers

2016
we're the first sector to commit to the UN Sustainable Development Goals

$600bn
annual 5G contribution to global economy in 10 years

75%
of the global fixed broadband market is represented by GSMA members

12
Regions worldwide

Connecting **23,000** experts through InfoCentre2 – our online community for members

10.1bn+
cellular connections worldwide (including IoT)

Nearly **200,000** attendees worldwide come to our MWC and Mobile 360 Series events

30m data points included in GSMA Intelligence's database

93.8m
lives impacted through Mobile for Development

GSMA Membership:

750+
mobile operators

400
companies in the broader ecosystem

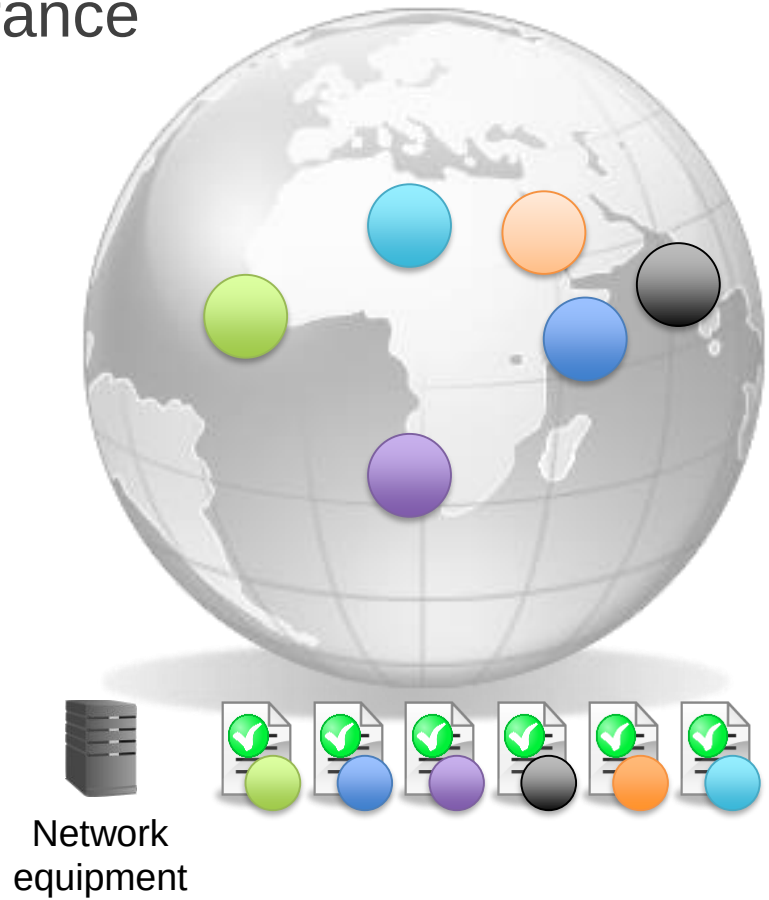
Over **600** meetings in the past year amongst the GSMA Working Groups

2.7m
visitors to MobileWorldLive.com

NESAS Recap

Why we need security assurance

- Mobile networks are critical infrastructure and need to be robust and reliable
- Nation states beginning to regulate and restrict mobile network equipment supply
- Security requirements and conformance obligations at risk of fragmenting
- Isolated initiatives introduce complexity but do not demonstrably improve security



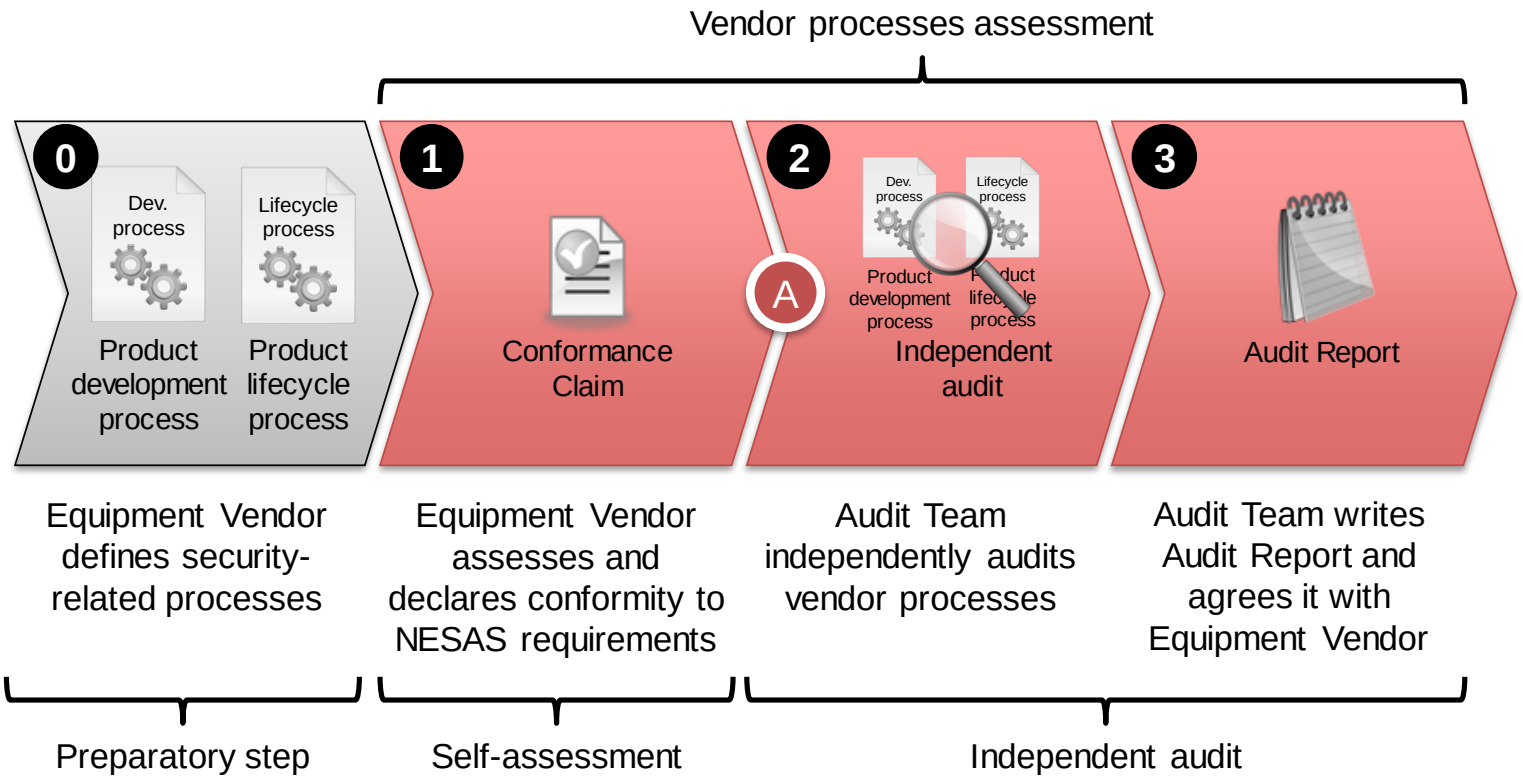
NESAS Elements

Security assessment of vendors' development and product lifecycle processes

Accreditation of security test laboratories, in accordance with ISO/IEC 17025, to undertake product evaluations

Product evaluations by competent test labs using standardised security requirements and test cases

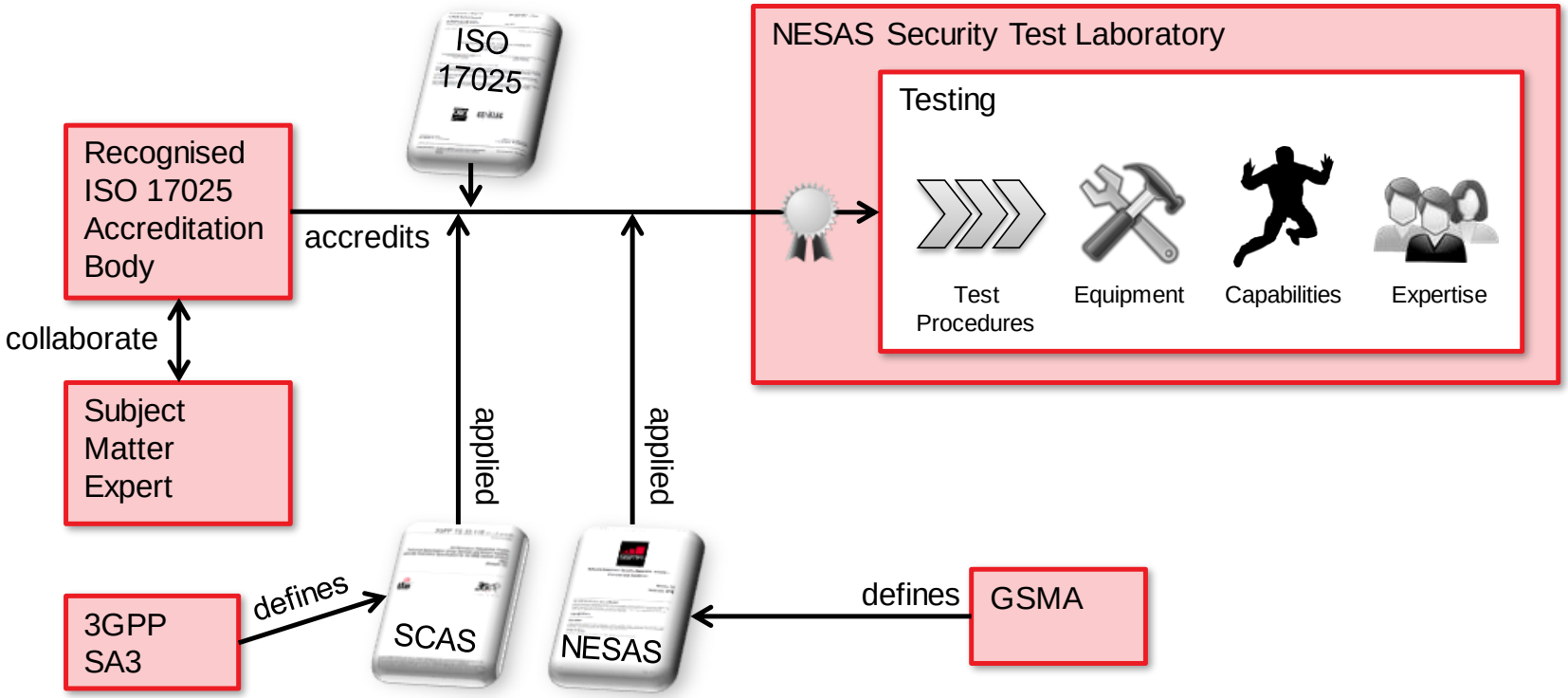
Vendor Processes Assessment – Steps



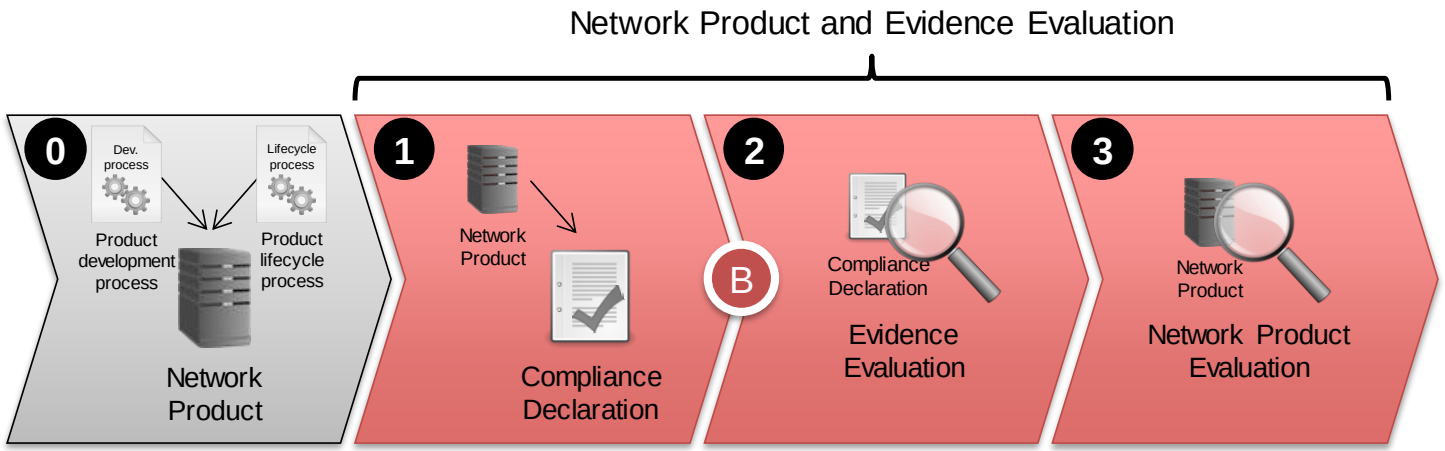
A

Prerequisite for independent audit: filled and signed Conformance Claim

Accreditation of Test Laboratory



Network Product & Evidence Evaluation – Steps



Equipment Vendor builds network product, following the assessed processes

Equipment Vendor declares compliance to assessed processes for the Network Product to be evaluated

Test Lab evaluates Compliance Evidence, contained in Compliance Declaration

Test Lab evaluates Network Product against applicable SCASes

Preparatory step

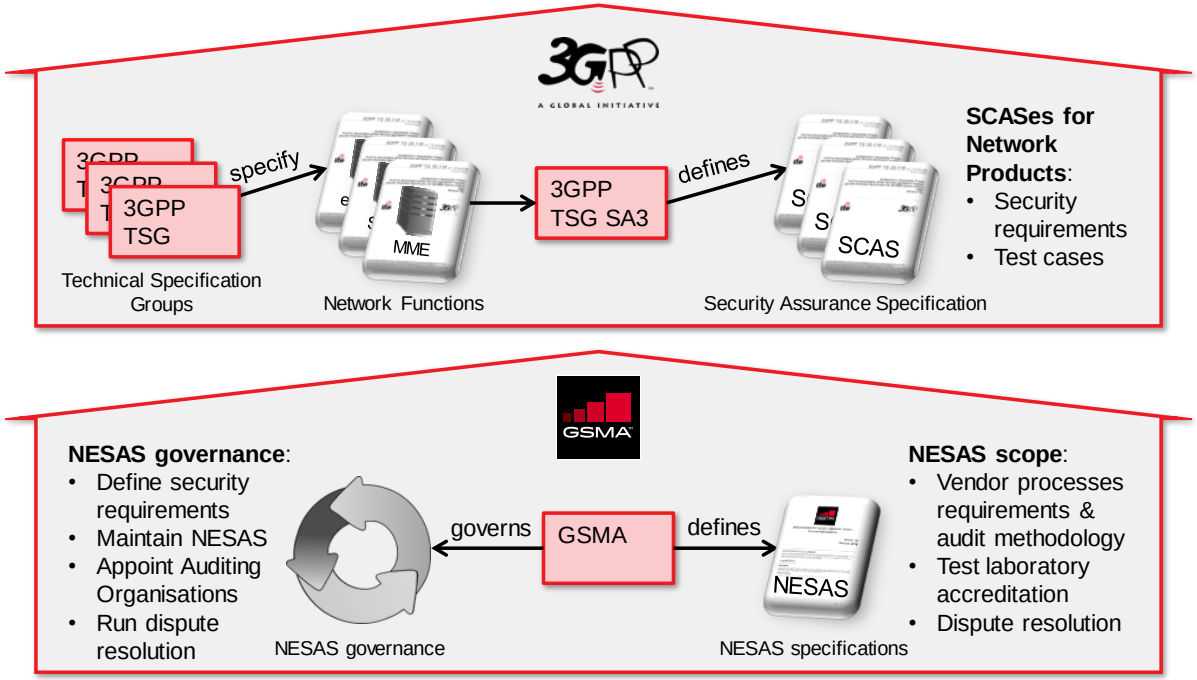
Compliance Declaration

Evaluation

B

Prerequisite for evaluation: Vendor processes assessment confirms compliance to all NESAS requirements

Collaborative Roles of GSMA and 3GPP in NESAS



3GPP

- Defines product security requirements and test cases
- Specified in Security Assurance Specifications (SCAS)

GSMA

- Defines methodologies and vendor process security requirements
- Appoints auditors and lists test labs

NESAS SCAS Coverage

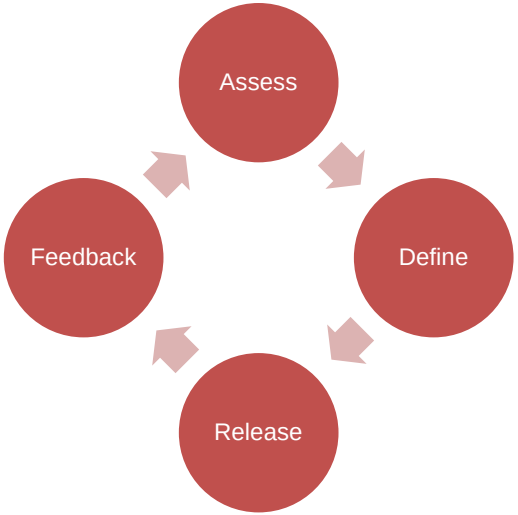
- TS 33.116 - Mobility Management Entity (MME)
- TS 33.117 - General security assurance requirements
- TS 33.216 – eNodeB (eNB)
- TS 33.250 - Packet Data Network Gateway (PGW)
- TS 33.511 - gNodeB (gNB)
- TS 33.512 - Access and Mobility management Function (AMF)
- TS 33.513 - User Plane Function (UPF)
- TS 33.514 - Unified Data Management (UDM)
- TS 33.515 - Session Management Function (SMF)
- TS 33.516 - Authentication Server Function (AUSF)
- TS 33.517 - Security Edge Protection Proxy (SEPP)
- TS 33.518 - Network Repository Function (NRF)
- TS 33.519 - Network Exposure Function (NEF)

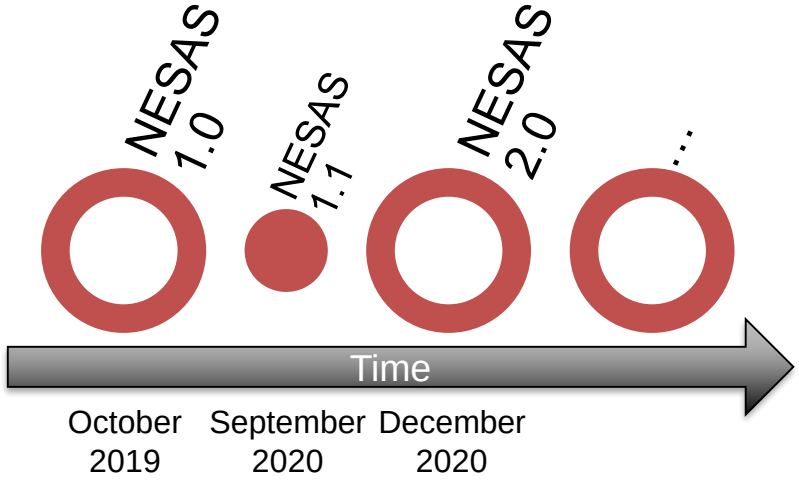
NESAS

Network Equipment Security Assurance Scheme

Current Status of NESAS

Iterative Enhancement of NESAS





- Experience from using NESAS in practice is considered
- Feedback from stakeholders is considered
- Adaptation to needs of certain stakeholders possible

Auditor Appointment

- GSMA defined eligibility and competency criteria
- GSMA conducted an open selection process
- Auditing organisations currently selected are:

atsec

nccgroup

- Selection process will be re-run periodically

Vendor Development Process Audits - 12

ERICSSON	3 processes audited
HUAWEI	3 processes audited
NOKIA	3 processes audited
SAMSUNG	2 processes audited
ZTE	1 process audited

Vendor development process details available at
https://www.gsma.com/security/nesas-participating-vendors/

Accredited NESAS Test Labs - 7

Test lab details available at https://www.gsma.com/security/nesas-security-test-laboratories/

Product Evaluations - 37

Vendor	Network Product	Product Version / Release
Ericsson	Evolved Node B (eNodeB)	20.Q4
Ericsson	Baseband Radio Node (gNodeB)	20.Q4
Huawei Technologies Co. Ltd.	Access and Mobility Management Function (AMF)	UNC 20.3.2.10
Huawei Technologies Co. Ltd.	Next Generation Node B (gNodeB)	BTS3900 V100R016C10SPC100
Huawei Technologies Co. Ltd.	Access and Mobility Management Function (AMF)	UNC 20.3.2.10
Huawei Technologies Co. Ltd.	Network Repository Function (NRF)	UNC 20.3.2.10
Huawei Technologies Co. Ltd.	Session Management Function (SMF)	UNC 20.3.2.10
Huawei Technologies Co. Ltd.	Unified Data Management Function (UDM)	UDM v20.3.0
Huawei Technologies Co. Ltd.	User Plane Function (UPF)	UDG v20.3.2.10
Huawei Technologies Co. Ltd.	Next Generation Node B (gNodeB)	DBS5900 V100R016C10SPC112
Huawei Technologies Co. Ltd.	Evolved Node B (eNodeB)	BTS3900 V100R016C10SPC112
Huawei Technologies Co. Ltd.	Next Generation Node B (gNodeB)	DBS5900 V100R016C10SPC112
Huawei Technologies Co. Ltd.	Access and Mobility Management Function (AMF)	UNC v21.1.0
Huawei Technologies Co. Ltd.	Authentication Server Function (AUSF)	UDM v21.1.0
Huawei Technologies Co. Ltd.	Network Repository Function (NRF)	UNC v21.1.0
Huawei Technologies Co. Ltd.	Session Management Function (SMF)	UNC v21.1.0
Huawei Technologies Co. Ltd.	Unified Data Management Function (UDM)	UDM v21.1.0
Huawei Technologies Co. Ltd.	User Plane Function (UPF)	UDG v21.1.0

Vendor	Network Product	Product Version / Release
Huawei Technologies Co. Ltd	Evolved Node B (eNodeB)	BTS3900 V100R017C10SPC110
Huawei Technologies Co. Ltd	Next Generation Node B (gNodeB)	DBS5900 V100R017C10SPC110
Nokia	Next Generation Node B (gNodeB)	5G20B
ZTE Corporation	Next Generation Node B (gNodeB)	gNB v3.00.30.10
ZTE Corporation	Access and Mobility Management Function (AMF)	ZXUN uMAC v7.20
ZTE Corporation	Authentication Server Function (AUSF)	ZXUN USPP v7.20
ZTE Corporation	Network Exposure Function (NEF)	ZXUN NCEE v7.20
ZTE Corporation	Network Repository Function (NRF)	ZXUN NSR v7.20
ZTE Corporation	Session Management Function (SMF)	ZXUN xGW v7.20
ZTE Corporation	Unified Data Management Function (UDM)	ZXUN USPP v7.20
ZTE Corporation	User Plane Function (UPF)	ZXUN xGW v7.20
ZTE Corporation	Next Generation Node B (gNodeB)	5G NR gNB V3.00.30.20P10
ZTE Corporation	Access and Mobility Management Function (AMF)	ZXUN uMAC v7.20
ZTE Corporation	Authentication Server Function (AUSF)	ZXUN USPP v7.20
ZTE Corporation	Network Exposure Function (NEF)	ZXUN NCEE v7.20
ZTE Corporation	Network Repository Function (NRF)	ZXUN NSR v7.20
ZTE Corporation	Session Management Function (SMF)	ZXUN xGW v7.20
ZTE Corporation	Unified Data Management Function (UDM)	ZXUN USPP v7.20
ZTE Corporation	User Plane Function (UPF)	ZXUN xGW v7.20

Product details at https://www.gsma.com/security/nesas-evaluated-network-equipment-products/

NESAS Documentation

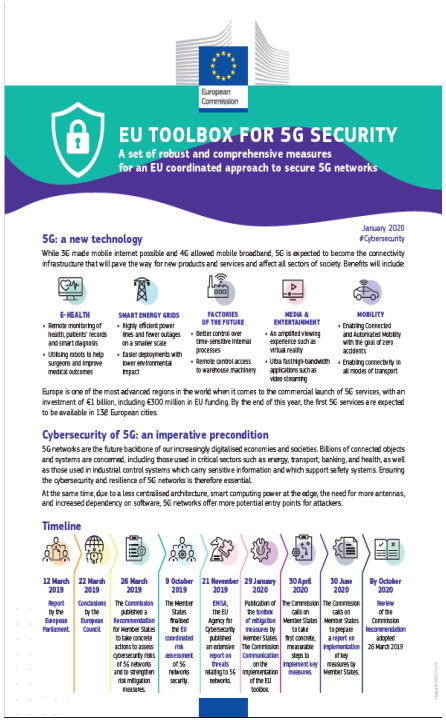
No.	Title (shortened)	Description
FS.13	NESAS Overview	Describes NESAS as a whole
FS.14	Test Laboratory Accreditation	Procedures and requirements for Test Lab accreditation
FS.15	Assessment Methodology	Procedures for vendor process assessment
FS.16	Security Requirements	Security requirements for process assessment

No.	Title (shortened)	Description
FS.46	NESAS Audit Guidelines	Guidance on auditor expectations for process audits
FS.47	Product Evaluation Methodology	Procedures for product and evidence evaluations

All NESAS Documentation is available at https://gsma.com/nesas

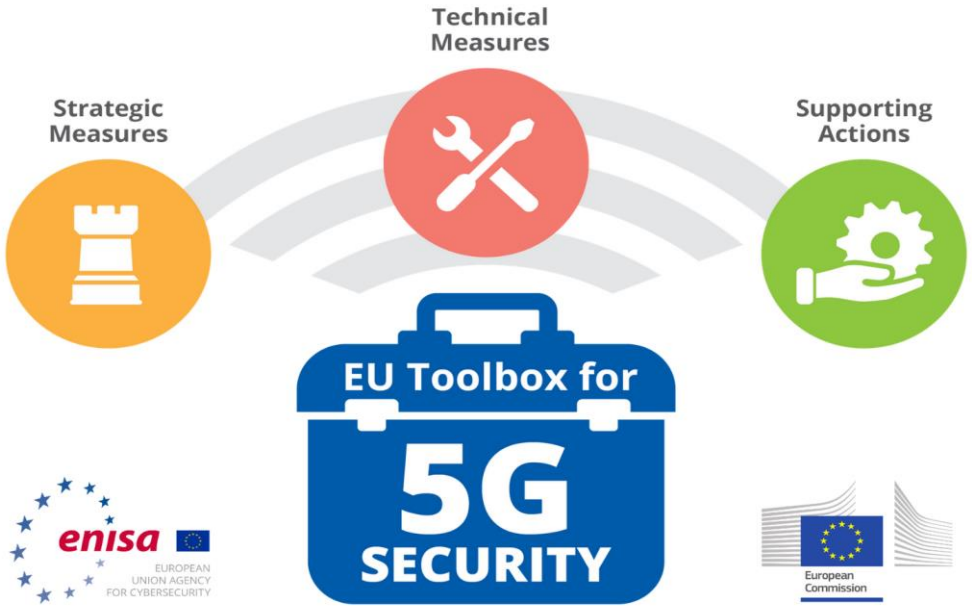
NESAS and the EU Cybersecurity Act

EU Leadership on 5G Security



Source: ENISA

EU Toolbox for 5G Security



Source: ENISA

EU Cybersecurity Certification

Source: ENISA

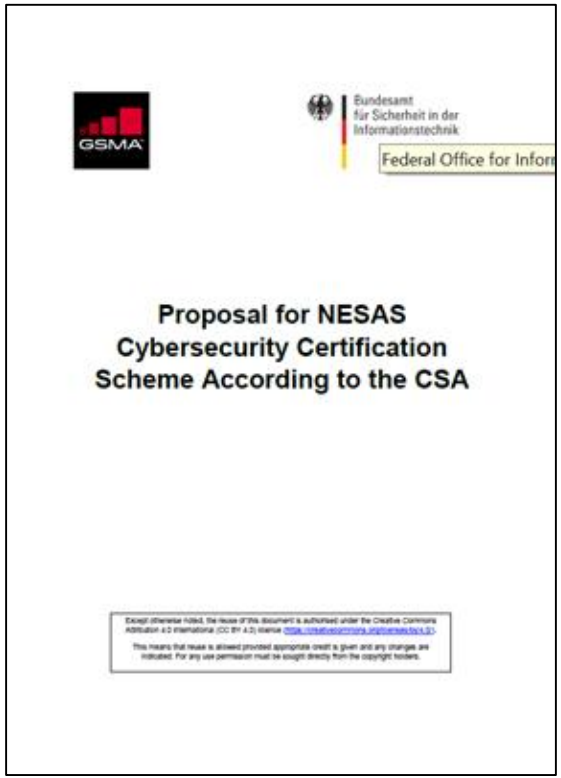
Feb 2021 Announcement

- European Commission request for candidate cybersecurity certification scheme on 5G networks
- Overall objective is to enhance cybersecurity of 5G networks by addressing certain risks
- EU scheme will build on actions already underway and on pre-existing cybersecurity certification schemes
- ENISA certification experience and expertise will be leveraged to ensure Cybersecurity Act requirements are met
- ENISA committed to cooperate and accept inputs from relevant stakeholders through ad hoc working group

GSMA Response

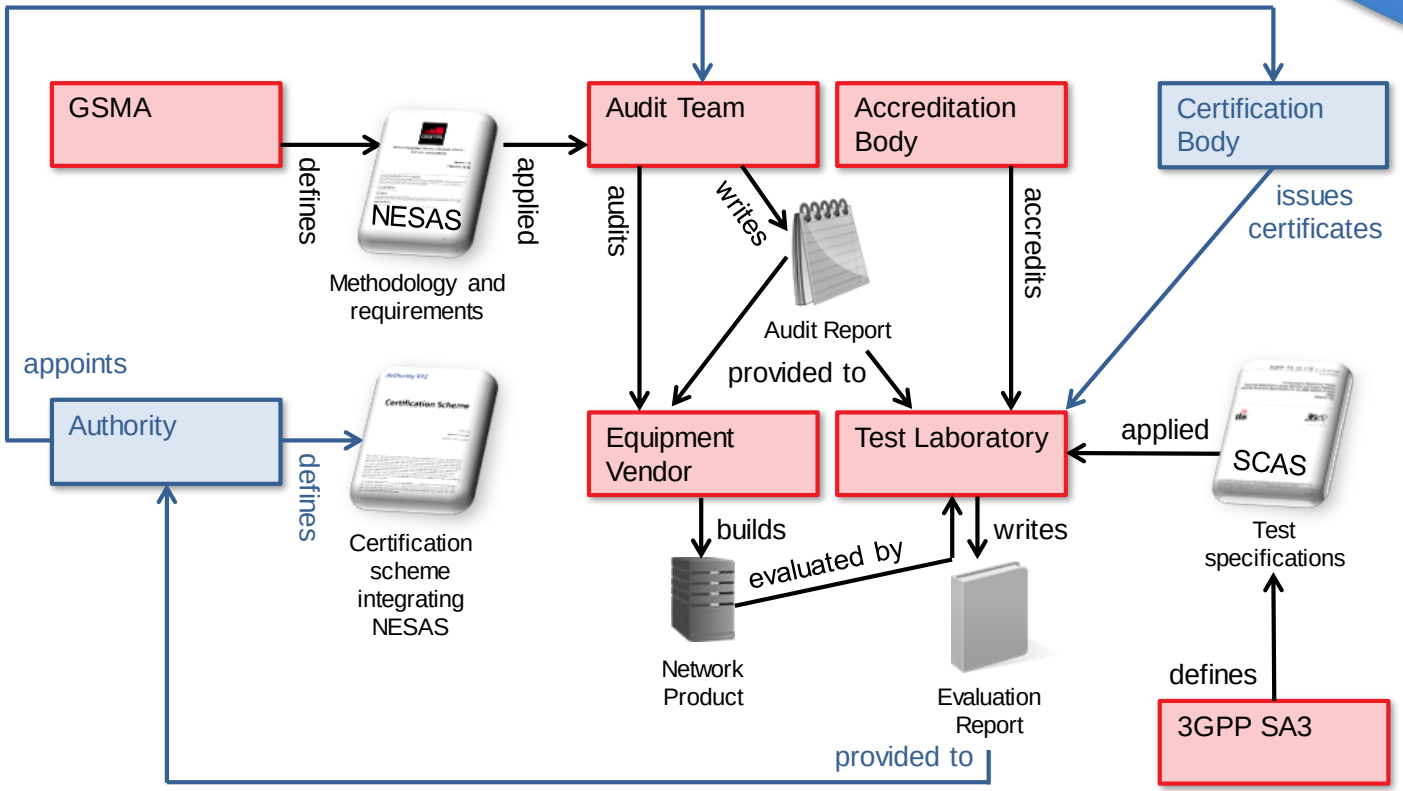
- 22nd Feb communication - GSMA Director General to ENISA Executive Director
- Noted EU Commission announcement of request to ENISA to develop certification scheme
- Expressed GSMA support for single common scheme in accordance with EU CSA certification framework and EU Cybersecurity Strategy
- Highlighted need for security assurance of 5G network equipment and development of NESAS
- Offered NESAS as an existing scheme that can be adopted and adapted to meet the EU needs
- Formal proposal, developed in conjunction with Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI), submitted
- Registered interest in participating in ad hoc expert group to advise on the development of the EU scheme

NESAS Proposal to ENISA



NESAS Interfaces well with Certification

Possible integration as an example



NESAS Compliance to EC 1025/2012

Requirement	Fulfilled?
1. Market acceptance	yes
2. Coherent with European standards	yes
3. (a) openness	yes
3 (b) consensus	yes
3 (c) transparency	yes
4 (a) specifications maintenance	yes
4 (b) specifications availability	yes
4 (c) specifications intellectual property rights	yes
4 (d) specifications relevance	yes
4 (e) specifications neutrality and stability	yes
4 (f) specifications quality	yes

Wrap up

NESAS Ongoing Work

- NESAS v2.1 work complete and due to be published in November
- NESAS v3.0 will include revised security requirements
- Development of marketing materials and plan to promote scheme
- Collaboration under way to ensure virtualised functions are included
- Expansion of NESAS to cover non-3GPP defined network functions
- Engagement with ILAC & test labs to ensure continuous improvement
- Restoration of certification under consideration
- Contributions will be provided to ENISA Ad hoc WG on EU CCS
- Evolution of scheme to ensure alignment with EU CCS

Conclusions

- NESAS covers vendor processes assessment and product and evidence evaluation to establish a security baseline
- Voluntary global scheme, created and supported by the industry designed to avoid fragmented security and conformance requirements
- NESAS is designed to be enhanced as needed and continues to evolve through each release
- Operators, vendors, nation states are encouraged to support the scheme and get involved
- NESAS complements EU CCS initiative and GSMA pledges its support for an EU certification scheme

Questions?

Network Equipment Security Assurance Scheme

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

Contact: nesas@gsma.com or jmoran@gsma.com

James Moran
Head of Security
GSM Association