Network Equipment Security Assurance Scheme (NESAS) Overview

James Moran, GSMA

NESAS

Network Equipment Security Assurance Scheme

Supply Chain

Supply chain

A chain of all the individuals, organisations, resources, technologies (hardware and software) and activities involved in product or service development and its lifecycle

Supply Chain Security

Part of supply chain management focused on minimising risk for supply chain, logistics and transportation to identify, assess and prioritise risk management efforts

- Supply chain security needs to take into account cybersecurity and physical threats
- Volume and complexity of cybersecurity threats from hackers, nation states, etc. increasing
- Motivation of attackers varies widely from desire to monitor, steal, destroy, compromise, etc.
- Supply chain can be targeted as a means to gain a foothold and use it to mount attacks
- Contractors, sub-contractors & suppliers throughout the supply chain under constant attack

Supply chain security importance

- Highlights vendor ability to achieve/maintain security levels
- Societal and business reliance on networks is increasing
- Regulatory pressure on security provisions / requirements are rising
- Supply chains are becoming longer and broader
- Complexity of networks is increasing – architecture / components / functions
- Nation state intelligence gathering is a concern
- Security breaches could undermine consumer trust

Multi Dimensional Supply Chain Aspects

LEGAL

Rules & Regulations
Impacts and understanding

(GEO) POLICY

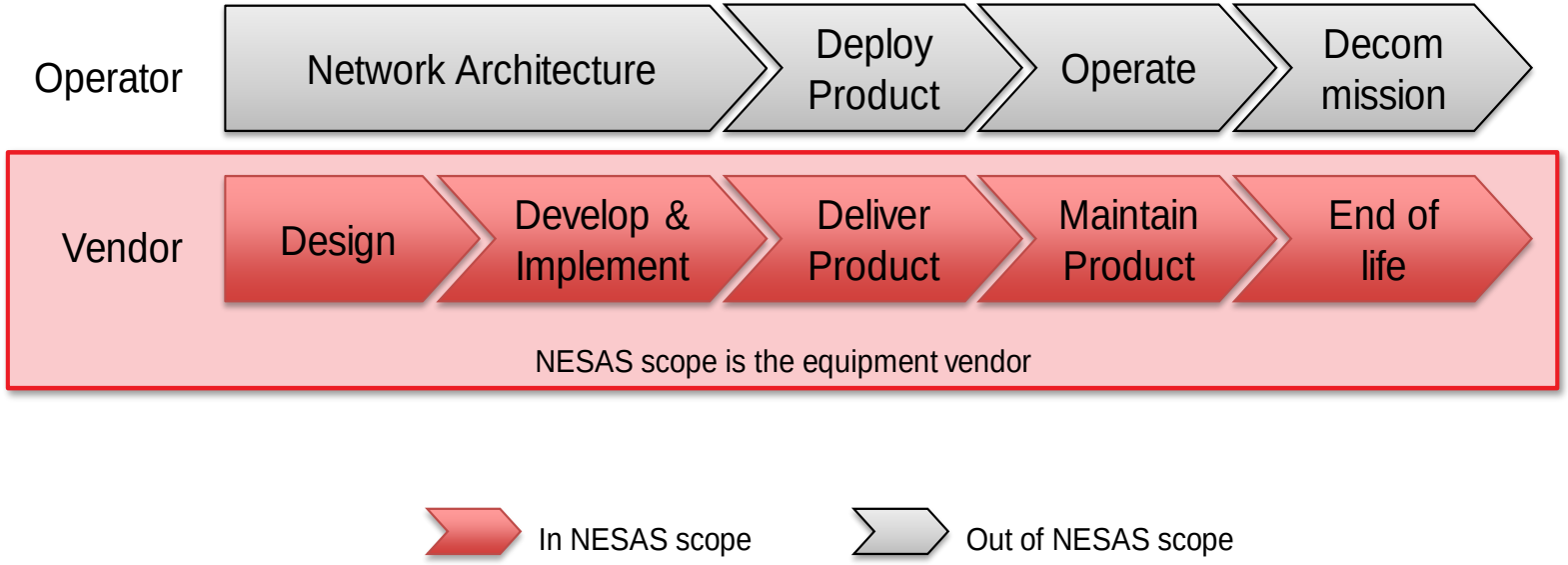
Rules & Regulations
Influence / Inform
Gather and guide

TECHNICAL

Assurance
Operability / Standards

NESAS primarily focussed on technical aspects of product development but touches on legal and policy aspects

Product Development Lifecycle



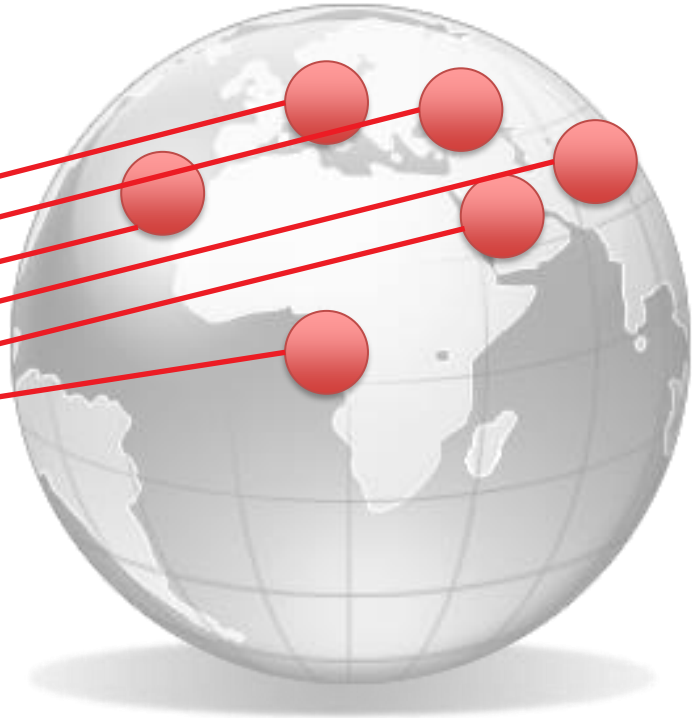
Product development is not the only element of supply chain … but it is vitally important

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

Why NESAS?

Stakeholders need common set of security assurance requirements



Network equipment

What NESAS is

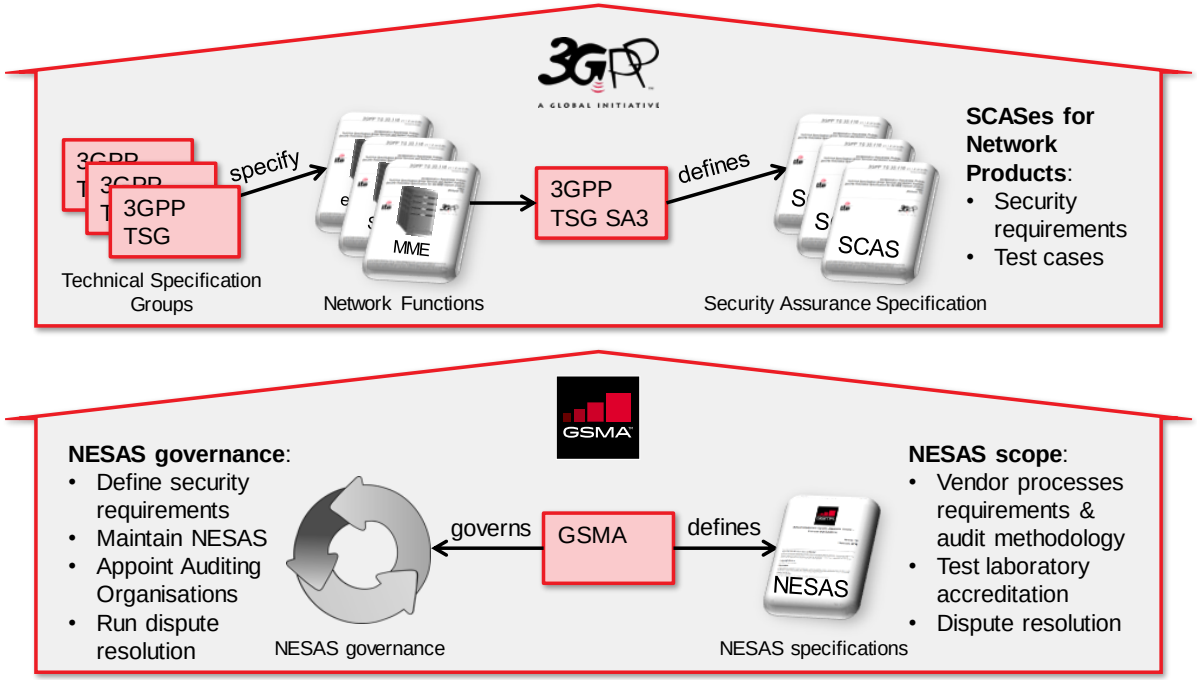
A security baseline to evidence that:

- Network equipment has been developed according to standard secure by design guidelines
- Network equipment satisfies defined security requirements;

Achieved by:

Assessment of equipment vendor processes **+** Security evaluation of network equipment products

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

Network Equipment Security Assurance Scheme

Overview

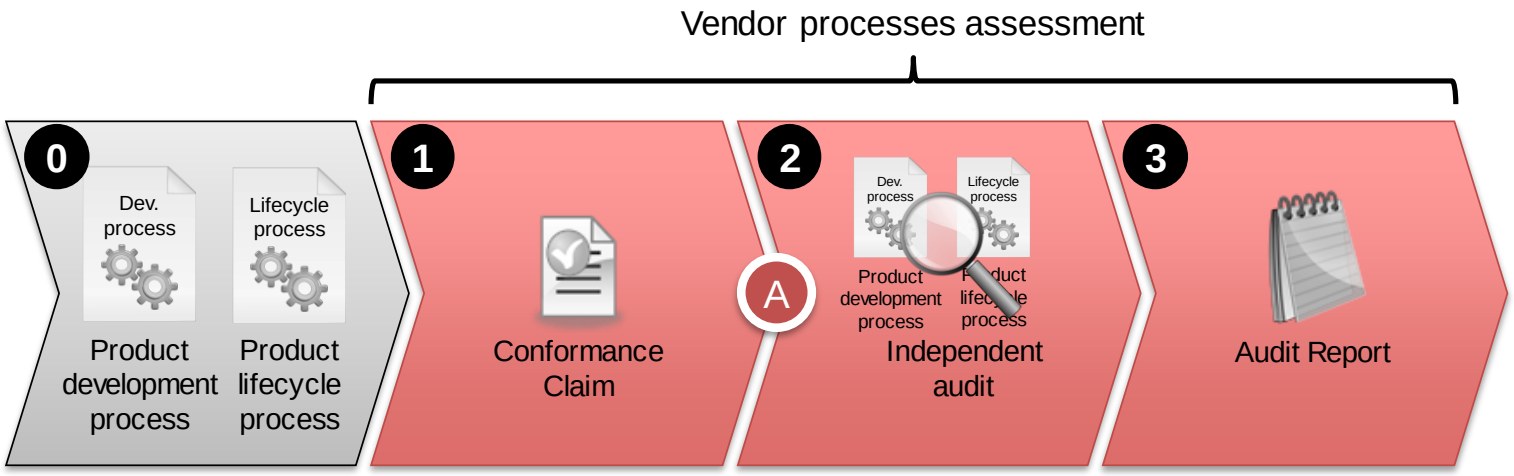
NESAS Elements

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

NESAS Development and Lifecycle Requirements

Defined by GSMA in FS.16 using threat based approach

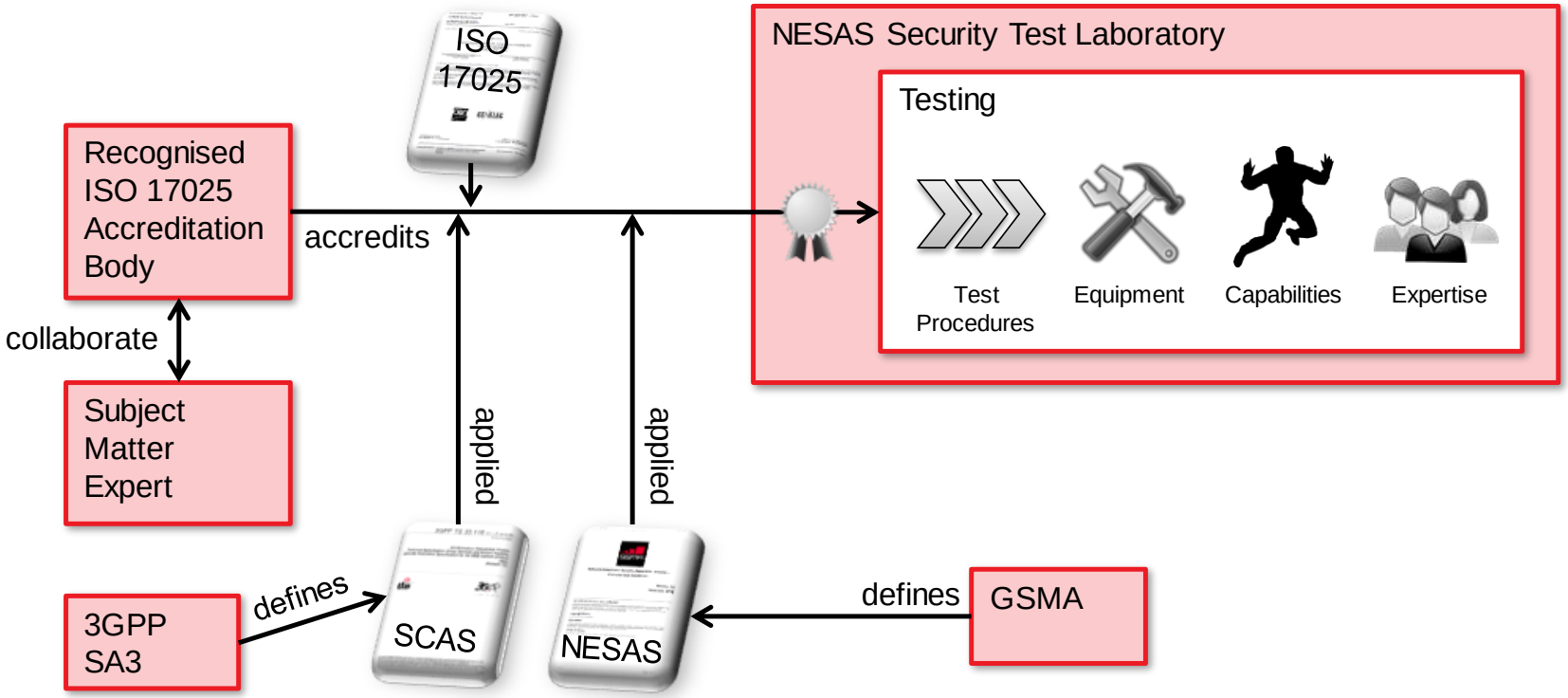
Assets
Source Code
Software packages
Finished products
Security documentation
Operated products
Development support systems

Threats
16 high level threats defined

Objectives
15 high level objectives defined

Requirements (20)
Design
Coding
Compilation
Testing
Release
Operation
General

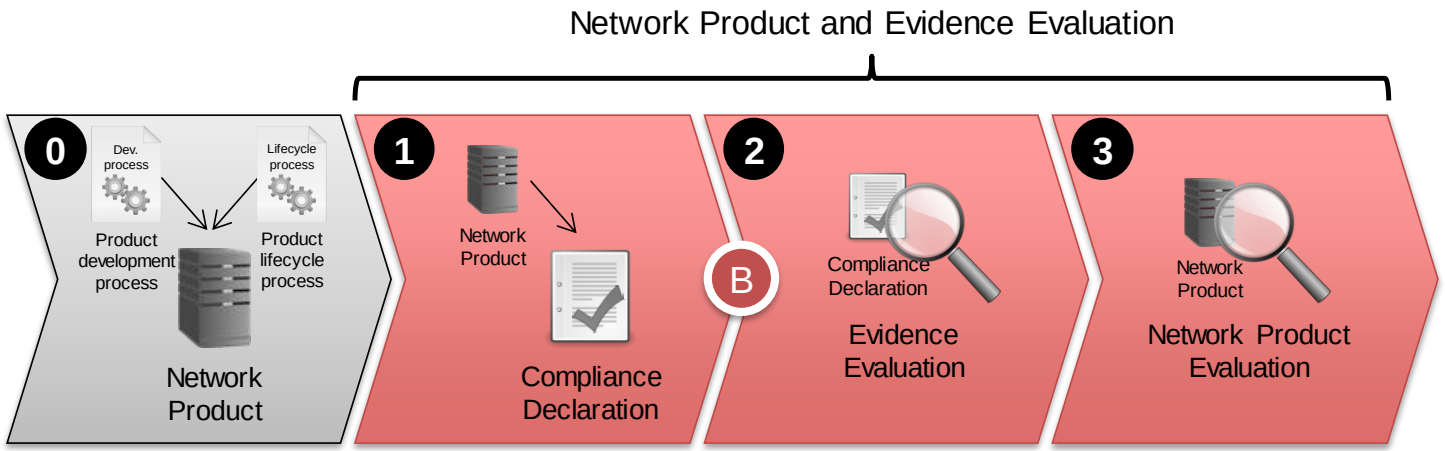
Accreditation of Test Laboratory



NESAS Test Lab Competency Requirements

- Must be ISO/IEC 17025 accredited
- Must demonstrate competency to undertake product evaluations
  - Comprehend principles and methods used in NESAS
  - Understand relationship between 3GPP SCAS documents and NESAS
  - Demonstrate understanding of the overall evaluation planning process
  - Competency to analyse the results of SCAS testing
  - Ability to evaluate product development according to audited process
  - Capability to document results to ensure reproducibility of the test results
  - Understanding of required inputs, SCAS requirements and which to apply
  - Familiarity with telecom equipment, network architecture & interfaces

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

NESAS SCAS Coverage

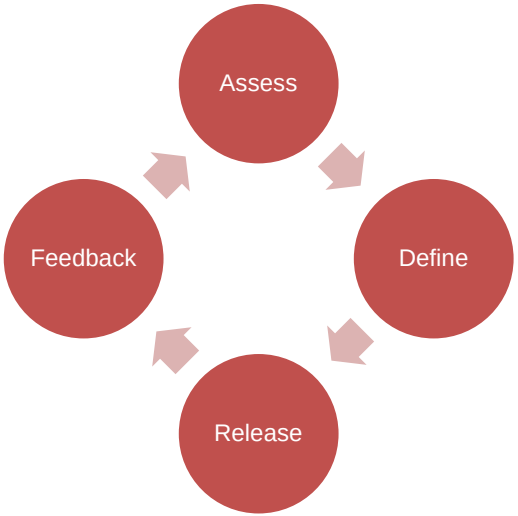
- TS 33.116 - Mobility Management Entity (MME)
- TS 33.117 - General security assurance requirements
- TS 33.216 – eNodeB (eNB)
- TS 33.250 - Packet Data Network Gateway (PGW)
- TS 33.511 - gNodeB (gNB)
- TS 33.512 - Access and Mobility management Function (AMF)
- TS 33.513 - User Plane Function (UPF)
- 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)

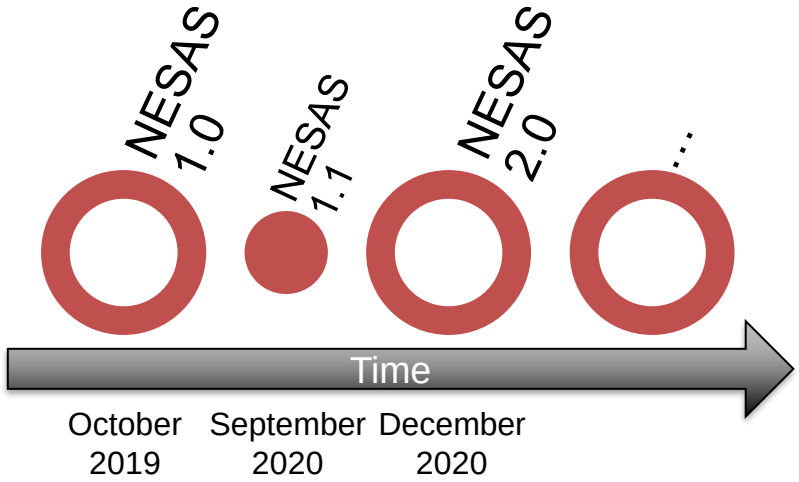
NESAS

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

NESAS Documentation

No.	Title (shortened)	Description
FS.13	NESAS Overview	Describes NESAS as a whole
FS.14	Test Laboratory Accreditation	Defines procedures and requirements for Test Laboratory accreditation
FS.15	Assessment Methodology	Defines procedures for Equipment Vendor processes assessment
FS.16	Security Requirements	Defines requirements the Equipment Vendor must meet for processes assessment

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

Auditor Appointment

- GSMA defined eligibility and competency criteria
- GSMA ran 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

Product line details available at

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

Accredited NESAS Test Labs - 7

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

Product Evaluations - 35

Vendor	Network Product	Product Version / Release
Ericsson	Evolved Node B (eNodeB)	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.	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.	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
Huawei Technologies Co. Ltd.	Evolved Node B (eNodeB)	BTS3900 V100R017C10SPC110
Huawei Technologies Co. Ltd.	Next Generation Node B (gNodeB)	DBS5900 V100R017C10SPC110

Vendor	Network Product	Product Version / Release
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

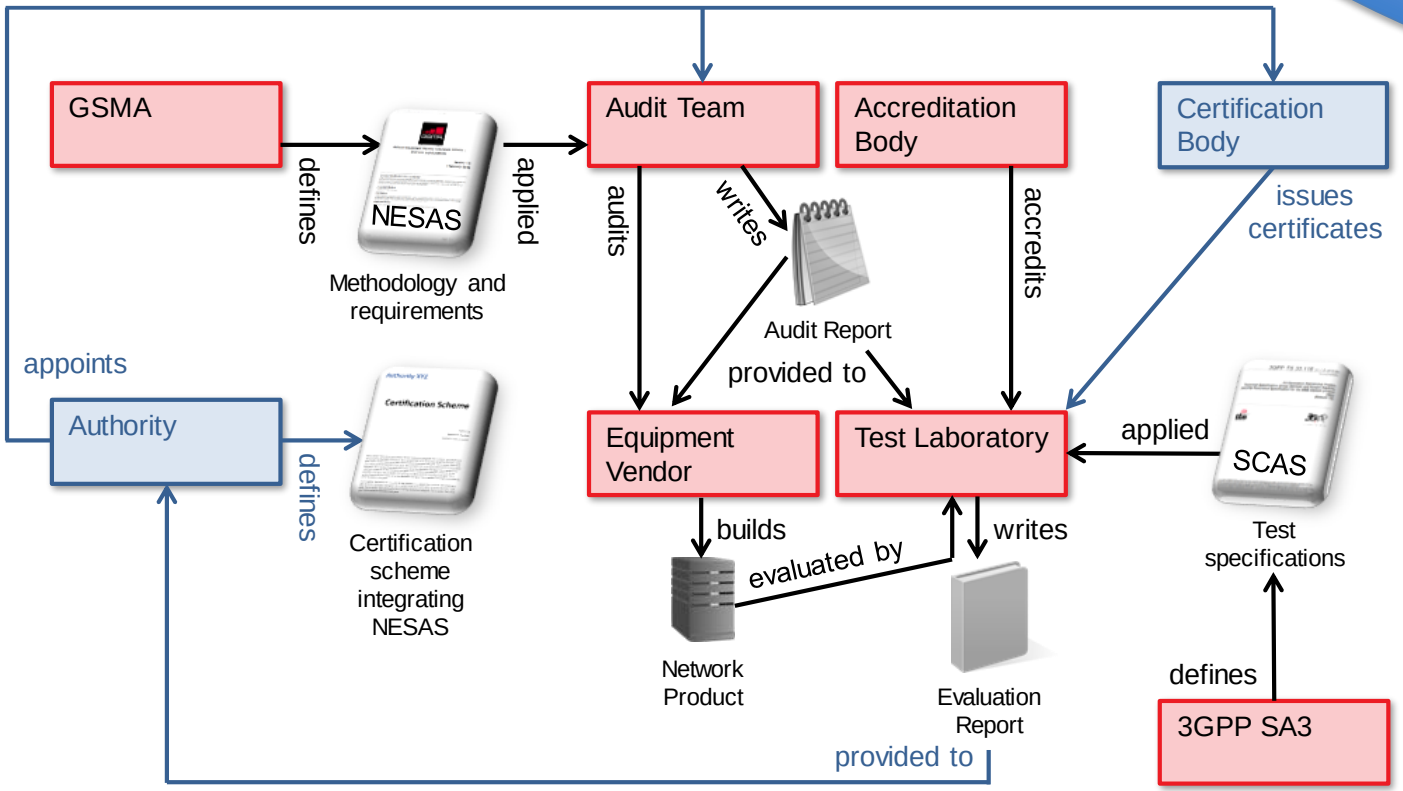
NESAS

Network Equipment Security Assurance Scheme

NESAS for Certification under EU Cybersecurity Act

NESAS Interfaces well with Certification

Possible integration as an example



Proposal: NESAS for EU Cyber Security Act

- European Union (EU) introduced legislation on cybersecurity & the establishment of a certification framework
- Critical infrastructure, such as mobile networks will fall within the scope of the legislation
- EU plans to introduce a network equipment certification scheme for 5G networks
- NESAS will be proposed to ENISA for adoption as EU Cybersecurity Certification Scheme (CCS)
  - Proposal completed in Dec 2020
  - NESAS revised accordingly in Release 2.0

NESAS Benefits

NESAS Benefits for Industry

- Provides reference security assurance requirements for all
- Removes duplication of work to define / respond to individual requirements
- Level of security assurance of network equipment is visible and understood
- Encourages security by design culture across the entire vendor community
- Highlights vendor ability to achieve/maintain security levels
- Shared cost of security among vendors and across all 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

What is required to ensure NESAS success?

- **Network operators** should require their equipment vendors to fully participate in NESAS by subjecting their processes and products to assessment and evaluation
- **Equipment vendors** should have their development and lifecycle management process assessed and their products evaluated
- **Test laboratories** should become ISO/IEC 17025 accredited, in the context of NESAS, to become eligible to undertake product evaluations.
- **ISO/IEC 17025** accreditation bodies should understand the competency requirements candidate test laboratories must demonstrate and be ready to recognise compliance.

Conclusion

NESAS Scope

NESAS is

- A scheme to provide a baseline security level for 3GPP defined functions
- Evolving and will be able to be strengthened
- Flexible by giving network vendors a choice of auditors and test labs
- Monitored by an oversight board to ensure relevance and industry needs are met

NESAS is not

- A guarantee that a product is free from vulnerabilities
- A solution for end-to-end security assurance
- Concerned with network deployment, configuration and interfaces to
- A replacement for operators or national security requirements
- A certification scheme

Conclusions

- NESAS covers **vendor processes assessment** and **product and evidence evaluation** to reach **baseline of security**
- Voluntary global scheme, created and supported by the industry
- NESAS interfaces well with certification frameworks
- NESAS is designed to be enhanced as needed
- Avoiding global security requirements and conformance fragmentation is key
- Operators, vendors, nation states are encouraged to get involved

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