The Standards People

Security Conference

NESAS Update

Presented by: Alex Leadbeater

16/10/2023

Why NESAS?

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

Individual nations started regulating on mobile network equipment security

Security requirements and conformance fragmentation undesirable

What NESAS is

A security baseline to evidence that:

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

Achieved by:

Security evaluation of network equipment + Assessment of equipment vendors

NESAS Approach

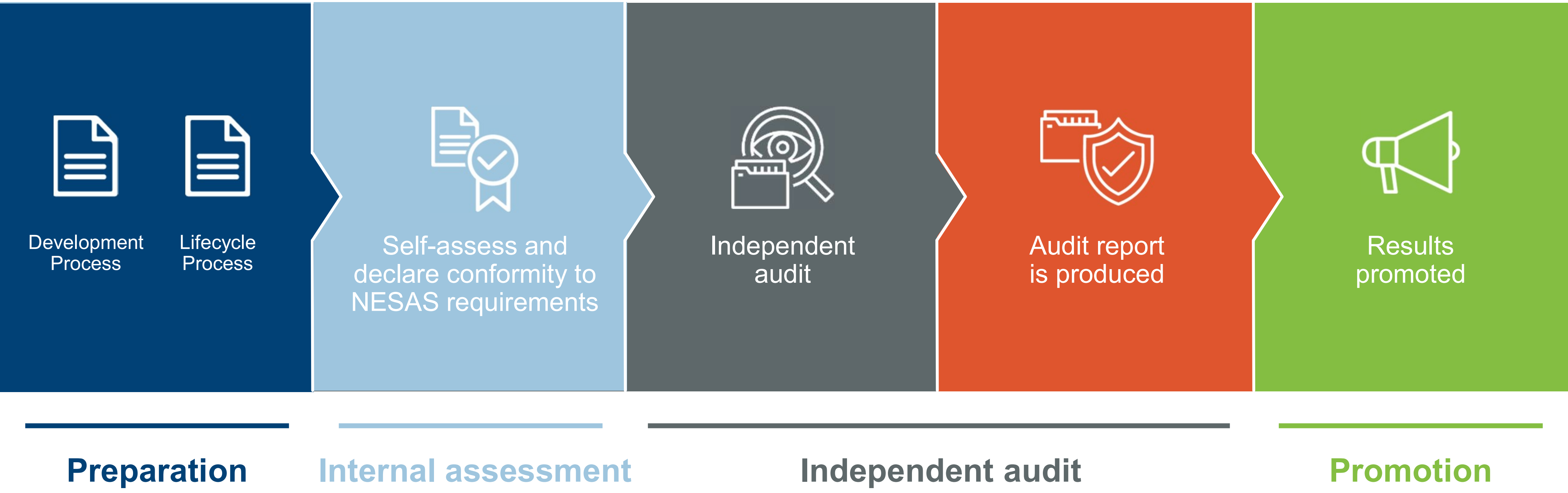
Security assessment of equipment vendors'

- product development processes and
- product lifecycle processes

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

Accreditation of test labs

Development and lifecycle management process audit



Development Process

Lifecycle Process

Self-assess and declare conformity to NESAS requirements

Independent audit

Audit report is produced

Results promoted

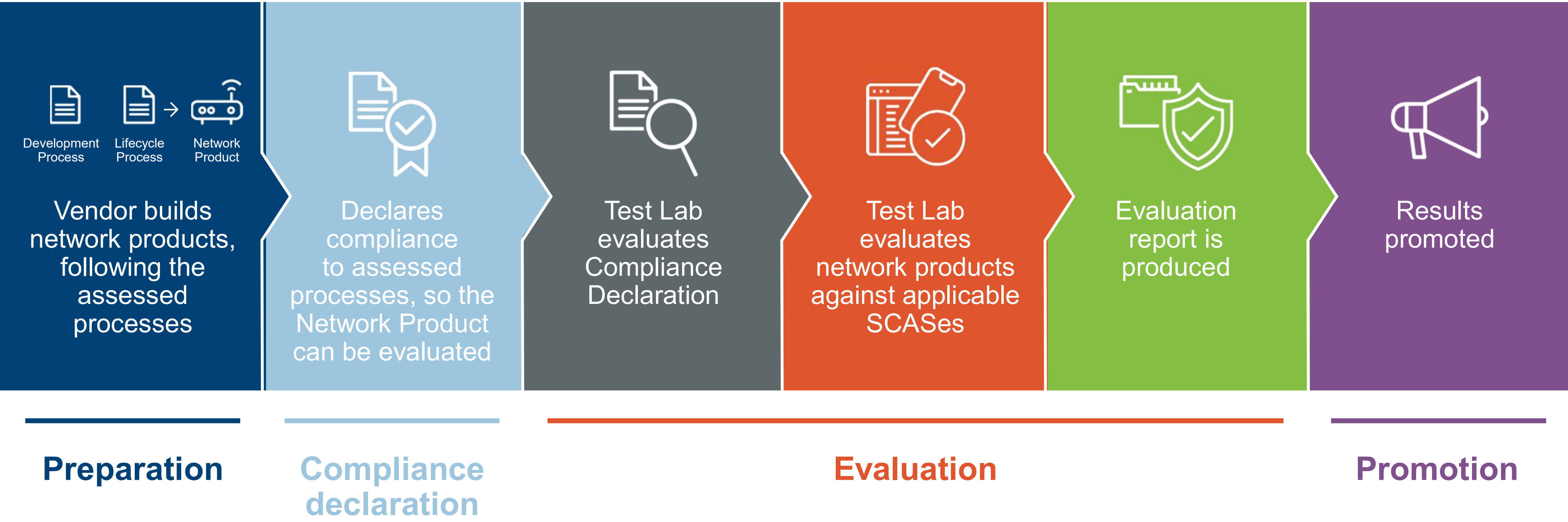
Preparation

Internal assessment

Independent audit

Promotion

Product and evidence evaluation



Development Process

Lifecycle Process

Network Product

Vendor builds network products, following the assessed processes

Declares compliance to assessed processes, so the Network Product can be evaluated

Test Lab evaluates Compliance Declaration

Test Lab evaluates network products against applicable SCASes

Evaluation report is produced

Results promoted

Preparation

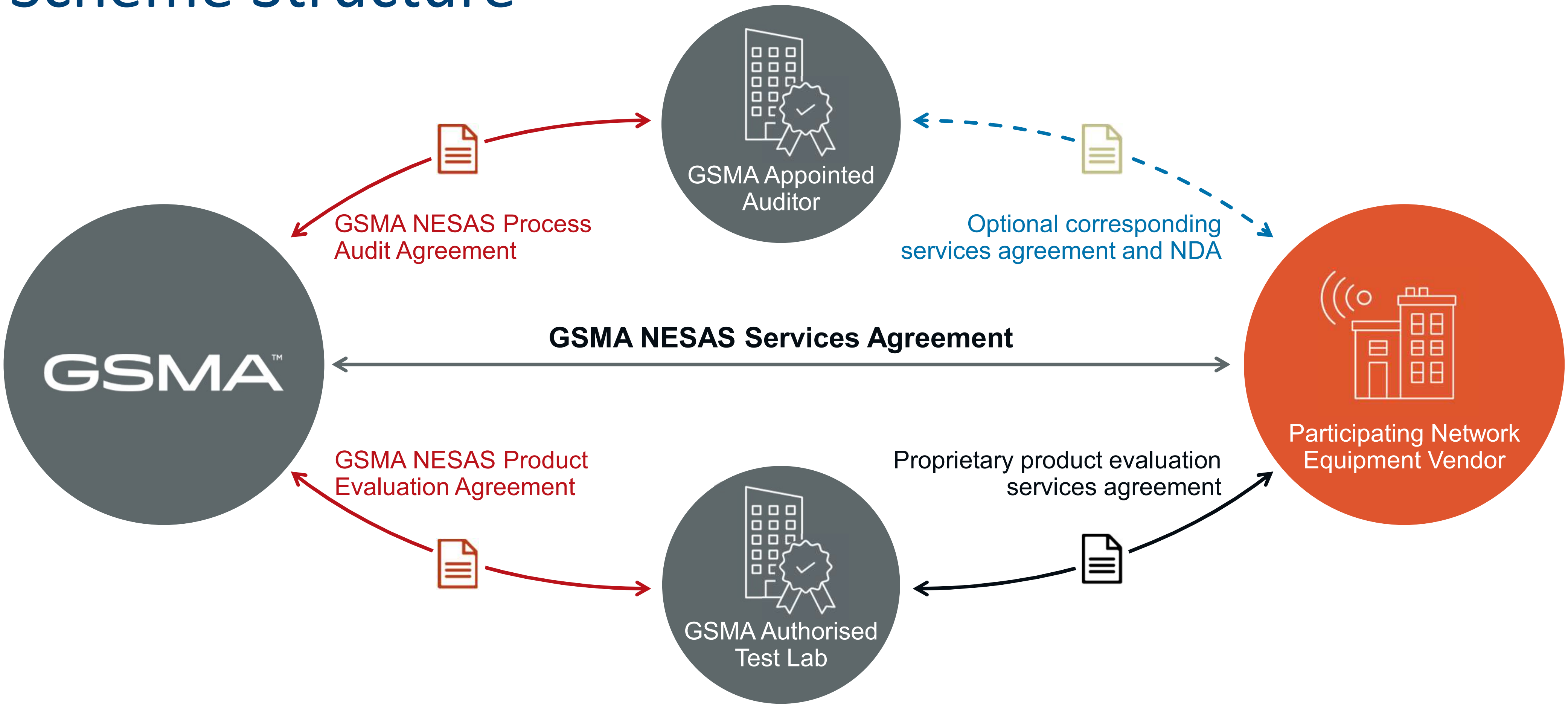
Compliance declaration

Evaluation

Promotion

GSMA

Scheme Structure



GSMA Appointed Auditor
GSMA NESAS Process Audit Agreement
Optional corresponding services agreement and NDA
GSMA
GSMA NESAS Services Agreement
Participating Network Equipment Vendor
GSMA NESAS Product Evaluation Agreement
Proprietary product evaluation services agreement
GSMA Authorised Test Lab

NESAS Benefits

Nation States

Security assurance scheme accepted and funded by industry

Single scheme that is globally relevant

Low barrier for innovation and entering markets

Cost effective scheme that drives security gains

Extensible as needed

Reuses mature models to deliver security gains

Operators

- Raise confidence and trust in equipment
- Increase transparency and comparability of security levels on offer
- Industry defined requirements decreases the need for individual security requirements
- Provides reference requirements for use in procurement RFPs
- Avoids duplications / fragmentation

Vendors

- Common set of assurance requirements
- Lowers duplication of work and security testing needs
- Highlights vendor ability to achieve/maintain security levels
- Encourages security by design culture across the entire vendor community
- Reduces workload responding to operator procurement processes

The GSMA Network Equipment Security Assurance Scheme

PROCESS AUDITS

23 PROCESS AUDITS HAVE TAKEN PLACE

16 DAYS AVERAGE AUDIT DURATION

11 DISTINCT DEVELOPMENT PROCESSES AUDITED

6 DISTINCT CLOUD-RELATED PRODUCT LINES

10 5G-RELATED PRODUCT LINES AUDITED

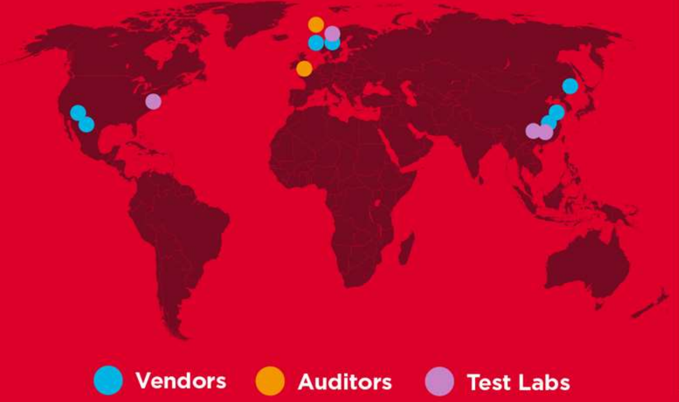
4 4G-RELATED PRODUCT LINES AUDITED

21 SPECIFIC SECURITY REQUIREMENTS

7 PARTICIPATING VENDORS

2 APPOINTED AUDITORS

7 AUTHORISED TEST LABS



PRODUCT EVALUATIONS

42 COMPLETED PRODUCT EVALUATIONS

40 DAYS AVERAGE PRODUCT EVALUATION

9 EVALUATIONS FOR NEXT GENERATION NODE BS (GNODEB)

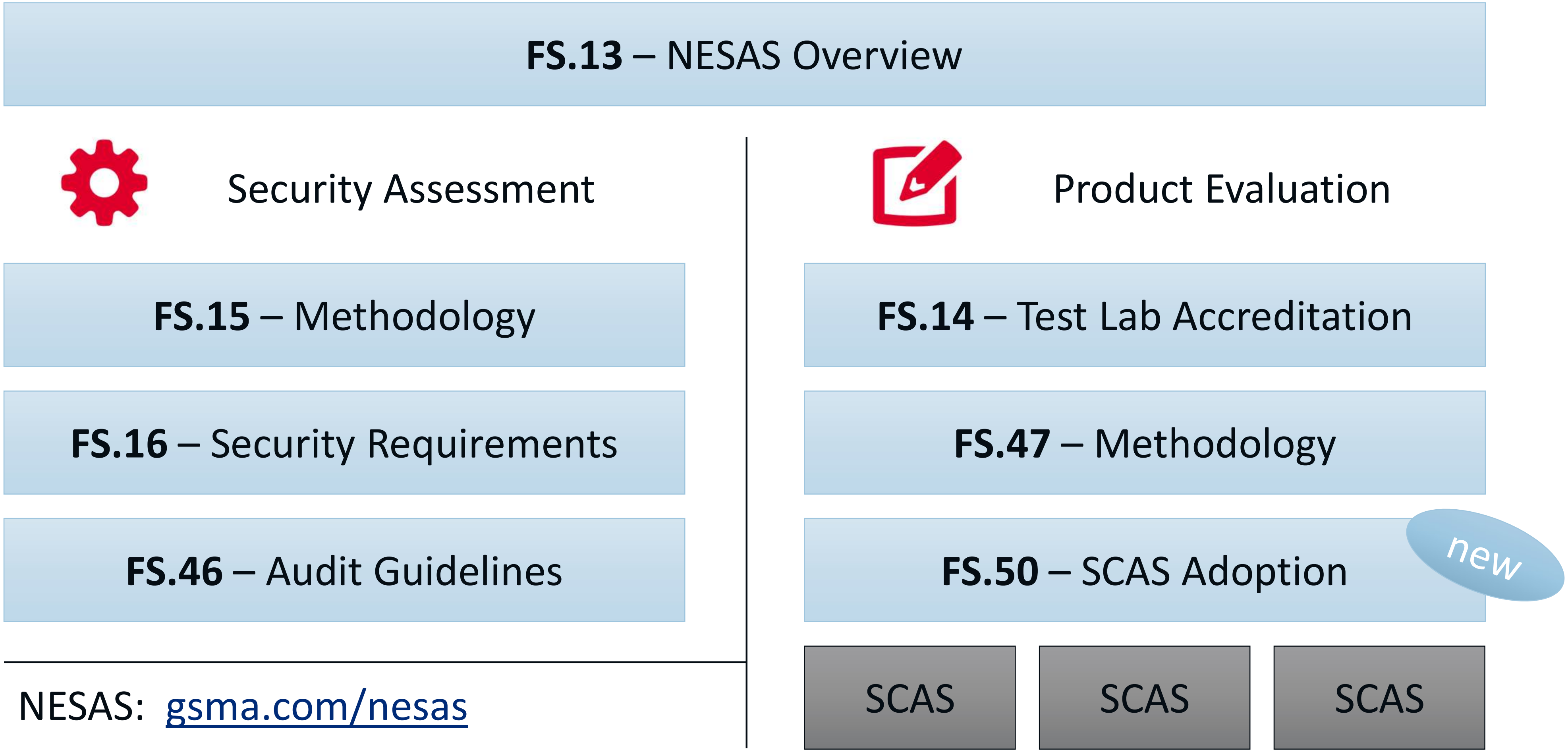
EVALUATIONS COVERING **14 DISTINCT** NETWORK FUNCTIONS

GROWING NUMBER OF EVALUATIONS RELATING TO 5G TECHNOLOGIES

GSMA™

NESAS Documentation

SCAS = Security Assurance Specification



FS.13 – NESAS Overview

Security Assessment

FS.15 – Methodology

FS.16 – Security Requirements

FS.46 – Audit Guidelines

Product Evaluation

FS.14 – Test Lab Accreditation

FS.47 – Methodology

FS.50 – SCAS Adoption

new

SCAS

SCAS

SCAS

NESAS: gsma.com/nesas

NESAS Document Updates 2023

FS.13 – expands SDO definition beyond 3GPP to develop and maintain SCASes and references added to new SCAS requirements and adoption process

FS.14 – clarification that test labs must be independent, test lab record retention requirement specified, test tool competency requirement added and references to new SCAS requirements and adoption process added

FS.15, FS.16 & FS.46 – minor changes to align with other documents changes – changes not material and do not require

FS.47 - SCAS adoption process defined, attacker potential vulnerability analysis added, clarification that product evaluations shall be performed by independent test labs, product evaluation prerequisites and evidence evaluation guidelines added

FS.50 – New document describes what structure and content Security Assurance Specifications (SCASes) that are to be adopted for use by NESAS shall meet

New SCAS Adoption Process

Analysis of NESAS compliance with CSA identified need for NESAS to have a formal process to review and adopt SCASes

Essential that SCASes are uniformly structured, can be applied consistently and have utility for test labs

SCASes can be developed by internationally recognized standards development organisations that have open, transparent, collaborative and consensus based decision-making processes and that grant IPR access to and use of the specifications on an open, fair, non-discriminatory and royalty-free basis.

Publication of a new SCAS can be notified to GSMA and NESAS Group will review and consider the SCAS and its compliance with SCAS requirements after which it will be referenced on NESAS website

Process of gathering continuous feedback on SCAS quality being introduced to ensure test lab experience and views are collected

New SCAS Development Requirements

Structure and format of SCASes described in FS.50 to enable uniformity and quality to ensure verifiability and repeatability

SCASes must be in English language, have clear versioning control, describe network functions to which they apply and include catalogue of security requirements and test cases that describe purpose, preconditions, execution steps, expected results and expected format

Requires developer to provide network product class description, describe security problem definition, identify security requirements and specify test cases

Guidelines, template and worked examples provided to help SDOs

Based on 3GPP SCAS development format and structure and will assist other SDOs which will facilitate the extension of NESAS to cover non-3GPP defined network functions

SCAS Improvement

NESAS depends on 3GPP-defined SCASes for product evaluations

NESAS Test Labs require clear guidance on performing tests - ISO 17025 requires reproducibility

NESAS Test Labs and NESAS Group members and regulators have identified some inconsistencies, gaps and room for improvement

Industry must ensure SCASes are high quality to avoid risk of fragmentation that could arise if regulators choose to create their own national requirements and schemes

GSMA NESAS Group working collaboratively with 3GPP SA3 on improving SCAS quality

Meetings held to date to explain rationale for changes and change requests to 3GPP TS 33.117 have been developed

Changes will be submitted for consideration at SA3#113 in November 2023

Categories of SCAS Improvements

Basic Editorial	Typos, incorrect section references, formatting, etc.
Use of Normative Text	Use of normative text needs to be clarified
Definition/Clarification of Terms	The terms used are not defined or the meaning is unclear
Inconsistent Use of Terms	One or more terms are used to refer to the same thing and therefore consolidation to a single term is required
Missing References	Fields of specific test case definitions have been left incomplete and therefore need to be completed
Clarification of Test Cases	The wording of test cases is ambiguous and/or uses subjective language and is therefore unclear

NESAS Scheme Document Publication as ETSI Specifications

NESAS has been accepted as a candidate scheme for EU 5G Cybersecurity Certification Scheme in accordance with EU Cyber Security Act

EU scheme will not reference GSMA specifications but will reference ETSI publications

GSMA will seek to have NESAS specifications adopted and published by ETSI in accordance with ETSI PAS process

Work underway between GSMA and ETSI to execute changes to existing cooperation agreement and new PAS agreement to allow GSMA documents to be published as ETSI TSs

Feedback received from ETSI secretariat on changes that will be needed for GSMA NESAS documents to comply with ETSI drafting rules

Changes will be made to GSMA documents by end 2023

Additional Scheme Enhancements

Addition of certification component – NESAS is currently an assurance, and not a certification, scheme

Alignment of terminology between NESAS and EU 5G scheme requirements

Broadened recognition of test labs

‘Security-by-default’ auditing and evaluation

Expand coverage of non-3GPP functions

Evaluation of virtualised functions

Evaluation of products with high release frequency

Evaluation report acceptance and guidelines

Making NESAS Successful

NESAS continues to evolve and GSMA remains committed to making it better – others can help

Network operators should require their equipment suppliers to fully participate in NESAS by subjecting their processes and products to assessment and evaluation – make this an RFP procurement requirement

Equipment vendors should have their development and lifecycle management processes assessed and their network 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.

Conclusions

GSMA has offered NESAS as basis for EU initiative to develop cybersecurity certification scheme for 5G network equipment and is working with ENISA

NESAS covers **vendor processes assessment** and **product and evidence evaluation** to reach **baseline of security**

NESAS satisfies most needs defined in EU Cybersecurity Act and has been selected as a candidate scheme

NESAS interfaces well with certification frameworks and can be adapted as needed with ongoing work to improve scheme alignment

Need to avoid fragmentation is essential and GSMA looks forward to collaborating with all stakeholders to further enhance NESAS