ETSI
World Class Standards

Indo-European dialogue on
ICT standards &
Emerging Technologies
(Growth, Profitability & Nation Building)
13-14th March 2014 • New Delhi, INDIA

IN THE FRAMEWORK OF
Project
SESEI
http://eustandards.in/

3GPP – From Security to Security Assurance

Dr.ir. Anand R. Prasad, 3GPP TSG SA WG3 Chairman, NEC Corp.

3GPP A GLOBAL INITIATIVE
NEC

Outline

- 3GPP SA3 & activities overview
- Security assurance related activity in 3GPP SA3

Indo-European dialogue on
ICT standards & Emerging Technologies
13-14th March 2014 · New Delhi, INDIA

3GPP
A GLOBAL INITIATIVE
NEC

3GPP TSG SA WG3 (Security)

- The WG has the overall responsibility for **security and privacy** in 3GPP systems
  - performs analysis of potential threats to these systems
  - determines the security and privacy requirements for 3GPP systems
  - specifies the security architectures and protocols
  - ensures the availability of cryptographic algorithms which need to be part of the specifications

Alf Zugenmaier,
Vice-chairman
NTT DOCOMO

Mirko Cano Soveri,
Secretary
MCC, ETSI

Anand R. Prasad,
Chairman
NEC Corporation

Judy Zhu,
Vice-chairman
China Mobile

http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security

3GPP SA3 Activities (partial list)

- Machine Type Communication (MTC) i.e. Machine-to-machine (M2M): secure binding, small data and trigger delivery
- Small Cell Enhancements: key management when a user equipment has data bearers with secondary eNodeB
- Proximity based services (ProSe): discovery, configuration and communication
- Group Communication System Enablers for LTE (GCSE_LTE): security aspects of group communication in LTE
- Security for Web Real Time Communication access to IMS: authentication and required enhancements to IMS media plane security
- Security Assurance Specification for 3GPP Network Products

Security Assurance Methodology (SECAM)

SECAM Agenda

- Why?
- What is being done?
- What is the current status?
- What is planned?

SECAM: Security Assurance Methodology

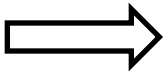
Indo-European dialogue on
ICT standards & Emerging Technologies
13-14th March 2014 · New Delhi, INDIA

3GPP
A GLOBAL INITIATIVE
NEC

Problem

Today's world & mobile network:

- Part of society's **critical infrastructure**
- Increasingly **complex** and **evolving** networks
- With **multiple** entry points and unclear borders
- Broader **knowledge** and **tools** available for attackers



Increasing need for efficient security evaluation

3GPP specifications cover interfaces and protocol security
3GPP specifications do not cover correctness of design or implementation, proprietary solutions and product lifecycle security

Protect the confidentiality, integrity and availability of mobile networks

Security Evaluation Today

- **Hundreds of non-standards** security requirements from operators in procurement process
- Pressure on vendors from **regulators** to certify their products
  - e.g. Indian regulator mandates Indian operators to deploy certified “Safe to Connect” equipment
- No **test-oriented** and **cost effective** method to access security level of network products
  - Expensive custom security audit/review by security experts

⇨ **Need for a standard process supported by operators and vendors**

Disparate methods / requirements increasing product cost & lead time

Security Evaluation Tomorrow

2012: Need for a cost-effective & reliable evaluation process identified but no agreement on the method

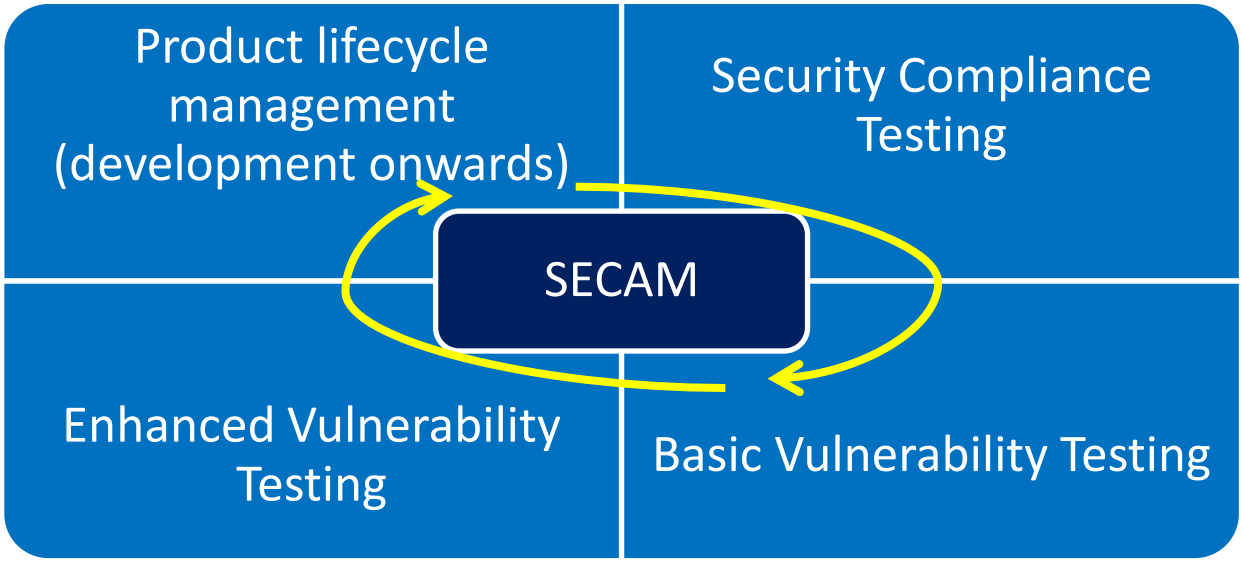
The SECAM Study was launched to find a suitable methodology

- **Phase 1: SECAM study phase in 3GPP – 2012**
  - study existing methodologies & adapt them to 3GPP needs
  - goal to have only testable requirements
  - define which 3GPP Network elements are in the scope
  - Loïc Habermacher, Orange, rapporteur (TR 33.805)

- **Phase 2: SECAM normative phase in 3GPP – 2014**
  - use methodology agreed in phase 1 (TR 33.916)
  - developing requirements starting from MME (TR 33.806) other network products will follow
  - specification on security assurance to follow (TS 33.116)
  - Alf Zugenmaier, NTT DOCOMO, and Judy Zhu, China Mobile

Agreed Methodology

- Security tests described in **3GPP** documents
  - 3GPP lists security tests per type of network equipment in a SCAS document
  - Tests are to be performed by an accredited vendor or third party

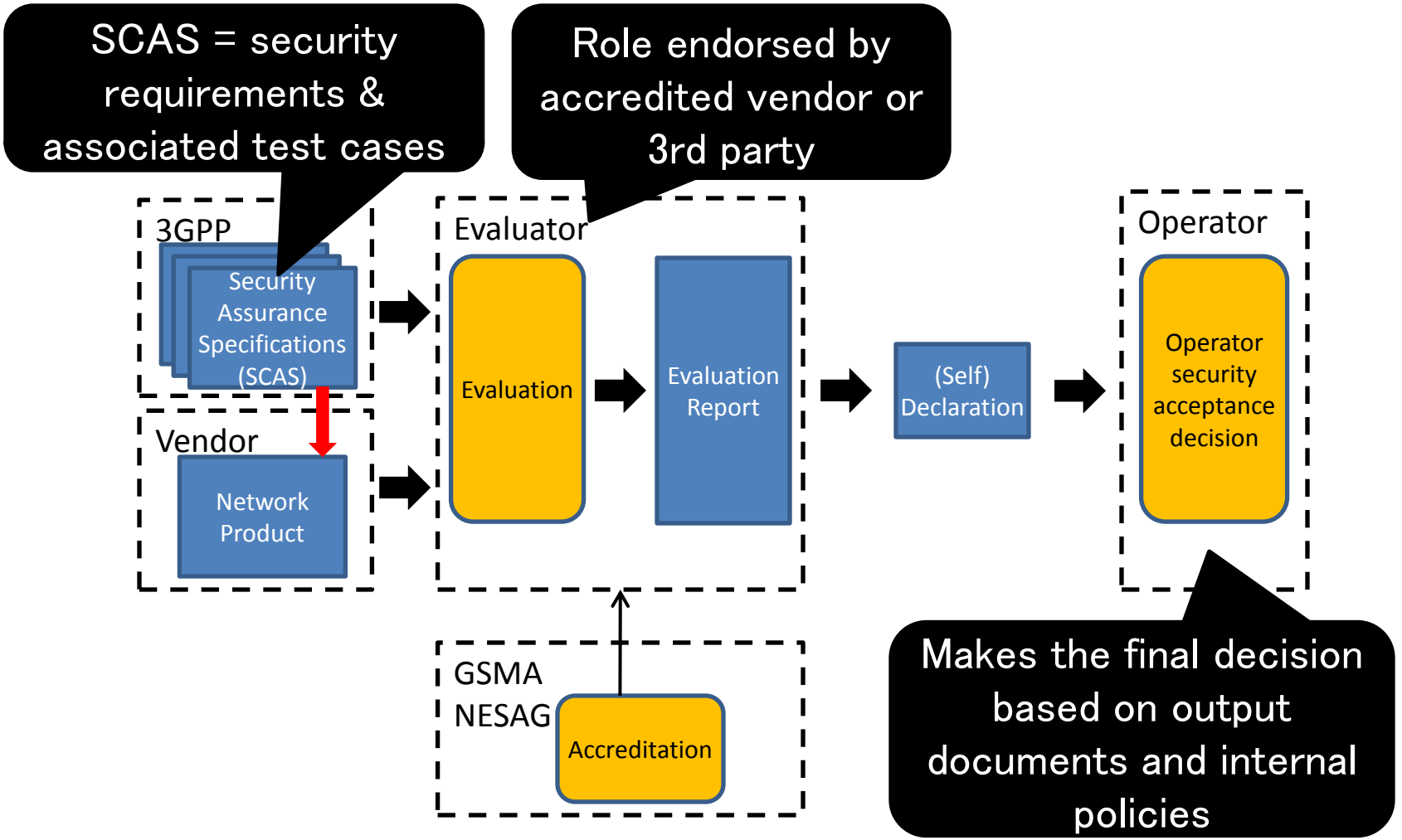


- **GSMA (NESAG)** takes care of accreditation and conflict resolution
- In the end, **the mobile operator can still decide** whether to choose the product or not

Security from product design onwards

NESAG: Network Security Assurance Group; SECAM: Security Assurance Methodology; SCAS: Security Assurance Specification

SECAM Overview



Legend:

Product / Documentation | Role | Process

SECAM: Security Assurance Methodology

GSMA NESAG Overview

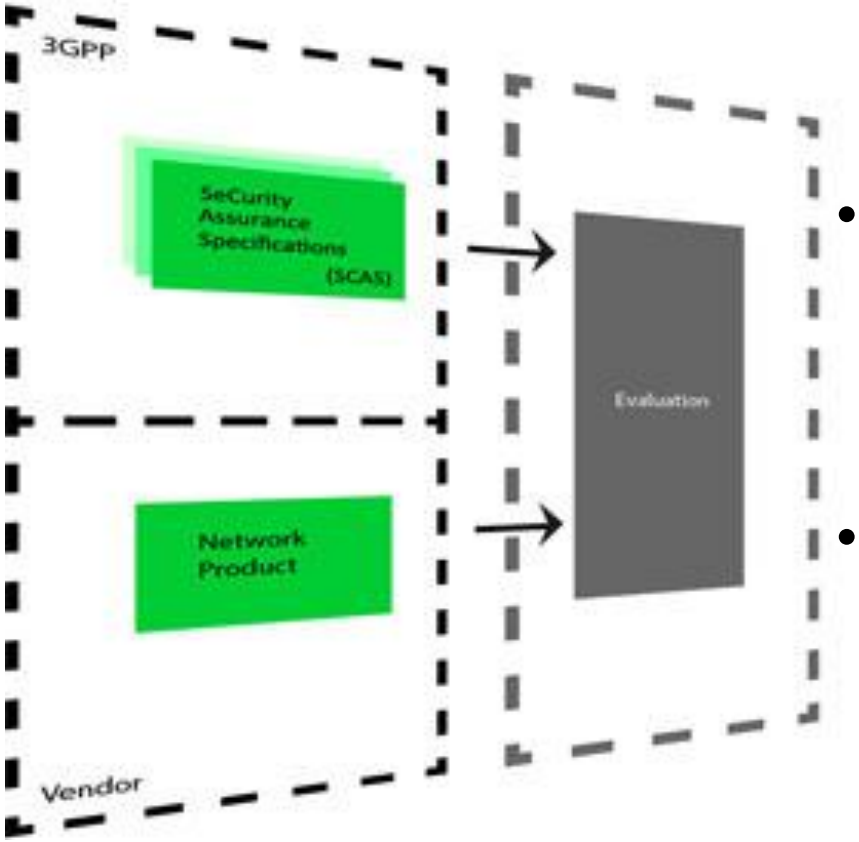
- The Network Equipment Security Assurance Group (NESAG) is a subgroup of the GSMA Security Group
  - First face-to-face meeting on 7 Feb. 2014 in London
  - Chairman: Sven Lachmund, Deutsche Telekom
- Established to provide the administrative framework needed for the implementation of SECAM.
- Responsible for:
  - Accrediting
    - vendor network product development and network product lifecycle management to ensure vendors manage security all along product lifecycle
    - test laboratories (vendor or 3rd party) to ensure they have the skills necessary to conduct SECAM-conformant evaluations
  - Govern & maintain accreditation process and provide appeal process in event of any conflict pertaining to security evaluations.

Accreditation of test-labs & vendor processes and conflict resolution

NESAG Work-Items and Time-Plan

Work Item		Start	End
1	Security test laboratory accreditation *Leader: Bengt Sahlin, Ericsson*	Feb. 2014	Feb. 2015
2	Vendor development and product lifecycle accreditation *Leader: Martin Peylo, NSN*	Feb. 2014	Feb. 2015
3	Conflict resolution process *Leader: Stuart Lyle, Telefónica UK*	Feb. 2014	Feb. 2015
4	Selection of third party audit company *Leader: James Moran, GSMA*	Jun. 2014	Mar. 2015
5	Pilots of SECAM evaluation and test lab accreditations *Leader: TBD*	Sept. 2014	Jan. 2015

In a Nutshell



- SECAM is a new cost-effective & reliable evaluation process
- SECAM addresses technical, business concerns, and regulatory requirements
- The first complete set of security requirements and detailed test cases is expected in 2014
- GSMA NESAG will provide accreditation and conflict resolution

NESAG: Network Security Assurance Group; SECAM: Security Assurance Methodology

Acknowledgement

- Isabelle Kraemer, Orange R&D Center, for her slides on SECAM and significant support in preparing the presentation.
- Sven Lachmund, Deutsche Telekom, and Alf Zugenmaier, NTT DOCOMO, for their review and valuable comments.

Q&A: anand@bq.jp.nec.com

Abbreviations

NESAG: Network Security Assurance Group

SCAS: Security Assurance Specification

SECAM: Security Assurance Methodology