Impart
Assurance

Instill
Trust

Inspire
Confidence

3GPP SECAM

Mike Stauffer

Palindrome Technologies is uniquely positioned to be among the first accredited test labs for the emerging 3GPP/GSMA SECAM Process. This process provides a standard and repeatable test procedure to ensure a baseline of security built in to mobile network equipment.

Palindrome Technologies
100 Village Ct.
Hazlet, NJ 07730
Tel: +1 (732) 784-2892
www.palindrometech.com

3GPP Security Assessment Methodology (SECAM)

Michael Stauffer, Director Security Assurance Compliance

Introduction

With new and increasing national regulations regarding the robustness and security of Mobile Networks, Mobile Network Operators (MNO) need a way to ensure that Network Equipment deployed in their networks can be operated in a secure manner. MNOs can only apply and enforce security controls during operation, the last phase in the system life cycle. They need assurances that security is built into the design, development, and implementation phases of the equipment life cycle. The Mobile Network Operator is responsible for operating a reliable mobile network and relies on the equipment vendor to provide an adequate level of security in their products. Regulators expect MNOs to run robust, reliable and secure mobile networks and MNOs are increasingly being made accountable to satisfy that requirement. Different national regulations and different security demands from MNOs introduce the potential for fragmentation and extra overhead for vendors. Product design and development activities become more complex if varying and disparate security requirements must be met and network equipment products have to be customized for individual markets. The risk of conflicting security requirements poses even greater difficulty for equipment vendors trying to produce products for a global market. This fragmentation has the potential to significantly raise the level of effort and cost for equipment vendors that ultimately impacts MNOs and their customers. Collective and collaborative efforts are required by various stakeholders to effectively and efficiently address the risk of disparate security requirement emerging. All stakeholders, particularly in the Mobile Network industry, need to work together to ensure good mobile network security. The mobile industry needs:

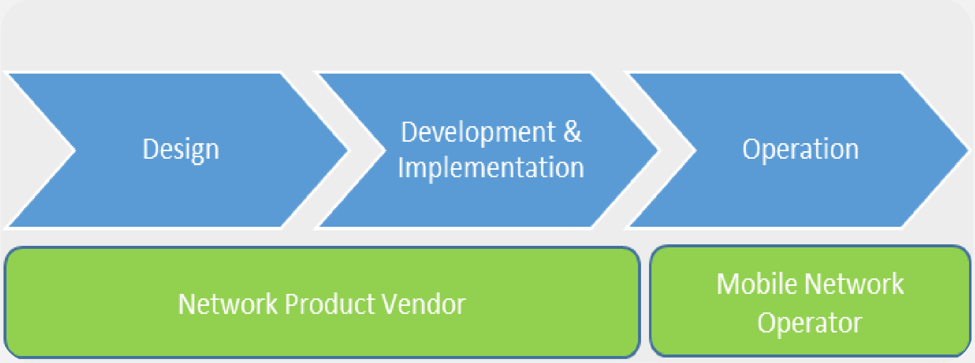


Figure 1: Responsibility and Accountability

- ✓ Built-in security in network equipment
- ✓ Consideration of security in all stages of design, development, and operation
- ✓ Objective measurement of security levels
- ✓ Demonstration and visibility of compliance to security requirements

The Network Equipment Security Assurance Scheme (NESAS) provides an industry solution to meet the needs of industry and other stakeholders.

3GPP SECAM and GSMA NESAS

To meet the needs of all stakeholders, the 3GPP and GSMA have collaborated to form a security assurance testing methodology. The 3GPP Security Group specifies security requirements and test cases for network products such as an eNodeB or an MME. These requirements and test cases are contained in a *Security Assurance Specification* (SCAS). The GSMA defines and maintains the NESAS specifications which cover accreditation of the vendor development and product lifecycle processes, test laboratory accreditation, and security evaluation of network equipment, based on the SCAS developed by 3GPP.

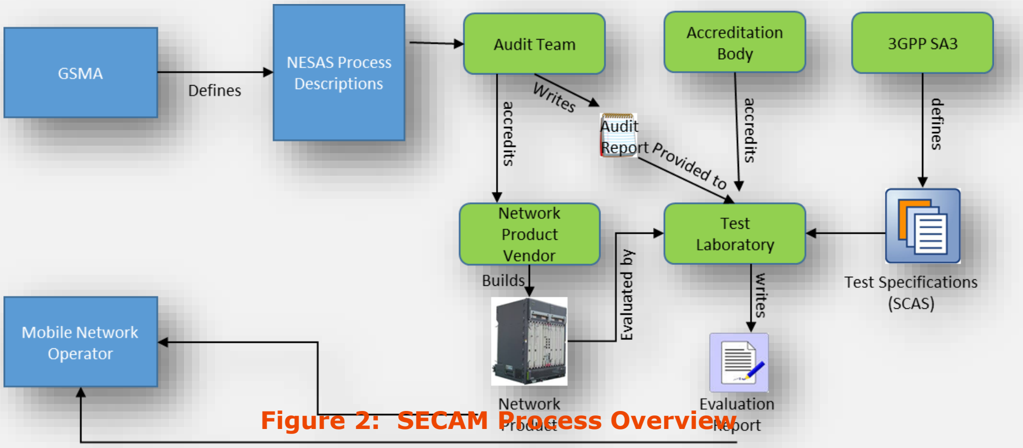
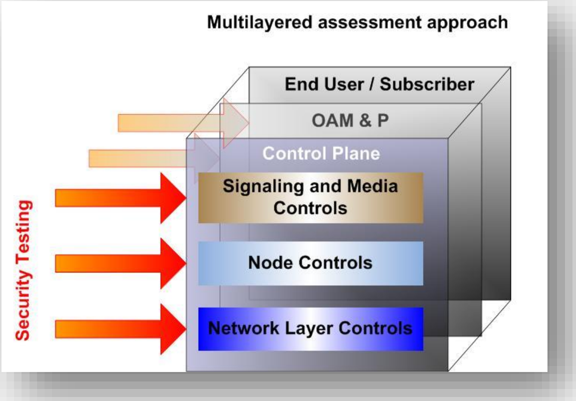


Figure 2: SECAM Process Overview

The GSMA appoints an audit team that audits the Equipment Vendor. Results of the audit are documented in the audit report. The GSMA awards accreditation of the Equipment Vendor. The Equipment Vendor builds the Network Product which is given to a NESAS Security Test Laboratory for evaluation. The Test Laboratory is accredited by an ISO 17025 Accreditation Body that determines if the Test Laboratory is capable of performing meaningful Network Product tests as described in the SCASes. The Test Laboratory evaluates the Network Product against the relevant SCASes and verifies that the accredited development processes of the vendor are applied to the tested Network Product. The Audit Report provides the required information for verifying the processes. The Test Laboratory then produces an Evaluation Report containing the results. The Network Product can then be shipped to customer's MNO, together with copies of the Evaluation Report.

Palindrome's Position and Product Security Assurance Service

The process selected by the GSMA to accredit Test Laboratories is ISO 17025. Palindrome Technologies is already ISO 17025 accredited and will add SECAM to its scope as soon as the process is available. Furthermore, the security assurance testing process defined by SECAM and NESAS is almost identical to the process Palindrome Technologies has been using for many years.



We have been following the development of the SECAM/NESAS process since it began as a study item within the 3GPP Security Working Group. Palindrome Technologies is uniquely positioned to become one of the first NESAS-accredited Test Labs in the world.

As an accredited ISO 17025 Testing laboratory, Palindrome implements the Network Equipment Security Assurance Scheme (NESAS) leveraging the 3GPP security requirements (*Security Assurance Specification* (SCAS)) for Network Elements (e.g., eNB, MME) to provide security assurance testing and certification for Telecommunication products. Palindrome's SECAM security testing framework covers all the necessary dimensions defined in NESAS including node security, management and signaling security. The results of our assessment are captured in a detailed technical report along with recommendations to remediate any exposures. Furthermore, our team works closely with your subject matter experts to provide all the necessary details (e.g., logs, network traces, exploits) and knowledge transfer to remediate deficiencies.

Reference Documents

[1] 3GPP TR 33.916 Security Assurance Methodology for 3GPP network products

[2] 3GPP TS 33.116 Security Assurance Specification for the MME network product class

[3] 3GPP TS 33.117 Catalogue of General Security Assurance Requirements

[4] FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process

[5] FS.15 Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process

[6] FS.16 Network Equipment Security Assurance Scheme – Dispute Resolution Process

[7] GSMA NESAS WI 4a Doc Network Equipment Security Assurance Scheme – Request for Information; to be published in April 2016

[8] GSMA NESAS WI 4b Doc Network Equipment Security Assurance Scheme – Request for Proposal; to be published in June 2016

[9] Palindrome Technologies ISO/IEC 17025 Testing Lab Accreditation (circa 2012)