Standards Driven Security Assurance for Mobile Networks

Sven Lachmund

Deutsche Telekom, Germany
E-mail: sven.lachmund@telekom.de

Received 13 February 2016;
Accepted 14 March 2016

Abstract

A new security assurance scheme for mobile network infrastructure equipment is described in this article. In introducing an effective security assurance scheme, constraints need to be considered as the environment in which the scheme is introduced defines some boundaries. Technology is not the only aspect that counts and it is necessary to achieve a real balance between technical and organisational security improvement, visibility of security levels of network equipment, operational feasibility, and market acceptance and participation. The end goal is to involve a range of stakeholders that need to commit to the scheme so the likely effectiveness, cost, effort and complexity are important parameters that need to be taken into consideration. The mobile industry operates worldwide and thrives on the development of open standards by multiple standards development organisations. Solutions that are designed and agreed must meet the needs of all involved stakeholders around the world to secure support for their delivery to market. This paper explains how standardisation works in and for the mobile industry and introduces the objectives, the constraints, the reasons for developing a security assurance scheme, and describes the proposed scheme for mobile network equipment and lifecycle processes. The article illustrates that the new Network Equipment Security Assurance Scheme (NESAS), as it is called, meets the various and different needs of mobile network operators, network equipment vendors, and regulators in a time of ever growing complexity of mobile networks.

Journal of ICT, Vol. 3, 105–132.
doi: 10.13052/jicts2245-800X.321

Keywords: 3GPP, accreditation, development lifecycle, evaluation, evidence, mobile industry, mobile network, network equipment, product lifecycle, regulation, regulator, security, security assurance, security assurance scheme, security requirement, specification, standardisation, test case.

1 Introduction

This industry initiative is about information security, network security, ICT security and telecommunication security. As the terms *security* and *security assurance* are commonly used to describe a broad range of areas, it is worth scoping what industry has in mind when embarking on this new scheme. The types of security and associated needs addressed in this publication are relevant for all stakeholders that deal with information systems, ICT systems, communication networks and telecommunications. These stakeholders include equipment vendors, operators, national regulators and authorities, and mobile users. Each of these may have different interests and priorities but only if they all approach security with a common sense of purpose to make things better will there be an effective increase in security levels. Undertaking a collaborative approach is necessary to get security right and each of the stakeholders described below have needs and a role to play.

1.1 The Mobile Industry – Stakeholders and Roles

The **mobile industry** maintains the ecosystem that allows mobile users to conduct mobile data and voice communications worldwide. **Mobile Network Operators** (MNO), as the term suggests, operate mobile networks and the network equipment used in those networks, such as the radio base stations, Internet gateways, etc. are developed and provided by **network equipment vendors**. The mobile devices used to avail of services, e.g. Smartphones, are produced by **mobile device manufacturers**. **SIM vendors** produce the SIM cards that are inserted into the mobile devices to securely store mobile user credentials. Mobile devices attach via radio to mobile networks, are authenticated to those networks by the SIM cards, and get connectivity to the global phone network and to the Internet (or other networks). Users are free to take out a subscription with a MNO of their choice, which then provides them with a SIM card, and they can purchase a mobile device of their choice. With this equipment, users conduct voice and data communications over mobile networks, being billed and charged by their chosen MNO. This is what enables mobile users to enjoy the use of their Smartphones as an inherent part of their daily lives.

1.2 Standardisation Is Key for the Mobile Industry

Users can choose any mobile device and any mobile network in their home country. They will get connectivity in their home market and, in most cases, when they travel with their mobile device to another country they can choose any of the MNOs there and connect to their network. This interoperability and interworking is testament to the efforts and solutions provided by network equipment vendors, mobile device manufacturers and MNOs who jointly work together on a global level to enable these international roaming services. The functionality that mobile users enjoy and use on mobile networks today was agreed and developed by these stakeholders over a period of years. That work continues for the next generation of services All of these stakeholders come together in standards development organisations to propose and discuss solutions to be developed and delivered to market. In addition to the mentioned benefits for the user, vendors and MNOs benefit from standardised solutions because of the economy of scale benefits over proprietary solutions. Stakeholders wishing to promote solutions for standardisation must achieve consensus from the other industry partners participating in the standardisation process thereby ensuring nobody has a monopoly on ideas or outcomes.

1.3 Security Assurance in the Mobile Industry

Security assurance has the potential to introduce a variety of security controls during design, development, implementation, and operation of systems to protect data, information, and resources. This is done to ensure business continuity and to satisfy national/international regulations.

Security assurance per se is not a new concept, but it makes sense to formally roll this out to the mobile industry. There is currently a range of disparate and uncoordinated security assurance schemes that partially cover some aspects of the mobile industry. These include the *Security Assurance Scheme* (SAS) for SIM cards [22] and the *Center for Internet Security* (CIS) *Security Benchmarks* for network services and operating systems [5] on ICT systems, for example.

Technically, the mobile industry is moving away from old legacy technologies to standards based IP solutions. This *all IP* transformation was started with the introduction of the 3$^{\mathrm{rd}}$ generation mobile network (3G, aka. UMTS) [18] and will be fully achieved with the 4$^{\mathrm{th}}$ generation mobile network (4G, aka. LTE) [18]. However, the air interface, the communication protocols used between network equipment, the architecture of the mobile network, operation and maintenance of the mobile network, and the SIM card remain artefacts

of the mobile industry being integral part of the current and next generation networks.

Existing security assurance schemes were developed for different time and constituency of stakeholders. For example, CIS Security Benchmarks were created for the Internet and its supporting technologies but they can equally be applied to modern IP based mobile networks although they would only cover a fraction of what would need to be covered. The mobile industry also needs comparable schemes for the specific network services, communication protocols and network equipment that are commonly used in mobile networks that are not already covered. Capturing the needs of the entire mobile network is key for effective security assurance, as the level of security can only be determined and increased if all the deployed elements and technologies are captured.

A security assurance scheme will only enjoy broad recognition in the mobile industry, if the scheme is standards based and universally applicable. As pointed out in Section 1.2, all the major technologies are defined and developed based on consensus achieved within the recognised standards development organisations.

1.4 Mobile Industry Challenges

The mobile industry is facing a range of challenges that pose some risk in terms of extra overhead, (mainly for equipment vendors), that serve no discernible benefit. These challenges are explained below.

1.4.1 Security incidents impacting mobile network equipment

Although mobile network equipment vendors care about security of the equipment they develop and produce, security issues occasionally arise. Often, basic security best practices are not followed and several vendors experience similar issues. Two examples of weaknesses discovered in 2015 are hard coded non-changeable default passwords on network equipment and incomplete hardening.

The very existence of these weaknesses proves there is room for improvement in two areas:

1. design and implementation, and
2. procedures for integration and maintenance.

Evidence suggests that existing security controls may not be entirely adequate. Multiple vendors had, and have, similar security issues with their network equipment, suggesting it is likely that the root cause might be the same.

This is not a phenomenon that is specific to the mobile industry as the Internet community and the ICT industry in general suffer from the same problems, too.

1.4.2 Growing complexity

The number of 3GPP defined network functions and their complexity is growing from one 3GPP release to another. The growth in network functionality and the complexity of network protocols is attributable to the need to support more traffic more efficiently. Keeping control over all these standards and ensuring there is consistency across them is increasingly difficult, which increases the risk of unintentional and unidentified design flaws.

Inevitably, the complexity also increases for the network equipment vendors who implement these network functions in their products. For them, it is increasingly difficult to ensure a design that is free of flaws. The implemented code, being a derivate of the design, is required to be correct, robust, and free of faults and only stringent and systematic approaches to secure design, development, and implementation eliminates the risks.

1.4.3 Regulatory demands

Regulators increasingly demand from network operators that they security assess their mobile networks and the equipment to be deployed within them. Many regulators consider mobile networks as critical national infrastructure and expect assurances that these networks are reliable, robust and secure. It is expected by regulators that in crisis situations mobile networks remain functional. As a consequence, regulators are beginning to expect that MNOs only deploy security assessed network equipment within their networks. At the time of writing (Feb 2016) India requires that locally licensed MNOs only deploy network equipment which has been "tested as per relevant contemporary Indian or International Security Standards [. . .] Telecom and Telecom related elements against 3GPP security standards [. . .]" [14]. Other countries are likely to follow.

1.4.4 Increasing demand for consumer protection

Several security research activities, such as breaking the GSM air interface encryption algorithm A5/1 and highlighting vulnerabilities in the international signalling network, have been widely reported and covered by the media. The goal of publicising many of these known security compromises is to ensure that industry reacts to these developments and fixes the root causes.

1.4.5 Security levels not defined

Generally speaking, network security levels are left to individual MNOs to define. They need to bilaterally agree with their equipment vendors what level of security they want to have and in which way this will be achieved. There is no standard for common network security requirements in the mobile industry at present. Consequently, there is a broad variety of demands from MNOs all over the world.

1.4.6 Risks and consequences for the mobile industry

There is increasing pressure on the mobile industry to get network equipment security and mobile network security right. Approaches need to be identified and applied that enable effective mobile network security.

The lifecycle of network equipment consists of a number of different stages. In its simplest form it starts with design, is followed by development and implementation, and then the equipment is operated until it reaches end-of-life. Design, development and implementation are the responsibility of the equipment vendor, whereas the MNO is responsible for operation of the equipment. Figure 1 depicts this lifecycle and the assigned responsibilities. The MNO is responsible for operating a reliable mobile network and relies on the equipment vendor to get security right. Regulators expect MNOs to run robust, reliable and secure mobile networks and MNOs are increasingly being made accountable for satisfying that requirement. Network design, operating procedures and maintenance of deployed network equipment falls within the MNO's responsibilities but the vendor must ensure that the network equipment is secure in the first instant. It is in the interests of all MNOs, and the customers that use those networks, to source secure network equipment from their vendors. Failure to do so makes it virtually impossible to operate a secure mobile network.

Different national regulations and different security demands from MNOs introduce the potential for extra overhead for vendors. Product design and development activities become more complex if varying and disparate security

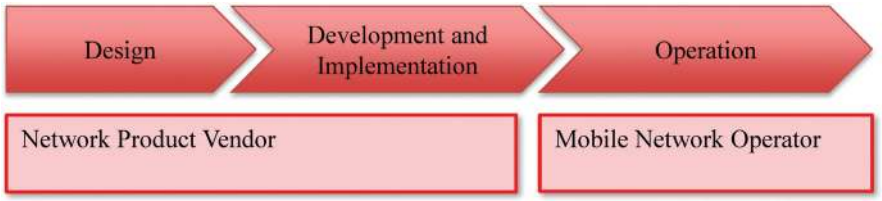

Figure 1 Responsibility and accountability.

requirements must be met and network equipment products may have to be customised for individual markets. The risk of conflicting requirements emerging poses even greater difficulty for equipment vendors seeking 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 requirements emerging. All stakeholders, particularly in the mobile industry, need to work closely together and that is a real prerequisite for good mobile network security. What the mobile industry needs most of all is:

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

The *Network Equipment Security Assurance Scheme* (NESAS) that is described in Section 5, provides an industry solution to meet these demands.

1.5 Balanced Approach

When finding solutions for the challenges described above, it was recognised from the outset that a balanced approach is required to ensure effectiveness and acceptance by the wider mobile industry. The best approach needs to achieve a balance between real technical and organisational security improvement, visibility of security quality of network equipment, operational feasibility, and reduction of residual risk. Technology, although important, is not the only critical factor if all stakeholder concerns are to be addressed and those stakeholders are to be convinced to support the collective effort. The mobile industry is a mature ecosystem wherein roles are well defined and any proposed solution needs to neatly fit this ecosystem to gain wide acceptance. Therefore, additional factors such as effectiveness, cost, complexity, etc. need to be considered and dealt with. The new security assurance scheme for mobile network equipment that is presented in Section 5 seeks to take cognisance of these needs.

1.6 Scope

As already mentioned, the focus of the desired security assurance scheme for the mobile industry is on network equipment. The approach that is laid out in

Section 5 addresses the needs and challenges described above by taking the following multifaceted approach:

- Accreditation of vendors' product development processes;
- Accreditation of vendors' product lifecycle processes;
- Network equipment product evaluation by competent test laboratories using industry defined and standardised security tests.

To achieve the needed balanced approach (see Section 1.5), certain aspects have been excluded from the initial scope and these are as follows:

- There is no certification of network equipment by an officially recognised authority.
- There is no proof of absence of certain functionality (e.g. backdoor) in the network equipment.
- The scheme does not replace existing operator or national requirements.
- The scheme does not include security of interfaces between network equipment.
- The scheme does not address the need for end-to-end security.

1.7 Intended Audience

This article is written for readers who are interested in security assurance in general and want to see an example of how a given industry defines its own security assurance scheme. It is also meant for readers who wish to learn more about the mobile industry, standardisation in the mobile industry, and the new Network Equipment Security Assurance Scheme.

The article is deliberately high level, as it focuses on illustrating all the influencing factors and dependencies that led to the decisions made by industry for the security assurance scheme.

The reader will learn about technical aspects of security assurance and how they are dealt with in the given security assurance scheme, as well as dependencies and constraints that are relevant to defining the scheme.

As the scheme will be standardised and as standardisation is key for the scheme's acceptance, the focus on standardisation is essential, which is reflected in this article, too.

1.8 Organisation of This Article

After some terms are defined and the setting in which the security assurance scheme will be applied is explained in Section 1, Section 2 talks about standardisation in the mobile industry before Section 3 addresses security

assurance in general. Security assurance applied to the mobile industry is covered in Section 4. Section 5 contains the main body of this article that describes the *Network Equipment Security Assurance Scheme* (NESAS) that is being developed by the mobile industry.

2 Standardisation in the Mobile Industry

With the introduction of the first fully digital mobile network, called GSM (*Global System for Mobile Communications*) [18], the European inventors had international roaming in mind when designing it in the 1980s. Their vision was that users could take their mobile device to another European country and use a foreign mobile network there for their voice communication and have use of the services billed by their home network. They intended to avoid using proprietary national solutions and were interested in developing open standards that would deliver significant economy of scale. This vision required the involved stakeholders to collaborate. European countries agreed to reserve a particular frequency band and a couple of European MNOs jointly developed and deployed GSM which was launched in 1992. In the beginning, membership was mainly limited to the authorities for post and telecommunications of the involved countries because at that time, telecommunications were strictly regulated, controlled and owned by state agencies. Over time, the consortium transferred responsibility and control over the GSM standards to the *European Telecommunications Standards Institute* (ETSI). After some time equipment vendors began to participate in standardisation activities. The merit of a global solution was seen by many other MNOs and vendors outside Europe who joined in and adopted GSM for their countries with the result that the first truly global mobile network was introduced. The success, rapid distribution, and rapid growth of the digital mobile networks demonstrate the importance and advantages of collaborative international standardisation [9–11].

2.1 3rd Generation Partnership Project

Motivated by the success of GSM, the successor standard, called 3G (also known as UMTS and WCDMA), was designed by a newly founded global standardisation initiative – the *3rd Generation Partnership Project* (3GPP) [2]. Members consisted of MNOs and vendors from all over the world and they continue to work and engage collaboratively today. Started in 1998, from 3G onwards, 3GPP defined and defines mobile networks, their functions, and network protocols. After 3G, 4G followed and 5G is being discussed today

as each generation evolves from the previous one. Over time, 3GPP took ownership of the GSM specifications from ETSI.

All the standards that are agreed and approved by 3GPP are automatically ratified by the officially recognised national or pan-national standardisation bodies. These are ETSI (*European Telecommunications Standards Institute*) [9] in Europe, the TTC (*Telecommunication Technology Committee*) [24] in Japan, and the ATIS (*Alliance for Telecommunications Industry Solutions*) [3] in the USA, for example. 3GPP is a partnership of standardisation bodies for telecommunications worldwide and it is in the powerful position of defining normative standards that are officially recognised in virtually all countries. National regulators accept that MNOs that operate in their countries deploy and operate technologies standardised by 3GPP, using certain frequencies and transmitting data by the techniques and transmission powers defined in the standards [2, 9, 10].

Participation in 3GPP is open to anybody in the mobile industry who is member of one of the standardisation bodies mentioned above. Equipment vendors, mobile device vendors and mobile operators jointly define the standards there. Regulators and other organisations or interest groups can also join and it is this aspect that is key to 3GPP's success. Since all the relevant stakeholders are involved, there is broad acceptance of the standards that are defined by 3GPP [2].

Work at 3GPP is contribution driven and every agreement is consensus-based. If an idea is to become part of a standard, it must be brought to 3GPP and members must be convinced and there must be enough support to get it accepted. If there is no objection, agreement and approval is achieved [2].

3GPP is organised in various *Technical Specification Groups* (TSG) dealing with network functions, network protocols, mobile devices, radio, voice coding/decoding, billing information, cryptographic aspects, authentication, and security. They are organised in subgroups, the so called *Working Groups* (WG) that share the work. Work is split in radio access network, core network terminals, and services and system aspects [2].

3GPP specifications are designed to allow any mobile device of any vendor to be used on any mobile network without any problems arising. It is 3GPP's objective to ensure this interoperability is achieved. Each mobile network generation, e.g. 3G, consists of a *release* that consists of a fairly large number of 3GPP *Technical Specifications* (TS). The releases are complete system specifications for mobile telecommunications. Releases are frozen and stable and are what vendors implement and MNOs deploy. 3GPP TSs are publicly accessible on the Internet from the 3GPP Web site [1]. The TSGs work on

several releases in parallel to evolve them continuously while defining future generations [2].

2.2 GSM Association

While GSM was initially specified, trials were run, and the first operational GSM networks launched in the 1980s and 1990s, all the MNOs that launched GSM, or were committed to do so, joined a special interest group which became the *GSM MoU Association* (GSMA). It all started by a memorandum of understanding between the co-founding countries France, Germany, Italy, and United Kingdom. Quickly, more countries joined and eventually in 1994 the GSMA was formally registered in Switzerland. At present there are approximately 800 member MNOs in the GSMA that operate in over 200 countries [11].

In the beginning, it was the founding members of the GSMA who owned the GSM specifications. Ownership was transferred to ETSI in 1989. The GSMA is not a standards development organisation – it is a trade association. Nonetheless, it has been and is involved in developing standards. ETSI, and later 3GPP, cover technical specifications of mobile network functions and related aspects (see Section 2.1) but they do not cover processes and procedures of any kind, nor do they cover international roaming related aspects. This is the domain of the GSMA.

GSMA is organised in various *Working Groups* (WG) [11] that each have a particular focus topic and area of expertise. WGs work on a range of topics from technical aspects, such as international signalling and data transmission between MNOs, through to international handling of billing records, security and fraud, to legal aspects, such as templates for roaming agreements and contracts between MNOs. The GSMA WGs create specifications which are not ratified by recognised standardisation bodies, but they are mandatory for all MNOs to adopt and observe, as they are subject to legal contracts and roaming agreements negotiated by and between MNOs. As a consequence, the effect of specifications produced by GSMA WGs can be comparable to 3GPP standards, although the mechanism by which they become relevant for the mobile industry is different.

Members of the GSMA are MNOs and vendors. They meet regularly to discuss and agree on the topics covered by the WGs. Like 3GPP, GSMA WGs are driven by contribution and agreements are consensus-based. Technical specifications of the GSMA WGs are also detailed enough to allow MNOs for reliable and robust international information exchange. The majority of GSMA standards are restricted to members but some are publicly available.

2.3 Security and Standards

As further elaborated upon in Section 3, there is the need for a comprehensive approach to security for it to be effective. All stakeholders involved in the mobile industry and all the network equipment, protocols, functions, applications, services, architectures, mobile devices, and procedures need to be defined and built with security in mind. To enable the mobile industry to do so, both the 3GPP and the GSMA have working groups that deal with security matters.

3GPP TSG SA WG3 (SA3) deals with all security matters related to the specifications created by the other 3GPP TSGs. SA3 specifies security architectures, protocols, and requirements and covers a broad range of security aspects, such as air interface encryption, authentication, cryptography, and secure data transmission between network equipment [2].

The GSMA's *Fraud and Security Group* (FASG) also deals with a broad range of security aspects. These are related to the activities of the GSMA WGs. Among other matters, FASG covers signalling security, secure configuration of network equipment, secure operation of mobile networks, international roaming security, and cryptography. FASG also writes specifications and guidelines that are there to help members to do security right.

The *Network Equipment Security Assurance Scheme* (NESAS) that is presented in this article is a joint activity of 3GPP TSG SA WG3 (SA3) and GSMA FASG. SA3 specifies security requirements and test cases for network equipment and FASG defines the processes and operational aspects of the scheme. These processes cover accreditation of stakeholders and how to perform network equipment security testing. More on all that is provided in Section 5 below. Due to the fact that this activity is driven by standards, NESAS has the potential to enjoy wide acceptance in the mobile industry once it is launched.

2.4 Other Standardisation Organisations

There are more standardisation organisations in the mobile industry that contribute and play their part in developing a unified global standard for mobile telecommunications. As these are not relevant for this article, they are out of scope but for the reader's benefit some of those other relevant organisations are as follows;

- NGMN Alliance, *Next Generation Mobile Networks*, MNO consortium active in pre-defining 5G, www.ngmn.org.

- OMA, *Open Mobile Alliance*, active in defining data formats for applications and mobile devices, www.openmobilealliance.org.
- GCF, *Global Certification Forum*, independent certification scheme for mobile devices, www.globalcertificationforum.org.
- ITU-T, *International Telecommunication Union – Telecommunication Standardisation Sector*, telecommunications standardisation organisation of the United Nations, www.itu.int/en/ITU-T/Pages/default.aspx.

3 Security Assurance

"Data security is the most significant domain supporting information reliability. If installed systems are inadequately protected, data may not be properly protected." [21] p. 29. In other words, data and system security are business critical for ICT organisations. A system that is exploited due to a vulnerability is no longer reliable. An insecure system can fail to process data correctly, can be manipulated to leak data to unauthorised destinations, and can be damaged. These incidents could have serious implications for the operators, such as the amount of effort and cost to repair or replace vulnerable systems, image and reputation damage, and unavailability of the service to the customer. It is in the interests of the operators to source secure systems, to configure them securely and to operate them securely in a secure environment.

In order to reach an adequate level of security, a variety of security controls must be applied. These consist of introducing and maintaining processes for secure design, development and deployment of ICT systems, secure network design, security testing, secure operation, secure change management, and regular reviews of the effectiveness of all these security controls. An interdisciplinary approach is required where knowledge in all the disciplines listed above and in security generally is required. Controls, such as security tests and compliance tests can objectively measure and reflect what level of security has been reached and how effective the other controls are. Eventually, the goal is to create a reliable ICT system and to achieve reliable service provision by applying effective security controls. Defining, applying, and reviewing all these controls can be described by the term **security assurance**. In brief, the controls are there to ensure the desired level of security can be reached and to measure the achieved level of security [4, 7, 8, 13, 15, 19–21, 23].

It is also common to review the effectiveness of security controls by using the help of an external auditor who reviews the defined processes, the extent of accuracy to which they are applied, and their actual effectiveness. A successful audit can be used for **accreditation** of an organisation to demonstrate that

certain security controls are applied and/or criteria have been met. If such an audit is performed by authorities who are awarded state recognition, the accreditation turns into a **certification**. A *Common Criteria for Information Technology Security Evaluation* [6] and an ISO 27000 family [17] certification are examples.

Security is a matter of attitude. If an organisation truly wants to build or operate systems or services securely, security controls must be implemented everywhere in the processes and in the systems/services. A corporate culture must exist that ensures that employees, whenever they do something, consider the security implications. Closely related to this is awareness. Employees must be aware of both the security controls that are to be applied and the potential security issues that can arise. Continuous education of staff on security matters is therefore essential.

Security assurance starts with defining a security policy. The organisation's security policy should define how security is treated within the organisation, in which processes and procedures it is involved, what kind of security controls should exist, and when and how these controls should be applied. Next, assets and their importance for the organisation are identified and defined. For instance, an asset can be information, software, a network service, or a product. For a particular asset, security requirements should be defined that reflect the organisation's security policy and tailor it to the asset for which security controls are to be defined.

Hardware, software and services of the ICT industry, which also includes the mobile industry, run through a *development life cycle* (DLC). This DLC may vary from organisation to organisation, but it typically starts with an idea, is followed by a feasibility study, and then design, development/ implementation, quality assurance testing, production, and shipping follow. In each of these stages of the DLC, security is to be dealt with in some way. The most effective security controls are those that are integrated into the DLC and built-in from the very beginning [12].

Once a product has been built as a result of applying the DLC, it enters the *product lifecycle* (PLC). The product lifecycle covers maintenance tasks, such as correcting errors, creating and distributing patches and updates, and preparing it to be dismantled when it has reached end-of-life. Again, there are security controls required which are complimentary to those that are relevant for the DLC. The vendor needs to apply these security controls. In addition, the built product is operated somewhere and the operator needs to configure and run it securely. This requires the operator to also apply security controls. These are different from the ones applied by the vendor.

Table 1 presents a non-exhaustive list of common security controls assigned to stages of the DLC and PLC, as well as responsible stakeholders.

For each of the security controls there is a need for an internal process. These processes must be derived from the security policy and must be tailored

Table 1 Security controls by stage of development and product lifecycles

Stage	Security Control	Responsible
Development Lifecycle (DLC)		
Design	• Security by design (architecture) • Identify assets and perform threat analysis • Define specific security requirements (derived from security policy, design, and threat analysis) • Define required security functionality	Vendor
Development/ Implementation	• Clear approach from requirements to lines of code • Secure coding • Input validation • Code review • Comprehensible build process • Automated code analysis • Correct implementation of security functionality, such as authentication, authorisation, encryption, secure communication • Apply access control (local users, via network, physical)	Vendor
Quality assurance testing	• Security testing • Penetration testing • Fuzzing	Vendor
Production	• Secure creation and distribution of secrets, cryptographic keys, and certificates • Secure configuration by default • Installation of genuine software/firmware releases	Vendor
Shipping	• Prove authenticity of the product	Vendor
Product Lifecycle (PLC)		
Configuration management	• Secure configuration by default	Vendor
Update/upgrade	• Fix errors without introducing new ones • Prove authenticity of the upgrade pack	Vendor
Patch & change management	• React quickly if errors or vulnerabilities are discovered, fix them, and distribute patches	Vendor
End-of-life procedures	• Provide procedures to securely dismantle the product (e.g. erasing all data)	Vendor

(*Continued*)

Table 1 Continued

Stage	Security Control	Responsible
Deployment and Operation		
Deployment	• Provide a secure environment for the product (e.g. secure network architecture, network segregation, firewalls at network edges) • Secure configuration • Define and test a backup strategy	Operator
	• Define and apply access control concept on all assets (physical, network, host, service, application)	Operator
Operation	• Monitor to identify anomalies and failures • Regularly run backups • Personnel security • Environmental controls (e.g. power supply, air conditioning, fire prevention/protection)	Operator
Change management	• Quickly test and install patches as soon as they are provided	Operator
Configuration management	• Comprehensible and documented changes • Keep achieved security level during and after changes	Operator
End-of-life procedures	• Ensure that all data is transferred to the new system and erased on the dismantled one	Operator

to the stages of the lifecycles and to the product classes that are built. Processes must be written down and communicated to staff. All staff need to be trained and need to follow the processes. All processes need to be validated for their effectiveness and be improved as needed on a regular basis.

The security controls can be grouped in two categories: (1) security functionality that is implemented explicitly to provide certain secure behaviour. Examples are authentication of users and machines, encryption of communications for confidentiality reasons and integrity validation of data; (2) defensive design and implementation to ensure that certain weaknesses and vulnerabilities are countered. These types of security control do not actually provide any additional functionality or behaviour and they are generally *invisible*. Nonetheless, both types of control are equally important for real and comprehensive security. In fact, most of the security controls that are integrated in the DLC and the PLC are of type (2) [13].

Security assurance is not just about defining and applying processes and procedures. Assurance means that there is a kind of certainty that there is real security in place. This requires verification. Consequently, testing becomes an important and relevant part of security assurance. Only if tests verify that certain vulnerabilities or weaknesses do not exist, and that security functionality works as specified, can security assurance be attained. Therefore, security testing should receive thorough attention and dedication to its performance. Typical quality assurance testing is complimentary to security testing. Where quality assurance tests verify if the system behaves as specified, security tests verify the absence of certain behaviour, functionality, and vulnerabilities. Compliance testing verifies if the security requirements are met. Security testing and compliance testing are best automated as much as possible. This allows tests to be repeated during development as often as intended to see if the system improves. The tests can also be executed regularly during operation to see if the system has changed. The latter testing approach is particularly of interest after the system under operation is upgraded or otherwise modified. In that respect, test driven development is a useful approach. When the security requirements are collected, and when the security criteria for the design are defined, the developers should immediately assign test cases to verify if all the requirements are met by the developed system. Full coverage of security requirements can be reached for the requirements in that way. If a requirement cannot be broken down into test cases, it is necessary to think of redefining the requirement.

4 Security Assurance for Mobile Networks

Transforming what is described in Section 3 to the mobile industry means that if installed systems are inadequately protected, reliable provision of mobile voice and data services to customers cannot be assured. A network equipment vendor applies the security controls described in Section 3 during the development lifecycle of the network equipment, as well as during the product lifecycle of the developed network equipment. The MNO applies the security controls on the network implementation, the deployment plan for the network equipment, and its operation (see Section 1.4.6). Effective security is only achieved if all the involved stakeholders cover all the stages in the lifecycles of the asset that is to be protected. For the vendor, the asset is the network equipment. For the mobile operator the asset is the mobile network and the services that are offered thereon.

Due to national regulation, MNOs in many countries are, or will be, held accountable by law and/or regulation for running a reliable and robust mobile network (see Section 1.4.3). However, MNOs can only apply security controls during operation. They rely on secure network equipment being provided by their vendors from the outset (see Section 1.4.6). For MNOs it is important to measure the achieved level of security of network equipment. The following approaches are particularly suitable to achieve this:

- Accreditation of the security related development and product lifecycle processes of a vendor;
- Security evaluation of network equipment by a competent test laboratory with defined and standardised security tests.

The vendor defines its own internal processes that describe how security is integrated into the design, development, implementation, and maintenance processes. An external auditor examines these processes and determines if they are actually applied in practice. If the auditor is satisfied, the vendor will be accredited. The accreditation demonstrates to the outside world that the vendor is capable of creating secure products. While undergoing the accreditation, the vendor does not have to reveal details about their internal processes to the public. Only the auditor sees them. This way, a qualified and recognised auditor can increase trustworthiness of a vendor without the vendor having to reveal internal secrets to the public. A MNO can choose to only purchase network equipment from a successfully accredited vendor to increase confidence in network equipment security.

The second pillar is security evaluation of network equipment. If there is a pre-defined set of security tests for network equipment, and if all network equipment is tested against these requirements, the achieved level of security can be objectively measured and visualised. That way, new network equipment, as well as upgraded network equipment, can be evaluated. If these tests are outsourced to a recognised and competent test laboratory, a high quality of testing can be assured. If in addition evaluation reports are made available to potential customers, efficiencies can be achieved as tests are performed once and are not repeated by each stakeholder individually.

The fact that network functions are standardised in the mobile industry (see Section 2) is beneficial for security evaluation of network equipment by way of testing. The standards clearly define the functionality and capabilities of network functions. These network functions are implemented by equipment vendors and sold as network equipment. As the functional range of network equipment is clear, dedicated security requirements and test cases can be

defined and standardised for all defined network functions. It is then easy to ensure that all network equipment is tested against these test cases, which will ensure that tests are comparable and as complete as the test cases are.

Both approaches – accreditation and evaluation by testing – significantly help the MNO to determine the achieved level of security of a network product. The MNO is well positioned to select its vendors according to its security requirements.

NESAS is a security assurance scheme that follows these approaches and is described below.

5 Network Equipment Security Assurance Scheme (NESAS)

The *Network Equipment Security Assurance Scheme* (NESAS) that is jointly defined by 3GPP and GSMA, and operated and maintained by GSMA, is a voluntary network equipment security assurance scheme defined for the mobile industry. It provides a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed according to standard guidelines.

In brief, NESAS defines the following approach:

- Vendors define and apply secure design, development, implementation, and product maintenance processes;
- Vendors demonstrate these processes to external auditors;
- Level of security of network equipment is tested and documented;
- Tests are conducted by competent test laboratories against 3GPP SA3 defined security requirements;
- Documentation is forwarded to operators together with network equipment.

Therefore, NESAS follows the approach outlined in Section 4, making the achieved level of security of network equipment measurable and visible. NESAS consists of both technical aspects, expressed by equipment tests, and organisational aspects, defined by processes.

5.1 NESAS High Level Overview

The GSMA defines all the processes pertaining to NESAS, which cover accreditation of the vendor development and product lifecycle processes, test laboratory accreditation, and security evaluation of network equipment.

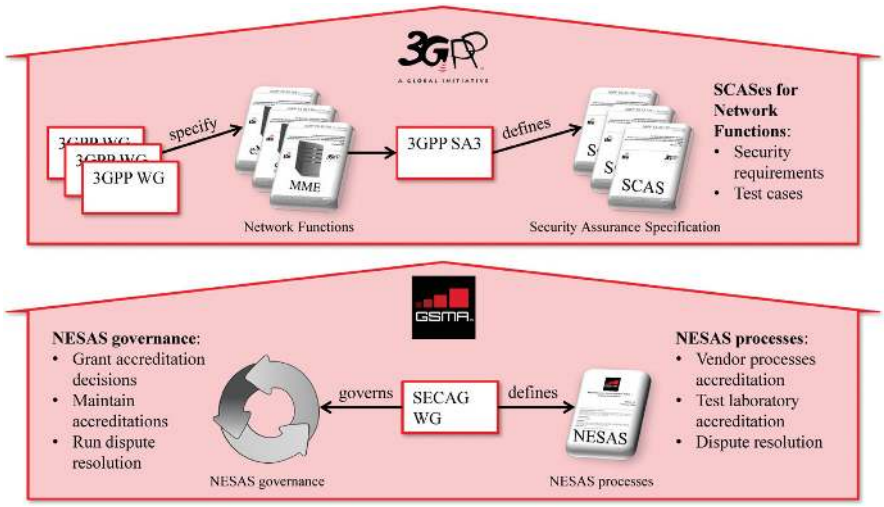

Figure 2 Roles of 3GPP and GSMA in NESAS.

3GPP defines security requirements and test cases per network function (see Section 2.3) – specified in the so-called *Security Assurance Specification* (SCAS). The GSMA also defines a dispute resolution process and governs the overall scheme. All this together builds what is known as NESAS. Figure 2 illustrates the roles of 3GPP and GSMA in NESAS.

Network equipment that is produced and sold by an Equipment Vendor is called *Network Product* in NESAS. A mobile base station from a particular vendor is an example of a Network Product.

Figure 3 illustrates the high level overview of NESAS.

The GSMA appoints an Audit Company that accredits the Equipment Vendor. The Equipment Vendor builds the Network Product which is given to a Test Laboratory for evaluation. The Test Laboratory is accredited by an 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 produces an Evaluation Report containing the results. The Network Product can then be shipped to a MNO, together with the Evaluation Report.

5.2 Accreditation of Vendor Processes

The Equipment Vendor defines its own processes for the Network Product development lifecycle and the Network Product lifecycle. These processes also define how security is integrated in all the stages of both processes.

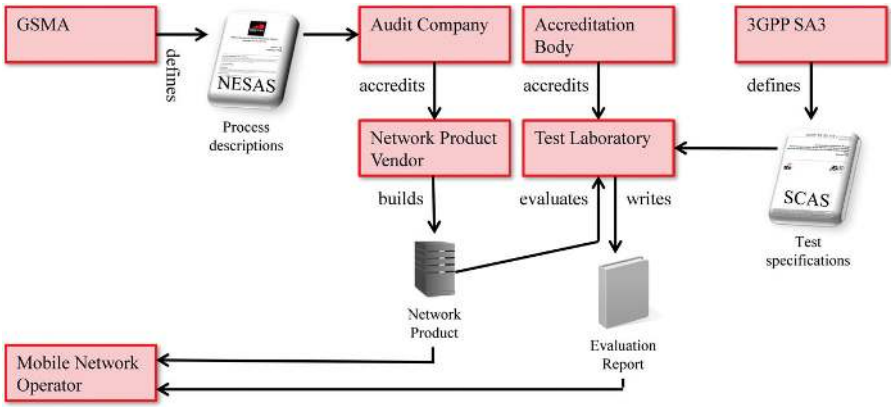

Figure 3 NESAS high level overview.

The processes are accredited by the GSMA appointed Audit Company. Figure 4 illustrates this. NESAS describes how accreditation is to be performed and which requirements are to be fulfilled by the vendor defined processes. Accreditation consists of both process documentation review and on-site audit.

The vendor defined processes need to ensure that, for the Network Products to achieve security levels, requirements are defined and design and implementation of the Network Product follows these requirements in a comprehensible way. This is what the Audit Company confirms in the course of successful accreditation.

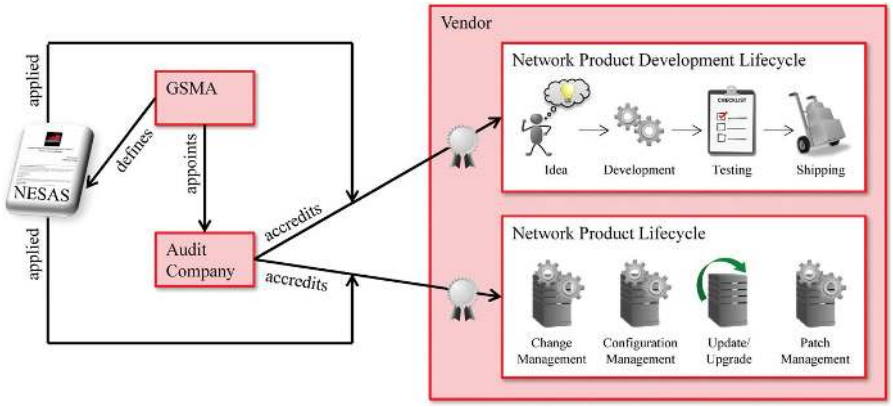

Figure 4 Accreditation of vendor processes.

5.3 Accreditation of Test Laboratories

Test Laboratories can either be owned by the vendor or be external. In any case, they need to undergo ISO 17025 [16] accreditation. ISO 17025 covers general requirements on testing procedures, documentation, maintenance and review of procedures, competence, independence, and impartiality. As ISO 17025 is generic, Test Laboratories are always accredited in the context of additional standards from the field in which the laboratories will perform their tests. For NESAS, this means that Test Laboratories need to demonstrate during accreditation that they are capable of performing tests described in SCASes and that they meet the additional requirements applicable to NESAS.

An officially recognised ISO 17025 Accreditation Body performs an audit upon request by the Test Laboratory. As illustrated in Figure 5, the Test Laboratory is audited against ISO 17025 in the context of NESAS and SCASes. A Subject Matter Expert performs the audit in collaboration with the Accreditation Body, as it is this Subject Matter Expert who brings the required expertise in the field of network equipment security to the audit. Once the audit is conducted successfully and the requirements have been satisfied, the Test Laboratory is accredited.

5.4 Network Equipment Evaluation

After both the vendor and the Test Laboratory are accredited, Network Products can be evaluated. This is done as depicted in Figure 6.

After the Network Product is built by the Equipment Vendor, it is provided to the Test Laboratory. The Test Laboratory takes the test specifications from

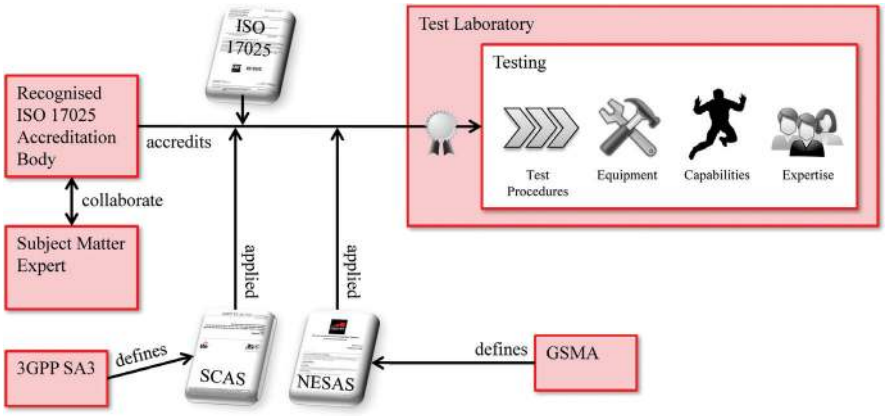

Figure 5 Accreditation of test laboratories.

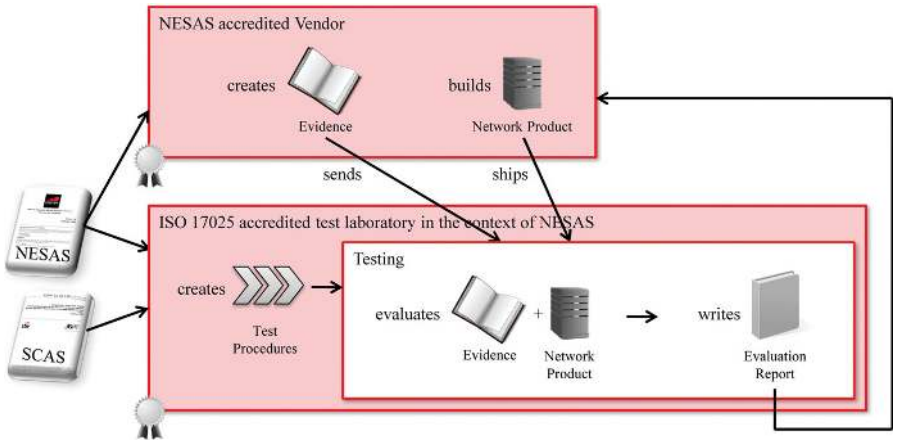

Figure 6 Evaluation of a network product.

the corresponding SCASes, derives detailed test cases from them, and tests the Network Product. Results of the tests are recorded in an Evaluation Report.

In addition, the Equipment Vendor creates the so-called *Evidence* that contains a rationale that allows the Test Laboratory to assess and comprehend if the vendor is following its own accredited internal processes when building the Network Product. Additionally, the results of Evidence evaluation are added to the Evaluation Report. It is the Evidence evaluation that links the tested Network Product to the accredited vendor processes and this is why only an Evaluation Report that contains both results – from Network Product evaluation and from Evidence evaluation – is meaningful to a MNO.

The completed Evaluation Report is handed over to the Equipment Vendor. The Equipment Vendor can then provide the Evaluation Report to any interested MNO together with the Network Product.

It is at the discretion of the MNO to determine from the Evaluation Report if the level of security that is reached by the Network Product is sufficient for deployment in the mobile network. The Evaluation Report contains the information that makes Network Product security and security of the corresponding development lifecycle measurable and visible to the MNO.

5.5 Benefits of NESAS for the Mobile Industry

NESAS brings a multitude of benefits for various stakeholders in the mobile industry.

The level of security assurance and as such the level of security achieved by network equipment, is measurable, visible, comparable and understood. MNOs benefit significantly as this introduces transparency that helps MNOs to determine if the network equipment of a vendor meets the security requirements of the MNO. For vendors, this provides a platform to highlight the vendor's ability to achieve/maintain good security levels.

Vendors demonstrate commitment to secure development and maintenance processes. This is beneficial for MNOs, since it increases trust in the vendor and confidence for MNOs when engaged in vendor selection decision making. In return, it encourages and rewards vendors to reinforce security in their products and engenders a security-by-design culture across the entire vendor community.

Evaluation of network equipment conducted by competent accredited Test Laboratories allows MNOs determine the level of security of network equipment even before it is deployed anywhere. Furthermore, it reduces the security testing burden on MNOs.

NESAS ensures a baseline security level and a common set of security requirements for all customers and markets. MNOs can remain free to set their individual security requirements on top of NESAS. Both vendors and MNOs benefit from the reduced set of requirements, as requests for quotation processes and contract negotiations require less security requirements to be listed, considered and agreed. This is significantly beneficial for Equipment Vendors as the overhead of dealing and responding to different security requirements coming from various stakeholders (see Section 1.4.6) is reduced.

As soon as the baseline security level that is delivered by NESAS is built-in, overall costs for network equipment are shared by vendors and across all operators as this security level becomes standard for the products. The need for individual functionality that is to be implemented for individual MNOs is reduced.

With NESAS, a single audit replaces the need to host and fund audits from individual operators and regulators. This saves costs and overhead on the vendor side, which may also be reflected in Network Product prices.

One of the goals and intentions of industry is to demonstrate to regulators the value of NESAS. If considerate can be shown that NESAS security requirements are commensurate with national security requirements national authorities are likely to endorse NESAS as a legal requirement for the regulation of mobile networks without having additional requirements. This is significantly beneficial for Equipment Vendors, since the overhead of dealing

with and having to satisfy different security requirements coming from various regulators worldwide is reduced. In fact, the needs of regulators are one of the key drivers for the mobile industry to develop a tailored security assurance scheme.

NESAS reuses effective and mature accreditation models which deliver security gains and improvements whilst keeping work and costs for all stakeholders at manageable levels.

5.6 Status of NESAS Development and Outlook

The processes and documents pertaining to NESAS have almost reached pilot stage. In 2016 a pilot will be conducted to learn and assess in practice how the scheme works. NESAS is designed to be improved iteratively. All the lessons learnt from the pilot will be considered and reflected in the initial official release of NESAS, which is planned for 2017. Thereafter, updated releases will be issued regularly that will take the feedback of the industry into account. This facilitates and encourages stakeholders to get involved in order to help develop the scheme in a way that it satisfies their needs and that accredited vendors and more secure network equipment benefit their business.

If it is determined necessary in the future, the scope of NESAS can be extended and additional security requirements can be added to existing SCASes. New network equipment types can be added to the scheme by producing and approving new corresponding SCASes. Additionally, vendor process accreditation and test laboratory accreditation can be extended by adding/modifying requirements as considered necessary.

List of Abbreviations

3GPP	3rd Generation Partnership Project
CC	Common Criteria
CIS	Center for Internet Security
DLC	Development Lifecycle
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
ICT	Information and Communication Technology
ISO	International Organisation for Standardisation
IT	Information Technology
LTE	Long Term Evolution

MNO	Mobile Network Operator
NESAS	Network Equipment Security Assurance Scheme
PLC	Product Lifecycle
SAS	Security Accreditation Scheme
SCAS	Security Assurance Specification
SAS	Security Assurance Scheme
SIM	Subscriber Identity Module
TTC	Telecommunication Technology Committee
TS	Technical Specification
TSG	Technical Specification Group
UMTS	Universal Mobile Telecommunications System
WCDMA	Wideband Code Division Multiple Access
WG	Working Group

Acknowledgements

My gratitude goes to all active members of 3GPP SA3 and GSMA FASG who participate in creating NESAS. Their valued contributions are part of what we defined so far as NESAS. Their dedication is key to the scheme's success. In particular I want to particularly thank James Moran from the GSM Association who supported me significantly in producing promotion material and this article.

References

[1] 3GPP Specifications. *3rd Generation Partnership Program (3GPP)*, [online]. Available at: www.3gpp.org/ftp/specs/

[2] 3rd Generation Partnership Program (3GPP), [online]. Available at: www.3gpp.org

[3] Alliance for Telecommunications Industry Solutions (ATIS), [online]. Available at: www.atis.org

[4] Schneier, B. (2004). *Secrets & Lies – Digital Security in a Networked World*. Hoboken, NJ: Wiley Publishing Inc.

[5] CIS Security Benchmarks. *Center for Internet Security (CIS)*, [online]. Available at: benchmarks.cisecurity.org/

[6] Common Criteria for Information Technology Security Evaluation (CC), [online]. Available at: www.commoncriteriaportal.org

[7] Gollmann, D. (2005). *Computer Security*, 2nd ed. Hoboken, NJ: John Wiley & Sons Ltd.

[8] E. A. Roback. (2000). *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, 800–823. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication [online]. Available at: csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf

[9] European Telecommunications Standards Institute (ETSI), [online]. Available at: www.etsi.org

[10] Hillebrand, F. (ed.). (2013). *The Creation of Standards for Global Mobile Communication*, [online]. Available at: www.etsi.org/images/files/news/CreationOfStandardsForGlobalMobileCommunication.epub.

[11] GSM Association (GSMA), [online]. Available at: www.gsma.com

[12] McGraw, G. *How to develop security the secure, Gary McGraw way, Internet Blog on SearchSecurity* [online]. Available at: search security. techtarget.com/opinion/Gary-McGraw-on-software-security-assurance-Build-it-in-build-it-right

[13] McGraw, G. (2006). *Software security – building security*. Boston: Addison-Wesley.

[14] Government of India, Ministry of Communications and IT, Department of Telecommunications, Security Certification of Telecom Equipment within India, New Delhi, India, letter, 31 July 2015 [online]. Available at: www.dot.gov.in/sites/default/files/u10/Letter%20related%20to%20extension%20of%20Security%20Certification%20Time%20(1)_3.pdf

[15] Hamidovic, H. (2012). Fundamental concepts of IT security assurance, Vol. 2, ISACA [online]. Available at: www.isaca.org/Journal/archives/2012/Volume-2/Documents/12v2-Fundamental-Concepts.pdf

[16] International Organisation for Standardisation ISO/IEC 17025:2005. *General requirements for the competence of testing and calibration laboratories* [online]. Available at: www.iso.org/iso/catalogue_detail.htm?csnumber=39883.

[17] International Organisation for Standardisation ISO/IEC 27000:2014. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, [online]. Available at: www.iso.org/iso/catalogue_detail?csnumber=63411

[18] Sauter, M. (2010). *From GSM to LTE: an introduction to mobile networks and mobile broadband*. Hoboken, NJ: John Wiley & Sons.

[19] Making Security Measurable, Software Assurance, mitre.org, October 2013 [online]. Available at: measurablesecurity.mitre.org/directory/areas/softwareassurance.html.

[20] Shirey, R. (2007). *Internet Security Glossary, Version 2, RFC 4949, IETF* [online]. Available at: www.ietf.org/rfc/rfc4949.txt

[21] Davis, R. E. (2009). *Ensuring Information Assets Protection, lulu.com* [online]. Available at: books.google.de/books?id=yCtXPh5rwdoC&
[22] Security Assurance Scheme (SAS). *GSMA Association* [online]. Available at: www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[23] Software Security Assurance (Wikipedia). (2015). Version from 13 January 2015 [online]. Available at: en.wikipedia.org/wiki/Software_security_assurance
[24] Telecommunication Technology Committee (TTC) [online]. Available at: www.ttc.or.jp

Biographies

S. Lachmund received his degree in computer science from the University of Applied Sciences Munich, Germany. Thereafter he got his Ph.D. from the Technical University Munich, Germany while working in parallel with the European research laboratory of the Japanese mobile network operator NTT docomo in Munich. In 2011 he joined Deutsche Telekom in their headquarters in Bonn, Germany. Within the last 15 years, Sven Lachmund gained broad and deep expertise in ICT security, network security, and telecommunication security. He developed several security solutions and security architectures, filed patents, and published on some of his achievements. His current job is to support the engineering departments with his security expertise while they introduce new technologies on the mobile network. He accompanies them through all the stages of the introduction process. Sven is involved in requests for quotation, in design, and he appoints security tests before the technology goes live. Since 2014, when the work on NESAS started, Sven Lachmund is chairman of the Working Group at the GSMA that creates the security assurance scheme for network equipment.