BTG Webinar

‘Secure safety of ICT networks through certification’

October 14th 2020

Program

16.00 uur	Opening and welcome by Peter Rake and Petra Claessen
16.05 uur	Explanation Network Equipment Security Assurance Scheme (NESAS) by Jon France, GSMA
16.20 uur	Advantages of certification for providers by Jaap Meijer, Huawei
16.25 uur	Observations on Safety of ICT infrastructure by Jacob Groote, KPN
16.30 uur	Statements in relation to certification by Joris den Bruinen, The Hague Security Delta
16.40 uur	Discussion with attendees and panel based on questions and statements
16.55 uur	Conclusions, next steps
17.00 uur	Agenda new webinars BTG and closing

Petra Claessen
CEO BTG/TGG

BTG theme 2020 “Intelligent Connectivity”

Events & Meetings

Networking
Representation of interests
Knowledge gaining & sharing
Experience sharing and gaining
Expertgroups
Peergroups
Articles with opinion
Awards

Members & Partners

Demand-driven
Solution of marketimperfections
Supporting
&
collaboration
Content partners
Strategy partners
Educational partners

Collaboration & Representation

Co-creation
Strategic and structural collaboration
&
dialogue with EZK, ACM, INTUG, GSMA, UN, ITU, I-POORT,
Agentschap Telecom
(knowledge)partners,
Other associations

Knowledge institute & Sourcing

Promotion and keeping up knowledge and expertise
Accreditation of curricula
Certification (diploma)
Standards
Sourcing i.r.t. market

Added value & products/services

Content driven products/services for members/partners.
Strategic advise/support.
Innovation

5G

Smart Society

Artificial Intelligence

Data Analytics Science

Indoor coverage

Internet of Things

Cyber Security
Black Listing
GDPR

Tenders

Circular economy

Mission Critical
& Business Critical

Purchase advantage/ Hardware/ Software/Expense mgmt/RFP Advise

Program

16.00 uur	Opening and welcome by Peter Rake and Petra Claessen
16.05 uur	Explanation Network Equipment Security Assurance Scheme (NESAS) by Jon France, GSMA
16.20 uur	Advantages of certification for providers by Jaap Meijer, Huawei
16.25 uur	Observations on Safety of ICT infrastructure by Jacob Groote, KPN
16.30 uur	Statements in relation to certification by Joris den Bruinen, The Hague Security Delta
16.40 uur	Discussion with attendees and panel based on questions and statements
16.55 uur	Conclusions, next steps
17.00 uur	Agenda new webinars BTG and closing

Jon France
GSMA

BTG TGG

Jaap Meijer
Huawei

NESAS Tailored for Telecom, Benefits for Telecom Vendors

Date: 2020.10.14

Jaap Meijer
Cyber Security Officer
Jaap.Meijer@Huawei.com

Security Level:

Benefits of GSMA/3GPP NESAS

NESAS is jointly defined by 3GPP and GSMA. Scheme defined for the mobile industry to provide a security baseline and comprehensive security audit to evidence that network equipment satisfies security requirements and that network equipment vendors comply with security standards during their product development and lifecycle processes.

Specific advantages to vendors

- NESAS comprehensively analyzes telecom equipment threats and adds threat points and cases about, for example, air interfaces, 3GPP protocols and web security, that are not covered by other schemes. - Tailored for Telecom.
- It is a universal standard through which the level of security, achieved by telecom equipment, is measurable, visible, comparable.
- Reduces the fragmented needs for telecom equipment accreditation and reduces the cost in security accreditation in the long term. -> Fewer individual audits.
- Compared with Common Criteria, NESAS is characterized by a shorter turnaround time and lower cost.
- Uniform/Harmonized approach to security certification in Europe once adopted by the EU Cyber Security Act.
- Demonstrates commitment to security and reduces risks for customers.
- Provides accreditation delivers a world-class security review of products and security related processes.
- High recognition in the industry (regulators, carriers, auditors/labs, vendors).
- Avoids fragmented and potentially conflicting security assurance requirements in different markets.
- Increases the predictability of product usage
- Provides for a transparent level playing field for all suppliers

Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI

Jacob Groote
KPN

Joris den Bruinen
The Hague Security Delta

Statement 1

As far as I am concerned, innovations based on technological developments should be given free, for the benefit of our economic prosperity, but must comply with cyber security. See also the recent research by Rathenau Instituut and the advice of the Cyber Security Council. Requirements will have to be made to do this. We must also avoid unnecessary costly corrections in large-scale digital infrastructures. We must therefore be able to estimate in advance which potential problems with new technologies and suppliers may arise. Matters such as (European) standards, supervision and certification, as well as standardization, must be in line with this. While work has already been done in these areas, there is still much to be gained.

Statement 2

BTG and HSD triple helix partners also work together on a European level. Moreover, we note with positive appreciation that the Ministry of Economic Affairs is taking a proactive role towards the EU with regard to IoT and telecom standards and certifications, among other things. By forming targeted international coalitions of like-minded European countries around specific new technologies, the Netherlands can stimulate its technological and industrial capabilities more widely. Instruments that can promote this development (such as standardization, standardization and certification) must be used for this purpose. Objective and verifiable criteria and audits are of great importance here. In short, don't just believe in blue eyes, but ensure a level playing field, which is ultimately of economic importance.

Statement 3

I note that the demand for assurance about information, IT / OT and cybersecurity is still increasing and I expect mandatory certification to start with a low accountability level, for example based on self-assessment. This will eventually grow towards a greater accountability requirement and require that the effect of measures be accounted for (demonstrably) independently to the regulators and other stakeholders. As far as I am concerned, this growing up should take place asap. A voluntary test based on a certification scheme is not sufficient in my opinion. If I understand correctly, the NESAS model consists of two phases. From first self-test on a voluntary basis. But fortunately followed by the 2nd phase with an independent external audit and a technical lab investigation. Trust is good checking is better. And this includes a technical assessment and not only via a process check list audit. Above all, I believe in the role of regulators and in this case the Telecom Agency. Fortunately, it is also taking on an increasingly proactive role in cyber resilience.

Statement 4

The yardstick used for this should be in line with existing standards for information security, such as the ISO27001 guideline and the NIST Cybersecurity Framework. In addition, it will have to be in line as much as possible with the Network and Information Systems Security Act (Wbni) from 2018, which states that providers must take "appropriate and proportionate technical and organizational measures" to protect stored or processed data. In addition, also the previously adopted European Cybersecurity Act, which already provides for a Cybersecurity Certificates Framework for digital products and services. Incl certification and European quality mark. It is desirable, even more necessary, to arrange it at a European level with as much alignment as possible with the global frameworks.

Statement 5

I start my last point with a statement I came across from Martin Vliem of Microsoft: “There are many methods for testing reliability, but it is quite complex. There is a forest of certifications, legal constructions, laws and regulations. Large companies still have the knowledge and manpower to find out, but that is not easy for SMEs. It is therefore important that we work with the Online Trust Coalition, among others, on more consensus about the methods and make them simpler, clearer and more accessible. ” The better, based on broad consensus, the more effective and the simpler the more efficient. The overall objective of NESAS is to provide a security assurance framework and security baseline to facilitate improvements in security levels across the whole mobile industry. To achieve this, NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as security test cases for the security evaluation of network equipment. This seems to me to be a good objective of NESAS and therefore I suspect that it can form the basis of the confidence to work towards a European framework and certification scheme.

Next BTG Knowledge Café:
12 november 2020 ‘Van duur naar duurzaam’
i.s.m. partners Forza Refurbished en CHG Meridian

BTG TGG

Thanks for your attendance and contribution!