Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cyber security cOmpeteNCe fOr Research anD InnovAtion[†]

Work package 5: Exploitation, dissemination, certification and standardization

Report on Cybersecurity Certification, the schemes under development and the related challenges

Abstract: This document describes the results of discussions carried out within the Certification Group of the CONCORDIA project. The purpose of the document is to provide an introduction to basic cybersecurity certification terms and standards, to present the certification schemes currently in process and to enumerate some of the related challenges.

Contractual date of delivery	*31/03/2023*
Deliverable dissemination level	*Public*
Contributors	*Argyro Chatzopoulou (TÜV TRUST IT)* *Hendrik Dettmer (TÜV TRUST IT)* *Daniel Schnetzke (TÜV TRUST IT)* *Kostas Lampropoulos (University of Patras)* *Luis Barriga (Ericsson)* *Shahid Raza (RISE)* *Felicia Cutas (EIT Digital)* *Roland Atoui (Red Alert Labs - A4CEF project)* *Spyros Papastergiou (CYRENE project)*

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
ADS	Airbus Defence and Space GmbH (as a replacement for Airbus Protect GmbH)	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF BV	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as a replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~

NCSA	Ministry of Digital Governance - National Cyber Security Authority	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia
ICENT	Innovation Centre Nikola Tesla	Croatia
Utilis	Utilis d.o.o	Croatia
Polito	Politecnico di Torino	Italy

Contents

1. Introduction to Conformity Assessment 5
1.1. Terms and definitions 5
1.2. Conformity Assessment techniques 7
1.3. Relationship between Conformity Assessment techniques 8
2. Conformity Assessment within the EU CSA 9
2.1. Existing Cybersecurity Certification schemes 10
2.1.1. EUCC 10
2.1.2. EUCS 10
2.1.3. EU5G 11
3. Cybersecurity Certification challenges 11
3.1. Regarding the EUCC: 11
3.2. Regarding the EU5G: 13
3.3. Regarding the EUCS: 16

1. Introduction to Conformity Assessment

The process of conformity assessment demonstrates whether a product, service, process, claim, system or person meets the relevant requirements. Such requirements are stated in standards, regulations, contracts, programmes, or other normative documents[1].
The purpose of Conformity Assessment lies close to the need of an interested party to gain assurance that a product, service, process, claim, system or person that will be used for a specific purpose, fulfill the relevant proclaimed and necessary requirements.
The European Cybersecurity Act (EU CSA)[2], introduces a *framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.*
As stated in Article 46 of the EU CSA, the European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the **ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements** for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.
In simple terms, the EU CSA introduces conformity assessment for ICT products, ICT services and ICT processes, in order to provide information to the interested parties of the degree they fulfil specified security requirements.

1.1. Terms and definitions

The following table, includes the basic definitions related to the subject of conformity assessment in general and for cybersecurity specifically, as stipulated by the EU CSA.

Table 1: Conformity Assessment related terms and definitions

Term	Short Description[3]
Product	result of a process Note 1 to entry: Four generic product categories are noted in ISO 9000:2005: — services (e.g. transport); — software (e.g. computer program, dictionary); — hardware (e.g. engine, mechanical part); — processed materials (e.g. lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. Note 2 to entry: Products include results of natural processes, such as growth of plants and formation of other natural resources. Note 3 to entry: Adapted from ISO/IEC 17000:2004, definition 3.3.

[1] https://www.iso.org/conformity-assessment.html
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN#d1e40-15-1
[3] The relevant descriptions have been obtained from the applicable ISO 170xx standards as also described within the ISO CASCO website. https://casco.iso.org/techniques-and-schemes.html

Term	Short Description[3]
	ISO/IEC 17020:2012(en), 3.2.
ICT product	an element or a group of elements of a network or information system [EU CSA]
Service	output of a service provider with at least one activity necessarily performed between the service provider and the customer Note 1 to entry: The dominant elements of a service are generally intangible. Note 2 to entry: Service often involves activities at the interface with the customer to establish customer requirements as well as upon delivery of the service and can involve a continuing relationship, such as services provided by banks, accountancies or public organizations, e.g. schools or hospitals. Note 3 to entry: Provision of a service can involve, for example, the following: — an activity performed on a customer-supplied tangible product (e.g. a car to be repaired); — an activity performed on a customer-supplied intangible product (e.g. the income statement needed to prepare a tax return); — the delivery of an intangible product (e.g. the delivery of information in the context of knowledge transmission); — the creation of ambience for the customer (e.g. in hotels and restaurants). Note 4 to entry: A service is generally experienced by the customer. [ISO/IEC TR 17028:2017]
ICT Services	a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems [EU CSA]
Process	set of interrelated or interacting activities which transforms inputs into outputs [ISO/IEC 17021:2012]
ICT Process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service [EU CSA]
Claim	information declared by the client Note 1 to entry: The claim is the object of conformity assessment by validation /verification. Note 2 to entry: The claim can represent a situation at a point in time or could cover a period of time. Note 3 to entry: The claim should be clearly identifiable and capable of consistent evaluation or measurement against specified requirements by a validation body /verification body. Note 4 to entry: The claim can be provided in the form of a report, a statement, a declaration, a project plan, or consolidated data. [ISO/IEC 17029:2019]
declaration of conformity; (manufacturer's) declaration of conformance	a statement by a supplier claiming under his sole responsibility that an IUT (Implementation Under Test) is in conformity with a specific standard or other normative document. Note 1 to entry: 1 — Compare with attestation of conformity and certification of conformity. 2 — The term "self certification" should not be used, in order to avoid any confusion with the concept of certification which should imply the involvement of a third party. [ISO 10303-31:1994]
Implementation Under Test (IUT)	that part, of a product which is to be studied under testing, which should be an implementation of one or more characteristics of the standard(s) based on a given implementation method. [ISO 10303-31:1994]
System	set of interrelated or interacting elements [ISO 9000:2015]
Management System	set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives Note 1 to entry: A management system can address a single discipline or several disciplines e.g. quality management, financial management or environmental management.

Term	Short Description[3]
	Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes, etc.to achieve those objectives. Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations. [ISO 9000:2015]
Person	any entity which is a natural or legal person [ISO/IEC 23126:2021]

1.2. Conformity Assessment techniques

In order to provide this assurance, different conformity assessment techniques are used. Examples of assessment techniques include assessment (as used within accreditation and peer assessment), auditing, evaluation, examination, inspection and testing.
The following table, includes the basic definitions related to conformity assessment techniques.

Table 2: Conformity Assessment techniques related terms and definitions

Term	Short Description[4]
Assessment	Assessment applies to the process of determining whether an organisation fulfils requirements related to its technical competence. [ISO/IEC 17011:2017, ISO/IEC 17040:2005]
Auditing	An audit is a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Audit criteria are contained in policies, procedures and requirements adopted by an organization and may include applicable laws and regulations, policies, procedures, standards, management system requirements, contractual requirements or industry/business sector codes of conduct. Audit criteria are used as a reference against which conformity is determined. [ISO/IEC 17021-1:2015, ISO 19011:2018]
Evaluation	Evaluation is the process of gathering evidence about whether an object of conformity, such as a product, process or service, meets specified requirements. It is also sometimes used in the context of person certification.
Examination	Examination is one of the terms used almost interchangeably to cover a number of techniques, but it is used in a more specific way when referring to methods for certifying the competence of a person. In this context, examination is defined as a mechanism that measures a candidate's competence by one or more means, such as written, oral, practical and observational, as defined in the certification scheme. Examinations need to be planned and structured in a manner which ensures that all specified requirements are objectively and systematically verified, with sufficient documented evidence produced to confirm the competence of the candidate. [ISO 19011:2018]
Inspection	One of the key aspects of inspection is that the determination of conformity with specific requirements is made on the basis of professional judgment of the inspection bodies' personnel. Inspection as a conformity assessment technique can include: • visual examination of physical items; • measurement or testing of physical items; • examination of specification documents such as design drawings;

[4] The relevant descriptions have been obtained from the applicable ISO 170xx standards as also described within the ISO CASCO website. https://casco.iso.org/techniques-and-schemes.html

Term	Short Description[4]
	• comparison of the findings with the requirements of specification documents or with generally accepted good practice in the field; and • drawing up a report on the results of the inspection. [ISO/IEC 17020:2012]
Testing	Testing is defined as the determination of one or more characteristics of an object of conformity assessment, according to a procedure. A procedure is defined as a specified way to carry out an activity or a process. Testing typically applies to materials, products or processes. In the case of testing used for conformity assessment, the characteristics will be included in the 'specified requirements' which form the focus of the testing. [ISO/IEC 17025:2017]

1.3. Relationship between Conformity Assessment techniques

To better depict the relationship between the different conformity assessment techniques and the possible objects and purposes, the following cases (examples) are provided.

- an organization that implements an Information Security Management System can be independently audited against the requirements of ISO/IEC 27001:2022. If the result of the audit is positive and following a Certification's Body processes as prescribed by ISO 17021 and ISO 27006, a certificate may be issued. In this case, the Information Security Management System of the organization (meaning the set of interrelated or interacting elements of the organization to establish information security policies and information security objectives and processes to achieve those objectives) has been certified. The certificate only indicates that the way the organization manages information security fulfils the requirements of ISO/IEC 27001. The certificate does not extend to products or services provided by the organization.
- an organization has / uses / produces materials, products, installations, plants, processes, work procedures or services, for which they would like to receive information about the conformity of these items with regulations, standards, specifications, inspection schemes or contracts. In this case, an inspection can be carried out. Inspection can concern all stages during the lifetime of these items, including the design stage. The inspection provides information about the conformity of an item against inspection parameters like quantity, quality, safety, fitness for purpose or / and continued safety compliance of installations or systems in operations. Inspection requirements are included in ISO 17020. Inspection normally requires the exercise of professional judgement in performing inspection, in particular when assessing conformity with general requirements. Inspection normally
- an organization or other entity may have an object (object of conformity assessment = product, process, service, system, installation, project, data, design, material, claim, person, body or organization, or any combination thereof[5]) for which one or more characteristics need to be determined according to a procedure. A laboratory is a body that performs such testing. The standard that includes the requirements for a laboratory is ISO 17025.
- products, processes or services may be certified in order to give confidence to all interested parties that a product, process or service fulfills specified requirements.

[5] ISO/IEC 17000:2020

The value of certification is the degree of confidence and trust that is established by an impartial and competent demonstration of fulfillment of specified requirements by a third-party. Certification schemes are mandatory part of product certification. The basic standard governing such certification processes is ISO/IEC 17065. This standard does not provide detailed requirements of certification schemes. Guidelines for understanding, developing, establishing, maintaining or comparing certification schemes for products, processes and services will be provided in the future ISO/IEC 17067 "Fundamentals of product certification and product certification schemes.

2. Conformity Assessment within the EU CSA

The EU CSA introduces the concept of the European cybersecurity certification framework. This framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.[6]

ENISA shall prepare candidate certification schemes while consulting with all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process and with the assistance of the relevant ad hoc working group. The process of developing a scheme is available at https://www.enisa.europa.eu/topics/certification/from-candidate-to-certification-scheme.

The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes.

At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties.

A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident. Such assurance level shall be incorporated in the statement of conformity following the above-mentioned European Cybersecurity Certification Schemes.

A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.

ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.

[6] Article 46, EU CSA

The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.
Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:
(a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or
(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

2.1. Existing Cybersecurity Certification schemes

2.1.1. EUCC

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA. This has been named EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) and it looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.[7]
Users of the scheme may be:

- manufacturers or providers who wish to assess the security quality of their ICT products through third party certification;
- providers of ICT services or ICT processes who wish to benefit from the security evidence of certified ICT products for their clients;
- regulatory authorities who wish to establish security and assurance requirements on ICT products within their regulations and directives;
- end users who wish to comply with a regulation or gain security evidence on the ICT products that protect their sensitive assets.

To express their security requirements, both functional and in terms of assurance, these communities may use the methodology described in Chapter 24, ADDITIONAL ELEMENTS OF THE SCHEME to establish a Protection Profile for a category of products to be certified, or may establish an individual Security Target for individual products to be certified.

2.1.2. EUCS

The European Certification Scheme for Cloud Services was drafted with the support of an Ad-Hoc Working group and the support of Member States. The text should now enter the process of the ECCG opinion.
The candidate EUCS scheme (European Cybersecurity Certification Scheme for Cloud Services), looks into the certification of the cybersecurity of cloud services. The scheme draws from many different sources, the first one being the report of the CSP-CERT Working Group, which was delivered in 2019 and provided a basic framework on which the candidate scheme has been developed.

[7] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

EUCS supports the three assurance levels in the EUCSA: 'basic', 'substantial' and 'high'. The security requirements on cloud services and on their assessment increase with levels in several dimensions: scope, rigour and depth. The requirements at level 'high' are demanding and close to the state-of-the-art, whereas the requirements at level 'basic' define a minimum acceptable baseline for cloud cybersecurity. That baseline is nevertheless comprehensive, as it covers all major aspects of cloud security. Cloud service providers of any size can use it to demonstrate that they have set up a framework for guaranteeing some security of their customers. The 'substantial' level, in between, will serve to protect business, and may be the level of choice for many applicants and their users.
The candidate scheme targets a specific category of ICT services, so it is naturally based on the ISO/IEC 17065 standard in terms of applicable requirements to Conformity Assessment Bodies (CABs) performing certification.

2.1.3. EU5G

The European Cybersecurity Certification Scheme for 5G is developed in two phases. During a first phase which ended in Autumn 2022, ENISA, the experts gathered under an Ad-Hoc Working Group with the EU Commission and Member States analysed the existing industrial evaluations and certifications schemes and their necessary updates to comply with the Cybersecurity Act. A first draft scheme should be available for public consultation around mid-2023.
In terms of the context where certification should be applied, the EU 5G scheme should concentrate on certified security for subscriber-related use cases of the 5G ecosystem. In particular[8]:

1. The supply and deployment of identified 5G network equipment
2. Management of subscriber identities
3. Remote SIM provisioning
4. 5G authentication (incl. roaming)
5. Subscriber connectivity services

3. Cybersecurity Certification challenges

3.1. Regarding the EUCC:

- As mentioned above, the EU CSA, a European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products that present a low risk corresponding to assurance level 'basic'. But, it will be hard to keep up the reputation of the EUCC scheme if self-assessment is implemented even at this level without the implementation of other control mechanisms. The existence of self-assessment, especially for producers with low knowledge and incentive will allow malicious or untrustworthy actors to show a EUCC certification without any real security (even at a basic level).
- Due to the existence of national schemes and requirements, ICT products that preset a high risk corresponding to assurance level "High" would still need to go through a

[8] https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification/ad-hoc-working-group-on-5g-cybersecurity-certification

national Common Criteria (CC) certification under the relevant national schemes, which would therefore minimize the reputation of EUCC.

- The EU CSA mentions that certification shall be voluntary. This means that manufacturers are free to decide (even for products of medium or high risk corresponding to assurance levels "substantial" or "high") whether their products will be subjected to a certification process. As long as there is no defined regulation that all new products in the EU need to fulfill EUCC the possible candidates for this scheme will be limited and the impact of the EUCC small.
- There is also a related challenge here when it comes to the business buyers/industrials of ICT products. It seems that these interested parties still do not understand the value of the EUCC and do not know how to map it to their risk management processes in order to request such certification from their suppliers.
- Certification according to the EUCC, is dependent to the existence of the relevant applicable protection profiles. Currently there is a limited number of protection profiles available and even less that are recognized and accepted by all interested parties.
- For the time being, there is limited practical information provided, on how the certifications may be maintained especially in the cases of updates or identified vulnerabilities. Issues regarding IPR, time, effort and cost still exist making the process difficult and cumbersome.
- Currently the understanding of the ICT products that could fall into the scope of the EUCC, is not fully understood by the interested parties. Even further, it seems that it is not clear also how and why the different ICT products should be classified at substantial or high level.
- There is a great interconnection between the EU CSA, the resulting certification schemes and the proposed Cyber Resilience Act (CRA), but for the time being it is not fully apparent.
- One more challenge is related to the CABs (ITSEFs and CBs) accreditation and authorization processes required to enforce a harmonized evaluation processes across Europe. As mentioned above, the entire accreditation process will be governed under the ISO 17065 and ISO 17025 standards, although each country may have the right to add specific country related (accreditation) requirements. In such cases, harmonization and interoperability between countries may become a challenge.
- When speaking of implementation from different countries, one also needs to consider the economics related. The accreditation, certification and testing costs will depend on the market of the country where the CAB operates and / or is accredited. This may lead to price inconsistencies within Europe and a strain on the quality of service due to competition.
- Finally, special attention should be drawn to the EUCC recognition and operation in non-EU countries. For example, would there be an equivalence / mapping between the EUCC and other certification schemes? Would there be a way that an EU based manufacturer, that produces the products outside the EU, test and certify such products? Would there be a limitation on the level such products could claim (e.g. substantial)?

3.2. Regarding the EU5G:

- ENISA has defined that the EU5G certification scheme shall concentrate on certified security for subscriber-related use cases of the 5G ecosystem. This by definition includes ICT products (e.g. 5G network equipment), ICT processes (e.g. the procurement and deployment of identified 5G network equipment) and ICT services (e.g. Subscriber connectivity services)[9]. This means that the envisioned EU5G is a superset of certification schemes, each one focusing on the certification of each of the above-mentioned components, increasing the effort and complexity 3-fold. This complexity is natural, since 5G is not one product, but rather a collation / composition of different products and services that needs to be deployed to offer the final service. It should be noted that although from an accreditation point of view the standard to be employed for products, services and processes is ISO 17065 (see above), it is not usual that the same certification scheme can cover all three cases. (The EUCC for example only covers ICT products and focuses on specific Targets of Evaluation (TOE), whereas the EUCS only covers cloud services).
- Within the ENISA webpage for the 5G ad-hoc working group, it is stated that "This candidate EU 5G scheme addresses only a part of the 5G eco system that was selected by the Member States, based on criteria to achieve stakeholder value and manageable scheme development. Based on this approach, the project (EU5G certification scheme) will focus on the following use cases for cybersecurity certification:
  - The supply and deployment of identified 5G network equipment
  - Management of subscriber identities
  - Remote SIM provisioning
  - 5G authentication (incl. roaming)
  - Subscriber connectivity services

  What appears to be missing here is the certification of the ICT product development processes, where the focus is not only on the outcoming product but also on the how the product is developed. Although this seems to be absent, early discussions, mentioned that already existing certification schemes (e.g. NESAS) would be evaluated and re-used to the degree possible.
- The GSMA NESAS[10], is a Network Equipment Security Assurance Scheme, 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. The NESAS assessment process incorporates auditing and testing as shown in the figure below. Specifically, specialized audit teams audit the network equipment vendor in relation to the Network Product development and lifecycle processes by collecting and evaluating relevant evidence. To complement the audit processes, accredited Test Laboratories evaluate the network product and provide an evaluation report based on the applied standards and the results of the tests. In this way, the processes (e.g. security by design) followed during development and for the lifecycle of the product are verified at a first level through objective evidence and further validated through the performance of the product during the tests against specific test specifications. The NESAS

[9] https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification

[10] https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview/)

documentation are defined by GSMA where as the Test specifications are defined by 3GPP SA3. It should be mentioned that the above process includes accreditation (based on ISO 17025) for the Test Laboratory where as the audit teams are not accredited but rathe appointed by the NESAS oversight Board (AB). Especially the auditing part deviates from other cases of auditing, where conformity assessment bodies are accredited (ISO 17021 or ISO 17065) in order to be able to perform audits.

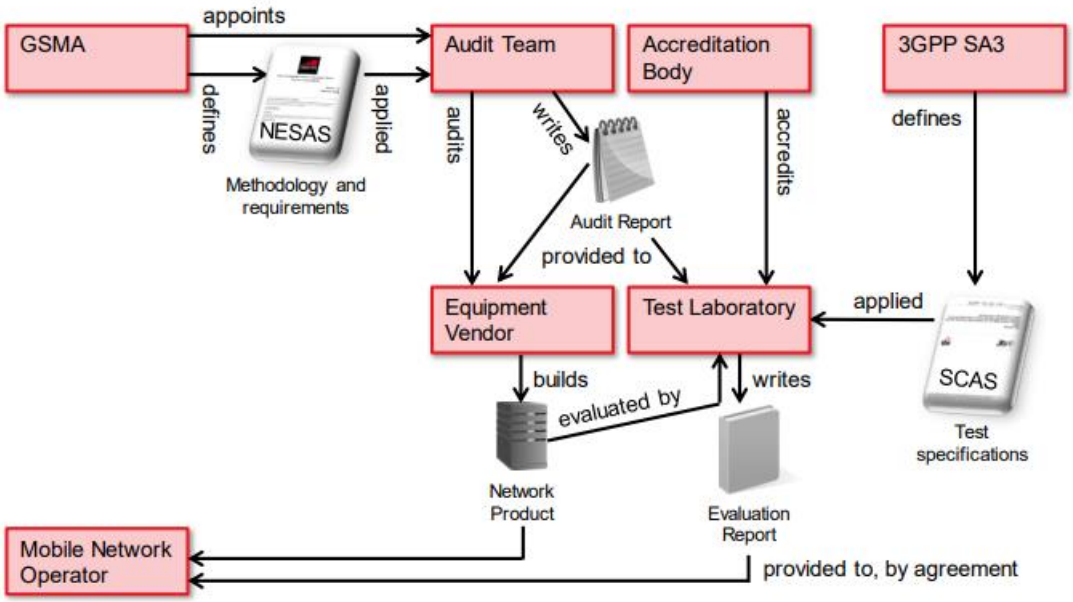

Figure 1. NESAS High Level Overview[11]

- Especially in the early implementations, 5G wireless telecommunications may be built upon legacy technology such as 4G LTE networks[12]. There is no indication at this point whether the EU5G certification scheme would be able to cover the complete 5G network implementation from a cybersecurity point of view or be limited to specific 5G components. If the later is the case, this could lead to the operation of 5G networks with unknown weaknesses.
- On the other hand, such risks can be avoided on minimized based on the security processes, controls or deployment utilized by the Mobile network operators. For example, applications relying on 5G networks can always use 5G disabling legacy 4G/3G, and avoid exposure to such risks. Or Mobile network operators can deploy SA (Standalone) 5G as opposed to NSA (Non standalone) 5G. As indicated by the name, NSA operates on legacy 4G LTE core and manages control plane functions, whereas SA 5G networks include both a 5G RAN and a cloud-native 5G core.
- The implementation of a 5G network, is expected to involve an increased use of open-source software[13]. Within the telecom sector, there are some proposed (or even recommended) methods e.g. Software Bill of Materials (SBOM), as well as other suggestions included as part of the NTIA Docket No. 210105–0001 "5G Challenge

[11] https://www.gsma.com/security/wp-content/uploads/2022/10/FS.13-v2.2.pdf
[12] https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2022KS-Jyothi-5G_Challenges_Solutions_Future_Prospect.pdf
[13] https://www.enisa.europa.eu/news/enisa-news/tackling-security-challenges-in-5g-networks

Notice of Inquiry"[14] For the time being, though, there is no consensus regarding how these components shall be treated from a certification point of view. (The proposed Cyber Resilience Act includes requirements for manufacturers of ICT products with digital elements, for the entire lifecycle from design to release, maintenance and vulnerability management. Such provisions are not extended to the open-source software which may be part of the 5G network implementation).

- Due to the less centralized architecture, 5G networks offer more potential entry points for attackers. Apart from everything else involving the components of the 5G network, controls (like the ones suggested in the EU toolbox for 5G security[15]) should be applied and audited for their compliance and security capability. (Some of the categories of these controls include physical and environmental security controls, business continuity and disaster recovery controls, supply chain resilience controls and others). In this case, again there is a different set of specifications and a different approach to auditing than on the cases of ICT products and processes mentioned above.
- Further to the decentralized architectures, one more critical aspect is the disaggregation that is promoted in both vertical and horizontal layers e.g., components inside a 5G core network may be provided by different vendors, 3rd party applications in O-RAN etc. In the future, network infrastructures as well as applications running on top of them will be a collection of different building blocks, services and functions that may be dynamically added, scaled-in, scaled-out or even completely removed during operation. Certification for all these building blocks (which can be composed of other smaller blocks) will play a significant role, since it will allow orchestrators (service, infrastructures networks etc.) to choose the most suitable parts for a specific system. One thing that must also be noted is that the same building block may need different security certification when used in different contexts.
- Also, from a standardization point of view, the 5G domain has an increased complexity since different standards or guidance documents exists for different components or functionalities of the 5G network. As mentioned above, 5G is a composition of different products and services, operated and deployed in a certain way by each operator. Depending on the which part of the 5G composition one is looking at, different standard with different conformity assessment processes may be applicable. This variation also increases the difficulty of creating one certification scheme. (The variety of the applicable standards is also evident within the ENISA publication 5G Supplement – to the Guideline on Security Measures under the EECC, especially within section 4 and annex 3).
- For the time being, as in the case of the EUCC, there is limited practical information provided, on how the certifications may be maintained especially in the cases of updates or identified vulnerabilities. Issues regarding IPR, time, effort and cost still exist making the process difficult and cumbersome.

[14] https://ntia.gov/federal-register-notice/5g-challenge-notice-inquiry
[15] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

3.3. Regarding the EUCS:

- As mentioned above, the EU CSA, a European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products /processes or services that present a low risk corresponding to assurance level 'basic'. For the time being the current text of the EUCS does not allow for such self-assessment, with the rationale that "it is preferable to only allow accredited CABs to use the scheme, making it easier to bring the various elements of the scheme to a higher level of maturity in a consistent way, and to control their usage in the meantime through guidance and guidelines for CABs"[16]. The way that the text is phrased though, it leaves the subject as open for discussion for the next versions of the scheme.
- The above statement makes the provision of direction, guidance, guidelines and requirements on the EUCS to the CABs more critical. For the time being no such documentation has been created and the Annex E of the EUCS – Cloud Service candidate cybersecurity certification scheme, is missing "The content of this Annex will be developed together with the requirements for accreditation for the scheme, whose development will be initiated after the external review."
- The application of the EUCS is voluntary and its adoption by the cloud service providers depends on their understanding, the cost, the effort, the need to disclose vulnerabilities and the market need (when such is created). It is unclear whether such certification will be adopted and to which degree.
- The EUCS identifies within the users of the scheme the cloud service providers. The issue of supply chain and composition of services is a crucial matter in the provision of services. There are major cloud service providers on which other cloud services are created, managed, operated by other cloud service providers. The certification schemes should have the ability to incorporate such dependencies and interactions.

[16] EUCS – Cloud Service candidate cybersecurity certification scheme, ENISA, December 2020.