EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TRANSITIONING EXISTING CERTIFICATION SCHEMES TO THE EMERGING EU CERTIFICATION FRAMEWORK

The case of SOG-IS MRA

LIMITED DITRIBUTION TO ENISA MB MEMBERS

NOVEMBER 2019

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTRIBUTORS

Elżbieta Andrukiewicz (ITL), Nils Tekampe (Konfidas)

EDITOR

Prokopios Drogkaris (ENISA)

ACKNOWLEDGEMENTS

We would like to thank the following experts (in alphabetical order) for their contributions in reviewing the study and providing their insights: Lionel Antunes (CTIE.ETAT), Jørn Arnesen (SERTIT), David Cerezo (CCN), Julie Chuzel (ANSSI), Antonello Cocco (OCSI), Marcellino Ferrazza (OCSI), Rob Huisman (NLNCSA), Tiziano Inzerilli (OCSI), Gereon Killian (BSI), Iben Lunding (CFCS), David Martin (NCSC), Dag Stroman (FMV) and Joachim Weber (BSI).

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This study was concluded in Q1 2019. At that time, the Cybersecurity Act (Regulation (EU) 2019/881) was still on a proposal phase. The discussion and the analysis conducted within the scope of this document are based on the proposal document. Following the findings of the study, SOG-IS MRA participants initiated an internal process of drafting the successor of SOG-IS MRA based on the Cybersecurity Act provisions. Currently, the Cybersecurity Act has entered into force (Regulation(EU) 2019/881) and ENISA has already received a request by the EC to draft a candidate EU cybersecurity certification scheme on SOG-IS MRA successor. However this is not reflected in the study, in terms of wording and analysis of articles and provisions as the ones on Cybersecurity Act proposal and Regulation (EU) 2019/881 differ slightly. This study has been based on the Cybersecurity Act proposal, which was only available at that time.

The Cybersecurity Act proposal put forward the set up of a European Cybersecurity Certification framework for ICT products, services and processes and rules governing European cybersecurity certification schemes. Within this framework, certificates issued under those schemes will be valid and recognised across all Member States towards addressing the current market fragmentation.

One of the most prominent efforts made in the past on mutual recognition of certificates in Europe is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA), which came as a response to the EU Council Decision of March 31st 1992 (92/242/EEC)[1] in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC)[2] on common information technology security evaluation criteria (CC). As it represents an important model for cooperation and mutual recognition in the field of security certification, SOG-IS MRA could be considered as a possible candidate for an EU cybersecurity certification scheme, which will not only leverage experience and expertise but also build on existing schemes.

Towards this direction, the overall scope of this study was to explore and provide an analysis of any likely impediments introduced by the Cybersecurity Act proposal [CSA_P] on a possible transposition of the existing SOG-IS MRA while identifying open challenges that should be further discussed and addressed by involved stakeholders during the transposition process. Taking into consideration the fact that the SOG-IS MRA has been developed before the Cybersecurity Act proposal, the agreement was considered to be a promising candidate for an implementation of a cybersecurity scheme. Lastly, following a consultation process with interested SOG-IS MRA participants, a number of considerations were brought up with regard to possible issues and challenges that pertain mainly to:

- The relationship between the new scheme, CCRA and EEA countries
- The role of Conformity Assessment Bodies
- The support to the EU Single Market and
- The possible extension of the new scheme's scope.

Following an additional consultation, a number of proposed aspects to be revisited and possible ways forward were also identified. Currently, the Cybersecurity Act has entered into force

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24121
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995H0144

(Regulation(EU) 2019/881) and ENISA has already received a request by the EC to draft a candidate EU cybersecurity certification scheme on SOG-IS MRA successor.

1. INTRODUCTION

1.1 BACKGROUND

The Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 4771[3], establishes, under Title III, a European cybersecurity certification framework for ICT products, services and processes and rules governing European cybersecurity certification schemes allowing certificates issued under those schemes to be valid and recognised across all Member States. The proposal for the European Cybersecurity Certification Framework within the Cybersecurity Act[4]:

- Lays down an overall framework of rules governing European cybersecurity certification schemes.
- Does not introduce directly operational certification schemes.
- Seeks to create a system (framework) for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes").
- Provides that certification schemes created in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.
- Provides what the minimum content of such schemes shall be.

The scope of this study, while the CSA was still a Proposal, was to explore aspects to be considered during the transposition of SOG-IS MRA.

1.2 SCOPE

The SOG-IS Agreement came as a response to the EU Council Decision of March 31st 1992 (92/242/EEC)[5] in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC)[6] on common information technology security evaluation criteria (CC). Participants in this agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries. It allows for the issuing of certificates for IT Products in the field of IT security that are mutually recognized by all signatories of this Agreement.

The overall scope of this study was to explore and provide an analysis of any likely impediments introduced by the Cybersecurity Act proposal [CSA_P] on the transposition of the existing SOG-IS MRA while identifying open challenges that should be further discussed and addressed by involved stakeholders during the transposition process.

In order to achieve this, the study provides:

- An overview of relevant terms and definitions
- An overview and analysis of European cybersecurity certification scheme elements (Art. 47);

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN
[4] In this version of the report, the following version of the CSA has been used: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24121
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995H0144

- An introduction to a structured way of describing certification schemes based on EN ISO/IEC TR 17067
- A detailed introduction to the SOG-IS Agreement processes and procedures
- A gap analysis and identification of potential areas of the SOGIS MRA non-compliance,
- Identifications of aspects to be considered during the (possible) transposition of the SOG-IS Agreement to the cybersecurity certification scheme, based on Article 47 - Elements of European cybersecurity certification schemes
- Overview of aspects to also be considered under other relevant articles

The term "transposition process" refers to the preparation of a candidate European Cybersecurity Certification Scheme, which will take into account and consideration existing certification schemes and practises, already operational across the EU.

This study was conducted and concluded in Q1 2019. At that time, the Cybersecurity Act (Regulation (EU) 2019/881) was still on a proposal phase. The discussion and the analysis conducted within the scope of this document are based on the proposal document. Following the findings of the study, SOG-IS MRA participants initiated an internal process of drafting the successor of SOG-IS MRA based on the Cybersecurity Act provisions.

Currently, the Cybersecurity Act has entered into force (Regulation(EU) 2019/881) and ENISA has already received a request by the EC to draft a candidate EU cybersecurity certification scheme on SOG-IS MRA successor. However this is not reflected in the study, in terms of wording and analysis of articles and provisions as the ones on Cybersecurity Act proposal and Regulation (EU) 2019/881 differ slightly. The current study was based on the Cybersecurity Act proposal, which was only available at that time.

1.3 DEFINITIONS

The Cybersecurity Act proposal, COM(2017) 477[7], EN ISO/IEC 170xx series of standards and Regulation(EU) 1025/2012[8] provide the following definitions in relation to the certification framework:

- **European cybersecurity certification scheme**: a comprehensive set of rules, technical requirements, standards and procedures defined at Union level applying to the certification of Information and Communication Technology (ICT) products and services falling under the scope of that specific scheme [9];

  Note: According to EN ISO/IEC 17065, 'certification scheme' means: certification system related to specified products, to which the same specified requirements specific rules and procedures apply.

- **European cybersecurity certificate**: a document issued by a conformity assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477
[8] http://data.europa.eu/eli/reg/2012/1025/oj
[9] Article 47 of the Proposal lists the elements, which shall be included in a European cybersecurity certification scheme.

In relation to the definitions provided hereinafter, the Proposal references Article 2 of Regulation (EC) No 765/2008[10] and Article 2 of Regulation (EU) No 1025/2012[11]

- **accreditation**: an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity;

  Note: According to EN ISO/IEC 17000, 'accreditation' means: third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.

- **national accreditation body**: the sole body in a Member State that performs accreditation with authority derived from the State;

  Note: According to EN ISO/IEC 17000, 'accreditation body' means authoritative body that performs accreditation

  Note: Under Regulation 765/2008 each Member State has one National Accreditation Body (NAB) which grants accreditation certificates to conformity assessment bodies

- **conformity assessment**: the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled;
- **conformity assessment body**: a body that performs conformity assessment activities including calibration, testing, certification and inspection;

  Note: Under SOG-IS MRA testing laboratories are called "IT Security Evaluation Facilities (ITSEF)"

- **certification body**– third-party conformity assessment body operating certification schemes [EN ISO/IEC 17065]
- **standard**: a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:
  a) 'international standard' means a standard adopted by an international standardisation body;
  b) 'European standard' means a standard adopted by a European standardisation organisation;
  c) 'harmonised standard' means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;
  d) 'national standard' means a standard adopted by a national standardisation body;
- **technical specification:** a document that lays out technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following:
  - the characteristics required of a product including levels of quality, performance, interoperability, environmental protection, health, safety or

[10] http://eur-lex.europa.eu/eli/reg/2008/765/oj
[11] http://eur-lex.europa.eu/eli/reg/2012/1025/oj

dimensions, and including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and conformity assessment procedures;

- production methods and processes used in respect of agricultural products as defined in Article 38(1) TFEU, products intended for human and animal consumption, and medicinal products, as well as production methods and processes relating to other products, where these have an effect on their characteristics;
- the characteristics required of a service including levels of quality, performance, interoperability, environmental protection, health or safety, and including the requirements applicable to the provider as regards the information to be made available to the recipient, as specified in Article 22(1) to (3) of Directive 2006/123/EC;
- the methods and the criteria for assessing the performance of construction products, as defined in point 1 of Article 2 of Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products[12], in relation to their essential characteristics;

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2011:088:TOC

2. ARTICLE 47 OF THE CYBER SECURITY ACT PROPOSAL

The basis for this study is provided in the following document

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), Brussels, 29 May 2018[13]

The following text reproduces article 47 from [CSA_P] in order to form a basis for the rest of this report.

Article 47

Elements of European cybersecurity certification schemes

A European cybersecurity certification scheme shall include at least the following elements:

(a) subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services covered as well as an elaboration of how the certification scheme suits the needs of the expected target groups;

(b) reference to international, European or national standards followed in the evaluation. Where standards are not available, a reference shall be made to technical specifications that meet the requirements of Annex II of Regulation 1025/2012 or, if such are not available, to technical specifications or other cybersecurity requirements defined in the scheme;

(c) where applicable, one or more assurance levels;

(ca) where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;

(e) where applicable, information to be supplied or otherwise be made available to the conformity assessment bodies by an applicant which is necessary for certification;

(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(g) rules for monitoring compliance with the requirements of the certificates or the EU statement of conformity, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

[13] http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

(h) where applicable, conditions for granting and renewing a certificate, as well as maintaining, continuing, extending or reducing the scope of certification;

(i) rules concerning the consequences of non-conformity of certified or self-assessed ICT products and services with the requirements of the scheme;

(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT processes, products and services are to be reported and dealt with;

(k) where applicable, rules concerning the retention of records by conformity assessment bodies;

(l) identification of national or international cybersecurity certification schemes covering the same type or categories of ICT processes, products and services, security requirements and evaluation criteria and methods;

(m) the content of the issued certificate or the EU statement of conformity;

(ma) the period of the storage of the EU statement of conformity and the technical documentation of all relevant information by the manufacturer or provider of ICT products and services;

(mb) maximum period of validity of certificates;

(mc) disclosure policy for granted, amended and withdrawn certificates;

(md) conditions for the mutual recognition of certification schemes with third countries;

(me) where applicable, rules concerning a peer review mechanism for the bodies issuing European cybersecurity certificates for high assurance levels pursuant to Article 48(4a).

3. STRUCTURAL APPROACH ON CERTIFICATION SCHEMES

3.1 INTRODUCTION

This section introduces a structured way of describing certification schemes in a general manner which can be used as the basis for the description of the SOG-IS scheme in the following section.

The document EN ISO/IEC TR 17067 Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes ([ISO17067]) can provide a useful and valuable base of information for this approach as it defines the fundamentals of product certification and specifically also defines guidelines for the development of product certification schemes.

While [ISO17067]) is not a normative standard but offers guidance and best practises it can be used as a structured source of criteria for the presentation of the SOG-IS scheme in section 4.

Certification schemes are subject to standardisation within the scope of EN ISO/IEC 170xx series offering potential users a structural approach allows for building schemes in two ways:

- top – down, when a scheme is being developed starting from the idea to implementation, and
- bottom-up, when the scheme already exists and the structural approach helps assess its components against a given set of requirements.

Based on standards EN ISO/IEC 17067 and 17026 the following subsections outline a checklist of requirements for a certification scheme.

3.2 IDENTIFYING THE SCHEME FUNDAMENTALS

Fundamentals of a certification scheme include:

1. Identifying the scheme owner: the managing workgroup, which holds responsibility for developing and maintaining a scheme, including all the decision-making. Usually, the group comprises members or experts from organisations that directly participate in the scheme or benefit from it, such as producers, certification bodies, laboratories, governmental agencies.
2. Identifying interested parties: the expectations, motivation and acceptance level of all interested parties need to be assessed. The assessment should include scheme operators, producers, end users, society's group of interest and regulators.
3. Identifying rules and procedures for membership: checking whether the process for accepting new members is open and transparent to any eligible applicant.
4. Analyzing a financial model: the business model needs to be defined, considering the issue of ownership and functionality of the scheme. Budgets have to include the degree of complexity and a number of working groups involved in the process, estimation the costs for producers and suppliers of the product and the certification body, as well as the model of distributing potential profits between entities responsible for managing and sustaining the scheme.

3.3 STANDARDS AND TECHNICAL SPECIFICATIONS

Within the scope of a certification scheme it is required to identify:

1. Appropriate standards or technical specifications, both functional and measuring (international or European), specifying requirements for products and their applications. In addition, relevant standardisation organisations and their working groups or industry associations should be identified that specify the cybersecurity requirements of the product.
2. Harmonized standards or local standards, which can be related to the harmonised ones.
3. Level of acceptance among interested parties of interest regarding identified standards, their modification or development.

3.4 IDENTIFYING DETAILED REQUIREMENTS FOR CONFORMITY ASSESSMENT

The certification scheme analysis should also address:

1. The scope of functional measurement and choice of threshold level- it should be specified how the assessment is performed about the functional measurement and the threshold set in the certification process. It should be clarified whether the certificate will be used to demonstrate conformity or validate the result of the assessment/evaluation[14].
2. Functional and non-functional requirements - this action includes identifying key requirements and functions subject to detailed testing, or threshold assessment, or compliance assessment.
3. Identification of requirements regarding threshold assessment and measurement of functional requirements - this action includes reviewing metrics for measurements (e.g. error rate) or threshold assessment criteria, i.e.' pass-fail'.
4. Differentiation between basic and additional requirements (possible variations); identification of levels for requirements levels (scalable requirements).
5. Identification of restrictions regarding the confidentiality of requirements taking into account possible local circumstances.

3.5 ANALYSING TEST METHODS

As part of a certification scheme, the evaluation methodologies are a subject of scrutiny, including:

1. A review of test methods - check whether test methods are defined in referenced standards. Also, local methods should be identified if they are used. Assessment methods and metrics for testing complex functions, e.g. using scenarios/types of threats, concepts of operation or use should be examined.
2. Checking the efficiency of adopting or developing test methods - it is necessary to analyse the process of adapting the identified testing methods as additions or extensions to existing ones. In case of the test method development, it can include real-world test methods or denial tests, sampling, re-testing and self-testing approach. Completeness of tests, sufficient level of detail and statistical confidence (number of test runs), as well as repeatability of tests, should be assessed.
3. Determining the sensitivity of testing methods - certain parts of the testing methods could be kept in confidence (e.g. elements of threats or artefacts for biometric presentation attacks). At the same time, the public character of all other elements of the testing methods should be confirmed, due to the need for widespread

[14] Such a distinction indicates the division of competences between conformity assessment bodies, which has a direct impact on the organization of the scheme: single-level (one entity evaluates and issues the certificate) or two-level (the entity issuing the certificates exercises supervision over the evaluation laboratories)

dissemination (e.g. among manufacturers) and the recognition of testing methods. The justification for the decision whether test results should be classified and, if so, how the appropriate levels of confidentiality are applied should be checked.

4. Identifying ethical considerations and compliance with relevant applicable legal framework, i.e. checking whether the test methods include activities that are related to European or national privacy or personal data protection legislation.

3.6 IDENTIFYING THE SCHEME STRUCTURE

The structure of a certification scheme is characterized by the following:

1. The scheme type - the nature of product certification for schemes dealing with the product's cybersecurity has to be determined according to EN-ISO / IEC 17067 standard "*Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes*".
2. Ownership and management of the scheme - the scheme owner is the organisation responsible for the development and operation of a given certification scheme, e.g. a government agency or a regulatory agency, an association of entrepreneurs or suppliers, a group of certification bodies.
3. Certificate of the scheme - it should be identified what information should be included in the certificate (see *ISO / IEC TR 17026 Conformity assessment - Example for a certification scheme for tangible products*, Annex C). Activities also include specifying a certificate mark/label and granting a license to use intellectual property.
4. Analyzing the rules of the scheme and procedures for classification of information, ie.
    a. Principles of cooperation between working groups and entities operating in the schema (operators),
    b. Working group responsibilities per various types of certified products,
    c. Procedures for handling sensitive information.
5. Identification of scheme operators - all participants should be identified: certification bodies and evaluation entities.

3.7 IDENTIFYING THE QUALITY MEASURES

Aspects related to ensuring the quality of a certification scheme to be inspected include:

1. Identification of qualification requirements for operators - general eligibility requirements for scheme participants should be identified. This applies to the potential, equipment enabling the testing or inspection to be carried out, and the skills and experience of the personnel implementing the quality management system. Usually, these are general requirements applied first to the accreditation process. However, participation in the scheme should be subject to additional requirements related to the evaluation objectives. Further to that, procedures on the role of the operator (within the scheme) should also be identified and assessed.
2. Identification of methods used to ensure laboratories' consistency which can encompass the following actions:
    a) Performing the inter - / intra - laboratory comparisons, for both cases: realistic and adversarial testing, for example by:
        - moderating the results (comparison of results in time),
        - mutual tests,
        - performing joint training for testers/ evaluators.
    b) Establishing and implementing the peer assessment programme to check periodically:
        - application of procedures and roles in the scheme,
        - the ability of testers/ evaluators to perform and interpret test results,
3. experience and skills of testers/ evaluators and
4. quality monitoring of evaluations performed across different scheme participants.

3.8 IDENTIFYING SURVEILLANCE METHODS

The scope of surveillance methods encompass:

1. Defining the needs for surveillance, e.g. whether the products assessed under the scheme require re-audits, assessments and/or certification of production sites and/or processes. In case such a need is identified, it can be implemented in the form of:
    a. Regular testing/inspection of market samples,
    b. Regular testing/inspection of production samples,
    c. Periodic assessment of production sites and/or manufacturing processes facilities,
    d. Periodic assessment of the manufacturer's quality management system.
2. Identification of the scope of testing supervision methods - test supervision methods may include sampling, full or limited tests, self-testing.
3. Identification of frequency and consistency of supervision.
4. Identification of certificate validity period - consideration should be given to scheme-specific factors affecting the rules and life cycle of the certificate, e.g. whether the need for frequent updating of requirements can be predicted. The criteria for non-compliance should be identified.

4. SOG-IS MRA OVERVIEW

4.1 INTRODUCTION

In the year 2000, several governmental agencies, responsible for IT security in their countries, started a world-wide cooperation under the Common Criteria Recognition Arrangement[15] (hereinafter called "CCRA") to enable mutual recognition of certificates attesting compliance to specified security requirements for IT products, confirmed by successfully passing evaluation using a common evaluation methodology. A year before, in 1999, European members of CCRA had created a separate agreement, called SOG-IS Mutual Recognition Agreement[16].

Version 3.0 of the Agreement, effective since 2010 ("Saragossa" Agreement, from now on named "the Agreement", see also [SOGIS]) regulates all formal relationships among the SOGIS member nations.

The Agreement is aimed at the following objectives:

- ensuring that evaluations of Information Technology (IT) products[17] and protection profiles[18] are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;
- improving the availability of evaluated, security-enhanced IT products and protection profiles;
- eliminating the burden of duplicating evaluations of IT products and protection profiles;
- continuously improving the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles.

It is worth noting that the objectives for the SOG-IS MRA are the same as for the CCRA, but the European structure differs from the latter one in the level of mutual recognition of issued certificates for specific types of products. The characteristics of SOG-IS MRA are presented in following subsections, according to the systematic approach presented in Section 3.

4.2 PURPOSE, SCOPE AND APPLICATION OF THE AGREEMENT

The purpose of the Agreement is to advance objectives as stated above by "*bringing about a situation in which IT products and protection profiles which earn a certificate can be procured or used without the need for further evaluation.*"

Any IT product, as defined in Annex A of the Agreement or protection profile, can be a subject to a security evaluation and subsequent certification after it successfully passes the evaluation. In case the certificate issued by any of the Authorized participant conforms to criteria set up in the Agreement (see section 4.5.4) it is recognised by all other participants. This mutual recognition applies to any conformant certificate issued by an authorized participant for the subject of evaluation against any of the Common Criteria Evaluation Assurance Level 1 through 4 or ITSEC Assurance Level E1 through E3 with Strength of Mechanisms 'basic'.

[15] https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf
[16] https://www.sogis.org/documents/mra/20100107-sogis-v3.pdf
[17] SOGIS MRA defines IT product as "*a package of IT software or hardware, providing functionality designed for use or incorporation within a multiplicity of systems or within a specifically defined operational environment and with a particular purpose"*
[18] SOGIS MRA defines protection profile (PP) as "a formal document defined in *C[ommon] C[riteria],* expressing an implementation independent set of security requirements for a category of *IT products* that meet specific consumer needs.

Recognition of higher assurance levels (including augmentations) is defined for specific IT technical domains as agreed by the Management Committee. Currently, there are two IT technical domains, namely:

- **Smart cards and similar devices**, i.e. products whereby significant portions of the required security functionality depend upon hardware features at a chip level (e.g. integrated circuits (IC), smart card composite products, TPMs used in Trusted Computing),
- **Hardware devices with security boxes**, which include products whereby significant proportions of the required security functionality depend upon a hardware physical envelope with installed counter-measures against direct physical attacks (so-called "Security Box") (e.g. payment terminals, tachograph vehicle units, smart meters, access control terminals, Hardware Security Modules), for which the EAL7 evaluation and subsequent certification is possible for mutual recognition. The recognition, however, requires additional proof of competencies as defined in the Agreement (see section 4.8.3).

Outside the scope are certificates which do not

- conform with the criteria or
- the product is considered for a specific application or
- authorised under the provisions of national law, subsidiary legislation, administrative regulation or other official obligation.

In such circumstances, Participants are allowed to decline the recognition of a certificate.

4.3 SOG-IS FUNDAMENTALS

4.3.1 Type of conformity assessment applicable to national schemes

Based on the formal classification of schemes introduced by harmonised standards, national schemes operating under the SOGIS MRA are the product certification scheme of type 1a, described in EN ISO/IEC 17067 "*Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes*,". In particular, the SOG-IS does not introduce any type of surveillance method defined in Clause 5.3.2.The product life-cycle processes are only considered at a given point in time i.e. during the evaluation, and insofar as they contribute to the product's security.

4.3.2 Current Participants

The Agreement, within Article 1, defines the memberships as follows: "*Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA, representing their country or countries. Participants may be producers of evaluation certificates, consumers of evaluation certificates, or both*". This means that any EU Member State is eligible to join the SOG-IS MRA (see Article 9).

However, the Agreement is open only to specific organisations, as it excludes from the membership (see Preamble):

- purely commercial certification bodies (CBs) as the Agreement "requires mutual trust and understanding between governmental organisations," and
- another certification body from a given participating country, i.e. the rule 'one CB per country' applies.

These exclusions are also in place in CCRA[19], for the same reasons (ensuring competence, availability of effort/manpower and impartiality with regard to financial interests).

As of 2019, the list of participants (in alphabetical order) includes:

- **Austria**, Bundeskanzleramt
- **Belgium**, Centre for Cyber Security Belgium
- **Croatia**, Information Systems Security Bureau
- **Denmark**, Centre for Cyber Security
- **Estonia**, RIA - Riigi Infosüsteemi Amet
- **Finland**, FICORA - Finnish Communications Regulatory Authority
- **France**, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- **Germany**, BSI - Bundesamt für Sicherheit in der Informationstechnik
- **Italy**, OCSI - Organismo di Certificazione della Sicurezza Informatica
- **The Netherlands**, NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- **Luxembourg**, ANSSI.lu - Agence Nationale de la Sécurite des Systèmes d'Information Luxembourg
- **Norway**, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- **Poland**, NASK - Naukowa I Akademicka Siec Komputerowa
- **Slovakia**, NBÚ - Národný bezpečnostný úrad
- **Spain**, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- **Sweden**, FMV - Försvarets Materielverk
- **United** Kingdom, NCSC - National Cyber Security Centre

The agreement is not only a certification scheme but rather a framework under which the national schemes for IT security evaluation and certification operate. The Agreement's objective is to establish conditions under which certificates issued by one national scheme are recognised by any other national scheme and consumer participants (see below).

The Agreement provides mechanisms for member nations to participate in two fundamental ways:

- as certificate consumers (no national scheme or the scheme is under development),
- as certificate producers (with the national certification scheme approved under the Agreement).

Further, certificate producers are divided into two categories:

- authorised to issue mutually recognised certificates up to EAL2[20] from now on called "Authorized Participants";
- authorised and further qualified to issue mutually recognised certificates in specific technical domains up to EAL7, from now on called "Qualified Participants".

The Agreement sets up the conditions for accepting a CB as the issuer of mutually recognised certificates upon unanimous consent of the existing participants. The set of requirements that

MC-2006-09-001, 18 september 2006, available at https://www.commoncriteriaportal.org/files/operatingprocedures/Multiple%20or%20commercial%20CBs%20MC%20policy%20procedure%202006-09-001%20v%201.0.pdf

[20] CCRA theoretically allows recognition up to EAL4 under conditions, but at present only recognition up to EAL2 exists in practice.

have to be met by the CB and the Evaluation and Certification Scheme it operates is discussed in section 4.5.

4.3.3 Ownership of the SOG-IS framework

All participants are considered to be owners of the SOG-IS MRA framework. Article 10 of the Agreement nominates the Management Committee (MC) to administer the Agreement. Annex H.1 of the Agreement imposes responsibilities for developing and maintaining the SOG-IS scope of applicability on the MC.

The MC consists of all participants' representatives. The rule "one country, one vote" applies. In the process of decision-making the following rules are in place:

- In cases explicitly written in the Agreement, where unanimity is required (such as voting on the compliance of CBs) then voting is mandatory and, if there are any abstentions, then it shall not be considered unanimous approval.
- In all other cases the aim should always be to achieve a unanimous vote, however, if it is not possible in the first ballot, the second ballot is open and then at least 2/3 of the whole membership is required to allow a decision to pass.

Organizational structures operating under the Agreement are discussed in section 4.3.

4.3.4 Financing the SOGIS MRA activities

National schemes develop their business models, which can differ from country to country. From the SOG-IS MRA perspective, there are no specific requirements on this, except the following one. A CB has to be a governmental organisation, but the scheme may consist of several evaluation bodies (ITSEFs) of any legal form (including private entities) operating under the supervision of the CB, and licensed by this CB.

According to Article13 of the Agreement "Except as specified otherwise elsewhere in this Agreement, each Participant is expected to meet all its own costs arising through its participation in this Agreement".

Although no written rules are in place for necessary common activities, each participant is expected, on a voluntarily basis, to provide the necessary resources to run the daily operations of the Agreement. This includes developing of new procedures, participating in various meetings and willingness to host meetings in such a manner that in the long term the cost of operation of all aspects of the Agreement is evenly distributed among the participants.

4.4 STANDARDS AND TECHNICAL SPECIFICATIONS USED FOR IT SECURITY EVALUATION

4.4.1 General evaluation standards

Regarding evaluation methods, SOG-IS relates to evaluations using the *Common Criteria* and ITSEC standards, but does not restrict the applicable version of these standards. Therefore, the following versions are applicable:

- All versions of Common Criteria (CC) and Common Evaluation Methodology (CEM)) maintained by the CCRA (publicly available on the Common Criteria portal);
- All versions of the ISO "counterpart" of Common Criteria : the ISO/IEC 15408 Evaluation criteria for IT security (currently consisting of 3 parts) and ISO/IEC 18045 *Methodology for IT security evaluation*[21] ;

[21] It should be noted that Common Criteria and ISO 15408 are not equivalent, and follow different update paths. For example:

4.4.2 Technical specifications used in the IT security evaluation

CC provides a useful tool in order to specify implementation-independent technical specifications for a product type to be evaluated i.e. Protection Profiles (PPs).

SOGIS MRA structures have developed a procedure for endorsing protection profiles under the SOGIS umbrella ("MC PP Endorsement Procedure[22]"). The purpose of this activity is to avoid unnecessary duplication of work among participating schemes and reference to agreed technical specifications. There are three categories of PPs collected:

- **Recommended Protection Profile (PP)** encompasses specifications, which are the unique or main PP reference for Security Targets (STs) of Targets of Evaluation (TOEs) included in the scope of such a PP. They required to be proposed to the JIWG [23]and are subject to technical studies. In case of any collision between existing PP is identified, e.g., they relate to the same scope, such situation is resolved by the JIWG before submitting to the MC for endorsement.
- **Common use Protection Profile (PP)** encompases specifications that can be collected and discussed at the JIWG meetings. However, they are for information only and do not need any endorsement from the MC
- **National Protection Profile (PP)** –in principle, they are relevant only for national schemes, although may be collected for informational purposes.

The catalogue of PPs is maintained by the JIWG chair. Only recommended PPs are subject to publication at the SOG-IS Website[24]. In particular, this category encompasses those PPs which are mandatory, according to relevant EU regulations. Such list includes:

- series of PPs related to Machine Readable Travel Documents, containing requirements of the International Civil Aviation Organisation (ICAO), working in several modes of operations and in different compositions
- series of PPs [25] related to secure signature creation device, in different compositions
- PPs for Digital Tachograph – Smart Card[26] published officially at the SOGIS Web site and recommended for evaluation activities[27].

4.5 DETAILED REQUIREMENTS FOR CONFORMITY ASSESSMENT

4.5.1 Common Criteria approach to conformity assessment

Common Criteria refer to one type of conformity assessment process, i.e., evaluation. Certification is out of the scope of the standard. As such, they address only one aspect of mutual recognition of the results of evaluations, i.e., the use of a Common Evaluation Methodology (CEM). CEM contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgment and background knowledge for which consistency is more difficult to achieve. The final evaluation

- Common Criteria 2.3 have been published as ISO/IEC 15048 :2005 and ISO/IEC 18045 :2005
- Common Criteria 3.1 revision 3 are similar to ISO/IEC 15048 :2009 and ISO/IEC 18045 :2008
- Common Criteria 3.1 revision 4 and 5 have no equivalent in ISO/IEC 15408 and ISO/IEC 18045
- ISO/IEC 15408 and ISO/IEC 18045 are currently undergoing a revision in ISO SC27 WG3, that may or may not be "translated" into Common Criteria

[22] https://www.sogis.org/documents/mra/MC_PP_endorsement-v1.1.pdf
[23] Joint Interpretation Library Working Group - its description and task are presented in section **Error! Reference source not found.**
[24] https://www.sogis.org/
[25] All these PPs are the European Standards EN 419211, Part 2 till 6, and according to the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 *laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, are mandatory for use
[26] COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) No 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components
[27] https://www.sogis.org/uk/pp_pages/tachograph/pp_tachograph_sc.html

results may be submitted to a certification process to enhance the consistency of the evaluation findings. Common Criteria do not state requirements for the regulatory framework.

4.5.2 Evaluation process and outcomes

A Target of Evaluation (TOE) (IT product or part of it) based on a technical specification contained in ST and/or PP(s), ST or PP can be a subject to evaluation.

A generic evaluation process is described in the CEM (ISO/IEC 18045). It contains four () main tasks: i) the input task, ii) the output task, iii) the evaluation sub-activities and lastly iv) the demonstration of the technical competence to the evaluation authority task. This methodology does not cover activities related to development, test and vulnerability analysis higher to EAL5. For those activities the scheme should be consulted. The SOG-IS MRA has published additional guidance to cover the gap and to define harmonized practices between its members (see 4.5.3).

The input and the output tasks are related to management of evaluation evidence and to report generation, respectively.

Several evaluation sub-activity tasks (action elements) are performed against specific requirements of ISO/IEC 15408 for a given subject of evaluation. A verdict is assigned to an applicable ISO/IEC 15408 evaluator action element as a result of performing the corresponding evaluation methodology action and its constituent work units.

The CEM recognizes three mutually exclusive verdict states:

a) Conditions for a pass verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST or TOE under evaluation are met.
b) Conditions for a fail verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST, or TOE under evaluation are not met, or that the evidence is incoherent, or an obvious inconsistency in the evaluation evidence has been found;
c) All verdicts are initially inconclusive and remain so until either a pass or fail verdict is assigned.

The overall verdict is *pass* if and only if all the constituent verdicts are also *pass*.

The last step concluding the evaluation i.e. demonstration of the technical competence to task may be performed by the evaluation authority which analyses the output tasks results, or may include the demonstration done by the evaluators of their understanding of the inputs for the evaluation sub-activities. This task has an evaluator authority verdict as the process outcome.

PP evaluations lead to catalogues of evaluated PPs. An ST evaluation leads to intermediate results that are used in the frame of a TOE evaluation. TOE evaluations lead to catalogues of evaluated TOEs. It should be noted, however, that the IT product is not always equivalent to the TOE. The description of the TOE is always specified in a dedicated, mandatory part of the relevant ST.

The most comprehensive catalogue of evaluated TOEs[28] and PPs[29] can be found at the CC portal. It should be noted the first list contains IT products with TOEs evaluated.

4.5.3 SOGIS MRA requirements for IT security evaluation

In order to ensure the consistent application of the criteria and methods between SOG-IS Evaluation and Certification Schemes, a uniform interpretation of the currently applicable criteria and methods is needed. The SOG-IS Management Committee has therefore established a

[28] https://www.commoncriteriaportal.org/products/
[29] https://www.commoncriteriaportal.org/pps/

group called the Joint Interpretation Working Group (JIWG). Its tasks are to conduct scheduled information sharing on interpretations, to host the discussions required to resolve differences of interpretation, and to develop the resulting supporting documents. Supporting documents will typically describe dedicated evaluation techniques like e.g. penetration methods or so-called application of Attack Potential, that shall be implemented by the CB claiming a Qualifying status for specific IT technical domains.

There are three types of supporting documents:

- **Guidance**: the objective of guidance documents is for developers, ITSEFS and certification bodys to improve the evaluation and certification process. Guidance documents may contain background material to improve the understanding of the evaluation approach or any other information. Such documents hold no obligations for any of the involved actors.
- **Mandatory**: supporting documents of the type 'Mandatory' contain a consistent set of interpretations that specify the use of the criteria and methodology within a particular field or domain of technology and shall be used where relevant. These documents contain the elements necessary for mutual recognition of certificates for such technologies. The Evaluation Technical Report and the Certification Report shall identify which mandatory supporting documents have been used (incl. version).

In the case where the scope of CCRA covered the SOG-IS MRA, practically all additional interpretations and application notes related to specific usage of reference standards, which have an impact on the evaluation process in the area of mutual recognition, are harmonized between CCRA and SOG-IS.

A mechanism for co-operation between SOG-IS and CCRA with regards to the supporting document distribution and recognition by the Agreement participants is in place. In fact, once approved by the SOG-IS MC, a public document is submitted to the Common Criteria Development Board (CCDB) for approval as a CC Supporting Document. All CCDB supporting document related to the SOG-IS technical domain have been produced by the JIWG and its subgroups.

Generally, JIL supportive documents can be divided into two categories:

- Publicly available, published on the SOG-IS MRA website, or on the website of the respective national scheme,
- Sensitive documents with controlled distribution done by the JIL Members to:
    - Licensed labs from the schemes represented in Joint Interpretations Working Group (JIWG).
    - Members of the subgroups related to the specific IT technical domain.
    - Sponsors/developers applying for a product evaluation/certification.
    - Issuers accepting CC certifications as part of an approval process.

4.5.4 SOG-IS MRA requirements for certification

The Agreement sets up a framework for mutually recognised certificates hence includes requirements to the certification process as well. Provisions from this perspective include:

- General conditions for recognizing the certificate as conformant within Common Criteria (Article 5, letters a and b),
- conditions for using the SOG-IS mark on the certification report and presentation of the logo (Annex E, see also Figure 1 below),

- a template for the certification report (Article 5 letter d and Annex I) with further clarification in a JIL supportive document “Assurance package declaration in certificate”,
- content of certificates (Annex J) .

Figure 1: Mark of the SOG-IS MRA[30]

It is interesting to note that neither CCRA nor SOG-IS MRA defines the validity period for certificates, this is left to national schemes. In widely accepted practice it is 5 years starting from the date of the issuance[31].

Information on certificates issued under the SOG-IS mark is available on websites of respective authorised/qualified participants. There is no consolidated repository for all conformant certificates issued under the SOG-IS MRA umbrella.

4.5.5 SOG-IS MRA requirements for schemes

The Agreement contains an important prerequisite for national schemes issuing mutually recognised certificates (see Article 5 letter c). It states the certificate shall be issued “*in the context of an Evaluation and Certification Scheme managed by a compliant CB in the authorising participant's country”.*

Further, Article 5 of the Agreement contains general requirements for (a) Evaluation Facilities and (b) Certification Bodies (CB). One can read:

a) the Evaluation Facility
   i. either has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO 17025 or in accordance with an interpretation thereof approved by all participants and has been licensed or approved in accordance with Annex B.3,
   ii. or has been established under the laws, statutory instruments, or other official administrative procedures valid in the country concerned and meets the requirements laid down in Annex B.3 to this Agreement;
b) the CB is accepted as compliant, and
   i. either has been accredited in its respective country by a recognised Accreditation Body in accordance with EN 45011 or in accordance with a national interpretation of EN 45011 which at minimum satisfies the requirements as specified in Annex C of this Agreement,

[30] https://www.sogis.org/documents/mra/20100107-sogis-v3.pdf
[31] Recently, the CCDB has approved a resolution to limit the validity of mutually recognized CC certificates over time to 5 years.

ii. or has been established under laws, statutory instruments, or other official administrative procedures valid in the country concerned and meets the requirements of EN 45011 or the requirements laid down in Annex C of this Agreement."

The Agreement describes the role of CB in the scheme in the following way (still Article 5):

(..) the CB shall undertake the responsibility for the monitoring of all evaluations in progress within the Scheme at an appropriate level, and carrying out other procedures to ensure that all IT Security Evaluation Facilities affiliated with the CB:

- perform evaluations impartially;
- apply the criteria and methods correctly and consistently;
- have and maintain the required technical competencies; and
- adequately protect the confidentiality of protected information.

Annex B.1 of the agreement contains high-level requirements for the Evaluation and Certification scheme (national scheme), B.2 – for the CB, and B.3 – for Evaluation Facilities.

The Agreement imposes specific responsibilities on the CB with regard to the consistency of the structure and the maintenance of high-level technical competence standards of evaluations. For that purpose, a policy (licencing or approval) towards this direction shall be established and implemented by the CB.

Annex B.2 expands the CB obligations related to the scheme operations indicated in Article 5. One of the most interesting requirements is this under letter a), i.e. the CB authorises the participation of Evaluation Facilities in the Scheme. Furthermore, it is within the CB responsibility to avoid that an Evaluation Facility is licensed by more than one Compliant CB of the Agreement. Nevertheless, such a situation is possible only under the specific agreement of the CBs concerned, and parties of such an agreement are obliged to inform the SOG-IS Management Committee.

It should be noted that the implementations of requirements contained in B.2 are different in various national schemes, see for example discussion on license policies for ITSEFs in section 4.2 "Licensing and supervising" of a relevant ENISA study[32]. Therefore, a need for checking the equivalency of practices has been clearly identified, and in fact it is a core activity of the JIWG performed with the Voluntary Periodic Assessment (VPA) procedure.

Again, an additional requirement is set up in case the scheme is not only an Authorizing participant but a Qualified one as well. Under such circumstances, the CB is obliged to provide technical support to activities relating to this Agreement in accordance with the provisions of this Agreement. It is not clear what kind of activities are mentioned here, but it can be assumed they include developing and implementing JIL Supportive documents on minimal requirements imposed on ITSEF and developers for all evaluation levels and all types of products.

Several requirements for CBs are listed in Annex C of the Agreement. They address the issues such as organisational structure, certification personnel, Documentation and Change control, Certification procedures, Quality manual, relations with Evaluation Facilities, Certificate management, Confidentiality and Publications, Periodic review of the scheme. In particular, CB are expected to:

- "to ensure that ITSEFs have appropriate competencies in the field of IT security and vulnerability analysis; "(B2/c)

[32] https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe

- "to monitor all evaluations in progress within the Scheme at an appropriate level and to ensure that thetechnical monitoring required by the agreement is performed by technical personnel of the governmental body as part of the CB." (B2/ f)

Annex B.3 is related to the ITSEFs, and first, it addresses two important issues, i.e. accreditation and licensing. The accreditation part describes general requirements with regard to impartiality and to generic technical, methodological and procedural competence and in particular that ITSEF meets the requirements of ISO/IEC 17025 as far as these requirements are consistent with the peculiarities of the of IT security domain. The licensing part relates to capabilities of ITSEF regarding technical competence in the specific field of IT security evaluation and in the considered IT technical domain. It also relates to the capacity to fully comply with the rules of the concerned Scheme. This not only includes demonstrating the ability to apply evaluation criteria and methods correctly and consistently, but also the compliance to stringent security requirements necessary for the protection of sensitive or protected information relating to IT products or protection profiles under evaluation and to the process of evaluation itself.

Overall, the CBs are given responsibilities for running the scheme and maintaining its consistency, high level of competences, and quality of processes. Any national scheme being an Authorized or Qualified participant can issue conformant certificates. The key challenge, however, is to share a platform for unification of all requirements necessary for recognition of certificates among participants of the Agreement. It will be discussed in section 4.8.

4.6 TEST METHODS USED IN THE IT SECURITY EVALUATIONS

Evaluation has been the traditional means of gaining assurance, and is the basis of ISO/IEC 15408 approach. Evaluation techniques can include:

- Analysis of the TOE security problem definition (assets and threats), and consistency of the requirements identified to address this security problem;
- analysis of the TOE design representation against the security functional requirements;
- analysis and checking of process(es) and procedure(s) against the security assurance requirements;
- analysis of the correspondence between different levels of TOE design representations;
- verification of proofs;
- analysis of guidance documents;
- analysis of functional tests developed and the results provided;
- independent functional testing;
- checking against publicly available vulnerability databases;
- vulnerability analysis (including flaw hypothesis/penetration testing);
- security audit on developer premises, including checking that process(es) and procedure(s) are being applied.

ISO/IEC 15408 asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon (see ISO/IEC 18045, Clause 5.3 ISO/IEC 15408 *Evaluation assurance scale*):

- scope -- the effort is greater because a larger portion of the IT product is included;
- depth -- the effort is greater because it is deployed to a finer level of design and implementation detail;
- rigour -- the effort is greater because it is applied in a more structured, formal manner.

The increasing level of effort is formalized by establishing scaled security assurance components. For example, the AVA_VAN (vulnerability analysis) component characteristics are presented in the table below:

	Baseline activities		Pen test scope based on:				Pen test strength with assumed attack potential of:			
	Formal assessment of the documentation compliance	Public domain research to identify known vulnerabilities	publicly known identified vulnerabilities	potential vulnerabilities identified after independent analysis of the TOE	the identified potential vulnerabilities to determine the TOE resistancy against specific attack	the identified potential vulnerability to determine methodicaly the resistance of TOE against attack excercized in the operational	Basic	Enhanced-Basic	Moderate	High
AVA_VAN.1 Vulnerability survey	√	√	√				√			
AVA_VAN.2 Vulnerability analysis	√	√	√	√			√			
AVA_VAN.3 Focused vulnerability analysis	√	√	√	√	√			√		
AVA_VAN.4 Methodical vulnerability analysis	√	√	√	√	√	√			√	
AVA_VAN.5 Advanced methodical vulnerability analysis	√	√	√	√	√	√				√

Table 1: Evaluation activities for AVA_VAN assurance component (source: ISO/IEC 15408-3, Clause 15.2)

In addition to the generic evaluation methodology, specific extensions in dedicated technical domains have been adopted by the SOGIS participants, (for example, with regard to application attack potential to smart cards[33], hardware devices with security box[34] and points of interaction (terminal payments)[35]).

Some illustrative guidelines, referred to as “Attack Methods” mandatory to be understood by ITSEF labs, have a controller distribution due to their sensitivity. However, they are available to any developer registered for an evaluation in Europe. These documents describe the application of generic attack methods examples for IT products ie. smart cards, hardware devices with security boxes and payment terminals.

4.7 STRUCTURE OF SOG-IS

4.7.1 Elements of the structure

The SOGIS structure is presented in Figure 2. All entities included in the figure are presented below.

[33] https://www.sogis.org/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf
[34] https://www.sogis.org/documents/cc/domains/hardware_devices/JIL-%20Application-of-Attack-Potential-to-Hardware-Devices-with-Security-Boxes-v2-0-(for_trial_use).pdf
[35] https://www.sogis.org/documents/cc/domains/hardware_devices/poi/JIL-Application-of-Attack-Potential-to-POIs-v1-0_2011_06_09-for_trial_use.pdf

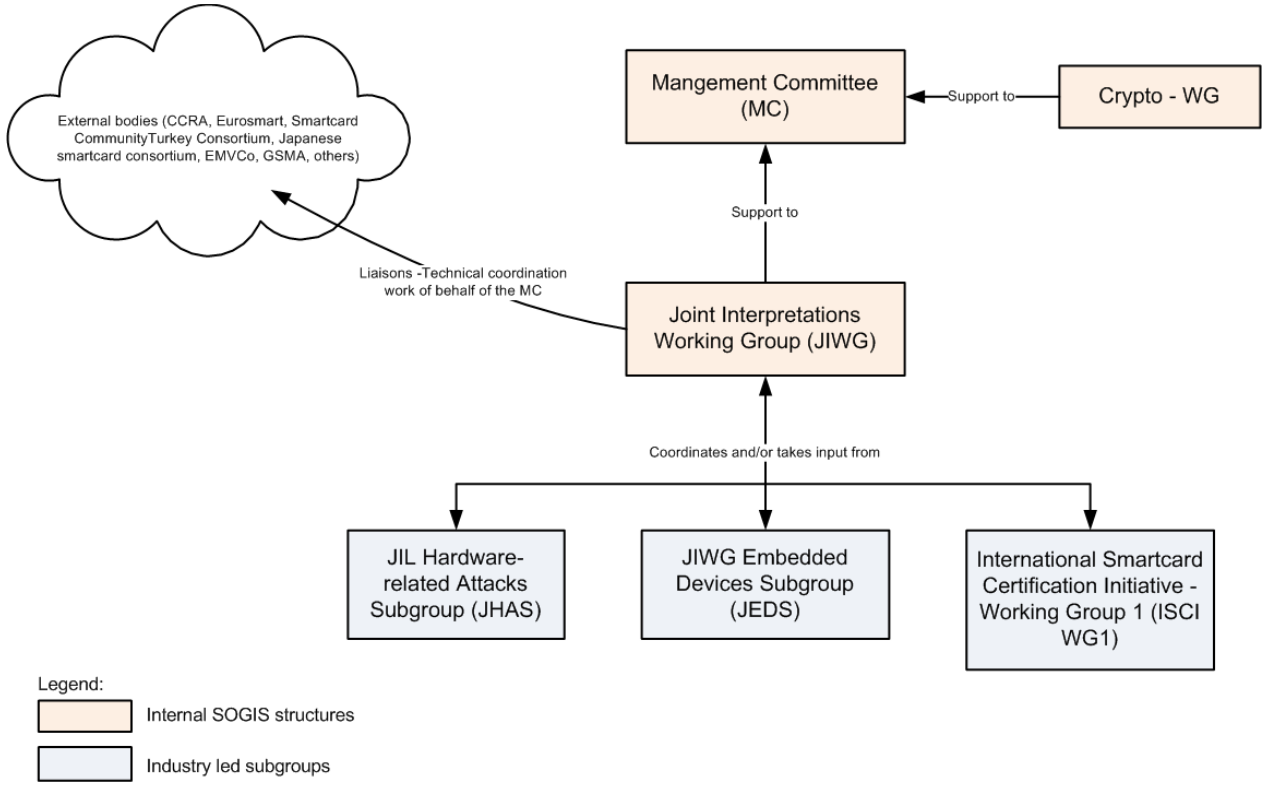

Figure 2: The SOG-IS MRA organisational structures

The **Management Committee (MC)** is responsible for administering the Agreement (see Article 10). The Chairman of the Management Committee is elected by the Management Committee itself for a 2-year term of office. The Chair is supposed to provide administrative support for the MC.

According to Annex H.1 "the Management Committee acts in any matters of policy relating to the status, terms, and operation of this Agreement. It decides upon the compliance of CBs and defines the procedures to address the application of CBs(...)".

Other responsibilities of the MC are dispersed among several SOG-IS procedures (e.g. VPA, see below).

The MC is directly supported by the **Joint Interpretations Working Group (JIWG)**. According to Article 10, JIWG provides technical advice and recommendations to the Management Committee, works on interpretations, including list of types of attacks related to IT technical domains within the scope of Agreement.

JIWG is working under its Terms of Reference [36](ToR). ToR specifies some constraints with regard to the membership. JIWG is limited to Authorized and Qualified participants. Other participants could join the JIWG at the discretion of Management Committee up to a numerical limit set up by the MC. The JIWG membership is unconditionally limited to governmental organisations representing participants in the MRA.

- According to the ToR, tasks of the JIWG include:
- "developing and recommending procedures for the conduct of the business of the MRA;

[36] https://www.sogis.org/documents/mra/JIWG%20ToR%20v2.2.pdf

- recommending revisions of the MRA under the mandate of the MC;
- advising on the technical disagreements about the terms and application of the MRA;
- harmonising MRA scheme practices;
- developing and managing the JIWG supporting documents as to the background to interpretations and advising on any resultant decisions that could affect the application of either the criteria or methodology. This includes developing list of types of attacks to be considered for IT technical domains;
- proposing new IT technical domains and the assurance level and augmentations for which recognition can be claimed by the Qualified participants;
- technical support to EU bodies developing regulations in this area."

As pointed out in the „JIL document submission and approval procedure" (bullet no 7), „*The creation of a new JIL document or update shall be done in most cases by a subgroup, but if needed the JIWG may create a JIL document themselves*". In case the first option applies, the JIWG coordinates and/or takes input from the work of a number of industry-led sub-groups including:

- JHAS (JIL Hardware-related Attacks Subgroup)
- JEDS (JIWG Embedded Devices Subgroup)
- ISCI WG1 (International Smartcard Certification Initiative - Working Group 1)

A procedure called „*JIL subgroup participation rules*[37]" sets up the co-operation rules between the JIWG and a given subgroup.

The procedure restricts the participation to meetings to productive parties, and excludes parties wanting to attend only for training purpose. . However, this restriction cannot be used to arbitrarily exclude a specific developer, as long as they have an actual evaluation activity in Europe .

As participation for ITSEF and CB qualified for the related technical domain is mandatory and are not defrayed for this, SOG-IS want to ensure that meetings would be productive and useful for participants Capacity building is encouraged but outside the meetings.

Subgroups work under their ToRs (non-public documents), approved by the JIWG. These documents, and the procedure itself, contain strict confidentiality rules with regard to sensitive subjects of discussions such as the Attack Methods in a given technical domain what is reflected in limited distribution, i.e. the consumers SOGIS participants do not receive by default all documents produced by the sub-group but all SOGIS participants are invited to join the JIWG (even as observer only) and will consequently receive all the inputs.

The last organisational unit in the SOGIS structure is **Crypto WG**. This group works directly with the MC, and there are no publicly written rules for its objectives and *modus operandi*. According to the public announcement, *"The SOG-IS Crypto WG is in charge of providing the SOG-IS MC with technical support for the establishment of a SOG-IS Crypto Evaluation Scheme, i.e. a set of requirements and evaluation procedures related to cryptographic aspects of Common Criteria security evaluations of IT products and mutually agreed by SOG-IS participants.*

The document « SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms » is primarily addressed to evaluators and developers. Its purpose is to specify which cryptographic mechanisms are recognised and agreed upon, i.e. ready to be accepted by all SOG-IS participants. For each of the main types of symmetric and asymmetric cryptographic mechanisms, a table summarising the set of all the agreed mechanisms of that type is provided. A result of an evaluation performed under the SOG-IS Crypto Evaluation Scheme is that a user of the target of evaluation (TOE) can get the assurance that she only uses agreed cryptographic

[37] https://www.sogis.org/documents/mra/JIL-SG-rules-v1.0.pdf

mechanisms. General and specific notes on how to implement/evaluate the various agreed cryptographic mechanisms correctly are also provided, as well as requirements related to key management."

4.7.2 Other issues

There are no specific provisions on intellectual property rights (IPR) in the Agreement. In practice, all JIL supportive documents are labelled in a unified way with a trademark consisting of the text "Joint Interpretation Library" and logo with Europe's map inside. Any internal document is equipped with the SOG-IS logo as presented in the Agreement, Annex E.

With respect to the sensitive information handling the Agreement introduces a concept of "protected information" defined as: "*Information gathered or obtained under the processes or activities in this Agreement whose unauthorised disclosure could reasonably be expected to cause (i) harm to competitive commercial or proprietary interests, (ii) a clearly unwarranted invasion of personal privacy, (iii) damage to the national security, or (iv) otherwise cause harm to an interest protected by national law, subsidiary legislation, administrative regulation or official obligation*". Rules for the exchange of sensitive information including labelling documents are contained in Annex G.

It is worth noting that the JIWG is currently working on the procedure for vulnerability disclosure related to certified products. This procedure is to describe information flow and the sequence of activities of the CBs, ITSEFs and developers concerned. Part of the information exchanged can be considered as confidential, at least to a specific point in time.

4.8 QUALITY MEASURES AND PEER ASSESSMENT

4.8.1 General

From the Agreement perspective, maintaining the quality of issued certificates within the SOG-IS framework of schemes should be considered in two aspects.

First, all national schemes are required to ensure consistent application of the criteria and methods between Evaluation and Certification Schemes. The quality measures identified in the Agreement are:

- common baseline requirements to be met by CBs and Evaluation Facilities with specific responsibilities imposed on CBs to achieve "the goal of consistent, credible and competent application of the criteria and methods" (discussed in section 4.8.3),
- continual work towards a uniform interpretation of the currently applicable criteria and methods and the schemes' commitment to accept the JIWG supporting documents that results from this work (discussed in section 4.5).

Second, the Agreement (Article 6) defines a mechanism for a peer assessment of compliant CBs, called Voluntarily Periodic Assessment (VPA), which should take place on a regular basis. The purpose of VPA is to assure that the participant continues to share the Agreement objectives. The mechanism is "voluntarily" as the participant can refuse or cancel the assessment at any stage.

It is interesting to note that the Agreement does not contain any provision, which allows excluding the participant based on the fact one cannot prove the participant is still committed to sharing the objectives. However, based on the VPA results the rest of participants can agree not to recognise certificates issued by relevant Participant any longer (they cannot be considered as conformant certificates according to Article 5). Such a situation has not happened yet.

The maximum period between two peer assessments for a given CB is set to 5 years.

4.8.2 Peer assessment

Peer assessments performed for Authorized participants by the CCRA are reused by the SOG-IS and focus only on the gap between the two i.e. SOG-IS MRA and CCRA (there is no need to duplicate efforts). For any peer assessment, a non-Authrized SOG-IS participant can nominate an observer, but the SOGIS rule is that two Authorized or Qualified Members of SOG-IS MRA must be represented in the assessment team.

The MC initiates the peer assessment, accepts experts proposed to the assessment team and finally approves the report from the VPA based on the recommendation from JIWG.

The assessment team chooses specific evaluation and certification processes (for two selected IT products) and performs detailed analysis, including the documentation review, on-site visits, both in the CB and relevant ITSEF facilities, and finally, preparation of a report.

A SOG-IS-shadow-VPA procedure (marked as for trial use) regulates the process, information flow, timing, checklists and interpretation of results.

4.8.3 New Authorized/Qualified Participant

A separate measure for confirming the quality of operations is reserved for these members requesting for the first time the status of the Authorized participant. This VPA instance is called ‘shadowing’.

Several conditions for compliance apply, and they include submitting the following (see Annex G.2):

- scheme documentation,
- list of certificates claiming to be conformant to the rules issued to date (min. 2),
- statements of legal nature related to any applicable national laws which could limit or disturb mutual recognition of certificates,
- information where the CB has already been granted a qualifying status through a similar procedure within the framework of another international Mutual Recognition Agreement (MRA), all necessary information on this Qualifying status and this MRA.

The MC performs a preliminary assessment of the application and decides whether the application is to be:

a) rejected,
b) accepted for further proceedings,
c) accepted without any further action upon recognition of relevant status done by other international MRA (in practice, this related to the activities of CCRA).

In case of option b) the applicant submits at least two IT products as candidates for a procedure called “shadow certification”. Upon accepting the candidates, the MC nominates the assessment team in a similar way as for the VPA. Again, the team consists of 2 experts representing Qualifying participants. Any Authorizing participant can nominate its expert (however, on its own expense), and any participant – an observer.

The shadow certification is performed in a similar way to VPA, and it ends with the assessment team’s recommendation on the acceptance or rejection of the application, subject to the decision of MC (in case of acceptance it shall be taken unanimously).

Achieving the higher level of recognition (i.e. the qualified participant status) requires that the applicants fulfil additional requirements including (see Annex G.4):

- submitting relevant documentation,

- proposing candidates for shadow certification (at least 2 per the technical domain the application is related),
- performing specific vulnerability analysis related to the products chosen, deemed as necessary by the MC,
- accepting the audit "on-site" done at the premises of relevant ITSEFs performing the product evaluation.

The prerequisites for the applicant to be fulfilled are:

a) to have the status of compliant CB (Authorized participant) for the EAL4 level under the Agreement for more than one year; and
b) to have issued at least three conformant certificates recognised under the Agreement.

Again, the assessment is performed in a similar way to two others. However, in this case, only qualifying participants could nominate experts for the assessment team, for obvious reasons.

4.9 IDENTIFYING SURVEILLANCE METHODS APPLIED TO THE NATIONAL SCHEME OPERATIONS UNDER THE SOG-IS MRA

4.9.1 Introductory remark

As stated in section 4.3.1 being classified as similar to the ISO/IEC 17067 type 1a scheme, no mandatory surveillance process is required by SOG-IS nor CCRA schemes. However, there are some activities, which can be considered as the follow-up processes, and they are discussed below.

4.9.2 Maintenance for certified products

All maintenance activities for issued certificates including setting up the validity periods are left to internal regulations of relevant national schemes. SOG-IS and CCRA agreements apply a maintenance process, that should not be confused with surveillance as maintenance does not include actual evaluation tests on the product. Maintenance reports for certificates are issued and published by relevant CBs. Some CBs have defined voluntary surveillance/reassessment processes, that take into account the evolution of the state-of-the-art with relevance to previously certified product. Neither CCRA nor SOGIS have actually harmonized this process yet although this topic is currently subject to discussion.

The only requirement existing in the Agreement is related to conformity conditions described in Article 5. If the certificate does not meet the requirements to with regard to conformity it cannot be mutually recognised by other SOG-IS Participants but usually it is related to initial certifications only.

Facing turbulences for certified products related to the ROCA vulnerability[38] the SOG-IS participants have recently identified differences in dealing with such unexpected issues among the participants. For that reason, the JIWG has started working on a procedure of disclosing and handling vulnerabilities. However, this work is not finished yet, nor any outcome is published.

4.9.3 Surveillance for Protection Profiles

Maintaining of PPs is a sole responsibility of the editor. JIWG has a passive role in this process, according to the procedure "MC PP Endorsement Procedure" (see section 4.4.3).

[38] https://crocs.fi.muni.cz/public/papers/rsa_ccs17

5. COMPARING THE REQUIREMENTS OF ARTICLE 47 AND SOG-IS MRA

5.1 INTRODUCTION

This section contains the gap analysis that compares the requirements from article 47 of [CSA_P] to the SOG-IS scheme. The approach of the gap analysis is as follows:

- Every single provision of article 47 from [CSA_P] is treated separately.
- Each such provision is compared to the current state of the SOG-IS scheme and discussed.
- If any provision was found that would make the application of the SOG-IS Agreement impossible in general, it will be explicitly marked.
- Primarily, it is the objective of the analysis to map the requirements from article 47 to a requirements or regulations laid down in the SOG-IS agreement itself ([SOGIS]).
- Only if the provision is not covered "as is" within the Agreement itself, other aspects of the SOG-IS have been used for argumentation.

5.2 MAPPING OF ASPECTS OF ARTICLE 47 TO ASPECTS OF SOG-IS MRA

The following subsections present an analysis between the [CSA_P] provisions within Article 46 and the SOG-IS Agreement as defined in [SOG-IS]. Every provision of [CSA_P] is discussed within a separate subsection.

5.2.1 Scope of the scheme

Art. 47 par.1a	**A European cybersecurity certification scheme shall include at least the following elements:** **(a) subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services covered as well as an elaboration of how the certification scheme suits the needs of the expected target groups;**
	Schemes under SOG-IS are pure IT product certification schemes and do not pertain requirements for the certification of IT services or IT processes. The SOG-IS Agreement does not limit the application of its requirements to any product type or category. However, recognition of certificates on higher assurance levels (EAL5-7) is limited to products of certain technical domains that are identified in the agreements. At the time that this report is written, these are "Smartcards and Similar Devices" and "Hardware Devices with Security Boxes"

5.2.2 Reference to standards

Art. 47 par.1b	**(b) reference to international, European or national standards followed in the evaluation. Where standards are not available, a reference shall be made to technical specifications that meet the requirements of Annex II of Regulation 1025/2012 or, if such are not available, to technical specifications or other cybersecurity requirements defined in the scheme**
	As outlined in section 4.1 the SOG-IS agreement refers to the internationally recognized standard known as Common Criteria. The Common Criteria maintain a dedicated recognition agreement and are also standardized within as ISO/IEC 15048-1/2/3. As such, the SOG-IS agreement meets article 47 1 b), sentence 1 but some adjustments or extensions are needed to fully align aspects relevant to operating procedures, including the JIWG and the

	JIWG Subgroup rules and ensure that the requirements of Annex II of Regulation 1025/2012 are respected.

Note #1: It should be further explored whether the SOG-IS scheme should only be used in combination with the internationally requirements of Common Criteria (aka ISO/IEC 15408).

5.2.3 Assurance Levels

Art. 47 par.1c	**(c) where applicable, one or more assurance levels;**
	Common Criteria that are used by the SOG-IS scheme offer seven (7) assurance levels named EAL 1-7 (EAL=Evaluation Assurance Level) as defined in the Common Criteria. As such, the SOG-IS agreement meets article 47 1 c). By the use of assurance levels defined in Common Criteria, the SOG-IS agreements de facto covers all levels (basic, substantial and high) that are mentioned in the [CSA_P] . *Note: It can be discussed whether an implementation of the SOG-IS Agreement as an implementation of article 47 of the [CSA_P] should consider all these levels or whether the application should be limited*

Note #2: It should be further discussed whether an implementation of the SOG-IS Agreement as an implementation of article 47 of the [CSA_P] should consider all these levels or whether the application should be limited

5.2.4 Requirements for conformity assessment bodies

Art. 47 par.1c a	**(ca) where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;**
	While the SOG-IS agreement leaves a lot of the concrete implementation of the scheme to the certification bodies in the authorising participants, it implements a very strong mechanism to ensure the quality of these bodies. As discussed in section 4.8.2 the SOG-IS scheme contains clear requirement on peer assessments to ensure that all authorising participants follow the same regulations and present comparable quality performance.

5.2.5 Specific evaluation criteria

Art. 47 par.1d	**(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;** **Where article 45 of [CSA_P] reads:** **A European cybersecurity certification scheme shall be so designed as to achieve, as applicable, at least the following security objectives:** **(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure during the entire process, product or service lifecycle;** **(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire process, product or service lifecycle;** **(c) authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;** **(d) record which data, functions or services have been accessed, used or otherwise processed, at what times and by whom;**

	(e) it is possible to check which data, services or functions have been accessed, or used or otherwise processed, at what times and by whom; **(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;** **(g) ICT processes, products and services are provided with up to date software and hardware that do not contain publicly known vulnerabilities, and are provided mechanisms for secure updates;** **(h) ICT processes, products and services are developed, manufactured and supplied according to the security requirements stated in the particular scheme.**
	The Common Criteria (which are used by the SOG-IS scheme) are agnostic of concrete functional requirements. However, all security objectives as listed in article 47 1 (d) can be easily expressed using specific security functionalities as described in ISO/IEC 15408 part 1 and 2. The way of expressing any security functionality for a given IT product is to use a security model as described in ISO/IEC 15408-1 and develop a technical specification in the form of Security Target or Protection Profile (see discussion in section 4.4).

In particular, for a specific type of products, Protection Profiles can be used to describe a specific security problem which requires a set of dedicated assurance and functional requirements that this security problem. Protection Profiles are developed and maintained or recommended to use by the certification authorities of the SOG-IS Agreement.

Last, but not least, it has to be mentioned that the SOG-IS schemes and the underlying standards are focused on IT product evaluations and certifications and can usually not be used to certify IT processes or IT services.

In summary, the question whether this [CSA_P] requirement is met by the SOG-IS Agreement cannot be completely answered by this analysis and should be further discussed during the actual transposition process.

Note #3: The SOG-IS scheme supports the use of Protection Profiles and this concept is key to the implementation of article 47, 1 (d). It should be further discussed, how a central repository of Protection Profiles in the context of [CSA_P] can be achieved and how Protection Profiles for relevant IT products should be developed.

5.2.6 Information to be supplied to the conformity assessment body

Art. 47 par.1 (e)	**(ca) where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;**
	The methodology used with respect to evaluations compliant to Common Criteria, and in particular Common Evaluation Methodology, requires specific documentation to be submitted by an applicant. The granularity and volume of documentation depends on the evaluation assurance level (EAL) the applicant claims to achieve for the subject of evaluation (usually, the higher assurance level, the more detailed documentation).

5.2.7 Marks and labels

Art. 47 par.1 (f)	**(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;**
	Annex E of the SOG-IS agreement presents a mark that can be used if a certificate has been obtained under the rules of the SOG-IS agreement (see Figure 1) and the rules to adhere to.

It should be noted that additional visual information might need to be added on the mark.

Note #4: Aspects around the IP and copyright for the use of the logo from the SOG-IS scheme should be further discussed

5.2.8 Monitoring compliance

Art. 47 par.1 (g)	**(g) rules for monitoring compliance with the requirements of the certificates or the EU statement of conformity, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;**
	The SOG-IS scheme does not contain any requirements on monitoring compliance.

Note #5: A mechanism for monitoring compliance will have to be established. Existing mechanisms of the SOG-IS scheme (specifically the approach of maintenance) should be taken into consideration. Currently, there are no known aspects of the SOG-IS scheme that should contradict such a development, however, currently, such a process can be initiated by the risk owner as a means of monitoring compliance through voluntary re-assessment.

Following consultation with SOG-IS MRA participants, a proposed approach to address this provision, in addition to 5.2.11, is as follows:

- CABs to establish the validity period of certificates, as defined in the draft CCRA document: certificate will be valid for 5 years.
- CABs to work on improving evaluation methods, so that assurance gained in the initial certification retains some of its validity on later updated versions (e.g. by evaluating the patch mechanisms on the product and patch processes from the developer), where evidence can be produced that those updates are issued according to a pre-defined set of requirements.
- Manufactures/Developers shall:
    - carry out an Impact analysis of all changes over the course of the product's life cycle, including fixes for errors and vulnerabilities, and minor functional modifications to the product;
    - monitor CVEs and other published security vulnerabilities that may apply to the certified product, and submitting an impact analysis where necessary to their CAB;
    - demonstrate that actions taken allow to maintain the security level; a responsible and public communication on analysis resulting from the previous points, including liaising with the CAB and its national CERT - part of the International CERT community - for the publication, where necessary, of a specific CVE associated to the product;
    - handling complaints received from their clients and responding to them with appropriate measures.
- CABs shall carry out a periodic review of certificates issued based on a security assessment from an ITSEF that takes into account the impact analysis of accumulated changes from the previous evaluation and an updated State of the Art, in order to confirm the validity of the issued certificate.
- CABs shall withdraw issued certificates in case:
    - there is evidence that the developer does not respect its commitments;
    - a security reassessment has led to a FAIL verdict and no correction may apply.

Note: #5.1: In order to allow the certificates to cover the corrected versions of a certified product, this might imply that the certificate regards the evaluated version x.y.1 and all following minor versions x.y.2 based on the permanent monitoring process.

Note: #5.2: Part of these requirements might be covered by a better use of existing flaw remediation requirements from the Common Criteria (ALC_FLR.x).

5.2.9 Granting, renewing, maintaining, continuing, extending and reducing the scope of certification

Art. 47 par.1 (h)	**(h) where applicable, conditions for granting and renewing a certificate, as well as maintaining, continuing, extending or reducing the scope of certification;**

The SOG-IS Agreement itself does not define the conditions for granting and renewing a certificate. The concept of maintenance and re-certification is identified by the SOG-IS participants but its implementation is left to national schemes and is not regulated on the Agreement level.

However, due to the approach of peer assessment (see section 4.8.2) is ensured that all participants use comparable processes and procedures.

The same holds for procedures about maintaining, continuing, extending or reducing the scope of a certification.

Note: #6: Conditions for granting and renewing a certificate as well as maintaining, continuing, extending or reducing the scope of certification should be defined more explicitly. In this context it should be carefully discussed what "reducing the scope of a certification" actually means. The implemented requirements from the certifications schemes that are authorizing participants of the SOG-IS scheme can be used as the basis for this implementation. It should also be noted that such discussions have already been initiated both within SOG-IS and CCRA.

5.2.10 Consequences of non-conformity

Art. 47 par.1 (i)	**(i) rules concerning the consequences of non-conformity of certified or self-assessed ICT products and services with the requirements of the scheme;**

The SOG-IS Agreement does not contain any requirements concerning the consequences of nonconformity.

While the Agreement lists several conditions under which the certificate is considered as "conformant" and based on this it can be mutually recognized (see section 4.8.1), there are no provisions what should be done if the certified product, for various reasons, does not comply with the requirements any longer. This is left to national schemes to deal with such cases.

Note: #7: Requirements concerning the consequences of nonconformity will have to be discussed and defined. There are no known aspects of the SOG-IS scheme that should contradict such a development.

During the consultations, it was noted that should withdrawal of an already issued certificate be considered as a consequence of non-conformity, secondary effects could be introduced if for example the certificate was mandatorily required during a public sector procurement process.

5.2.11 Dealing with undetected cybersecurity vulnerabilities

Art. 47 par.1 (j)	**(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT processes, products and services are to be reported and dealt with;**
	The SOG-IS Agreement does not contain any provisions for dealing with vulnerabilities undetected during IT security evaluations.

Note: #8: Rules concerning how previously undetected cybersecurity vulnerabilities in ICT processes, products and services are to be reported and dealt with have to be discussed and defined. The activities that have already been started by the SOG-IS JIWG in this area should be taken into consideration.

Following consulation with SOG-IS MRA participants, the provision of 5.2.8, could also be adopted.

Note: #8.1: Attention should be drawn to international standards which have been adopted in December 2018 as European standards in the subject matter ie.

- ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure
- ISO/IEC 30111 Information technology -- Security techniques – Vulnerability handling processes

5.2.12 Retention of records

Art. 47 par.1 (k)	**(k) where applicable, rules concerning the retention of records by conformity assessment bodies;**
	The SOG-IS Agreement references ISO/IEC 17025 as the standard that shall be met by the conformity assessment bodies (which are the evaluation bodies in the SOG-IS agreement). ISO/IEC 17025 in turn contains requirements that certain documents and information need to be kept by the evaluation body. Similar provisions are adopted for Certification Bodies although it should be noted the Agreement references obsolete standards EN 45011 and its national interpretations, and it should be replaced by ISO/IEC 17065, according to the EU Regulation 765/2008. From that perspective, the SOG-IS Agreement meets the requirements from article 47 1, (k). However, it is worth mentioning that the SOG-IS Agreement does not mandate any concrete period for which records have to be kept. This is left to the national certification bodies.

Note: #9: A concrete period for the retention of records should be discussed and explicitly specified. It should be unified based on practices implemented in national schemes. A typical period would be to keep all records documenting evaluation and certification processes until 5 years after the certificate is expired.

5.2.13 Identification of other schemes

Art. 47 par.1 (l)	**(l) identification of national or international cybersecurity certification schemes covering the same type or categories of ICT processes, products and services, security requirements and evaluation criteria and methods;**
	(l) identification of national or international cybersecurity certification schemes covering the same type or categories of ICT processes, products and services, security requirements and evaluation criteria and methods;

Note: #10: An overview of other national or international schemes covering the same product(s) should be added to address article 47, 1, (l).

5.2.14 Content of the certificate

Art. 47 par.1 (m)	**(m) the content of the issued certificate or the EU statement of conformity;** **(ma) the period of the storage of the EU statement of conformity and the technical documentation of all relevant information by the manufacturer or provider of ICT products and services;** **(mb) maximum period of validity of certificates;** **(mc) disclosure policy for granted, amended and withdrawn certificates;** **(md) conditions for the mutual recognition of certification schemes with third countries;** **(me) where applicable, rules concerning a peer review mechanism for the bodies issuing European cybersecurity certificates for high assurance levels pursuant to Article 48(4a).**
	The SOG-IS agreement identifies the relevant content for its certificates in Annex J.1. As such, it can be said that the kind of requirements from article 47, 1 (m) are also considered by the SOG-IS agreement. However, the details that are required by the following list of bullet points in article 47 are not met by Annex J.1. The fact that a certificate should have a validity period has also been discussed within the Common Criteria community, leading to a proposal documented in [CERTVALIDITY].

5.2.15 Other requirements from Article 47

The following three paragraphs from Article 47 do not contain any concrete requirements on the scheme itself but rather address questions around the application of an existing scheme As such, they have not been considered in the analysis in this section.

"(2) The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.

(3) Where a specific Union act so provides, certification or the EU statement of conformity under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.

4. In the absence of harmonised Union legislation, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements."

6. OTHER RELEVANT ARTICLES OF THE CYBERSECURITY ACT PROPOSAL

6.1 INTRODUCTION

Article 47 of [CSA_P] has been the primary focus of this study. However, in the course of the work on the various aspects of this article, other parts of the [CSA_P] came into focus that also contained relevant information. While it is not the intention of this section to extend the scope of the study, the authors wanted to conserve this information and discuss shortly how the SOG-IS MRA is related to these provisions.

6.2 ASPECTS FROM ARTICLE 48

6.2.1 Paragraph 3

"A European cybersecurity certificate pursuant to this Article referring to assurance level basic or substantial shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44."

Note #11: The rule 'one CB per one country' under SOG-IS MRA (see section 4.3) should be further discussed in relation to provisions from Article. 51.

6.2.2 Paragraph 4

"By way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity certification scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such body shall be one of the following:

a) a national cybersecurity certification supervisory authority referred to in Article 50(1);
b) a public body that is accredited as conformity assessment body pursuant to Article 51(1)"

Note #12: Criteria to be met for being CB or ITSEF (see section 4.3.2), should be further discussed in relation to the aforementioned provisions.

6.2.3 Paragraph 4a

"In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate can only be issued by a national cybersecurity certification authority referred to in Article 50(1) or, under the following conditions, by a conformity assessment body referred to in Article 51:

a) upon prior approval by the national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; or
b) upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority."

Note #12: Criteria to be met for being CB or ITSEF (see section 4.3.2), should be further discussed in relation to the aforementioned provisions.

6.2.4 Paragraph 5

"The natural or legal person which submits its ICT processes, products or services to the certification mechanism shall make available to the conformity assessment body referred to in Article 51 or the national cybersecurity certification authority referred to in Article 50, where this authority is the body issuing the certificate, all information necessary to conduct the certification procedure."

Note #13: This provision is relevant to Article. 47 (1) e.

6.2.5 Paragraph 5a

"The holder of a certificate shall inform the body issuing the certificate about any later detected vulnerabilities or irregularities concerning the security of the certified ICT process, product or service that may have an impact on the requirements related to the certification. The body shall forward this information without undue delay to the national cybersecurity certification authority."

Note #14: This provision is relevant to Article 47 (1) j.

6.2.6 Paragraph 6

"Certificates shall be issued the period defined by the particular certification scheme and may be renewed, provided that the relevant requirements continue to be met."

Note #15: This provision is relevant to Article. 47 (1) m.

6.2.7 Paragraph 7

"A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States."

Note #16: This provision should be discussed in relation to SOG-IS Agreement provisions as currently not all Member States are participants.

6.2.8 Paragraph 6

"National cybersecurity certification supervisory authorities shall:

(aa) monitor and enforce the obligations of the manufacturer or provider of ICT products and services established in their respective territories set out in Article 47a(2) and (3) and in the corresponding European cybersecurity certification scheme;

(b) without prejudice to Article 51(1b), assist the national accreditation bodies in the monitoring and supervision of activities of conformity assessment bodies for the purpose of this Regulation

(ba) monitor and supervise the activities of the bodies referred to in Article 48(4);

(bb) authorise conformity assessment bodies referred to in Article 51(1b) and restrict, suspend or withdraw existing authorisation in cases of non-compliance with the requirements of this Regulation;

(c) handle complaints lodged by natural or legal persons in relation to certificates issued by the national cybersecurity certification authority or, in accordance with Article 48(4a) by conformity assessment bodies, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

(d) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on possible non-compliance of ICT processes, products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;

(e) monitor relevant developments in the field of cybersecurity certification."

Note #17: Further discussion is needed as some responsibilities of the cybersecurity certification authority could be in in conflict with current responsibilities of CBs.

6.2.9 Paragraph 7

"Each national cybersecurity certification supervisory authority shall have at least the following powers:

(a) to request conformity assessment bodies, and European cybersecurity certificate holders and issuers of EU statement of conformity to provide any information it requires for the performance of its task;

(b) to carry out investigations, in the form of audits, of conformity assessment bodies, and European cybersecurity certificates' holders and issuers of EU statement of conformity, for the purpose of verifying compliance with the provisions under Title III;

(c) to take appropriate measures, in accordance with national law, in order to ensure that conformity assessment bodies, or certificate holders and issuers of EU statement of conformity comply with this Regulation or with a European cybersecurity certification scheme;

(d) to obtain access to any premises of conformity assessment bodies and European cybersecurity certificates' holders for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, certificates issued by the national cybersecurity certification authority or, in accordance with Article 48(4a) by conformity assessment bodies that are not compliant with this Regulation or a European cybersecurity certification scheme;

(f) to impose penalties, as provided for in Article 54, in accordance with national law, and to require the immediate cessation of the breaches of obligations set out in this Regulation."

Note #17: Further discussion is needed as some responsibilities of the cybersecurity certification authority could be in in conflict with current responsibilities of CBs.

6.3 ASPECTS FROM ARTICLE 51

6.3.1 Paragraph 1

"The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation."

Note #18: This provision is (at least, partly) relevant to Article 47(1)k.

6.3.2 Paragraph 1a

"In cases where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to Article 48(4)(a) and Article 48(4a), the certification body of the national cybersecurity certification authority shall be accredited as conformity assessment body pursuant to paragraph 1 of this Article."

Note #19: This provision is (at least, partly) relevant to Article 47(1)k.

7. OUTLOOK

Following the analysis presented earlier the following points are raised with regards to the possible transposition of SOG-IS MRA to the European Cybersecurity Certification Framework established under the [CSA_P] . However, during the actual transposition process, all involved stakeholders will be expected to contribute towards identifying and nominating possible solutions and ways forward.

The main points identified are briefly presented below:

- Under consideration of the fact that the SOG-IS agreement has been developed before [CSA_P] , the agreement is a promising candidate for an implementation of a cybersecurity scheme in accordance with article 47 of [CSA_P] .
- No aspects of SOG-IS MRA have been found during the analysis that contradict a use of the SOG-IS agreement in the context of [CSA_P] article 47.
- SOG-IS is organized as a decentralized scheme and is heavily based on the concept of a peer review of its participants. This leads to the situation that some aspects that are important in the context of the implementation of article 74 of [CSA_P] are actually not implemented on the level of the agreement but rather by the participants of the scheme (on national level). If the SOG-IS agreement should be used as an implementation of article 47, one primary work item will be to identify the relevant processes in the evaluation and certification bodies of the authorizing participants of the SOG-IS agreement and to document them on the level of the scheme.

8. FURTHER CONSIDERATIONS AND POSSIBLE WAYS FORWARD

During the consultation process that was conducted with interested SOG-IS MRA participants, a number of considerations were brought up with regard to possible issues and challenges that are expected to be addressed during the actual transposition process. As these considerations were not part of the scope of the analysis conducted,, which is considered only as the first step towards a possible transposition, they are briefly presented below and it is expected that they will be further elaborated upon during the actual transposition process, in order to on the one hand capitalize on the proven experience and expertise or SOG-IS Agreement while on the other hand to adhere to the provisions of the final [CSA_P] text.

This study was conducted and concluded during Q1 2019. At that time, the Cybersecurity Act (Regulation (EU) 2019/881) was still on a proposal phase. The discussion and the analysis conducted within the scope of this document are based on the proposal document. Following the findings of the study, SOG-IS MRA participants initiated an internal process of drafting the successor of SOG-IS MRA based on the Cybersecurity Act provisions. Currently, the Cybersecurity Act has entered into force (Regulation(EU) 2019/881) and ENISA has already received a request by the EC to draft a candidate EU cybersecurity certification scheme on SOG-IS MRA successor. However this is not reflected in the study, in terms of wording and analysis of articles and provisions as the ones on Cybersecurity Act proposal and Regulation (EU) 2019/881 differ slightly. The current study was based on the Cybersecurity Act proposal, which was only available at that time.

8.1 CONSIDERATIONS

The relationship between the new scheme, CCRA and EEA countries

EU cybersecurity certification schemes should leverage and be built upon what already exists at national and international level. In addition to adherence and take-up of European and international standards, a possible candidate EU cybersecurity certification scheme based on SOG-IS MRA should also address the current connection with CCRA and EEA countries, towards putting forward harmonized and widely accepted schemes.

Role of Conformity Assessment Bodies

Conformity Assessment Bodies are expected to have a key role in the deployment and operation of the EU cybersecurity certification framework, under the supervision of National Cybersecurity Supervision Authorities. Given also the wide spectrum of products, services and processes to be certified, in addition to the expertise needed, provisions on the eligibility and inclusion of both governmental and private conformity assessment bodies under the scheme should be explored. Such an approach is considered to support and further promote the uniform deployment of the framework across all Member States by reducing possible barriers.

Support EU Single Market

The Single Market encompasses the EU's 28 Member States and refers to the EU as one territory without any internal borders or other regulatory obstacles to the free movement of goods and services[39]. The market has been extended, with exceptions, to Iceland, Liechtenstein and Norway through the Agreement on the European Economic Area (EEA)[40]. As a possible candidate EU cybersecurity certification scheme under the [CSA_P] , SOG-IS MRA, being an agreement between governmental agencies, will be expected to advance towards meeting the requirements and provisions of EU Legal Framework and eventually supporting and promoting the EU Single Market. Building upon the experience and expertise of current SOG-IA MRA participants, such a candidate scheme could further promote the cooperation, collaboration, openness and transparency across EU Member States, relevant stakeholders and third countries. In so doing, it is essential to build on existing national and international schemes, in particular SOG-IS MRA, and to make possible a smooth and timely transition under the proposed EU cybersecurity certification framework.

Extension of scope to also include services and processes

Taking into account the wide scope of the [CSA_P] and the different levels of assurance foreseen, a possible candidate EU cybersecurity certification scheme based on SOG-IS MRA, could be further expand and cover additional application areas while also considering the operational environment of the certified product(s).

8.2 ASPECTS AND PROVISIONS TO BE CONSIDERED

Towards the direction of the considerations discussed earlier and towards the establishment of an open and transparent scheme, a non-exhaustive list of SOG-IS aspects to be considered and revisited has been proposed by some SOG-IS MRA participants in an attempt to align to the [CSA2] provisions. This non-exhaustive list is presented below:

- **Article 1: Membership (consuming member)**: voting procedures for interested members to join the Agreement and veto for new members must be revisited, in addition to the status and role of EU/EFTA countries within the EU cybersecurity certification framework.
- **Article 1: Membership (producing members)**: the provisions of commercial certification bodies or multiple certification bodies authorized by a Participant must be revisited.
- **Article 6: Voluntary Periodic Assessment**: aspects of certification bodies approval procedure must be revisited.
- **Article 9: New participants and compliant CBs**: similar to Article 1: Membership (consuming member) where a review of relevant MRA provisions is recommended.
- **Article 11: Disagreement**: provisions relevant to non-recognition and possibly processes for overcoming disagreements must be revisited.
- **Article 18: Effects of this Agreement**: provisions related to substantive or procedural rights, liabilities or obligations must be revisited.

Furthermore, aspects relevant to the operating procedures, Terms of Reference (ToR) of groups and subgroup rules will also have to be revisited towards ensuring and promoting compliance with [CSA2] provisions.

[39] http://ec.europa.eu/growth/single-market_en
[40] http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf

BIBLIOGRAPHY/REFERENCES

[CSA_P]	COM(2017) 477 final 2017/0225 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") Available at: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf
[CSA2]	Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") Available at: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf
[SOGIS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, VERSION 3.0, MANAGEMENT COMMITTEE of SOG-IS, January 2010
[CERTVALIDITY]	Common Criteria Recognition Arrangement Management Committee Operating Procedures, Subject: Certificate validity, Document Number: 2017-01-23, Version: 1.0 draft 0.5
[ITSEC]	Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom, 1991
[BSIApplicationForm]	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Antrag_Produktzertifizierung.pdf?__blob=publicationFile&v=5
[EC756]	Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance)
[ISO17067]	EN ISO/IEC TR 17067 Conformity assessment -- Fundamentals of product certification and guidelines for product certification scheme

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000