EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA IT SYSTEM FOR CERTIFICATION

An action plan to implement the EU certification framework

DECEMBER 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

EDITORS

ENISA

CONTRIBUTORS

Scott Cadzow
Ralph Eckmaier
Matthias Pocs
Miruna Bădescu, Eau de Web
Daniela Moșneagu, Eau de Web

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.
Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this study is to support ENISA in the development of an IT System that will enable all the involved stakeholders to collaborate, exchange and share information towards the preparation, adoption and review of cybersecurity certification schemes – the obligation stemming from the EU Cybersecurity Act [1]. It is divided into three distinct parts, identifying the concrete business needs, processes, and functional and technical requirements for such a system.

The first part provides an overview of the envisioned interactions between ENISA, the European Commission (EC) and other relevant stakeholders within the scope of the EU Cybersecurity Certification Framework, as described in the recently legislated EU Cybersecurity Act. In particular, it describes the requirements stemming from the Cybersecurity Act (CSA) in terms of business needs, processes, IT functions and IT use cases. It identifies business activities and provides a semi-formal description of the business logic of the IT System use cases.

The structure of the first part follows from the identification of processes and procedures described (explicitly and implicitly) under Title III of the Cybersecurity Act and categorised into the following domains:

- governance of the certification process,
- processes,
- requests,
- priorities,
- resources, and
- roles and responsibilities.

For each domain listed above, the document describes interactions between ENISA, the EC and other relevant stakeholders that derive explicitly from the content of Cybersecurity Act or are implicitly required to support key functionalities described in the Act. The aim is to provide the foundations for a holistic understanding on how ENISA and the European Commission will cooperate to effectively design and implement the EU's cybersecurity certification framework.

The goals of the second and third parts are:

- To provide the user requirements, use cases, functional and technical specifications of the IT System that will enable all the involved stakeholders to collaborate, exchange and share information towards the preparation, adoption and review of cybersecurity certification schemes. The IT System should take into account all the involved stakeholders: ENISA, Commission, ECCG, SCCG, National cybersecurity certification authorities, National accreditation bodies, Conformity assessment bodies, Standards Developing Organizations.
- To provide all the functional and technical specifications of the IT System that will enable all the involved stakeholders to collaborate, exchange and share information towards the preparation, adoption and review of EU cybersecurity certification schemes. An indicative description is given below:
  - Management of the Union rolling work programme for European Cybersecurity Certification: this includes the initial setup, the processing

[1] Link to be provided upon final publication of the Regulation

through the interaction with the related stakeholders and the final publication of the programme.
    - Preparation, adoption and review of a European cybersecurity certification scheme which indicatively includes: request, possible refusal of the request, preparation, consultation with all related stakeholders, establishment of ad-hoc working groups, ECCG opinion and close collaboration, transmission of the scheme to the Commission, evaluation of the scheme every 5 years, request from the Commission or ECCG group to revise an existing scheme.
- To provide all the non-functional requirements of the IT system that will ensure the proper operation of the system, including issues like Security, Data Privacy, Logging, Storage, Configuration, Performance, Cost, Interoperability, Flexibility, Disaster recovery and Accessibility.
- To provide the technical and functional specifications for the upcoming development of the Website on European cybersecurity certification schemes. Based on the provisions of the CSA:
    - The Agency shall maintain a dedicated website providing information on, and publicity of European cybersecurity certification schemes, certificates and EU statements of conformity, including with regard to withdrawn and expired cybersecurity certification schemes and certificates and the repository of links to cybersecurity information provided online by manufacturers and providers in accordance to corresponding article of the CSA
    - Where applicable, the website shall also indicate the national certifications schemes that have been replaced by a European cybersecurity certification scheme.

1. IDENTIFICATION OF BUSINESS AND TECHNICAL PROCESSES

1.1 GENERAL INFORMATION

1.1.1 Objectives of the review

The objective of this part of the study is to analyse the requirements stemming from the Cybersecurity Act (CSA) in terms of business needs and processes. It should identify business activities and provide a formal description of the business logic of the IT System use cases. Results of the review will be used by ENISA as input to the next step, which will consist in functional and technical specifications of the IT System that will enable all the involved stakeholders to collaborate, exchange and share information towards the preparation, adoption and review of cybersecurity certification schemes. It produces the input to the subsequent step, consisting in describing functional and technical requirements for such an IT system.

1.1.2 Scope of the review

This chapter examines the Cybersecurity Act (CSA) to identify particular actions, in the form of both business and technical processes that will enable ENISA to meet its objectives under the CSA. This therefore examines the recitals and articles of the CSA to identify such processes.

In particular we consider those EU needs related to emerging cybersecurity certification schemes, which will operate under the European cybersecurity certification framework.

1.1.3 Related documents

The study is based on the following documents:

- Regulation (EU) 2019/881 – the Cybersecurity Act[2]
- Rolling Plan for ICT Standardisation 2018[3]
- Baseline Security Recommendations for IoT, November 2017[4]
- IoT Security Standards Gap Analysis: Mapping of existing standards against requirements on security and privacy in the area of IoT, December 2018[5]

1.1.4 Applied methodology

No particular formal method has been applied. For the present document a more conventional text based analysis has been undertaken and used to present the results.

[2] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[3] https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en
[4] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[5] https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

1.2 GOVERNANCE OF THE FRAMEWORK

1.2.1 Introduction and rationale for the EU cybersecurity certification framework (EU CSCF)

The rationale for the EU cybersecurity certification framework is derived from the recitals of the CSA, in particular from Recital 75, which outlines the broad requirement for certification but explicitly relieves the regulation of any obligation to define the certification process itself. Rather it is indicated that ENISA and the other EU stakeholders build the required processes. With the remit of the EU cybersecurity certification framework covering ICT products, services and processes, which conceivably addresses many thousands of entities it should be clear that the EU cybersecurity certification framework should be strongly governed. As the EU expert body for matters relating to Cybersecurity it is reasonable to expect ENISA to be at the heart of this governance process but it is recognised that many other stakeholders will have roles to play in enforcing and implementing any EU cybersecurity certification programme.

1.2.2 Overview of the framework

The EU cybersecurity certification framework entails four main phases:

1. the creation and publication of the Union Rolling Working Programme (URWP);
2. the preparation of a candidate cybersecurity certification scheme;
3. the enforcement by legislation of the accepted candidate scheme; and,
4. the implementation of the scheme.

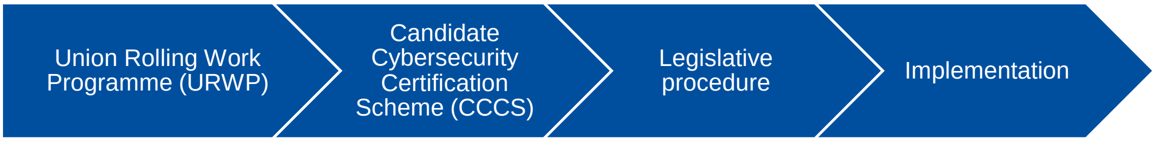

Union Rolling Work Programme (URWP)
Candidate Cybersecurity Certification Scheme (CCCS)
Legislative procedure
Implementation

Figure 1: Sequence of events in development of EU CSCF

Throughout these phases, multiple stakeholders are involved, with EC, ENISA, the European Cybersecurity Certification Group (ECCG) and the Stakeholder Cybersecurity Certification Group (SCCG) being the main entities responsible for the governance of the framework. The phases run in strict sequence with oversight through the stakeholder groups (ECCG and SCCG) operating continuously.

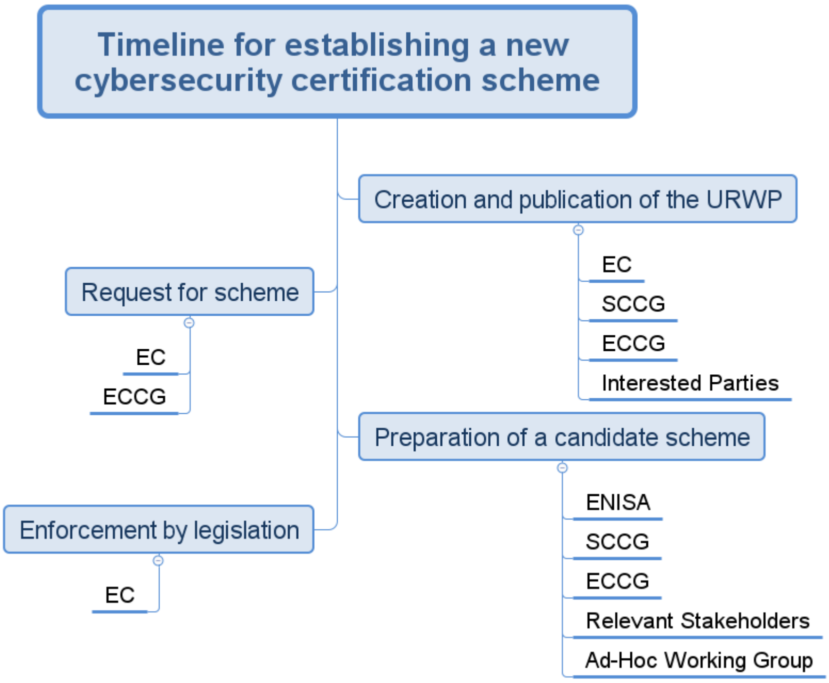

Timeline for establishing a new cybersecurity certification scheme
Creation and publication of the URWP
EC
SCCG
ECCG
Interested Parties
Request for scheme
EC
ECCG
Preparation of a candidate scheme
ENISA
SCCG
ECCG
Relevant Stakeholders
Ad-Hoc Working Group
Enforcement by legislation
EC

Figure 2: Sequence of events in development of EU CSCF identifying stakeholders for each phase

The stakeholders involved in each stage of the timeline are identified in Figures 1 and 2.

Details of the roles and responsibilities of each of the ECCG and SCCG are addressed in greater detail later in the present document.

1.2.3 Development, design and publication of the URWP

As a pre-requisite for the publication of the URWP (related to cybersecurity) a number of steps are required:

- The forming of the SCCG
  - EC prepares the Terms of Reference (ToR) document and the Call for expression of interest
  - EC and ENISA publish the Call for expression of interest
  - ENISA provides a list of candidate members to EC – this may be derived from the existing list of domain experts maintained by ENISA
  - EC selects based on gender and geographical balance criteria
- EC requests advice from SCCG and ECCG
- Transparent and broad consultation among all stakeholders based on specific criteria
- Publication of a legal non-binding document by EC (at least every three years)
- Identification of strategic priorities for future EU cybersecurity certification schemes
- Listing of ICT products, services and processes or categories that will benefit from being covered by a scheme
- Multiyear overview of requests for candidate schemes taking into account the URWP

1.2.4 The cybersecurity certification scheme

There is no requirement to have a single unified cybersecurity certification scheme, thus the CSA discusses the need for ENISA to prepare candidate European cybersecurity certification schemes described in RWP, or for a scheme separately requested by EC or ECCG in urgent cases, although in the latter scenario ENISA reserves the right to reject the request. Thus if the URWP identifies n schemes required ENISA shall prepare proposals for those n schemes (where n is at least 1).

Every candidate scheme should adhere to a number of common principles and in each case ENISA is expected to create an ad-hoc working group to assist in the preparation of the scheme. Thus ENISA, the ad hoc working group (consisting of contracted experts, including from the Member States’ competent authorities), and the ECCG (who may advice and express an opinion for the final candidate scheme), are all involved in the scheme's development. The normal operating model should be to seek consensus amongst these stakeholders although ENISA has the final say. ENISA is further tasked to provide information about all schemes, both candidates and adopted, to its website as well as indicate the national schemes replaced by European schemes. Finally, ENISA should evaluate periodically (every five years) all adopted European schemes and upon EC’s or ECCG’s request to commence the process for a revised candidate scheme.

NOTE: There is a risk of a disruption of business if unscrupulous suppliers propose many schemes as candidates knowing that even if they are not adopted that they have to be referred to. The existence of a scheme in a formally maintained EU/ENISA database however gives credence to the scheme even if it is marked as not-adopted. A minor change should be that only credible schemes are forwarded for consideration and invalid or non-credible schemes are filtered away from official recognition.

The content of ENISA's public facing website will be considered as authoritative and thus the data held and presented has to be verified for its overall integrity.

1.2.5 Recognition of an accepted scheme in a Commission Implementing Decision

Once a candidate cybersecurity certification scheme is communicated by ENISA to EC, the EC is empowered to adopt it through implementing acts. The process steps involved are:

- ENISA transmits the candidate scheme to EC
    - Comprehensive set of documents as defined in the Cybersecurity Act
        - Rules
        - Technical requirements
        - Standards
        - Procedures
    - Specified a minimum set of elements
        - Subject matter
        - Scope and object of the cybersecurity certification including ICT products, services and processes covered
        - Detailed specification of cybersecurity requirements with reference to standards or technical specifications
        - Evaluation criteria and methods
        - Levels of assurance and their respective evaluation levels
        - Specify conditions under which software or hardware updates may require recertification of an ICT product or service or the scope of this certificate being reduced
        - This set of elements could be provided to ENISA complementing the RWP
- EC is empowered to adopt the proposed candidate schemes by means of an implementing act.
    - EC to prepare an implementing Act

- EC to be notified by national certification authorities regarding the conformity assessment bodies accredited
    - Authorisation to issue certificates at specified assurance levels
- EC to publish a list of notified conformity assessment bodies in the Official journal (one year after the entry into force)
    - Amend the list based on notifications after the expiry date
    - Handle requests to remove conformity assessment bodies

1.2.6 Fines / complaint / courts, guidelines & regular re-assessment

Whilst governance of the European cybersecurity certification scheme requires that EU Member States lay down the rules on penalties applicable to infringements and measures necessary for compliance there is no direct role for ENISA over and above those noted here:

- Elaboration of guidelines: ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements of ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way. ENISA shall contribute to capacity-building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request.
- Regular re-assessment of schemes: The Commission acting alongside ENISA shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law
- Promotion: ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market.

1.2.7 Implementation of cybersecurity certification schemes

A number of stakeholders are involved in the implementation of any particular certification scheme with different roles and responsibilities. It is worth noting that ENISA is not explicitly involved in this stage apart from receiving feedback regarding the schemes. More specifically, the processes are:

- Manufacturers of ICT products or services submit applications to a conformity assessment body (CAB)
- Submissions for certification must provide to the conformity assessment body all necessary information to conduct the certification process
- Information should be in electronic format and available at least until the expiry date of the certificate or statement of conformity
- Each Member State (MS) to designate one or more national cybersecurity certification authorities responsible to supervise compliance with obligations arising from cybersecurity Act
    - MS to inform EC of the designated authorities and their tasks
    - MS can assign tasks to existing authorities
    - MS can assign authorities in the territory of other MS upon mutual agreement
    - Activities of national cybersecurity authorities related to activities of certification
        - Specific tasks and responsibilities
- Authorities to provide an annual summary report to EC and ENISA
    - Monitoring and enforcement
    - Activities of conformity assessment bodies
    - Activities of public bodies (accredited as conformity assessment bodies or national cybersecurity certification authorities)

- EC and national authorities to exchange information, experiences and good practice with the assistance of ECCG
- Share information on possible non-compliance

A critical element of the cybersecurity certification framework is to assess and subsequently seek the revision, where necessary, of adopted schemes. The processes are:

- EC to assess regularly and at least biannually the efficiency and utilisation of the adopted certification schemes
- EC to assess if certain schemes should be rendered mandatory through relevant Union legislation
    - Identify ICT, products, services and processes for mandatory schemes
    - Prioritise sectors listed in Annex II of 2016/1148 Directive
    - Selection of mandatory schemes based on the criteria described in cybersecurity Act

To ensure a uniform implementation, peer reviews for relevant certification authorities are mandatory. The processes for the peer reviews are:

- EC to organise with at least two MS peer reviews for authorities
    - ENISA may participate in the peer review
- Implementing acts may be adopted to establish plans for peer reviews
    - Peer reviews to cover a period of at least five years
    - Specific criteria for peer review teams and methodology used
- ECCG will draw up summaries of these reviews
    - Issue guidelines and recommendations on actions or measures for the relevant authorities

There are specific excerpts in the cybersecurity Act denoting how EC can engage in discussions with third countries to create mutual recognition agreements for cybersecurity certifications. The processes are:

- Mutual recognition agreements
    - ENISA and ECCG to advise EC on which negotiations to initiate with third countries
    - Mutual recognition agreements can be stated in the candidate cybersecurity certification scheme

1.3 PROCESSES

1.3.1 Registration of self-asserted certificates

A consequence of Article 53.3 is that ENISA has to be able to implement a process for receipt, cataloguing and storage/recovery of self-asserted conformity claims and the resultant "EU statement of conformity". The participants in this process are:

- ENISA;
    - Registrar
    - Claimant review authority
- The claimant;
- The evaluation authority of the claimant;
- The authority for the specification that the claimant asserts conformity.

Recital 75 and associated sub-recitals provide greater detail of the expectations for assessment.

The manufacturer shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity with the scheme available to the NCCA for the period provided for in the corresponding European cybersecurity certification scheme.

A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

1.3.2 The certification process

1.3.2.1 Introduction and CSA considerations

A key element throughout the CSA is an expectation that the certification process is available and can be readily adopted by developers and hence by the market as a whole. The practical position is that as of this writing there is no citable process of certification.

Certificates issued according to the ISO/IEC 15408 (the Common Criteria) are recognised internationally within the Common Criteria Recognition Agreement (CCRA) and by the SOG-IS Mutual Recognition Agreement (MRA). The wider intent is that the relatively restricted set of member states who are involved in either CCRA or MRA needs to be extended (Recitals 68 and 69 apply).

Article 54 of the CSA elaborates on the content of the certificate and the scheme that underpins it. There is a "chicken and egg" situation here that has to be carefully managed in order to ensure that content of the certificate does not define the scheme used to fill in the content.

The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

1.3.2.2 Developer and SDO obligations for certification

Much of the remainder of this chapter extends from that given in the ENISA publication "IoT Security Standards Gap Analysis"[6] to identify specific actions and processes that have to be addressed by each stakeholder (primarily the SDOs, the assessment agencies/authorities, and the affected industry sectors).

Very specifically Article 54.1c states that the certification scheme must make *references to the international, European or national standards applied in the evaluation* that leads to the granting of the certificate. The challenge to SDOs is therefore to make standards available that meet the necessary technical rigour for evaluation.

[6] https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

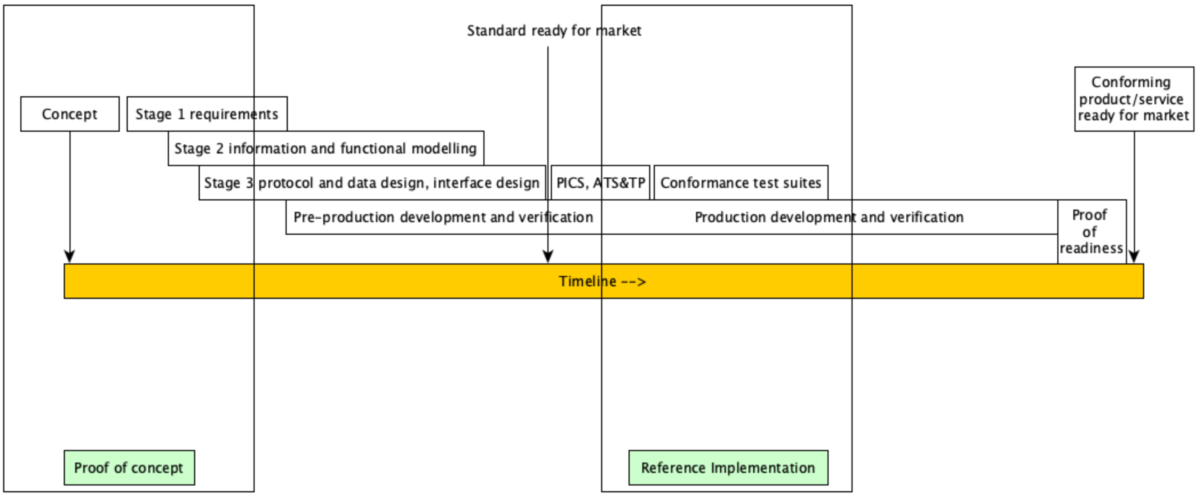

Standard ready for market
Concept
Stage 1 requirements
Stage 2 information and functional modelling
Stage 3 protocol and data design, interface design
PICS, ATS&TP
Conformance test suites
Conforming product/service ready for market
Pre-production development and verification
Production development and verification
Proof of readiness
Timeline -->
Proof of concept
Reference Implementation

Figure 3: Sequence of events in development of EU CSCF identifying stakeholders for each phase

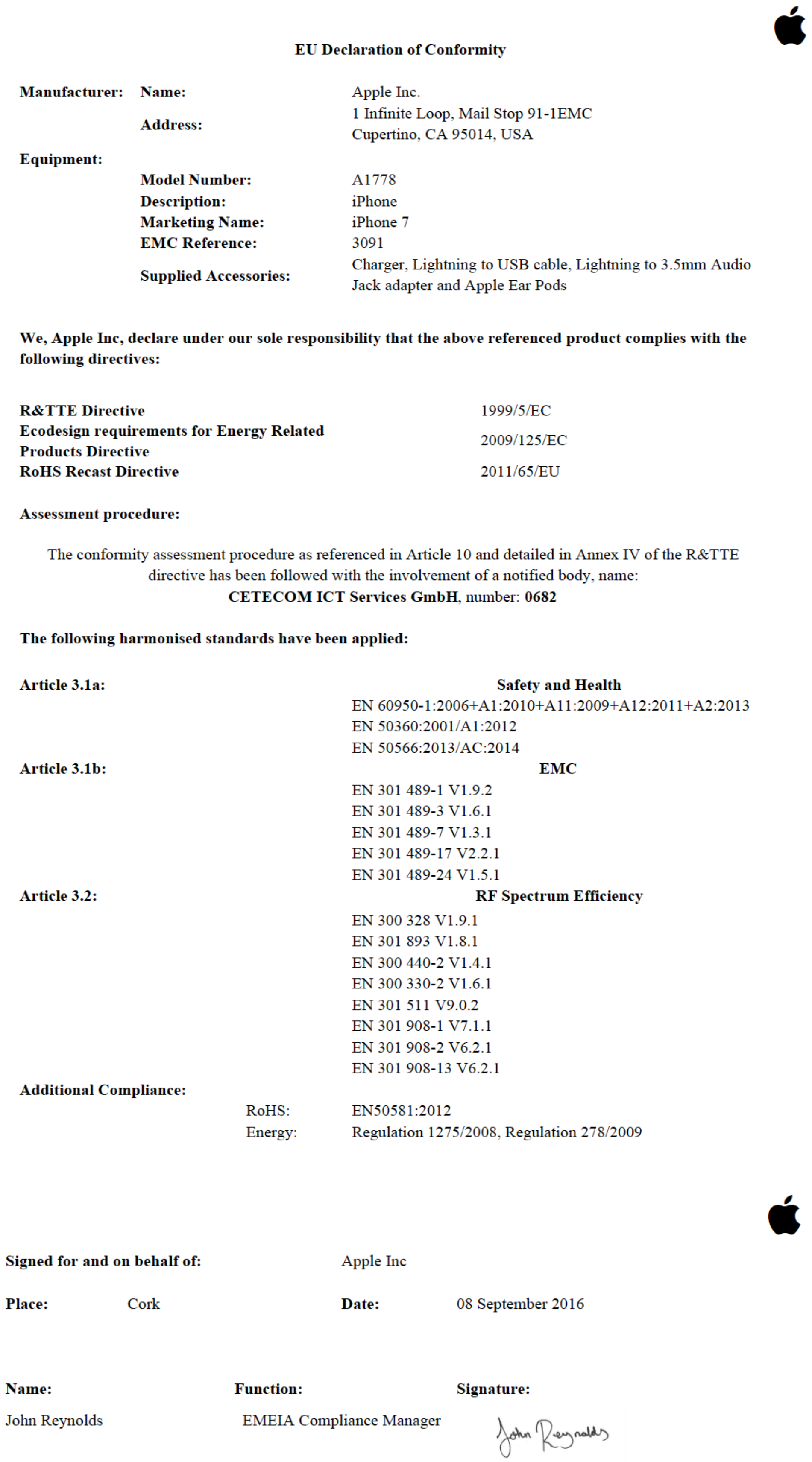
For self-assertion of a product or service it is the end point of the SDO role from the above picture that is the starting point for the process that ought to lead to certification. In other words, standards have to have some means of proving that the product or service conforms to them. Conventionally this is achieved using formal test cases and a statement of conformance (the Implementation Conformance Statement).

There is an issue with such testing – it tends to be positive in outlook, it doesn't really look under the covers. It is also clear that the number of standards that allow for conformance testing of security features is small in relation to the number of standards. In part, this may be that if a specific operation in the security domain, e.g. the generation of a digital signature is relatively commodity like, in that either the code works or it doesn't. It is in the purpose of a digital signature that the security lies and not necessarily in the specific operation.

1.3.2.3 What form of standards fit to use in certification?

There are several domains in which standards are specifically cited as part of the regulatory framework to allow market access. The obvious domains are in each of safety and in radio regulation. In each case, there are a set of Harmonised Standards cited at some point in the Official Journal and which are called out in a Declaration of Conformity (DoC) in a product. Examples of such DoCs for 2 models of smartphone are given below (see also the content of ETSI TS 103 346 regarding electronic versions of such DoC).

Whilst the purpose of certificates in the scope of the CSA are not the same as a Declaration of Conformity used in the safety and radio domains the value to the end user may be considered as equivalent.



EU Declaration of Conformity

Manufacturer:	**Name:**	Apple Inc.
	Address:	1 Infinite Loop, Mail Stop 91-1EMC Cupertino, CA 95014, USA
Equipment:		
	Model Number:	A1778
	Description:	iPhone
	Marketing Name:	iPhone 7
	EMC Reference:	3091
	Supplied Accessories:	Charger, Lightning to USB cable, Lightning to 3.5mm Audio Jack adapter and Apple Ear Pods

We, Apple Inc, declare under our sole responsibility that the above referenced product complies with the following directives:

R&TTE Directive	1999/5/EC
Ecodesign requirements for Energy Related Products Directive	2009/125/EC
RoHS Recast Directive	2011/65/EU

Assessment procedure:

The conformity assessment procedure as referenced in Article 10 and detailed in Annex IV of the R&TTE directive has been followed with the involvement of a notified body, name:
CETECOM ICT Services GmbH, number: **0682**

The following harmonised standards have been applied:

Article 3.1a:	**Safety and Health**
	EN 60950-1:2006+A1:2010+A11:2009+A12:2011+A2:2013
	EN 50360:2001/A1:2012
	EN 50566:2013/AC:2014
Article 3.1b:	**EMC**
	EN 301 489-1 V1.9.2
	EN 301 489-3 V1.6.1
	EN 301 489-7 V1.3.1
	EN 301 489-17 V2.2.1
	EN 301 489-24 V1.5.1
Article 3.2:	**RF Spectrum Efficiency**
	EN 300 328 V1.9.1
	EN 301 893 V1.8.1
	EN 300 440-2 V1.4.1
	EN 300 330-2 V1.6.1
	EN 301 511 V9.0.2
	EN 301 908-1 V7.1.1
	EN 301 908-2 V6.2.1
	EN 301 908-13 V6.2.1

Additional Compliance:

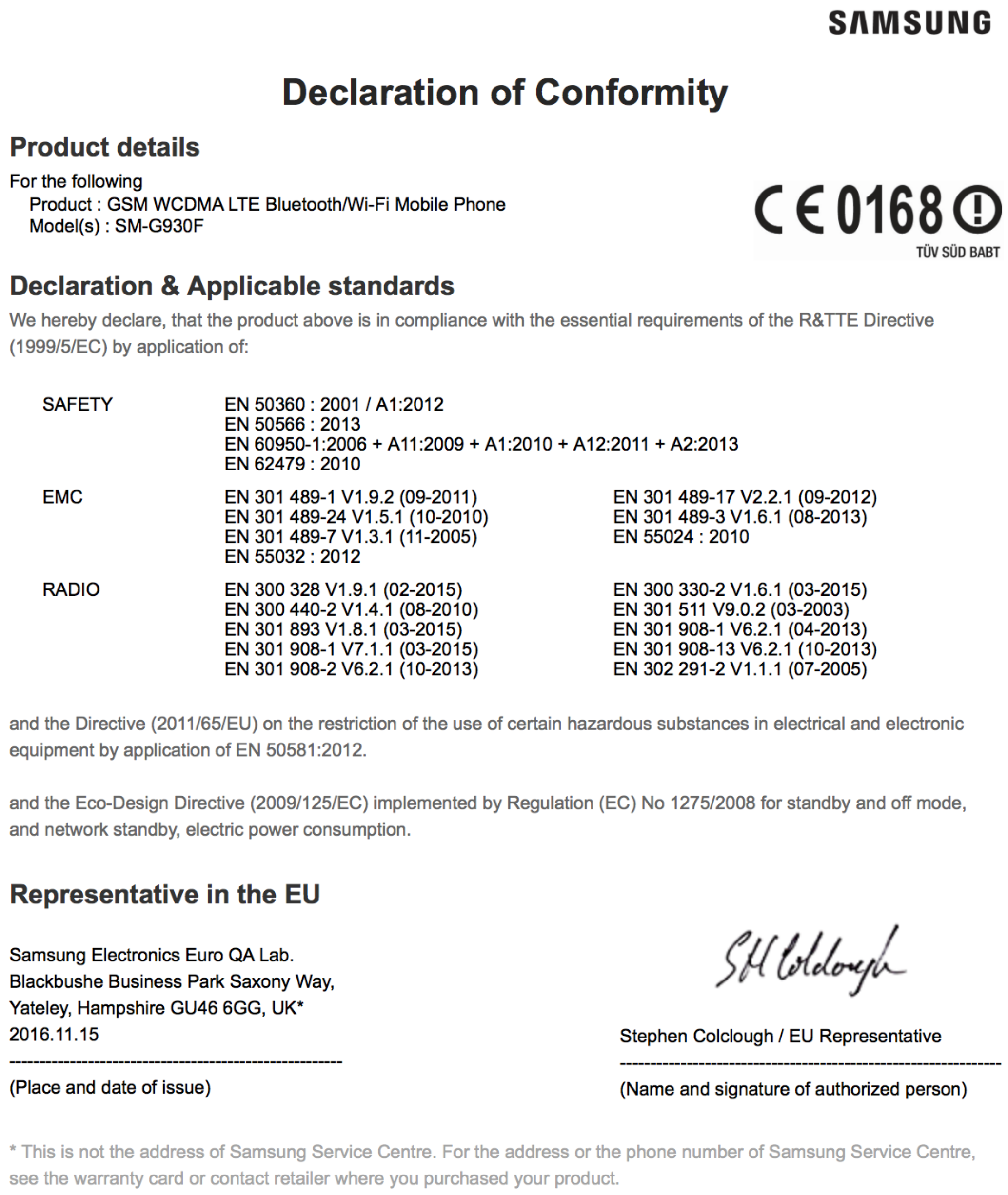
RoHS:	EN50581:2012
Energy:	Regulation 1275/2008, Regulation 278/2009

Signed for and on behalf of: Apple Inc

Place: Cork **Date:** 08 September 2016

Name:	**Function:**	**Signature:**
John Reynolds	EMEIA Compliance Manager	John Reynolds

Figure 4: Screenshot of DoC for the Apple iPhone 7



SAMSUNG

Declaration of Conformity

Product details

For the following
Product : GSM WCDMA LTE Bluetooth/Wi-Fi Mobile Phone
Model(s) : SM-G930F

CE 0168
TÜV SÜD BABT

Declaration & Applicable standards

We hereby declare, that the product above is in compliance with the essential requirements of the R&TTE Directive (1999/5/EC) by application of:

SAFETY	EN 50360 : 2001 / A1:2012 EN 50566 : 2013 EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013 EN 62479 : 2010	
EMC	EN 301 489-1 V1.9.2 (09-2011) EN 301 489-24 V1.5.1 (10-2010) EN 301 489-7 V1.3.1 (11-2005) EN 55032 : 2012	EN 301 489-17 V2.2.1 (09-2012) EN 301 489-3 V1.6.1 (08-2013) EN 55024 : 2010
RADIO	EN 300 328 V1.9.1 (02-2015) EN 300 440-2 V1.4.1 (08-2010) EN 301 893 V1.8.1 (03-2015) EN 301 908-1 V7.1.1 (03-2015) EN 301 908-2 V6.2.1 (10-2013)	EN 300 330-2 V1.6.1 (03-2015) EN 301 511 V9.0.2 (03-2003) EN 301 908-1 V6.2.1 (04-2013) EN 301 908-13 V6.2.1 (10-2013) EN 302 291-2 V1.1.1 (07-2005)

and the Directive (2011/65/EU) on the restriction of the use of certain hazardous substances in electrical and electronic equipment by application of EN 50581:2012.

and the Eco-Design Directive (2009/125/EC) implemented by Regulation (EC) No 1275/2008 for standby and off mode, and network standby, electric power consumption.

Representative in the EU

Samsung Electronics Euro QA Lab.
Blackbushe Business Park Saxony Way,
Yateley, Hampshire GU46 6GG, UK*
2016.11.15

(Place and date of issue)

Stephen Colclough / EU Representative

(Name and signature of authorized person)

* This is not the address of Samsung Service Centre. For the address or the phone number of Samsung Service Centre, see the warranty card or contact retailer where you purchased your product.

Figure 5: Screenshot of DoC for the Samsung Galaxy S7 (model G930F)

The Common Criteria approach in the form of a cPP or even in the form proposed for the "Direct Rationale" is somewhat different from the forms used in the SDOs cited in the CSA. This leads directly to a requirement for ENISA to work with the SDOs to define the format for an acceptable process of standards that will allow certification to be granted (i.e. if conformance to the standard is shown then some form of "safe harbour" is effectively granted by self-assertion).

1.3.2.4 Definition of European Security Norm standard format

The assurance role of security standards needs to be reinforced as opposed to the purely functional role that many standards seek to define.

I.e. most standards, when normative, specify in detail the stimulus-response behaviour expected of a device. Thus, for an action such as digital signature verification, the stimulus will be sending the signature and supporting data to a black box function, with an expected response of "True" if the signature is verified, and "False" otherwise. The rationale for the function is often not explicit, but to give assurance it is the rationale that is (arguably) more critical. Some SDOs do perform a risk analysis prior to the development of specific standards, where the risk analysis will provide the rationale for the provision of the security function.

Process partners: SDOs, ENISA, SDO participants, Evaluation authorities

As stated in [4] the overall purpose of standards from the perspective of the market is twofold in defining what a standard is intended to achieve: (1) interoperability, and (2) confidence. The role of standards in achieving interoperability is well defined by the SDOs themselves and has been extensively written about in [4] and elsewhere. The certification opportunity lies in addressing the role of standards in the domain of confidence. It is somewhat obvious to state that a failure to achieve interoperability will negatively impact confidence, however in the security domain the counter assertion, that interoperability will positively impact confidence with respect to security, is much less likely to be true.

Standards as technical specifications apply in a specific context: Generally, a standard will apply to a single product type, or even a single function within a product or service. Security standards are similarly contextual and this has to be recognised when evaluating the security offered and the resultant certificate request. A general concept for the role of standards in the evaluation process is presented in the figure below.

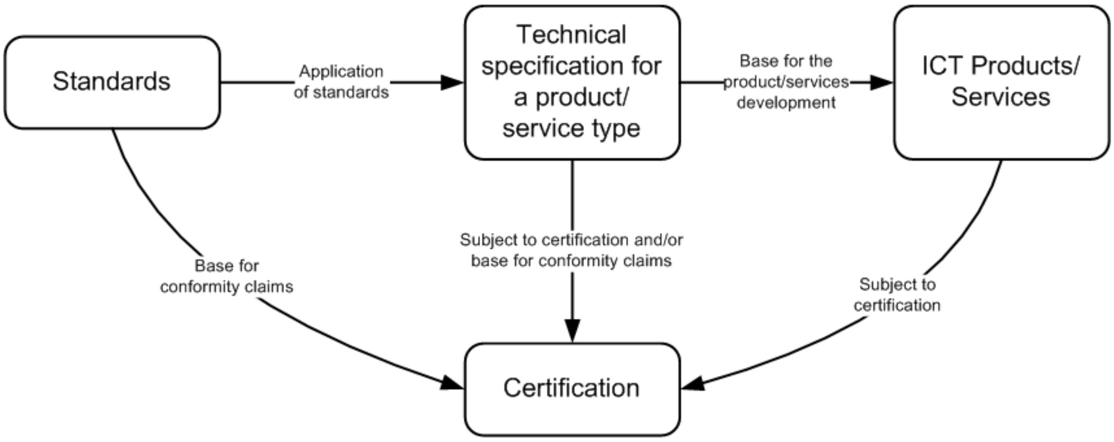

Standards
Application of standards
Technical specification for a product/ service type
Base for the product/services development
ICT Products/ Services
Base for conformity claims
Subject to certification and/or base for conformity claims
Subject to certification
Certification

Figure 6: Role of standards in certification process

1.4 RESOURCES, AND ROLES AND RESPONSIBILITIES

1.4.1 Notification of CABs

Notification of CABs: For each European cybersecurity certification scheme, the NCCAs shall notify the Commission of the CABs that have been accredited and of any subsequent changes. A NCCA may submit to the Commission a request to remove a CAB notified by that authority from the list.

Accreditation of CABs: The CABs shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Where a European cybersecurity certificate is issued by a NCCA, the certification body of the NCCA shall be accredited as a CAB. Where European cybersecurity certification schemes set out specific or additional requirements, only CABs that meet those requirements shall be authorised by the NCCA. The accreditation shall be issued to the CABs for a maximum of five years. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a CAB.

One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of the CABs notified under that scheme in the Official Journal of the European Union. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the OJEU within two months of the date of receipt of that notification. The Commission may adopt implementing acts to establish the circumstances, formats and procedures for notifications.

On notification by the NCCA, the Commission shall publish the corresponding amendments to that list in the OJEU within one month of the date of receipt of the national cybersecurity certification authority's request.

1.4.2 Role identification

The CSA identifies a number of roles that can be grouped against organisational type. This is shown pictorially in Figure 3.

In Figure 7 the entities highlighted in parallelograms are roles that should be assigned in the access control framework of the ICT facilities to be provided by ENISA for the management of the Certification Process.

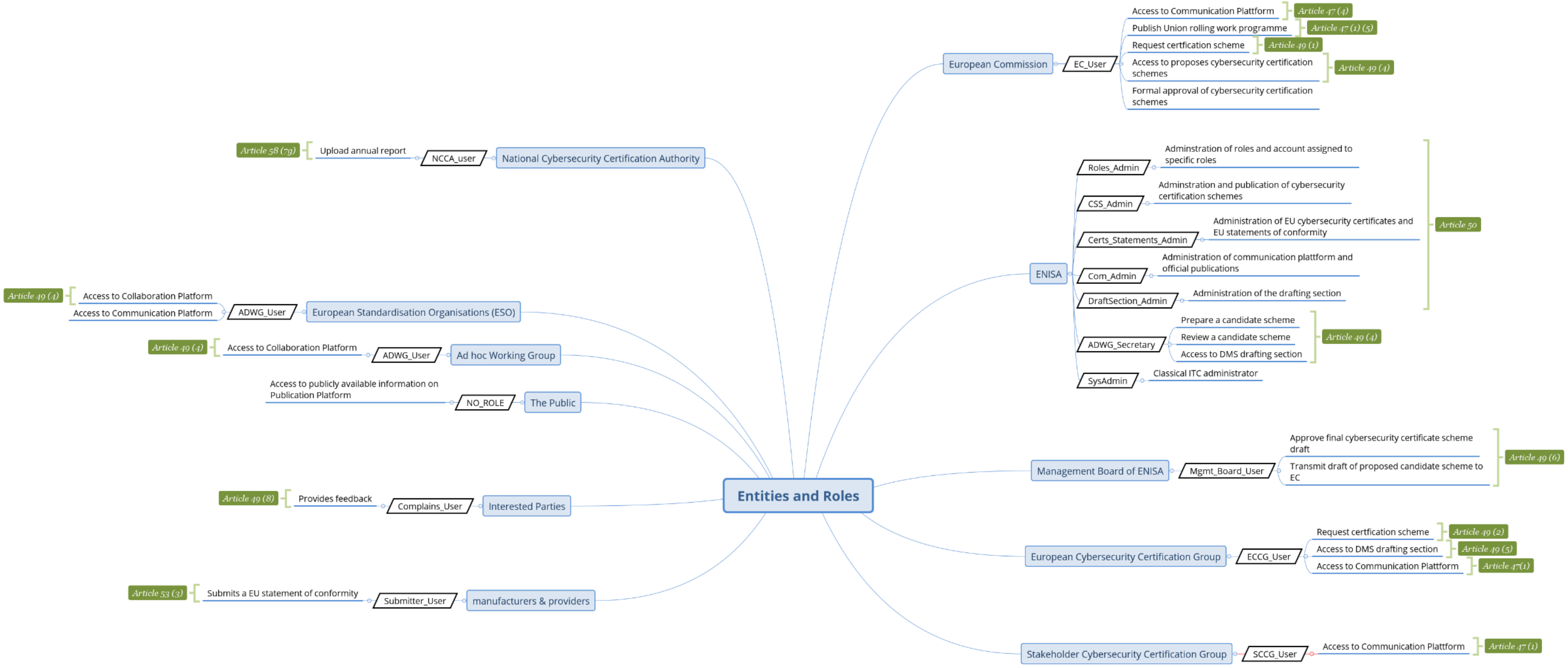

Entities and Roles
European Commission
EC_User
Access to Communication Plattform
Article 47 (4)
Publish Union rolling work programme
Article 47 (1) (5)
Request certfication scheme
Article 49 (1)
Access to proposes cybersecurity certification schemes
Article 49 (4)
Formal approval of cybersecurity certification schemes
ENISA
Roles_Admin
Adminstration of roles and account assigned to specific roles
CSS_Admin
Adminstration and publication of cybersecurity certification schemes
Certs_Statements_Admin
Administration of EU cybersecurity certificates and EU statements of conformity
Com_Admin
Administration of communication plattform and official publications
DraftSection_Admin
Administration of the drafting section
Article 50
ADWG_Secretary
Prepare a candidate scheme
Review a candidate scheme
Access to DMS drafting section
Article 49 (4)
SysAdmin
Classical ITC administrator
Management Board of ENISA
Mgmt_Board_User
Approve final cybersecurity certificate scheme draft
Transmit draft of proposed candidate scheme to EC
Article 49 (6)
European Cybersecurity Certification Group
ECCG_User
Request certfication scheme
Article 49 (2)
Access to DMS drafting section
Article 49 (5)
Access to Communication Plattform
Article 47(1)
Stakeholder Cybersecurity Certification Group
SCCG_User
Access to Communication Plattform
Article 47 (1)
National Cybersecurity Certification Authority
NCCA_user
Upload annual report
Article 58 (79)
European Standardisation Organisations (ESO)
ADWG_User
Access to Collaboration Platform
Access to Communication Platform
Article 49 (4)
Ad hoc Working Group
ADWG_User
Access to Collaboration Platform
Article 49 (4)
The Public
NO_ROLE
Access to publicly available information on Publication Platform
Interested Parties
Complains_User
Provides feedback
Article 49 (8)
manufacturers & providers
Submitter_User
Submits a EU statement of conformity
Article 53 (3)

Figure 7: CSA mapping of roles against organisational type

1.5 CSA REVIEW AND RELEVANT RECITALS AND ARTICLES

1.5.1 CSA analysis by recital and article

The analysis in the table below considers the CSA with specific attempt to identify process requirements (business or technical) by reference to specific Articles and Recitals of the CSA.

RECITAL/ ARTICLE	Text	Underlying process requirement	Business/ Technical
Article 49.7	The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).	Requires interaction with the Commission	B
Article 51	Security objectives of European cybersecurity certification schemes	No specific process requirement – this article states the overall objectives of the certification programme.	B
Article 52	Assurance levels of European cybersecurity certification schemes	No specific process requirement. However, the agreed assurance levels have to be cross referenced from the cataloguing process (see below)	B
Modified in Article 53.3	The manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.	ENISA has to be able to implement a process for receipt, cataloguing and storage/recovery of self-asserted conformity claims and the resultant "EU statement of conformity"	T
Article 54.1.a	… including the type or categories of ICT products, ICT services and ICT processes covered	A clear classification of type/category of such equipment needs to be maintained.	T
RECITALS			
Recital 75	The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to		B

	adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT processes should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications if no appropriate standards are available.		
Recital 76	The technical specifications to be used in European cybersecurity certification schemes should respect the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council (19). Some deviations from those requirements could, however, be considered to be necessary in duly justified cases where those technical specifications are to be used in a European cybersecurity certification scheme referring to assurance level 'high'. The reasons for such deviations should be made publicly available	Requires that ENISA engage with the EU-SDOs (CEN, CENELEC, ETSI). ENISA shall be held responsible for justifying any deviation from adoption of EU standards	B
Recital 77	A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services or ICT processes that are being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service or ICT process. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out. Depending on the assurance level, the European cybersecurity certification scheme should indicate whether the European cybersecurity certificate is to be issued by a private or public body. Conformity assessment and certification cannot guarantee per se that certified ICT products, ICT services and ICT processes are cyber secure. They are instead procedures and technical methodologies for attesting that ICT products, ICT services and ICT processes have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example in technical standards.	This in part defines the set of conditions that need to be identifiable in the resultant certificate.	T
Recital 78	The choice of the appropriate certification and associated security requirements by the users of European cybersecurity certificates should be based on an analysis of the risks associated with the use of the ICT products, ICT services or ICT processes. Accordingly, the assurance level should be commensurate with the level of the risk associated with the intended use of an ICT product, ICT service or ICT process.	It is suggested that this implies ENISA or a competent agency reviews the risk analysis associated to the request for certification. The mapping from basic – substantial – high to existing evaluation processes needs to be made.	T

The impact of Articles 50 and 55 is a number of published lists that are to be maintained in the ICT facilities of ENISA. This is shown figuratively in Figure 9.

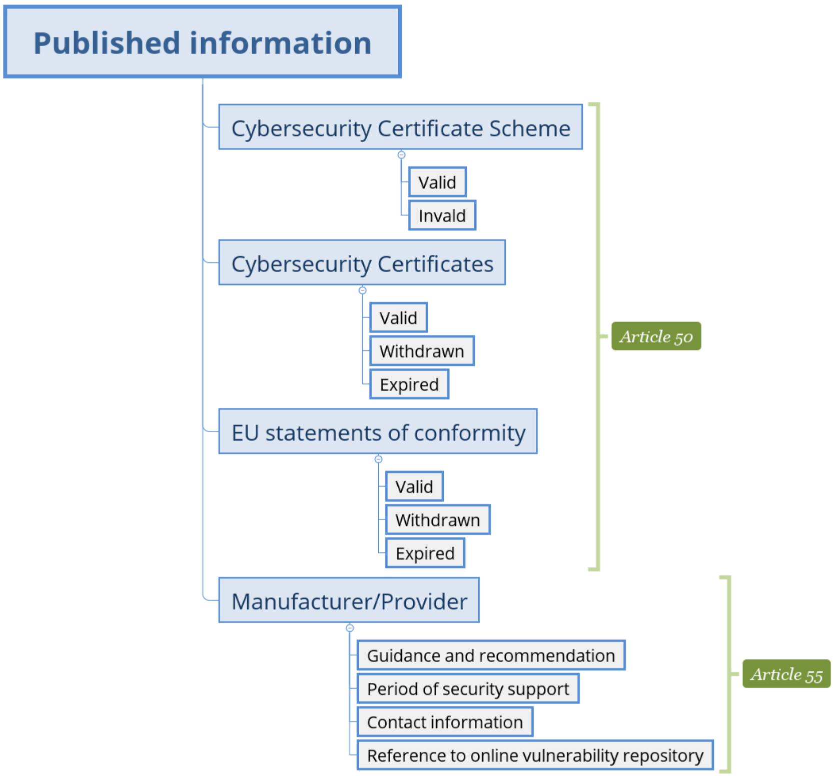

Published information
Cybersecurity Certificate Scheme
Valid
Invald
Cybersecurity Certificates
Valid
Withdrawn
Expired
EU statements of conformity
Valid
Withdrawn
Expired
Article 50
Manufacturer/Provider
Guidance and recommendation
Period of security support
Contact information
Reference to online vulnerability repository
Article 55

Figure 9: Scope of material to be published by ENISA against CSA article setting the obligation

ENISA's website (on the schemes/certificates) shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

1.6 OTHER CONSIDERATIONS

1.6.1 Role of the ECCG

Members of ECCG are representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. The ECCG is involved in the creation of the URWP and is empowered to propose to ENISA areas for potential schemes that are not included in the URWP. The ECCG provides advice to ENISA during the drafting of candidate EU cybersecurity certification schemes and expresses an opinion when the process is finalised. The ECCG further advises EC on the maintenance and review of existing European schemes. The EECG engages in capacity building activities between national cybersecurity certification authorities and supports the execution of peer assessment procedures. Finally, the ECCG can recommend ENISA to assist international standardisation organisations in order to address gaps in internationally recognised standards.

The ECCG shall be composed of representatives of NCCAs or representatives of other relevant national authorities.

A Member of the ECCG shall not represent more than two Member States.

ENISA shall provide the secretariat of the ECCG.

Consequence of this: ENISA shall be the sole authoritative source for data on all EU cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity for all cybersecurity certified products on the European market.

1.6.2 Role and construction of the SCCG

Members of the SCCG are appointed by EC, selected from a list of experts proposed by ENISA. *The Stakeholder Cybersecurity Certification Group shall be composed of members selected from among recognised experts representing the relevant stakeholders. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance*. EC and ENISA co-chair SCCG and the secretariat is provided by the Agency. The SCCG advises EC on strategic decisions regarding the European cybersecurity certification framework and upon request ENISA regarding the agency's tasks on certification. The SCCG's main role is to assist EC in the design of the RWP and on urgent situations to facilitate EC and the ECCG to decide for additional certification schemes not included in the RWP.

Consequence of this: ENISA shall be the co-chair and secretariat and shall maintain a record of all correspondence relating to the SCCG and a record of all meetings and decisions of the SCCG. ENISA shall also maintain a list of experts as both candidates and secondees (placements) to the SCCG.

1.6.3 Peer review process

With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, NCCAs shall be subject to peer review. Peer review shall be carried out by at least two NCCAs of other Member States and the Commission and shall be carried out at least once every five years.

The peer review process shall assess the following:

- whether the activities of the NCCAs under review that relate to the issuance of European cybersecurity certificates are strictly separated from their supervisory activities;

- the procedures for supervising and enforcing the rules for monitoring the compliance with European cybersecurity certificates;

- the procedures used by the NCCSs under review for monitoring, authorising and supervising the activities of the CABs;

- whether the staff of authorities or bodies that issue certificates for assurance level 'high' have the appropriate expertise.

The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it.

ENISA may participate in the peer review.

Consequence of this: As indicated further ENISA shall be the sole authoritative source for data on all EU cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity for all cybersecurity certified products on the European market, it is noted that this shall include an authoritative record of all peer reviews conducted, their target, their participants, and their reports.

1.6.4 Issuing EU certificates and the role of ENISA's website

The CABs (and NCCAs) shall issue European cybersecurity certificates referring to assurance level 'basic' or 'substantial' (or 'high') on the basis of criteria included in the European cybersecurity certification scheme. The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the CAB all information necessary to conduct the certification. The (certificate) holder shall inform the NCCA or CAB of any subsequently detected vulnerabilities or irregularities concerning the security that may have an impact on its compliance with the (certification) requirements.

ENISA shall maintain a dedicated website providing information on the European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity. Such a database should also include:

- information on the European cybersecurity certification schemes which are no longer valid
- information on withdrawn and expired European cybersecurity certificates and EU statements of conformity
- repository of links to cybersecurity information provided in accordance with Article 55.

Consequence of this: ENISA shall be the sole authoritative source for data on all EU cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity for all certified products on the European market.

1.6.5 Functions and sub-functions of the IT-system

Considering the requirements contained in the CSA, the following functions are necessary for the IT system operated by ENISA:

Function	Sub-Function
Publication Portal (PUB)	Provide a portal for the publication of EU cybersecurity certification schemes
	Provide a portal for the publication of EU cybersecurity certificates
	Provide a portal for the publication of EU statements of conformity
Collaboration Platform (COL)	Provide a collaboration platform for preparing a EU cybersecurity certification scheme
Communication Platform (COM)	Provide secure communication between the different entities
Document Management System (DMS)	Retain information about EU cybersecurity certification candidate schemes
	Retain information about EU cybersecurity certificates
	Retain information about EU statements of conformity

An illustration explaining the interaction between these functions can be found in picture 7 (earlier in the present document).

The Communication Platform is facilitated for any communication or information exchange between the different stakeholders mentioned in the CSA.

The Collaboration Platform is used for preparing the EU cybersecurity certification candidate schemas. In the backend a CMS supports the web server connected with a database, document management system, message board, collaborative work environment and ticketing system. During the preparation of these candidate schemes the Communication Platform is used within the Ad hoc Working Group, the ECCG and the CSSG for communication. Any work progress and others outcome of the Ad hoc Working Group is stored in the Document Management System.

The Document Management Systems additionally provides document control all provided EU. In the frontend a web server (for example, `certification.enisa.europa.eu`) offers different content depending on the classes of users.

Entity	IT role	IT use case
European Commission	EC_User	Access to Communication Platform
		Publish Union rolling work programme
		Request certification scheme
		Access to proposes cybersecurity certification schemes
		Formal approval of cybersecurity certification schemes
ENISA	Roles_Admin	Administration of roles and account assigned to specific roles
	CSS_Admin	Adminstration and publication of cybersecurity certification schemes
	Certs_Statements_Admin	Administration of EU cybersecurity certificates and EU statements of conformity
	Com_Admin	Administration of communication platform and official publications
	DraftSection_Admin	Administration of the drafting section
	ADWG_Secretary	Prepare a candidate scheme
		Review a candidate scheme
		Access to DMS drafting section
	SysAdmin	Classical ITC administrator
Management Board of ENISA	Mgmt_Board_User	Approve final cybersecurity certificate scheme draft
		Transmit draft of proposed candidate scheme to EC
European Cybersecurity Certification Group	ECCG_User	Request certfication scheme
		Access to DMS drafting section
		Access to Communication Plattform

Entity	IT role	IT use case
Stakeholder Cybersecurity Certification Group	SCCG_User	Access to Communication Plattform
manufacturers & providers	Submitter_User	Submits a EU statement of conformity
Interested Parties	Complains_User	Provides feedback
The Public	NO_ROLE	Access to publicly available information on Publication Platform
European Standardisation Organisations (ESO)	ADWG_User	Access to Collaboration Platform
		Access to Communication Platform
Ad hoc Working Group	ADWG_User	Access to Collaboration Platform
National Cybersecurity Certification Authority	NCCA_user	Upload annual report

For users logged in, the above-mentioned classes of users should be defined. In justified cases additional roles may be foreseen including Conformity Assessment Body, National Accreditation Body and Other stakeholders (as a default value like in online stores). Users have their own accounts, belonging to one of the classes above. Accounts are created by individual users, ENISA activates them (in specific cases, ENISA can also create these accounts).

Different web server elements are available to different classes of users. The following web server elements support the functions of the IT system:

1. Requests for schemes
2. Schemes under the EU framework (database of schemes)
3. Conformity Assessment Bodies
4. Documents repository
5. Message board
6. Ad-hoc Expert Groups management
7. Database of national schemes
8. Last events
9. Contact ENISA

1. **Requests for certification scheme**
    - Requests can be initiated by European Commission or ECCG
    - Specific attribute of the user (EC/ECCG) required to launch the request
    - Online form with the following fields:
        - Name of scheme
        - Reference to Rolling Plan
        - Requestor

        - Assurance level
        - Scope
        - Requirements
        - Other information (specific documents can be uploaded later, to the working folder)
    - Scheme, after being requested, shows on the web server with the following status:
        - Request received
        - Pending MB approval
        - Under elaboration
        - Transmitted to European Commission
        - Published (reference to COM decision)
        - Rejected
        - + status - Received, Pending MB approval, Under elaboration, Scheme transmitted to COM, Scheme published (number of COM decision), scheme rejected (by whom, on which grounds)
    - Validation service required:
        - Requests receives a number and a “service ticket” is issued
        - ENISA acknowledges reception of request
        - Management Board allows to launch the preparation of the scheme (art.49.2)
        - Ticket “solved” when the draft scheme is delivered to the European Commission
        - All changes communicated to the requestor, EC and ECCG
        - General observation: the EC, according to CSA, doesn’t intervene in the process of writing schemes

2. **Database of schemes**
    - Content
        - Status of schemes (request / elaboration / published / withdrawn)
        - Documentation of the scheme (all parts)
        - Certificates issued under the scheme
        - National schemes withdrawn
        - CABs accredited for the scheme
        - Date of last evaluation of the scheme
    - Schemes documents - uploaded by ENISA
    - National schemes affected - uploaded by ENISA
    - Certificates/statements of conformance and their status will be managed by national bodies and will include:
        - Name of product/service/process
        - Assurance level
        - Status of certificate (valid, withdrawn, expired)
        - Date of granting
        - CAB issuing certificate
        - Date of validity
        - Link to more information (art.55)
    - If evaluation date approaches 5 years
        - Notification has to be issued to ENISA
        - Option to receive feedback from logged stakeholders should be provided through an online form
3. **Database of Conformity Assessment Bodies**
    - In principle, CABs should be notified to the European Commission, not to ENISA. However, for consistency, ENISA should maintain this information as well
    - National Accreditation Bodies could “notify the European Commission” through ENISA system

- Alternatively, the information about accredited CABs could be received by ENISA from the Commission – to be discussed with EV
- Content of database
- Name of the CAB
- Name of the accrediting NAB
- Scheme for which CAB is accredited (automatic link to the database of schemes)
- Link to the information about accreditation
- Date of accreditation
- Date of expiry of accreditation

4. **Documents repository**
   - Suggested format – like used by SDOs
   - Purpose: exchange of documents between ENISA, EC, ECCG and SCCG
   - Folders
   - Meetings / Type (ECCG, SCCG, other) / Year / Meeting number
   - Projects / Scheme (number of the request) or short name
   - Proposed file names:
     - REQ – request,
     - INE – input ECCG
     - INS – input SCCG
     - DRS – draft of a scheme
     - SOV – summary of votes
   - Documents can be uploaded either by ENISA, or by the allowed bodies
5. **Message board**
   - Main purpose
   - Exchange of information with ECCG
   - Exchange of information with SCCG
   - “Forum” type, structured according to type of communication
   - Subgroups
   - Input ECCG
   - Input SCCG
   - General discussions
   - Possibility of commenting in threads and uploading documents
   - Possibility of weighted voting (for eventual use – user definition should contain the field “number of votes” for specific entity, like “ECCG France = 5”)
   - Threads started after reception of request (common format needed – to be elaborated)
6. **Ad-hoc Expert Groups management**
   - Information about “CEI” for experts for ad-hoc EGs
   - Upload of experts applications through webpage
   - Announcements of selection of experts for specific schemes
   - For logged in experts already contracted
   - Repository of documents
   - Collaborative working environment
7. **Database of national schemes**
   - Internal database, accessible to ENISA, European Commission, ECCG and SCCG
   - Responsibility of national bodies (or SCCG members) to provide input when requested, at the beginning of elaboration of schemes
   - Request to SCCG for information on industrial schemes
   - Information should contain attributes basing on requirements from Art.54 (elements of the scheme)
   - ENISA selects the entries with potentially affected schemes
   - Final draft of schemes includes schemes selected as overlapping
8. **Last events**

- Information filtered according to class of user
- Content
- Announcements (from ENISA)
- Information about new documents uploaded
- Information about new messages on the board
- Public information on progress in preparing candidate schemes ("ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process", Art. 49.3.)

9. **Contact ENISA**
   - A "mailbox" supporting various types of communication
   - Request for scheme
   - General opinion
   - Specific opinions (for example: on existing European cybersecurity certification schemes)

In principle, the responsibility is on the Commission and/or the ECCG, but ENISA might be involved in peer reviews of National certification bodies and "Bodies that issue certificates" at the high assurance level. ENISA carries out evaluation of schemes every 5 years. IT system functionality other than message board might not be necessary. Templates for requests, comments on schemes, evaluation of schemes, applications for ad-hoc EGs etc. have to be developed. Documents, exchange of information etc should be available and traceable at all times (like all work in SDOs, especially ISO). Security, backups etc. should be the duty of the contractor. The system designed should be portable, in case of change of service provider.

1.7 BUSINESS PROCESSES

Based on the above, we describe the main business processes and associated activities, being part of EU Cybersecurity Certification Framework

1.7.1 Design and Publication of URWP

EC leads the design and publication of the URWP. The Stakeholders Cybersecurity Certification Group (SCCG) and the the ECCG have an advisory role in this process. Therefore, the processes required for the publication of the URWP are:

- The forming of SCCG
  - EC prepares the Terms of Reference (ToR) document and the Call for expression of interest
  - EC and ENISA publish the Call for expression of interest
  - ENISA provides a list of candidate members to EC
  - EC selects based on gender and geographical balance criteria
- EC requests advice from SCCG and ECCG
  - Transparent and broad consultation among all stakeholders based on specific criteria
- Publication of a legal non-binding document by EC (at least every three years)
  - Identification of strategic priorities for future EU cybersecurity certification schemes
  - Listing of ICT products, services and processes or categories that will benefit from being covered by a scheme
  - Multiyear overview of requests for candidate schemes taking into account the URWP

1.7.2 Preparation of the Candidate Cybersecurity Certification Scheme

ENISA is responsible to prepare the candidate cybersecurity certification scheme. Other stakeholders involved in this process include the ECCG, EC and an ad-hoc working group.

More specifically, to provide a final candidate cybersecurity certification scheme the processes and procedures required are:

- Publication of the URWP and request from EC to ENISA to prepare the candidate scheme
    - ENISA must respond and commence the process without undue delay
    - In urgent cases the ECCG and EC can request a candidate scheme not included in the URWP
        - ENISA's Management Board (MB) members are entitled to decline the request from ECCG provided they justify their decision
        - URWP is updated accordingly by EC
- Setting up an ad-hoc working group
    - Publish Term of Requirement (ToR) document
    - Create a call for the expression of interest (CEI)
        - ENISA will select members based on gender and geographical balance criteria
- Set the principles for the candidate scheme
    - Security objectives
    - Assurance levels
    - Conformity self-assessment
    - Elements of European cybersecurity certification schemes
- Draft candidate scheme with the advice of ECCG and ad-hoc group
    - Formal, open, transparent and inclusive consultation
    - Iterations and qualification of feedback
- Opinion of the ECCG for the final candidate scheme
    - ENISA shall take utmost account of the ECCG's opinion but the opinion is not binding nor is the absence thereof blocking ENISA to transmit the candidate scheme
- ENISA to transmit the finalized candidate scheme to EC
    - Comprehensive set defined at Union level
        - Rules
        - Technical requirements
        - Standards
        - Procedures
    - Specified a minimum set of elements
        - Subject matter
        - Scope and object of the cybersecurity certification including ICT products, services and processes covered
        - Detailed specification of cybersecurity requirements with reference to standards or technical specifications
        - Evaluation criteria and methods
        - Levels of assurance and their respective evaluation levels
        - Specify conditions under which software or hardware updates may require recertification of an ICT product or service or the scope of this certificate being reduced

1.7.3 Inclusion of an accepted candidate certification scheme in a Commission Implementation Decision

Once a candidate cybersecurity certification scheme is communicated by ENISA to EC, EC is empowered to adopt it through implementing acts. The processes are:

- ENISA transmits the candidate scheme to EC
- EC is empowered to adopt the proposed candidate schemes by means of an implementing act.

  - EC to prepare an implementing Act
- EC to be notified by national certification authorities regarding the conformity assessment bodies accredited
  - Authorization to issue certificates at specified assurance levels
- EC to publish a list of notified conformity assessment bodies in the Official journal (one year after the entry into force)
  - Amend the list based on notifications after the expiry date
  - Handle requests to remove conformity assessment body

1.7.4 Implementation of Cybersecurity Certification Scheme

A number of stakeholders are involved in the implementation of the certification scheme with different roles and responsibilities. It is worth noting that ENISA is not explicitly involved in this stage apart from receiving feedback regarding the schemes. More specifically, the processes are:

- Manufacturers of ICT products or services submit applications to a conformity assessment body (CAB)
- Submissions for certification must provide to the conformity assessment body all necessary information to conduct the certification process
- Information should be in electronic format and available at least until the expiry date of the certificate or statement of conformity
- Each Member State (MS) to designate one or more national cybersecurity certification authorities responsible to supervise compliance with obligations arising from cybersecurity Act
  - MS to inform EC of the designated authorities and their tasks
  - MS can assign tasks to existing authorities
  - MS can assign authorities in the territory of other MS upon mutual agreement
  - Activities of national cybersecurity authorities related to activities of certification
    - Specific tasks and responsibilities
- Authorities to provide an annual summary report to EC and ENISA
  - Monitoring and enforcement
  - Activities of conformity assessment bodies
  - Activities of public bodies (accredited as conformity assessment bodies or national cybersecurity certification authorities)
- EC and national authorities to exchange information, experiences and good practice with the assistance of the ECCG
  - Share information on possible non-compliance

1.7.5 Request deriving from the implementation of the scheme

There are obligations for ENISA, which occur after the adoption of the scheme and revolve around gathering information during the lifecycle of every scheme. These are:

- Receive feedback for the finalized scheme
  - Identify key stakeholders to provide feedback
    - EC, ECCG, national authorities, self-certified organizations, manufacturers
  - Design a system to receive feedback
    - Establish a template for stakeholders to provide feedback
    - Receive annual reports from EC and national authorities
    - EC's information exchange system for peer review is a potential system that ENISA can utilize
  - Establish criteria to assess the effectiveness of schemes
    - Key Performance Indicators

- Make available an up-to-date website
    - Publish information for adopted schemes
        - Request EC to notify ENISA when a scheme is adopted
        - Specify timeframe within which to receive this information
        - Publish information for candidate schemes
        - Establish a template
    - Specify timeframe for publication
        - Create publicly available reports for the candidate schemes
        - Establish a template for such a report with withdraw and expiration dates
    - Specify timeframe for publication
    - Automatically check internally when schemes are due to expire
        - Create notifications for expired schemes and commence the revision process
        - Set the timeframe for the triggering mechanism (how many months before the expiry date)
- Elicit certificates and EU statements of conformity from all relevant stakeholders
    - Establish a system that will allow national authorities, conformity bodies and manufacturers to report when certificates are issued, revoked or altered
    - Design a template for stakeholders to report such information for every case
    - Create a repository of links for information provided by manufacturers
    - Identify and publish which national certification schemes are replaced by European schemes
- Respond to invitation from EC to support the peer review process
    - EC to create ToR

1.7.6 Registration of self-asserted certificate

This process is mainly the process for receipt, cataloguing and storage/recovery of self-asserted conformity claims and the resultant "EU statement of conformity".

The participants in this process are:

- ENISA
    - Registrar
    - Claimant review authority
- The claimant
    - The evaluation authority of the claimant;
    - The authority for the specification that the claimant asserts conformity to

The manufacturer shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity with the scheme available to the NCCA for the period provided for in the corresponding European cybersecurity certification scheme.

A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

1.7.7 Assessment and subsequently seek the revision

A critical element of the cybersecurity certification framework is to assess and subsequently seek the revision, where necessary, of adopted schemes. The processes are:

- EC to assess regularly and at least biannually the efficiency and utilization of the adopted certification schemes

- EC to assess if certain schemes should be rendered mandatory through relevant Union legislation
    - Identify ICT, products, services and processes for mandatory schemes
    - Priorities sectors listed in Annex II of 2016/1148 Directive
    - Selection of mandatory schemes based on the criteria described in the Cybersecurity Act

1.7.8 Peer review and mutual recognition

To ensure a uniform implementation, peer reviews for relevant certification authorities are mandatory. The processes for the peer reviews are:

- EC to organize with at least two MS peer reviews for authorities
    - ENISA may participate in the peer review
- Implementing acts may be adopted to establish plans for peer reviews
    - Peer reviews to cover a period of at least five years
    - Specific criteria for peer review teams and methodology used
- The ECCG will draw up summaries of these reviews

There are specific excerpts in the cybersecurity Act denoting how EC can engage in discussions with third countries to create mutual recognition agreements for cybersecurity certifications. The processes are:

- Mutual recognition agreements
    - ENISA and the ECCG to advise EC on which negotiations to initiate with third countries
    - Mutual recognition agreements can be stated in the candidate cybersecurity certification scheme

2. FUNCTIONAL REQUIREMENTS

2.1 IT SYSTEM ARCHITECTURE AND FUNCTIONAL COMPONENTS

2.1.1 Logical architecture

Based on the processes identified and the associated activities, the main components of the integrated IT system to support all functionalities are presented in the diagram below. Yellow boxes depict the information available for a general public, while the green ones refer to collaborative tools

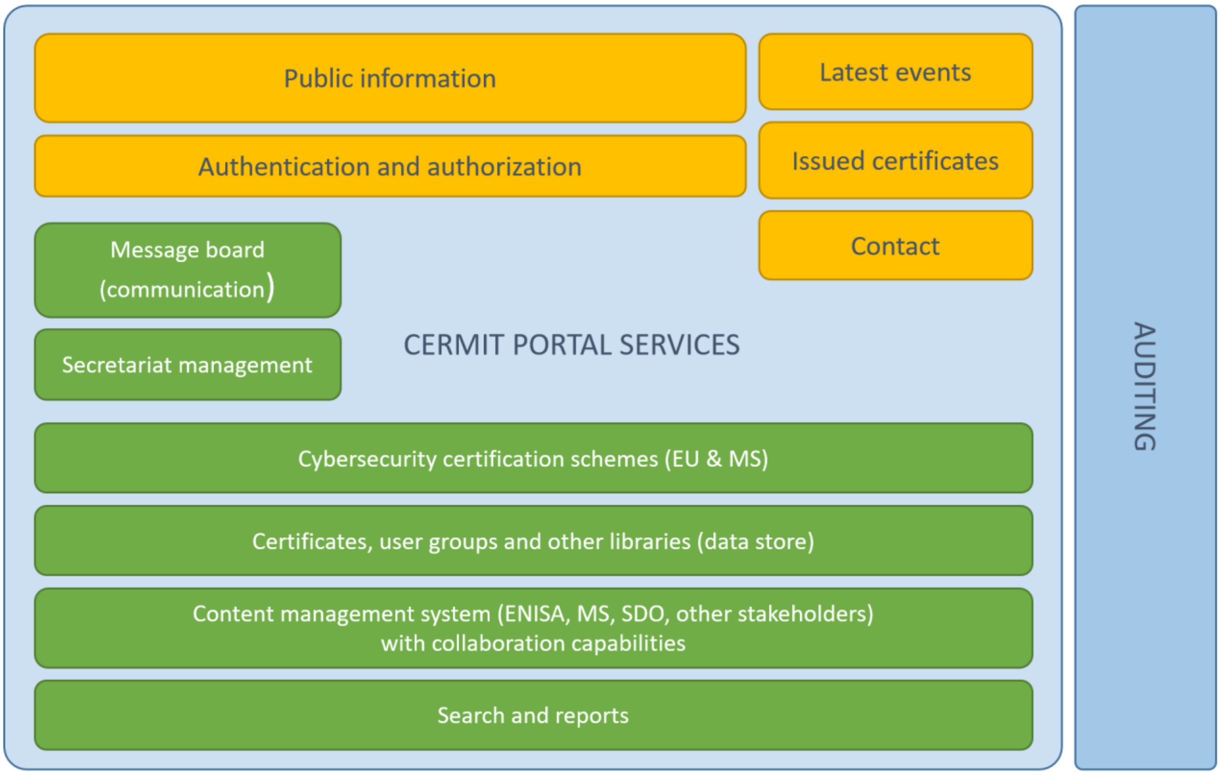

Public information
Latest events
Authentication and authorization
Issued certificates
Message board (communication)
Contact
Secretariat management
CERMIT PORTAL SERVICES
Cybersecurity certification schemes (EU & MS)
Certificates, user groups and other libraries (data store)
Content management system (ENISA, MS, SDO, other stakeholders) with collaboration capabilities
Search and reports
AUDITING

Figure 10 – IT system logical architecture

This section extends the analysis of the processes that are described in the Cybersecurity Act, as presented in Section 2.2 of this document, and identifies the key building blocks for an integrated system that will underpin ENISA's activities. For every key building block of the system, we detail the functional and technical requirements in the next stages.

2.1.2 Major Functional Components

The new IT System will provide the following major components:

- Databases for the storage and publication of cybersecurity certification schemes, certificates, statements of conformity, conformity assessment and other bodies

- Collaboration platform for the preparation and approval/rejection of the above-mentioned types
- Communication platform for the secure, traceable communication between the different entities
- Content Management System with configurable publishing workflows, versioning and commenting capabilities:
  - Links to internal and external pages
  - Regular pages with static content
  - Files (any type), with extended functionality detailed in section
  - Videos and images
  - Events and meetings

The main access to all system functionalities will be done through the portal. Users should feel as they are interacting with a single platform, in a coherent sequence across devices. They should also be agnostic of the different technologies used to build the IT System.

The main functional components identified for the IT System are detailed in section 2.4. Functional requirements include:

- Authentication and authorization
- Document and content management
- Libraries (data store)
- Reporting, data mining and auditing
- Collaboration on documents
- Functional public website

2.2 USE CASES

Based on business needs identified and the main functionalities of the IT System, we have identified the following use cases, which will be detailed in this section.

2.2.1 Use cases overview

Entity	IT Role	Use Cases	Use Case Notation
European Commission	EC_User	Access to communication platform	UC01
		Publish Union rolling work programme	UC02
		Request certification scheme	UC03
		Access to propose cybersecurity certification schemes	UC04
		Formal approval of cybersecurity certification schemes	UC05
		Request revision of schemes	UC23
		Provide feedback for schemes	UC24
		Request for mutual agreement	UC29
		Formal peer review	UC25
		Access Meeting management	UC14

Entity	IT Role	Use Cases	Use Case Notation
ENISA	Roles_Admin	Administration of roles and assignation of accounts to specific roles	UC06
	CSS_Admin	Administration and publication of cybersecurity certification schemes	UC07
	Certs_Statements_Admin	Administration of EU cybersecurity certificates and EU statements of conformity	UC08
	Com_Admin	Administration of communication platform and official publications	UC09
	DraftSection_Admin	Administration of the drafting section	UC10
	ADWG_Secretary	Prepare a candidate scheme	UC11
		Review a candidate scheme	UC12
		Access to Content management system (CMS) drafting section	UC13
		Prepare reports	UC26
		Access Meeting management	UC14
	ENISA_User	Access to collaboration platform	UC21
		Access to CMS drafting section	UC13
		Access to communication platform	UC01
		Mutual recognition	UC32
Management Board of ENISA	Mgmt_Board_User	Approve requests to prepare a candidate scheme	UC15
		Transmit draft of proposed candidate scheme to EC	UC17
		Reject request for candidate scheme	UC27
European Cybersecurity Certification Group	ECCG_User	Request certification scheme	UC03
		Access to DMS drafting section	UC13
		Access to Communication Platform	UC01
		Provide feedback for schemes	UC24
		Approval of cybersecurity certification schemes	UC05
		Access Meeting management	UC14
Stakeholder Cybersecurity Certification Group	SCCG_User	Access to Communication Platform	UC01
		Access Meeting management	UC30
Manufacturers & Providers	Submitter_User	Submit an EU statement of conformity	UC18

Entity	IT Role	Use Cases	Use Case Notation
Interested Parties	Complains_User	Provide feedback	UC19
The Public	NO_ROLE	Access to publicly available information on publication platform	UC20
		Search	UC28
European Standardisation Organisations (ESO)	ESO_User	Access to communication platform	UC01
		Access to collaboration platform	UC21
Ad hoc Working Group	ADWG_User	Provide feedback for schemes	UC24
		Provide voting for draft candidate certification scheme	UC16
		Access to collaboration platform	UC21
		Access to communication platform	UC01
		Access Meeting management	UC14
National Cybersecurity Certification Authority	NCCA_user	Upload annual report	UC22
All Entities	All Roles	Login	UC29
All Entities	All Roles	Register	UC30
All Entities	All Roles	Logout	UC31

2.2.2 Use Cases and Diagrams

Based on use cases identified, we propose a general use case diagram, which will be detailed in the next phase below.

2.2.2.1 UC01 – Access to the Communication platform

Use case name: **Access to Communication Platform**	**ID:** **UC01**	**Priority:** **High**
Actors: EC_user, SCCG_User, ECCG_User, ADWG_User, Com_Admin, ESO_User, ENISA_User		
Description: The use case describes the interaction between users and the communication platform of the IT System. This use case covers the main part of the Communication platform – the Message Board. The Meeting Management tool and the email notifications to subscribers are covered in separate use cases.		
Trigger: Actors are logged in the system and want to access the communication section from the website. *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the platform		
Normal course:	*Information for steps:*	

1. User accesses the Message Board and reviews the tasks for them and the team(s) 2. User follows up on the specific tasks using the portal functionality 3. User selects a group or specific e-mail address 4. User prepares the message 5. User sends a message to the group members or other entities involved in the process 6. User reviews the discussion threads (s)he is allowed to access 7. User responds to messages 8. System stored the messages posted 9. Notification emails are sent to subscribers	
Alternative courses: n/a	
Post conditions: 1. The actors accessed the communication platform, reviewed the messages received, sent messages	
Exceptions: n/a	

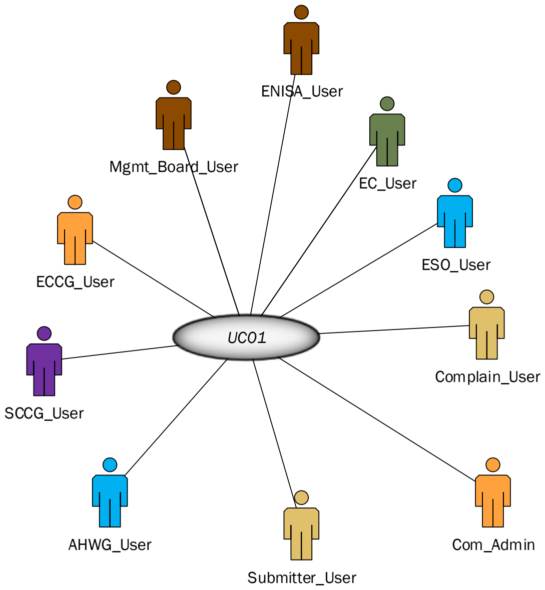


Figure 11: Access to the Communication Platform Use Case Diagram

2.2.2.2 UC02 – Publish Union rolling work program

Use case name: **Publish Union rolling work programme**	**ID:** **UC02**	**Priority:** **High**
Actors: EC_user		
Description: Publishing the URWP document on the website		
Trigger: Actors are logged in the system and want to publish a finalized URWP document *Type:* External		
Preconditions:		

Actor is logged in the system and has appropriate authorization to access the platform	
Normal course: 1. User browses the specific folders 2. User selects the finalized version of the document 3. User prepares the publishing conditions and location 4. User previews document in final draft 5. User reviews that document is published in a correct format and in the correct location 6. User pushes the 'Publish' button	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The actors accessed the specific document and document was published on the website	
Exceptions: n/a	

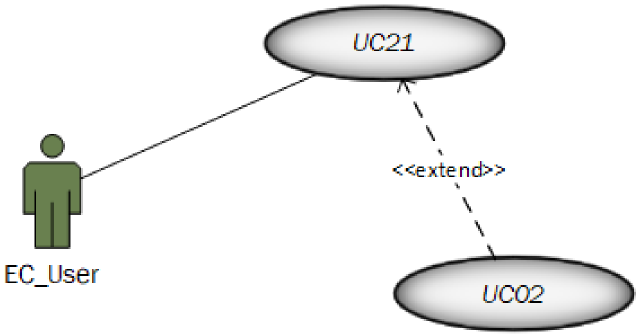


Figure 12: Publish Union rolling work program Use Case Diagram

2.2.2.3 UC03 – Request certification scheme

Use case name: **Request certification scheme**	**ID:** **UC03**	**Priority:** **High**
Actors: EC_user, ECCG_User		
Description: The use case describes the interaction between users and the communication platform of the IT System in order to request a certification scheme		
Trigger: Actors are logged in the system and want to access the communication section from the website. *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the communication platform		
Normal course: 2. User accesses the corresponding section of the portal and adds a new request 3. User fills in the corresponding fields of the factsheet	*Information for steps:*	

4. User selects one or more roles to send the message to 5. User prepares the request message 6. User sends a message to the group members of ENISA 7. System stores the request 8. System updates the progress bar	
Alternative courses: n/a	
Post conditions: 1. The actors accessed the communication part of the corresponding section of portal and sent the request to the group members of ENISA	
Exceptions: n/a	

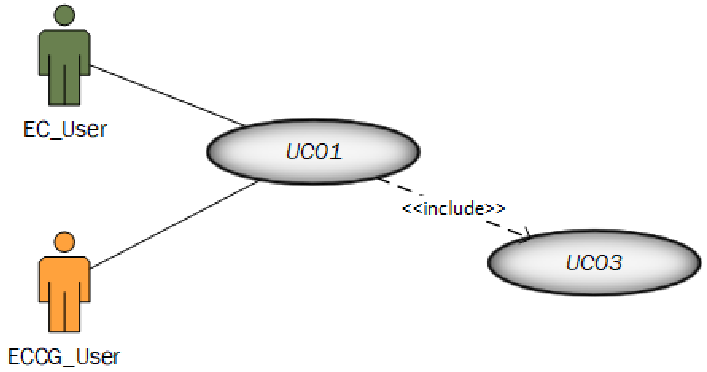


Figure 13: Request certification scheme Use Case Diagram

2.2.2.4 UC04 – Access to proposed cybersecurity certification schemes

Use case name: **Access to propose cybersecurity certification schemes**	**ID:** **UC04**	**Priority:** **High**
Actors: EC_user, ECCG_User, ENISA_User		
Description: The use case describes the interaction between users and the collaboration platform of the IT System, in order to access the proposed cybersecurity certification scheme		
Trigger: Actors are logged in the system and want to access the proposed cybersecurity certification scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the collaboration platform		
Normal course: 2. User accesses the corresponding section of the portal 3. User browses the folders and selects the specific location	*Information for steps:*	

4. User selects the specific factsheet that includes the proposed cybersecurity scheme 5. User assesses that all parameters are included in the proposal 6. User reviews the templates for certification	
Alternative courses: n/a	
Post conditions: 1. The user accessed the collaboration platform 2. System sent notification regarding the updated document to the relevant groups	
Exceptions: n/a	

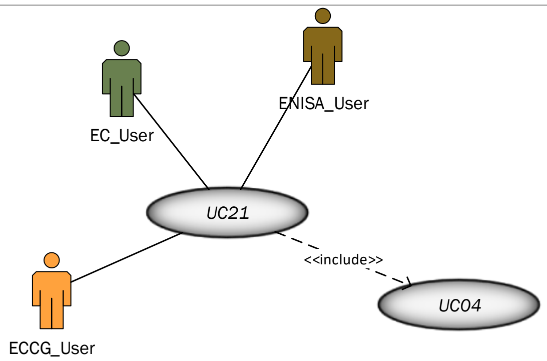


Figure 14: Access to proposed cybersecurity certification schemes Use Case Diagram

2.2.2.5 UC05 – Formal approval of cybersecurity certification schemes

Use case name: **Formal approval of cybersecurity certification schemes**	**ID:** **UC05**	**Priority:** **High**
Actors: EC_user		
Description: The use case describes the interaction between user and collaboration platform of the IT System in order to access and approve the final cybersecurity certification scheme		
Trigger: Actors are logged in the system and want to access the final cybersecurity certification scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the collaboration platform		
Normal course: 1. User access the corresponding section of the portal 2. User browse the folders and select the specific location 3. User select the specific document that includes the final version of cybersecurity scheme 4. User reviews the document 5. User pushes the ‘approve’ button	*Information for steps:*	

6. System sends an update notification to all group members	
Alternative courses: n/a	
Post conditions: 1. Cybersecurity Candidate scheme approved 2. The notification related to final status of document was sent to all relevant actors 3. Status of cybersecurity certification scheme is ‘approved’ 4. Progress bar was updated	
Exceptions: n/a	

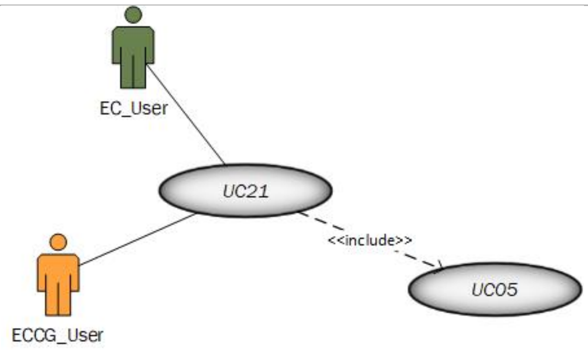


Figure 15: Formal approval of cybersecurity certification schemes Use Case Diagram

2.2.2.6 UC06 – Administration of roles and accounts assigned to specific roles

Use case name: **Administration of roles and accounts assigned to specific roles**	**ID:** **UC06**	**Priority:** **High**
Actors: Roles_Admin		
Description: The use case describes the interaction between user and administration platform of the IT System in order to manage the roles and accounts		
Trigger: Actors are logged in the system and want to access the administration section of IT System *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the administration section of the system		
Normal course: 1. User accesses the administration section 2. Users directed to the EU Login interface for creating accounts or retrieving passwords 3. User creates roles and assigns different rights for each role (view, change, review) 4. User assigns local roles to individual users to access different areas of the portal (entire portal, schemes’ revision section, collaboration sections, etc.) 5. System stores the information related to user accounts, roles, permissions	*Information for steps:*	

6. System sends notifications to users related to updating their rights	
Alternative courses: n/a	
Post conditions: 1. The roles, rights and permissions were assigned to all participants 2. User accounts, rights and permissions are stored in the system 3. Notifications regarding the updating rights in the portal are sent	
Exceptions: n/a	

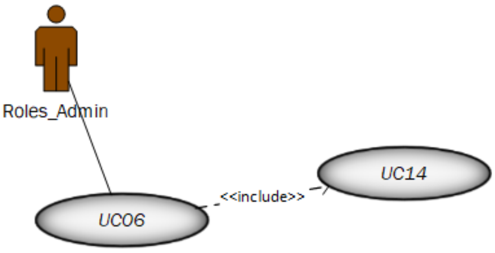


Figure 16: Administration of roles and account assigned to specific roles Use Case Diagram

2.2.2.7 UC07 – Administration and publication of cybersecurity certification schemes

Use case name: **Administration and publication of cybersecurity certification schemes**	**ID:** **UC07**	**Priority:** **High**
Actors: CSS_Admin		
Description: The use case describes the interaction between users and the administration platform of the IT System, in order to manage the cybersecurity certification scheme		
Trigger: Actors are logged in the system and want to access the administration of cybersecurity scheme section of IT System *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the administration section of the system		
Normal course: 1. User accesses the administration section 2. User creates a certification scheme factsheet 3. User prepares the information to be uploaded into the different fields of the factsheet 4. System stores all information inserted in certification scheme factsheet 5. User maintains the information up to date 6. User assigns permissions to access this data to one or more roles 7. System stores the specific rights and permissions related to user access	*Information for steps:*	

8. The administrator grants access for commenting and voting on the certification scheme for different user roles 9. User publishes the certification scheme in the desired location in the website 10. System updates the status of the scheme 11. System sends notification to associated recipients regarding the update	
Alternative courses: n/a	
Post conditions: 1. Certification scheme database was updated 2. All information of the factsheet was uploaded into the database 3. All participants in the process were assigned a specific role, with rights for accessing the certification scheme 4. System stored the information, along with the associated rights and permissions 5. Cybersecurity certification scheme was published and available to the public 6. System sent notifications to users regarding the update	
Exceptions: n/a	

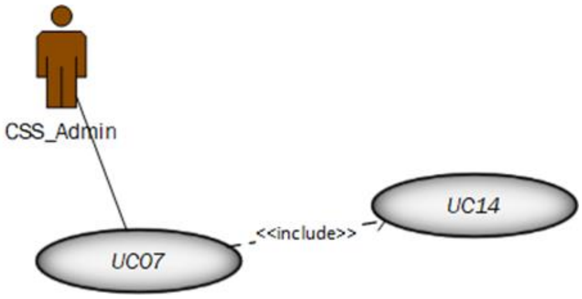


Figure 17: Administration and publication of cybersecurity certification schemes Use Case Diagram

2.2.2.8 UC08 – Administration of EU cybersecurity certificates and EU statements of conformity

Use case name: Administration of EU cybersecurity certificates and EU statements of conformity	ID: UC08	Priority: High
Actors: Certs_Statements_Admin		
Description: The use case describes the interaction between users and the administration of the IT System, in order to manage the EU cybersecurity certificates and EU statement of conformity		
Trigger: Actors are logged in the system and want to access the administration of cybersecurity certificates and statement of conformity of IT System *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the administration section of the system		
Normal course:	*Information for steps:*	

1. User accesses the section for certificates and statements of conformity 2. User checks the list of new cybersecurity certificates and statements of conformity 3. Updates the data on a certificate or statement of conformity, including their validity periods 4. Uploads the received certificate or statement of conformity in the document management component 5. Uploads the report with certificates issued received from NCCA 6. Prepares the format template for information related to the certificate or statement of conformity, in order to be published 7. System stores all information inserted in issued certificates database 8. User maintains information up to date 9. User assigns access permissions to different roles 10. System stores the specific roles and permissions related to users' access 11. User accesses the specific location in website to publish the report with certificates and statements of conformity issued 12. User previews each certificate or statement of conformity, properly linked to the corresponding schemes 13. User publishes the list of certificates and statements of conformity with associated validity period and status (valid, expired, etc.) 14. System sends notifications to associated recipients regarding the update	
Alternative courses: n/a	
Post conditions: 1. Certificates and statements of conformity metadata were created and stored in the system 2. All specific parameters are up to date 3. All information was uploaded into the database 4. Specific permissions were granted to the appropriate roles for accessing information related to certificates and statements of conformity 5. The information related to certificates and statements of conformity is published with associated status 6. System sent notifications to users regarding the update	
Exceptions: n/a	

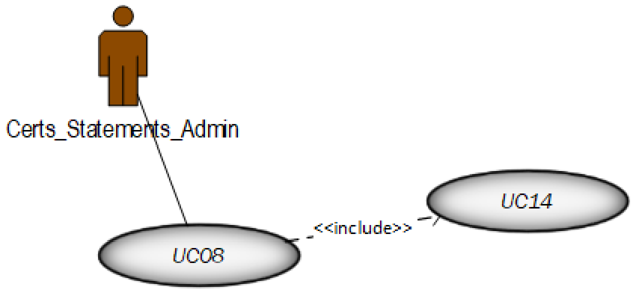


Figure 18: Administration of EU cybersecurity certificates and EU statements of conformity Use Case Diagram

2.2.2.9 UC09 – Administration of the communication platform

Use case name: Administration of communication platform and official publications	ID: UC09	Priority: High
Actors: Com_Admin		
Description: The use case describes the interaction between administrators and the communication platform of the IT System, in order to manage the work spaces		
Trigger: Actors are logged in the system and want to access the administration of communication platform *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the administration section of the system		
Normal course: 1. User accesses the corresponding administration section 2. User creates and configures the Message Board for communication, to ensure an appropriate workflow for communication 3. User defines the necessary message types 4. User provides access to the user's roles for each message type 5. User changes the specific rights of each role assigned during the process 6. System stores the information related to roles and permissions for communication spaces	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The Message Board was created and configured to ensure appropriate workflow for communication 2. All participants in the process were assigned a specific role, with the necessary permissions for the communication section 3. System stored the information related to roles, rights and permissions for each communication space		
Exceptions: n/a		

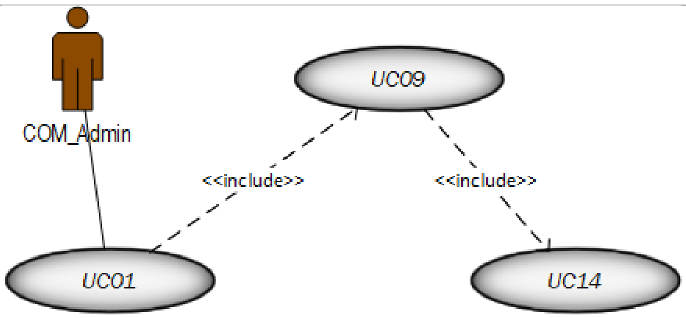


Figure 19: Administration of communication platform and official publications Use Case Diagram

2.2.2.10 UC10 – Administration of the drafting section

Use case name: **Administration of the drafting section**	**ID:** **UC10**	**Priority:** **High**
Actors: DraftSection_Admin		
Description: The use case describes the interaction between administrators and the document management platform of the IT System, in order to manage the draft documents for each section		
Trigger: Actors are logged in the system and want to access the document management platform *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the document management section of the system		
Normal course: 1. User accesses the document management section 2. User defines the default publishing workflow for documents across the section (all folders) 3. User defines the workflow for specific types of documents in specific locations (folders) 4. User implements the workflow for specific types of documents in specific locations 5. User sets up specific permissions for each folder containing documents 6. System stores the information related to roles and permissions for drafting sections 7. User establishes the list of documents that will be drafted in document management section 8. User creates and configures a draft for each specific type of document (certification scheme, URWP, revision report, assessment report, peer review document, mutual agreement document, minutes of meeting, ToR, etc.) 9. User forwards the status of drafted documents in the publishing workflow 10. System sends notification to users related to documents being updated	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The draft documents were created 2. The document publication workflows were defined and implemented 3. The documents drafted were associated a workflow and collaboration spaces 4. The folders and documents were granted access and editing permissions for collaboration section 5. System stored the information related to roles and permissions for each folders and documents 6. System sent notifications to users regarding the updating collaboration spaces		
Exceptions: n/a		

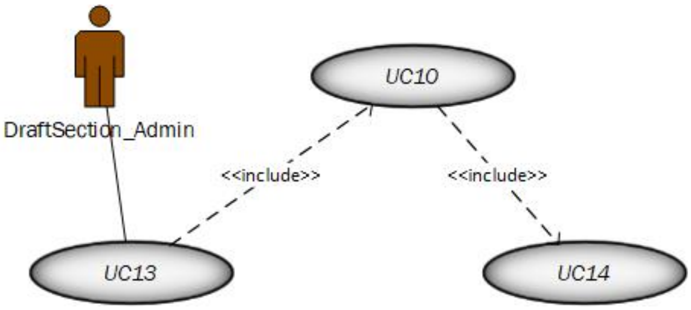


Figure 20: Administration of the drafting section Use Case Diagram

2.2.2.11 UC11 – Prepare a candidate scheme

Use case name: **Prepare a candidate scheme**	**ID:** **UC11**	**Priority:** **High**
Actors: ADWG_Secretary, ENISA_User		
Description: The use case describes the interaction between document management platform of the IT System in order to prepare a candidate schema		
Trigger: The candidate scheme request is approved and actors are logged in the system and want to access the document management platform *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the document management section of the system		
Normal course: 1. User accesses the document management section 2. User establishes the document format for candidate scheme 3. User prepares the content for the candidate scheme 4. User defines the workflow for document 5. User implements the workflow associated to the candidate scheme document 6. User sets up the specific permissions for documents drafted for each user group related to preparation of candidate scheme 7. System stores the information related to roles and permissions 8. User puts the draft document for commenting 9. System sends notifications to users related to updates and comments 10. System updates the progress bar	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The draft documents for candidate scheme were created 2. The document workflows were implemented 3. The documents drafted have associated workflows and collaboration spaces 4. The folders and documents were assigned permissions for collaboration 5. System stored the information related to roles and permissions for each folder and document		

6. The notifications were sent 7. The progress bar was updated
Exceptions: n/a

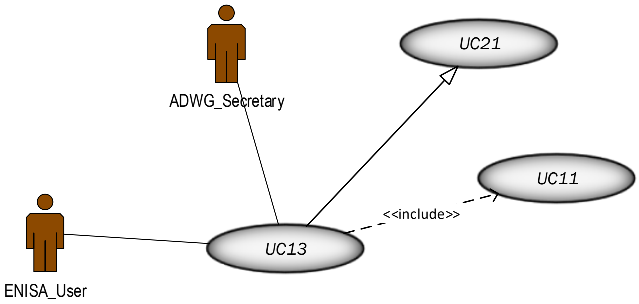


Figure 21: Prepare a candidate scheme Use Case Diagram

2.2.2.12 UC12 – Review a candidate scheme

Use case name: **Review a candidate scheme**	**ID:** **UC12**	**Priority:** **High**
Actors: ADWG_Secretary, ENISA_User		
Description: The use case describes the interaction between users and the collaboration platform of the IT System in order to review a candidate scheme		
Trigger: Actors are logged in the system and want to access the collaboration platform *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the collaboration section of the system		
Normal course: 1. User accesses the collaboration section of the content management system 2. User selects the specific location and document 3. User reviews the content of the document 4. User inserts comments in specific areas of the document 5. System stores the document together with the comments 6. System sends notifications to users related to the new comments 7. System updates the progress bar	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The candidate scheme was reviewed with embedded comments 2. System stored the information related to the comments and their place in the document 3. The notifications were sent 4. The progress bar was updated		
Exceptions: n/a		

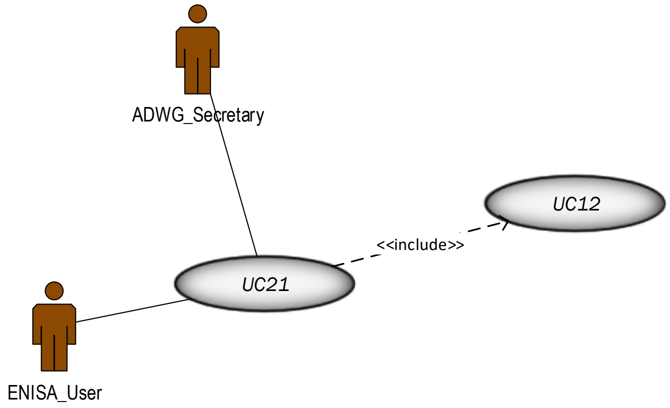


Figure 22: Review a candidate scheme Use Case Diagram

2.2.2.13 UC13 – Access to CMS drafting section

Use case name: Access to DMS drafting section	ID: UC13	Priority: High
Actors: ADWG_Secretary, ECCG_User, ENISA_User		
Description: The use case describes the interaction between user and content/document management platform of the IT System		
Trigger: Actors are logged in the system and want to access the content/document management section *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the document management section of the system		
Normal course: 1. User accesses the document management section 2. User selects the specific location and documents 3. User reviews the folders and documents 4. User establishes the list of documents that will be drafted in document management section 5. User creates and configures a draft for each specific type of document (certification scheme, URWP, revision report, assessment report, peer review document, mutual agreement document, minutes of meeting, ToR, etc.) 6. User defines the workflows for each type of document 7. User implements the workflows associated to each type of document	*Information for steps:*	

8. User sets up specific permissions for each folder of documents drafted 9. Reviews the document status on its workflow and decides to forward the status 10. System sends notification to users related to updating the collaboration spaces	
Alternative courses: n/a	
Post conditions: 1. The access on document management was permitted 2. System stored modifications on folders and documents 3. The collaboration spaces were updated 4. The notifications were sent	
Exceptions: n/a	

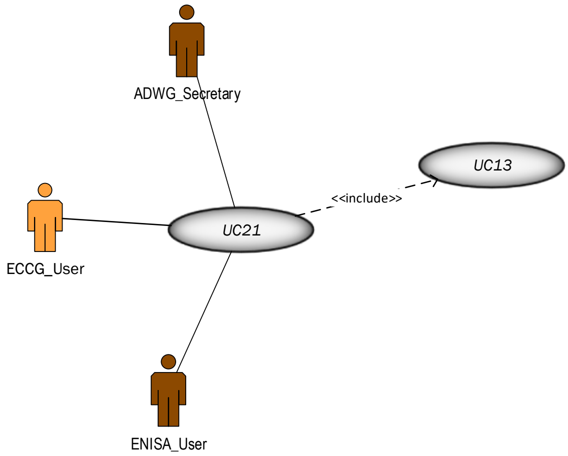


Figure 231: Access to DMS drafting section Use Case Diagram

2.2.2.14 UC14 – Access to Meeting management

Use case name: **Access to Meeting Management section**	**ID:** **UC014**	**Priority:** **High**
Actors: EC_user, SCCG_User, ECCG_User, ADWG_User, ENISA_User		
Description: The use case describes the interaction between users and the meetings platform of the IT System		
Trigger: Actors are logged in the system and want to manage the materials for a meeting *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the section.		
Normal course: 1. User accesses the Meetings section 2. User reviews the meeting schedule 3. User selects meeting creation form to create a new meeting	*Information for steps:*	

4. User selects the period (dates and times) and location for the meeting 5. User selects the participants for the meeting or allows users to register 6. User includes the agenda of the meeting 7. User uploads other background documents 8. User publishes the meeting on the website, either publicly available or restricted to a group 9. System stores the meeting, (day, time, agenda and participants) 10. After the meeting, user uploads presentations and meeting minutes 11. System sends notification to participant related to meeting	
Alternative courses: n/a	
Post conditions: 1. The meeting was created 2. The notifications to participants were sent 3. The meeting and associated information were stored in the system	
Exceptions: n/a	

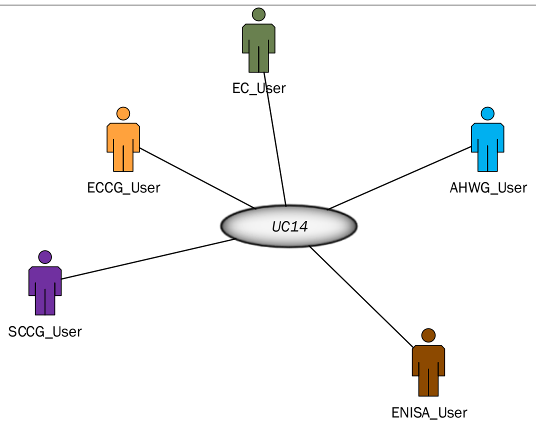


Figure 24: Access to Meeting Management

2.2.2.15 UC15 – Approve requests to prepare a candidate scheme

Use case name: **Approve requests to prepare a candidate scheme**	**ID:** **UC15**	**Priority:** **High**
Actors: Mgmt_Board_User		
Description: The use case describes the interaction between users and the candidate schemes area of the IT System		
Trigger: After having received a notification from the EC for the preparation of a candidate scheme, actors are logged in the system and want to approve the request to prepare the candidate scheme *Type:* External		

Preconditions: Actor is logged in the system and has appropriate authorization to access the communication section of the IT System	
Normal course: 1. User accesses the candidate schemes area 2. User reviews the candidate scheme 3. User evaluates the request 4. User prepares the response 5. User sends the answer to the request with attached status (approved) 6. System stores the request with its associated status, as well as response sent 7. System updates the status of the request	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The request was reviewed and has the status ‘approved’ 2. The answer for the request was transmitted 3. The request, associated status and response were stored in the system 4. The status of the request is updated	
Exceptions: n/a	

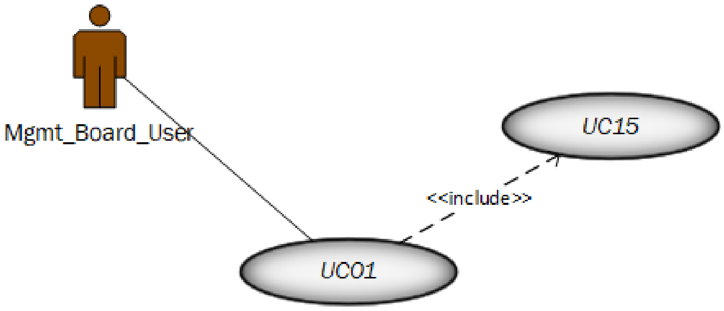


Figure 25: Approve requests to prepare a candidate scheme Use Case Diagram

2.2.2.16 UC16 – Provide voting for draft candidate certification scheme

Use case name: **Provide voting for draft candidate certification scheme**	**ID:** **UC16**	**Priority:** **High**
Actors: ADWG_User		
Description: The use case describes the interaction between users and the collaboration platform of the IT System		
Trigger: The candidate scheme is finalized and actor is logged in the system and want to access the section for candidate schemes from the website in order to vote the candidate certification scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the platform		

Normal course: 1. User access the schemes' section 2. User selects the proposed candidate scheme factsheet 3. User reviews the content of the proposed candidate scheme 4. User selects "Vote" button on the selected candidate scheme 5. System stores the vote on the candidate scheme 6. System updates the progress bar	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The candidate scheme was voted 2. The new status of scheme was stored in the system 3. The progress bar was updated	
Exceptions: n/a	

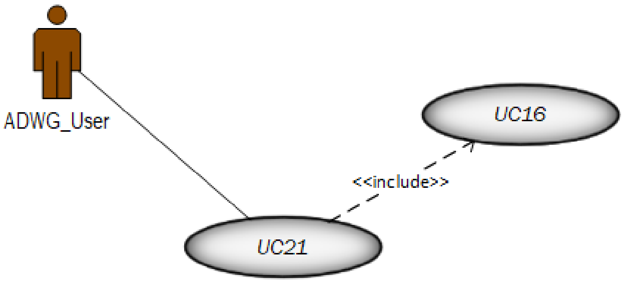


Figure 26: Provide voting for draft candidate certification scheme Use Case Diagram

2.2.2.17 UC17 – Transmit draft of proposed candidate scheme to EC

Use case name: **Transmit draft of proposed candidate scheme to EC**	**ID:** **UC17**	**Priority:** **High**
Actors: ENISA_User		
Description: The use case describes the interaction between users and the collaboration section of the system, in order to transmit the proposed schemes to EC		
Trigger: All feedback and voting are integrated in the final version of proposed candidate scheme and actors are logged in the system and want to transmit draft of proposed candidate scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the communication section of the IT System		
Normal course: 1. User accesses the candidate schemes section 2. User accesses the proposed candidate scheme (UC04)	*Information for steps:*	

3. User reviews the draft of proposed candidate scheme 4. User accesses the Message Board 5. User selects the type of message 6. User selects the specific recipients 7. User attaches the draft of proposed candidate scheme 8. User pushes 'transmit candidate scheme' to the selected recipients 9. System stores the proposed candidate scheme in the document management platform 10. System updates the collaboration platform with the reviewed draft of the proposed candidate scheme 11. System transmits the draft of proposed candidate scheme to the selected recipients (EC_User) 12. System updates the progress bar	
Alternative courses: n/a	
Post conditions: 1. The draft of proposed candidate scheme was reviewed 2. The proposed candidate scheme was transmitted 3. System stored the candidate scheme in collaboration platform and document management platform with associated version 4. The progress bar was updated	
Exceptions: n/a	

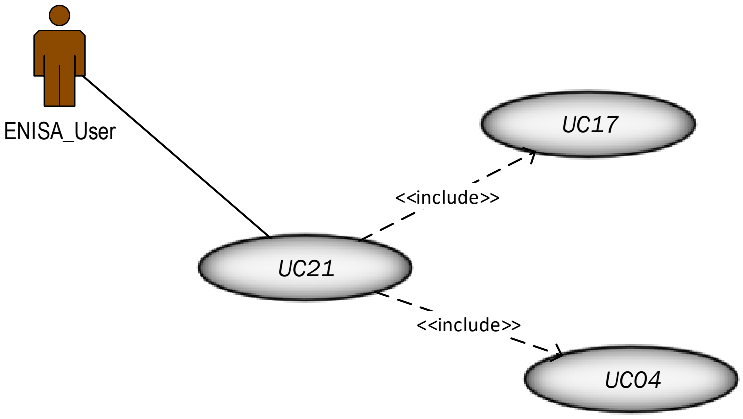


Figure 27: Transmit draft of proposed candidate scheme to EC Use Case Diagram

2.2.2.18 UC18 – Submits an EU statement of conformity

Use case name: **Submits an EU statement of conformity**	**ID:** **UC18**	**Priority:** **High**
Actors: Submitter_User		
Description:		

The use case describes the interaction between manufacturers/service-providers and the communication section of the system	
Trigger: Actors are logged in the system and want to submit an EU statement of conformity *Type:* External	
Preconditions: Actor is logged in the system and has appropriate authorization to access the communication section of the IT System	
Normal course: 1. User accesses the Message Board 2. User selects type of message 3. User selects the desired EU statement of conformity 4. User uploads the EU statement of conformity 5. User prepares the data associated to the EU statement of conformity 6. User selects the recipients 7. User pushes ‘submit statement of conformity’ 8. System stores the EU statement of conformity into specific location 9. System transmits the notification to the sender that the EU statement of conformity is loaded successfully	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The EU statement of conformity was submitted 2. The system was updated 3. The notification of successful submission was transmitted	
Exceptions: n/a	

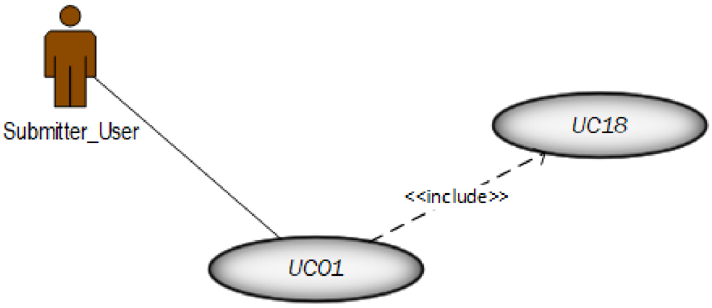


Figure 28: Submits an EU statement of conformity Use Case Diagram

2.2.2.19 UC19 – Provision of feedback for candidate schemes

Use case name: **Provides feedback**	**ID:** **UC19**	**Priority:** **High**
Actors: Complains_User		
Description:		

The use case describes the interaction between interested parties and the communication section of the system, in order to post feedback on a candidate scheme	
Trigger: Actors are logged in the system and want to send feedback for a candidate scheme *Type:* External	
Preconditions: Actors are logged in the system and want to send feedback for candidate scheme	
Normal course: 1. User accesses the specific candidate scheme 2. User prepares the feedback 3. User posts a comment on a new or existing thread 4. User associates the feedback to a particular version of the candidate scheme 5. User sends the feedback 6. System stores the feedback together with the specific version of the candidate scheme 7. System transmits the feedback to the relevant group of recipients	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The feedback on the candidate scheme was transmitted 2. The feedback on the candidate scheme was stored in the system	
Exceptions: n/a	

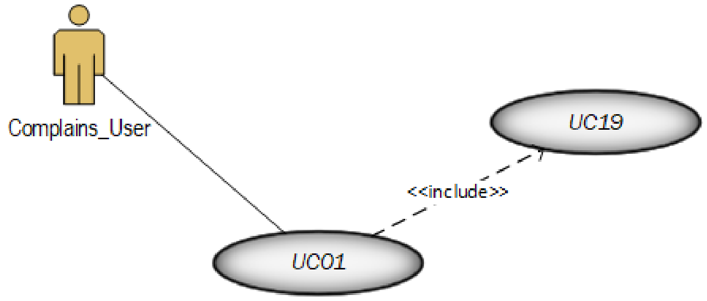


Figure 29: Provision of feedback Use Case Diagram

2.2.2.20 UC20 – Access to publicly available information on Publication Platform

Use case name: Access to publicly available information on Publication Platform	ID: UC20	Priority: High
Actors: NO_ROLE		
Description: The use case describes the interaction between all users and the portal		
Trigger: Actors want to access available information and publications *Type:* External		
Preconditions: n/a		

Normal course: 1. User accesses the portal interface 2. User browses the existing information 3. User searches for types of certificates from the certification scheme 4. User downloads the specific type of certificate 5. User reviews the events	*Information for steps:*
Alternative courses: n/a	
Post conditions: n/a	
Exceptions: n/a	

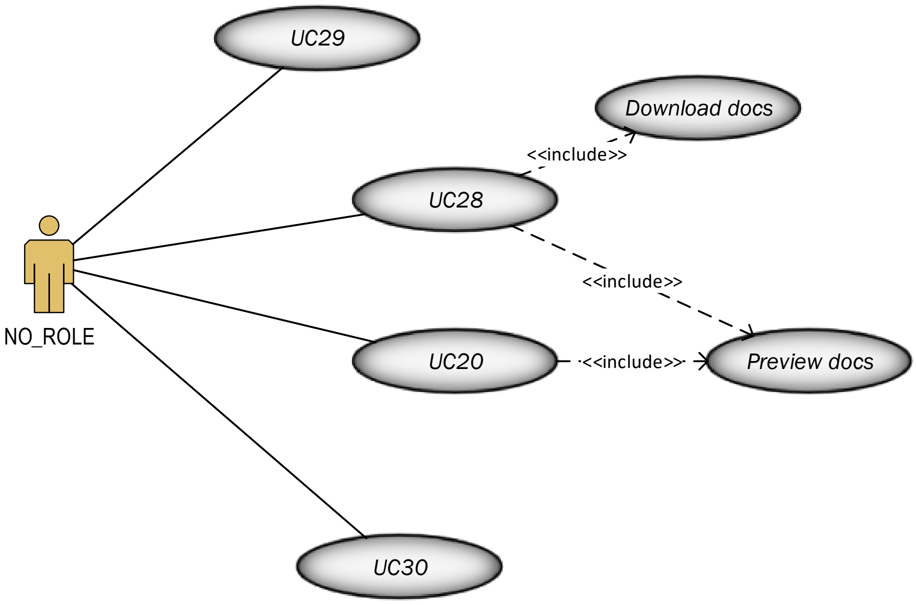


Figure 30: Access to publicly available information on Publication Platform Use Case Diagram

2.2.2.21 UC21 – Access to the collaboration platform

Use case name: **Access to the Collaboration platform**	**ID:** **UC021**	**Priority:** **High**
Actors: EC_user, SCCG_User, ECCG_User, ADWG_User, Com_Admin, ESO_User, ENISA_User		
Description: The use case describes the interaction between users and the collaboration platform of the IT System. The voting part of the collaboration platform is described separately, in UC07 and UC16. The inline commenting part of the collaboration platform is described in UC12.		
Trigger: Actors are logged in the system and want to access the collaboration section from the website *Type:* External		
Preconditions:		

Actor is logged in the system and has appropriate authorization to access the platform	
Normal course: 1. User accesses the collaboration part of the content management system 2. User selects a specific document 3. User reviews the existing comments for each version 4. User provides new comments, either by starting a new thread or by continuing an existing one 5. System stores the comments provided 6. System sends notifications to relevant users involved	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The feedback on documents was posted on specific versions 2. The updates were stored in the system 3. Notifications on new comments were sent	
Exceptions: n/a	

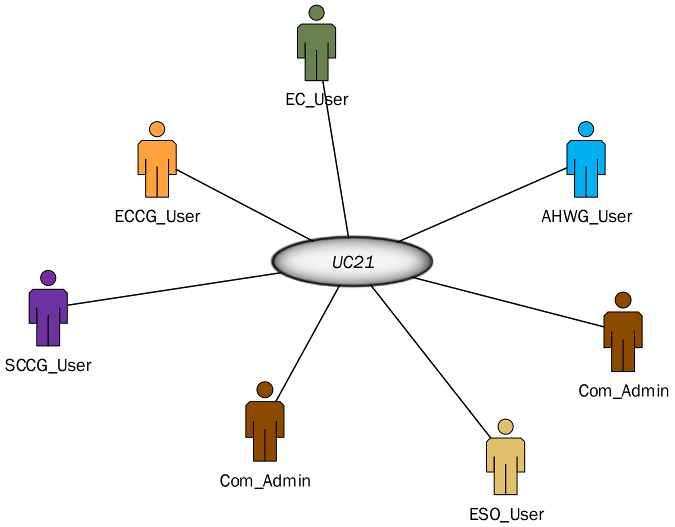


Figure 31: Access to Collaboration Platform Use Case Diagram

2.2.2.22 UC22 – Upload annual report

Use case name: Upload annual report	ID: UC22	Priority: High
Actors: NCCA_user		
Description: The use case describes the interaction between users and content management of the IT System		
Trigger: Actors are logged in the system and want to submit an annual report of issued certificates		

Type: External	
Preconditions: Actor is logged in the system and has appropriate authorization to access the content management system	
Normal course: 1. User accesses the relevant section of the content management system 2. User prepares the file and metadata associated to the annual report 3. User uploads the annual report 4. User pushes 'submit' for the annual report 5. System stores the report into the specific location 6. System sends upload notifications to the sender and relevant users	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The annual report was submitted 2. The system stored the annual report in specific location 3. Notifications of successfully submission were sent	
Exceptions: n/a	

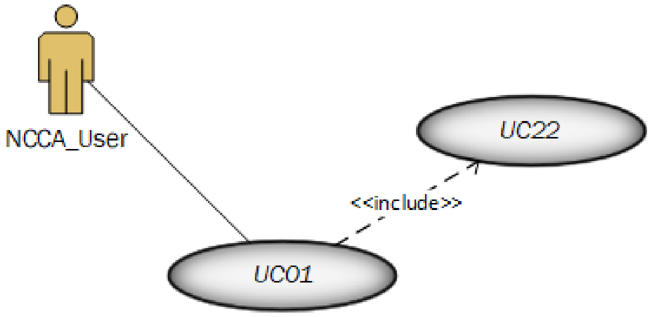


Figure 32: Upload annual report Use Case Diagram

2.2.2.23 UC23 – Request revision of schemes

Use case name: **Request revision of schemes**	**ID:** **UC23**	**Priority:** **High**
Actors: EC_user		
Description: The use case describes the interaction between users and the communication platform of the IT System		
Trigger: Actors are logged in the system and want to access the schemes section of the website *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the communication platform		

Normal course: 1. User accesses the Message Board and reviews the message received 2. User selects appropriate type of message 3. User prepares the revision request message 4. User selects the user groups to notify 5. User sends a message to the group members of ENISA 6. The message is stored in the system 7. System updates the progress bar	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The revision request was transmitted 2. The request was stored in the system 3. The progress bar was updated	
Exceptions: n/a	

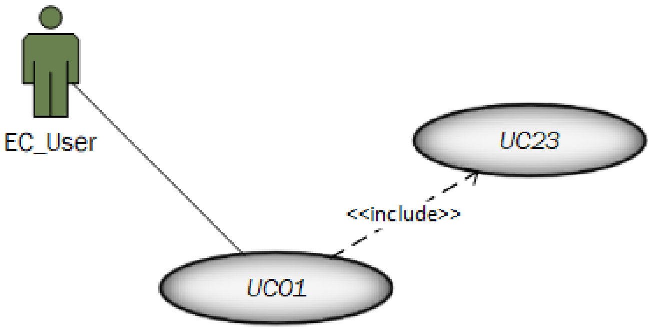


Figure 33: Request revision of schemes Use Case Diagram

2.2.2.24 UC24 – Provide feedback for schemes

Use case name: **Provide feedback for schemes**	**ID:** **UC24**	**Priority:** **High**
Actors: ECCG_User, Submitter_user, NCCA_user, EC_User, ENISA_User		
Description: The use case describes the interaction between user and collaboration and communication parts of the IT System		
Trigger: Actors are logged in the system and want to review and send feedback for candidate scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the collaboration and communication sections of the IT System		
Normal course: 1. ENISA_User design the system to receive the feedback retaled to implementation of new scheme 2. ENISA_User establish the criteria to assess the effectiveness of scheme	*Information for steps:*	

3. The actors provide feedback regarding implementation scheme 4. ENISA_User review the information regarding adopted scheme, the report for candidate scheme 5. ENISA_User publish the information regarding adopted scheme, the report for candidate scheme and scheme expiration 6. System stores the feedback 7.	
Alternative courses: n/a	
Post conditions: 1. The feedback on the candidate scheme was transmitted 2. The feedback on the candidate scheme was stored in the system 3. The information regarding implementation scheme are published 4. The expiration schemes are published 5.	
Exceptions: n/a	

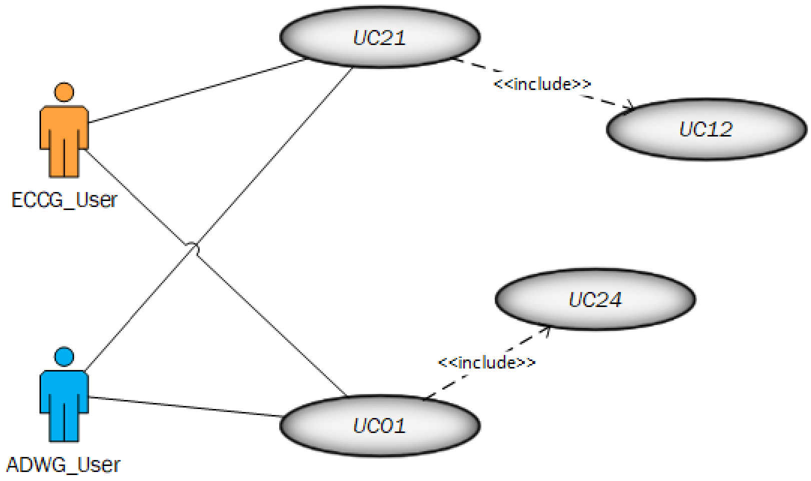


Figure 34: Provide feedback for schemes Use Case Diagram

2.2.2.25 UC25 – Formal Peer Review

Use case name: **Formal peer review**	**ID:** **UC25**	**Priority:** **High**
Actors: EC_User, ECCG_User, NCCA_User, Certs_Statements_Admin, Com_Admin, ENISA_User		
Description: The use case describes the interaction between users and collaboration and communication sections of the IT System		
Trigger: Actors are logged in the system and want to review and send feedback for a scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the collaboration and communication sections of the IT System		

Normal course: 1. EC_User accesses the schemes’ section and establishes the period of peer review for a scheme 2. EC_User accesses the Meeting management and creates a new meeting 3. EC_User prepares the meeting agenda and supporting documents and links 4. EC_User selects the member states involved 5. Com_Admin publishes the meeting 6. System sends notifications for the meeting 7. EC_User accesses the Message Board 8. EC_User selects type of message 9. EC_User prepares request for peer review 10. EC_User selects the specific recipients 11. EC_User sends the request to the selected recipients 12. System sends notifications to the selected recipients 13. EC_User accesses the collaboration section 14. EC_User drafts the criteria for peer review 15. System sends notifications to ECCG_User, NCCA_User and ENISA_User regarding selected criteria 16. ECCG_User accesses the collaboration platform and drafts the summary of the review 17. ECCG_User draws issue guidelines and recommendations on actions and measures for the relevant authorities 18. ECCG_User accesses the Message Board 19. ECCG_User selects the type of message 20. ECCG_User sends notifications to ENISA_User regarding the finalisation of the peer review report and recommendations 21. System stores the peer review report, together with the guidelines and recommendations 22. ENISA_User reviews and publishes the peer review report, guidelines and recommendations 23. System sends notifications on the newly published documents	*Information for steps:*
Alternative courses: n/a	
Post conditions: 1. The peer review was performed 2. The peer review report and recommendations were finalized 3. The peer review report and recommendations were stored in the system 4. The peer review report and recommendations were published 5. Notifications were sent to relevant users	
Exceptions: n/a	

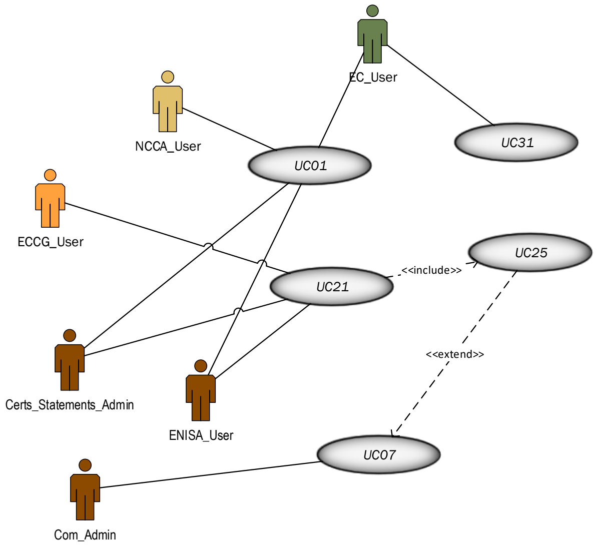


Figure 35: Formal peer review Use Case Diagram

2.2.2.26 UC26 – Prepare reports

Use case name: **Prepare reports**	**ID:** **UC26**	**Priority:** **High**
Actors: ADWG_Secretary		
Description: The use case describes the interaction between users and reports section of the IT System		
Trigger: Actors are logged in the system and want to prepare a report *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access reports section of the system		
Normal course: 1. User accesses the reports section of the website 2. Selects the specific location 3. User chooses a report template 4. System populates the report with data 5. User sets up the specific permissions for accessing report 6. User publishes the report 7. System stores the report in the chosen location	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The report was prepared 2. System stored the new report in the chosen location 3. Report was reviewed 4. Report was published		

Exceptions: n/a

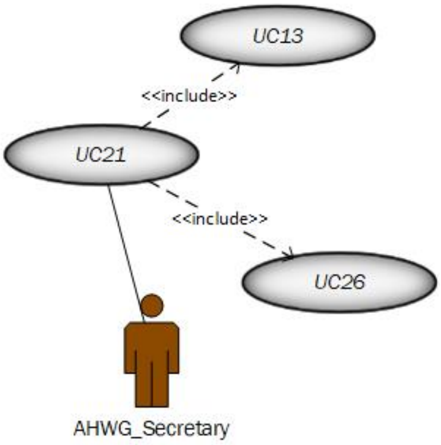


Figure 36: Prepare reports Use Case Diagram

2.2.2.27 UC27 – Reject request for candidate scheme

Use case name: **Reject request for candidate scheme**	**ID:** **UC27**	**Priority:** **High**
Actors: Mgmt_Board_User		
Description: The use case describes the interaction between users and the candidate schemes area of the IT System		
Trigger: Actors are logged in the system and want to reject the request to prepare a candidate scheme *Type:* External		
Preconditions: Actor is logged in the system and has appropriate authorization to access the candidate schemes area of the IT System		
Normal course: 1. User accesses the candidate schemes area 2. User reviews the candidate scheme 3. User evaluates the request 4. User prepares the response 5. User sends the answer to the request with attached status (rejected) 6. System stores the request with its associated status, as well as response sent 7. System transmits the status of the request and the reasons for rejection	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The request was reviewed and has the status ‘rejected’ 2. The answer for the request was transmitted 3. The request, associated status and response were stored in the system		

Exceptions: n/a

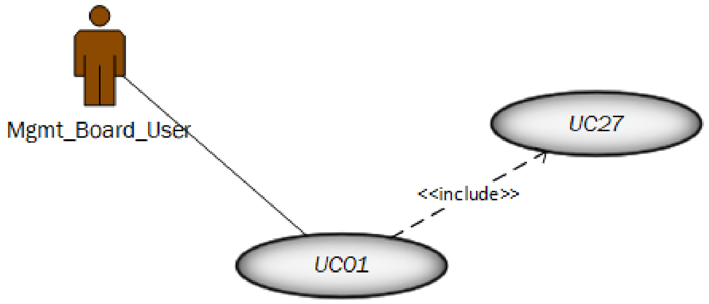


Figure 37: Reject request for candidate scheme Use Case Diagram

2.2.2.28 UC28 – Search

Use case name: **Search**	**ID:** **UC28**	**Priority:** **High**
Actors: NO_ROLE		
Description: The use case describes the interaction between users and the portal’s search section		
Trigger: Actors want to access available information and publications using search option *Type:* External		
Preconditions: n/a		
Normal course: 1. User accesses the portal interface 2. User selects the search bar 3. User inserts keyword to find specific information 4. The system displays relevant information 5. User selects the specific information from the list displayed		
Alternative courses: n/a		
Post conditions: 1. User retrieved the necessary data or information		
Exceptions: n/a		

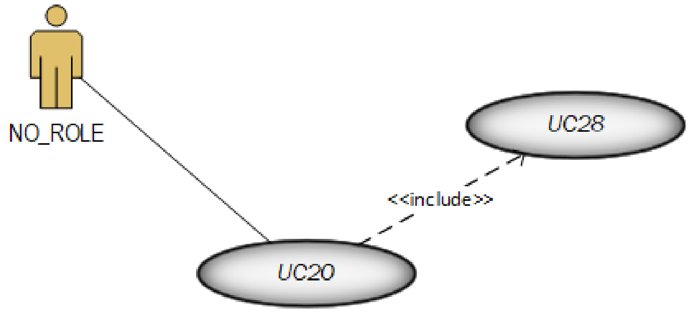


Figure 38: Access to publicly available information on Publication Platform Use Case Diagram (Search)

2.2.2.29 UC29 – User Login

Use case name: **User login**	**ID:** **UC29**	**Priority:** **High**
Actors: All users		
Description: Users will be prompted to login with their credentials account information before they can use the system.		
Trigger: User requests to login *Type:* External		
Preconditions: 1. The user has an account 2. User is not logged in 3. The user is trying to log in		
Normal course: 1. The System directs the user to the EU Login (ECAS) page 2. User follows the instructions and logs in 3. User is redirected to the System as authenticated user 4. The user gains access to the system's functionalities 5. System registers the new access	*Information for steps:*	
Alternative courses: If the User entered an invalid username and/or password, the following occurs: 1. EU Login interface describes the reasons why the User failed authentication 2. EU Login interface presents the User with suggestions for changes necessary to allow the User to pass authentication 3. EU Login interface prompts the User to re-enter the valid information.		

4. The Basic Flow continues where the User enters new information	
Post conditions: 1. The user was logged in to the system 2. The user had access to the appropriate functions of the system	
Exceptions: Incorrect credentials	

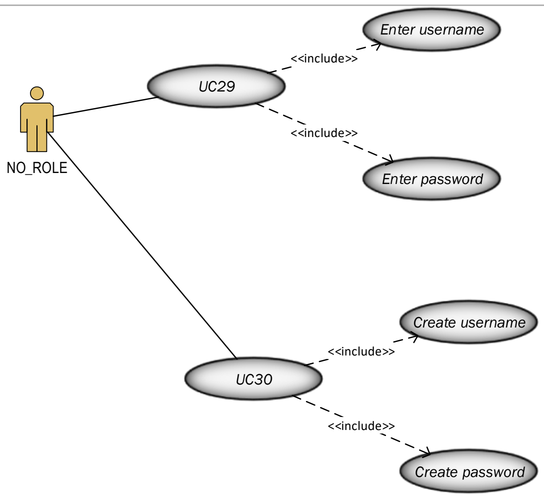


Figure 39: User Login Use Case Diagram

2.2.2.30 UC30 – User Registration

Use case name: **User register**	**ID:** **UC30**	**Priority:** **High**
Actors: All users		
Description: A user of the IT System creates an account		
Trigger: User requests to login *Type:* External		
Preconditions: The user doesn’t have an account		
Normal course: This use case starts when a system user is not logged in to the system and goes to the login page. 1. The System directs the user to the EU Login (ECAS) page 2. User follows the instructions and creates an account 3. User returns to the System and logs in with the newly created account	*Information for steps:*	
Alternative courses: n/a		

Post conditions: 1. The user entered successful information and is returned to the home page as a Logged in User 2. User was unable to log in for one or more reasons and is returned to the home page
Exceptions: n/a

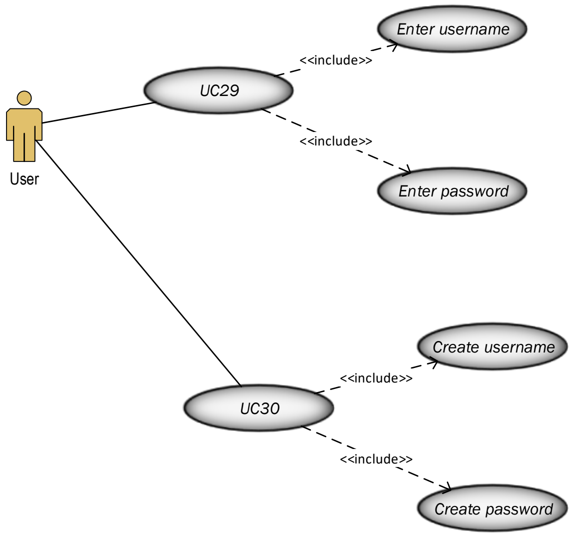


Figure 40: User Register Use Case Diagram

2.2.2.31 UC31 – User Logout

Use case name: **User logout**	**ID:** **UC31**	**Priority:** **High**
Actors: All users		
Description: The user clicks on “Logout” and their session is terminated.		
Trigger: User is done using the website *Type:* External		
Preconditions: 1. User is logged in 2. User no longer wants to be logged in		
Normal course: 1. User is done using the web application 2. User clicks on the ‘logout’ button 3. The system logs the user out and invalidates the cookie/session 4. The system redirects to the default logout page	*Information for steps:*	
Alternative courses: n/a		
Post conditions: 1. The user was logged out		

Exceptions: n/a

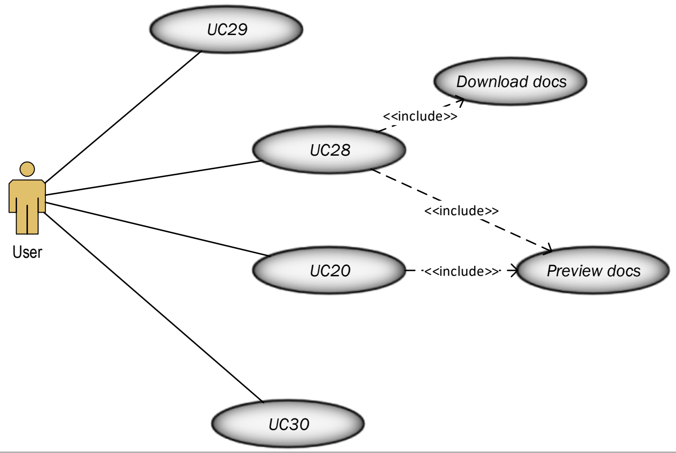


Figure 412: User Logout Use Case Diagram

2.2.2.32 UC32 – Interactions between EC and third counties for mutual agreements

Use case name: **Interaction between EC and third counties for mutual agreements**	**ID:** **UC32**	**Priority:** **Normal**
Actors: EC_user, ECCG_User, ENISA_User, NCCA_User		
Description: ENISA will facilitate interactions between EC and countries outside the EU for mutual recognition.		
Trigger: EC start the mutual recognition and ENISA receives a request from EC to facilitate interaction between selected third counties *Type:* External		
Preconditions: 1. EC start the mutual recognition and select the third countries		
Normal course: 1. EC_User request to ENISA_User and ECCG_User to provide advice to mutual recognition 2. EC_User access the candidate certification scheme and prepare the draft for mutual recognition 3. ENISA_User and ECCG_User provide advice draft for mutual agreements 4. NCCA_User access the mutual recognition document and provide agreements 5. EC_user review and finalised the mutual recognition document 6. EC_User transmit the request to ENISA to update the candidate certification scheme 7. ENISA_User includes the mutual recognition agreements in candidate certification scheme 8. ENISA_User publish the updated candidate certification scheme 9. System store the mutual recognition agreements	*Information for steps:*	

10. System store the updated candidate certification scheme	
Alternative courses: n/a	
Post conditions: 1. The mutual recognition agreements is finalised 2. The candidate certification scheme is updated 3. The updated candidate certification scheme is published	
Exceptions: n/a	

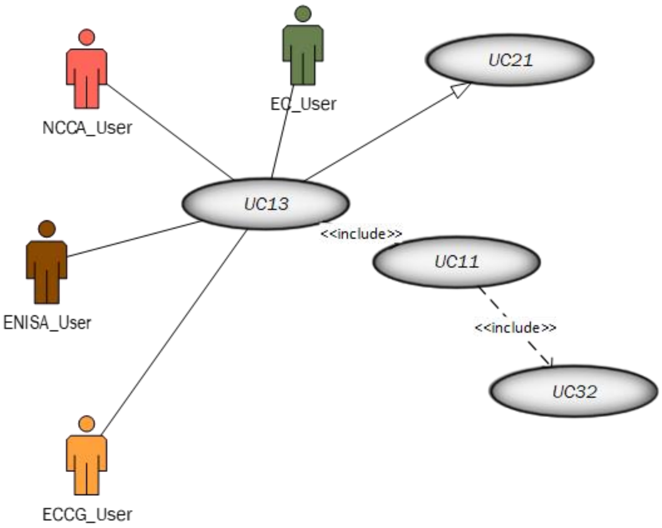


Figure 42: Mutual Recognition Agreements Use Case Diagram

2.3 STAKEHOLDERS MAP

In the figure below we present the entities, roles assigned for each entity in the IT System and use cases associated to each role.

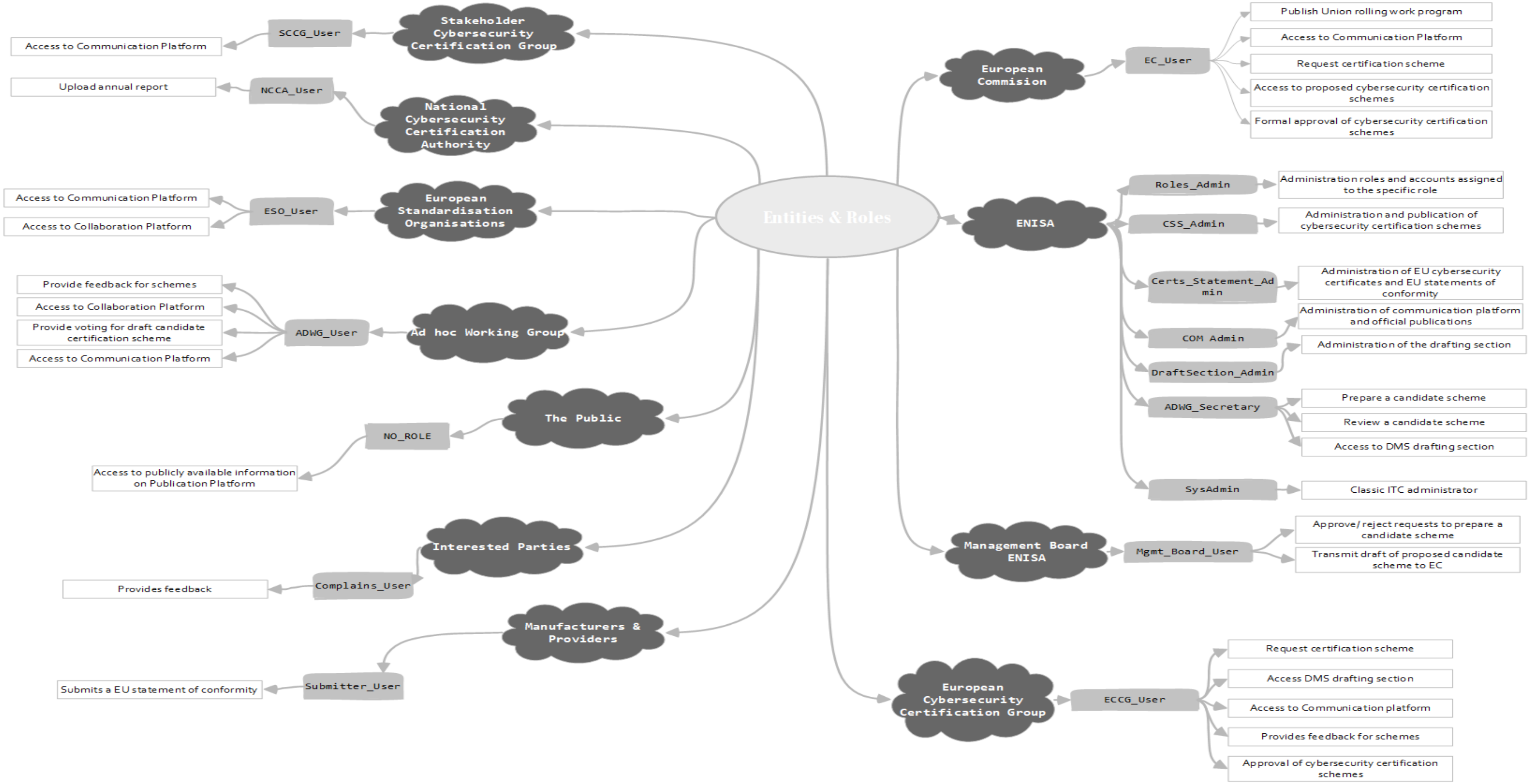

Entities & Roles
Stakeholder Cybersecurity Certification Group
SCCG_User
Access to Communication Platform
National Cybersecurity Certification Authority
NCCA_User
Upload annual report
European Standardisation Organisations
ESO_User
Access to Communication Platform
Access to Collaboration Platform
Ad hoc Working Group
ADWG_User
Provide feedback for schemes
Access to Collaboration Platform
Provide voting for draft candidate certification scheme
Access to Communication Platform
The Public
NO_ROLE
Access to publicly available information on Publication Platform
Interested Parties
Complains_User
Provides feedback
Manufacturers & Providers
Submitter_User
Submits a EU statement of conformity
European Commision
EC_User
Publish Union rolling work program
Access to Communication Platform
Request certification scheme
Access to proposed cybersecurity certification schemes
Formal approval of cybersecurity certification schemes
ENISA
Roles_Admin
Administration roles and accounts assigned to the specific role
CSS_Admin
Administration and publication of cybersecurity certification schemes
Certs_Statement_Admin
Administration of EU cybersecurity certificates and EU statements of conformity
COM Admin
Administration of communication platform and official publications
DraftSection_Admin
Administration of the drafting section
ADWG_Secretary
Prepare a candidate scheme
Review a candidate scheme
Access to DMS drafting section
SysAdmin
Classic ITC administrator
Management Board ENISA
Mgmt_Board_User
Approve/reject requests to prepare a candidate scheme
Transmit draft of proposed candidate scheme to EC
European Cybersecurity Certification Group
ECCG_User
Request certification scheme
Access DMS drafting section
Access to Communication platform
Provides feedback for schemes
Approval of cybersecurity certification schemes

Figure 43: Stakeholders Map

2.4 FUNCTIONAL REQUIREMENTS

The major requirements for the IT System in support for the EU Cybersecurity Certification Framework are:

- Website and content management system for presentation of data and information
- Storage and workflow for requested candidate cybersecurity certification schemes from the EC and the ECCG
- Storage and workflow for requests to update current schemes
- Support for the design and development of candidate cybersecurity certification schemes
- Communications and collaboration features to support the feedback loop (consultation process) with ECCG and other stakeholders
- Management of the content for the preparation and transmission of candidate schemes to EC
- Mechanism to receive feedback from EC and national authorities for the adopted cybersecurity certification schemes
- Mechanism to receive standards to be considered for the design of schemes
- Mechanism to receive information from manufacturers on conformity statements
- Notification mechanism and support for peer review processes
- Receipt, cataloguing and storage of self-asserted conformity claims and the resultant "EU statement of conformity"
- Ontology with (hierarchical) lists of terms for all data and content types
- Communication platform to engage ENISA with the EU-SDOs (CEN, CENELEC, ETSI).
- Support for the post-adoption lifecycle of the schemes (request feedback, participate in peer review of cybersecurity authorities etc.)
- Reporting functionalities (statistics and ad-hoc reports)
- Support for the automated identification of similarities between schemes and contributions of the various stakeholders of the promulgation of a scheme. (based on the concept of antiplagiarism software or service)
- Search and filtering for all data and information published in the website
- Ensure the alignment to storage management standards provided by AHWG, ECCG and ENISA
- Management of users, roles and permissions:
    - Authentication of EU Login users and retrieval of user details (full name, id, email address)
    - Support the creation, maintenance and deleting of user groups for the types of roles identified in this document (EC_User, Roles_Admin, CSS_Admin, Certs_Statements_Admin, Com_Admin, DraftSection_Admin, ADWG_Secretary, ENISA_User, Mgmt_Board_User, ECCG_User, SCCG_User, Submitter_User, Complains_User, ESO_User, ADWG_User, NCCA_user)
    - Administration of user groups, which will translate into portal roles, as well as assignment of permissions to them

The portal will make available the following information:

- EU cybersecurity certification schemes and feedback received in the consultation process, as well as those that are candidate schemes, those that are under revision and those that ENISA rejected to design
- Certificates, EU statements of conformity issued under the Cybersecurity Act, along with relevant documentation
- Componence of the Conformity Assessment Bodies

- Repository of links to cybersecurity information provided online by manufacturers and providers
- Message board (discussion forum), with threaded discussion topics for groups and subgroups
- Task list for each user and user group
- Inbox for specialised communication in the different collaboration processes
- Meeting management
- Componence of the Ad-hoc Expert Groups
- Calls for construction of calls for construction of Ad-hoc Expert Groups
- Various other information published in a hierarchical structure

2.4.1 Authentication and authorization

As multiple stakeholders with diverse roles and activities are involved throughout the lifecycle of a cybersecurity certification scheme, the system will enable ENISA to authenticate, register and manage permissions for different users.

All users involved in these processes either have accounts in the European Commission's CAS repository (EU Login[7], formerly known as ECAS) or can request login credentials, therefore it is suggested to use this service to authenticate users. While the EU Login will maintain the users' information (credentials and passwords), the upcoming portal will store the list of available roles and the mapping of roles per user.

The permissions to execute different operations (e.g. add a document, comment on drafts, review a schema) should be granular enough to allow tailoring roles for each of the foreseen stakeholders.

2.5 DOCUMENT AND CONTENT MANAGEMENT

One of ENISA's key roles is the preparation of the candidate cybersecurity certification scheme, with the assistance of an ad-hoc working group and the ECCG for each candidate scheme. Therefore, a document lifecycle management functionality is essential to coordinate the design of the candidate scheme. Also, the Document Management platform will maintain all documents related to the secretariat for SCCG, ECCG and AHWG.

The document management platform will have to:

- Retain information about EU cybersecurity certification candidate schemes
- Retain information about EU cybersecurity certificates
- Retain information about EU statements of conformity
- Allow publishing of various other documents/reports, either public or private

The structure of the documents published in the portal is essential to fit multiple needs, exceeding the traditional metadata and uploaded file capabilities, for which it is more accurate to refer to a document and content management system. It will offer typical document control functionalities:

- Versioning capabilities
- Notifications on changes to subscribed users
- Customisable publishing workflows, to be tailored by portal administrators (drafting, revision, approval, etc.)
- Comments on versions, with the possibility to turn the comments 'on' or 'off'' on individual documents

[7] EU Login https://webgate.ec.europa.eu/cas/

- Ability to compare content in files, to ensure transparency in the creation of schemes and consensus
- Append-only log of user activities which ensures a transparent traceability of user actions

The portal's user interface, accessible from an ENISA sub-domain (for example certification.enisa.europa.eu) will display content according to the rights of the logged in user. Documents and other content (documentation, certificates, statements of conformity, etc.) will be organised in folder-like sections, either public or restricted to different classes of users. Individual and bulk download capabilities will be available to the users with 'view' access to the documents.

The contents' metadata should be based on the Dublin Core[8] set, enriched with properties relevant for this context.

2.5.1 Libraries (data store)

To ensure a systematic approach, the system will include different structured data about:

- schemes (candidate, revision, approved, rejected)
- national schemes
- requests from ECCG and EC
- feedback from third parties
- ESOs and SDOs standards
- self-conformity certificates
- Conformity Assessment Bodies and their users
- various groups of persons, relevant to the system's processes

Such data will be stored in databases and maintained through the system, in a transparent way to users who visualise or administer the data. The interface for filling in data, managing or displaying it should be consistent throughout the entire system. Where applicable, the data should be linked by relations, ensuring data integrity and consistency.

Similar to the way the documents are stored and maintained, the data repositories will implement the following capabilities and functionalities:

- Versioning
- Notifications on changes to subscribed users or relevant user groups
- Publishing workflow (customisable, where relevant)
- Allow comments, feedback or other input from the stakeholders
- Append-only log of user activities which ensures a transparent traceability of user actions
- Ability to compare content in files to ensure transparency and consensus

The metadata should also be consistent with the metadata set of the documents.

2.5.2 Reporting, data mining and auditing

Cybersecurity certification schemes have different levels of conformity and expiry dates. Additionally, ENISA is responsible to gather feedback for the implemented schemes and revise those deemed out of date. The system will include auditing and mining capabilities for defined processes.

[8] Dublin Core Metadata Element Set http://www.dublincore.org/specifications/dublin-core/dces/

Based on the existing data and content, several reports will be built to explore data in meaningful ways, to allow searching and filtering or to prepare statistical reports. The reports will be dynamic pages, which bring together data and content from different areas. For instance, it would be relevant to have a filterable list of the certificates, which are about to expire, grouped by countries and other parameters.

The use of data mining is intended to ensure and demonstrate consensus in the design of schemes amongst AHWG and ECCG. A third-party component, built for antiplagiarism, should be used to find similarities between the texts of existing schemes and certificates and signal potential overlaps.

The auditing components will be available to all logical levels of the system and should focus on:

- Access and authentication: proper approval and authorization of all data and documents
    - Appropriate logins and passwords to restrict access
    - Lock records/documents for editing after approval
    - Retain the “envelope” for electronically signed documents
    - Don’t put faith in email – email approval is weak audit evidence
- Document management: availability and access to complete and accurate records
    - Make sure records/documents are searchable and retrievable
    - Consistent data/document retention period, so these are available upon request during an audit
    - Establish a solid form of version control
- Security and integrity of documents: protection of documents from accidental modification or deletion
    - Reliable active directory management that includes mobile devices
    - Limit access through use of logins and passwords
    - Two-factor authentication
    - Perform regular and timely backups
    - Perform periodic restore or other tests to ensure document integrity
- Retention and destruction
    - Have a disaster recovery plan in place
    - Destroy records/documents in an orderly and timely manner, and in accordance with the established policy

2.5.3 Communicating over a platform

Ensuring that interactions amongst all stakeholders are timely and efficient is crucial, given the various stages in the lifecycle of the scheme that information needs to be communicated and that key players require to collaborate and synchronise their activities. A platform that will facilitate communications amongst all key stakeholders is a key building block of the system. The communication platform will facilitate all communications or information exchange between the different stakeholders mentioned in the CSA. Communication functionalities are destined for authenticated users and include:

- Message board (discussion forum), with threaded discussion topics for groups and subgroups, allowing moderation
    - Task list for each user and user group
    - Inbox for specialised communication in the processes for adoption and review of certification schemes
- Automatic email notifications to users or groups

- Meeting management tool, with agenda, minutes, presentations and links to relevant documents; this tool will also allow the management of participants and printing of the participants list
- Possibility to subscribe to receive email updates on new or updated content

The management of the groups and subgroups needs to be done in relation with the user roles, each group having being associated a role. Permissions for viewing or executing various functionalities should be granted for roles, instead of per individual users.

2.5.4 Collaboration on documents

In almost all processes the communication is essential to provide and receive feedback and advice from different stakeholders. The collaboration functionalities will be used in creating and publishing the URWP with the assistance of the SCCG and the ECCG, as well as in the preparation of the candidate cybersecurity certification scheme with the assistance of an ad-hoc working group and the ECCG for each candidate scheme. In the process of creating and supporting the SCCG and the AHWG, the communication functionalities are a priority.

The collaboration platform is used for preparing the EU candidate cybersecurity certification schemes. In the backend, a CMS will support the web server connected to a database, document management system, message board, collaborative work environment and ticketing system. During the preparation of these candidate schemes the Communication Platform is used within the Ad hoc Working Group, the ECCG and the SCCG for communication. Any work progress and other outcome of the Ad hoc Working Group is stored in the Document Management System.

The collaboration functionalities consider authenticated users and include:

- Threaded comments on uploaded documents
- Possibility of weighted voting (user definition will contain number of votes per user group, e.g. 'ECCG France = 5'
- Online commenting on data (e.g. schemes or certificates of conformity), with threaded comments posted on various parts of the data structures

2.5.5 Functional public website (CERMIT Portal)

ENISA is required to publish information on a website regarding the candidate schemes, the implemented schemes and the self-conformed manufacturers. In order to ensure that the website will contain up-to-date accurate information it is important to have a back-end system collecting the required information from various stakeholders, as well as a user-friendly front-end software.

The website's functionalities should be accessible on all targeted devices (regular monitors, tablets, mobile phones). By 'targeted devices' we mean that simpler, more commonly used interfaces should be available on all devices, while some administrative features of complex editing should be accessible on larger devices, where the possibility of errors due to lower visibility is eliminated.

For authenticated and anonymous users, the portal interface should also follow the concept 'what you see is what you can do', entailing that users will not see functionality they are not allowed to execute.

The IT System website will make publicly available and accessible information related to candidate and adopted schemes, certificates and statements. The IT System will have to make available to a public website:

- EU cybersecurity certification schemes
- Requests for candidate cybersecurity certification schemes
- Feedback received in the consultation processes, to the extent the feedback is relevant and does not have a restricted nature
- Certificates and EU statements of conformity issued under the cybersecurity Act
- Withdrawn items and expiration dates
- Repository of links to cybersecurity information provided online by manufacturers and providers
- Information received from ICT manufacturers and national certification authorities
- National certification schemes replaced by European certification schemes
- Information received from national certification authorities
- Other relevant information (events, news, contact information, etc.) and the necessary search and filtering functions
- Access to the restricted areas for collaboration and communication

On a technical level, this architecture will be sustained by a content management system. It will encapsulate the authentication and authorization, document management, built-in or custom-built collaboration tools, as well as the integration with external databases for the storage and management of relational data.

2.6 NON-FUNCTIONAL REQUIREMENTS

2.6.1 Availability

It is required that the IT System is accessible to anonymous visitors 24 hours a day, 7 days a week, 365 days a year excluding scheduled maintenance or pre-agreed outage periods. The system performance availability standard will be a minimum of 99.95% (the “Availability Standard”). All services, supporting infrastructure and software code must be robust, resilient, stable, and established and maintained in accordance with the modern industry practices and standards for website development and maintenance.

The system shall be prepared to handle around 200 users connected at the same time.

2.6.2 Usability and accesibility

The user interface must be simple and comprehensible. Users will not be required to read long manuals for navigation, accessing the different types of information or functionalities. Contextual help should be provided when relevant.

The interface of the IT System will be easily accessible, modern, responsive, user-friendly, informative, well organised, visually attractive, up-to-date and reliable, taking into account modern European standards for usability and accessibility. The standards set out by the W3C Web Accessibility Initiative should be followed, together with the WAI-ARIA specification for accessible rich internet applications and best-practices.

The search must return relevant results, guiding users in retrieving content relevant for them. When searching, appropriate filters should be selectable, while typing search terms should be autocompleted using the portal’s ontology (lists of terms).

The pages should generally load under 3 seconds, with slower to retrieve content (e.g. rendered statistics) being showed progressively, after the rest of the page has loaded swiftly.

2.6.3 Reliability

The system must work reliably enough so that no data loss can occur in cases of system failure and the disruptions in the service can be rapidly spotted, traced and repaired. This also includes business recovery and disaster recovery scenarios.

2.6.4 Performance

The performance of the IT System is not critical, but should have minimal user-feedback delays. In particular, the time it takes to load and refresh database items has the potential to interrupt operator workflow. This should be mitigated by the use of expandable products and item categories.

The IT System shall have an uptime of more than 99% of the announced 24/7 availability, measured over any 30 days period.

2.6.5 Security

User authentication must be required in order to prevent any malicious or unintended manipulation of the configurable products. All activities which assign credentials to users and define workflows are logged separately for security monitoring activities.

The IT System will use secure protocols to ensure that the client - server communication is protected against third party intrusions.

Each form that allows data entry by users must contain security checks to ensure the integrity of submitted data and to avoid any kind of injection of potentially malicious bits of code that might affect the data or the overall system integrity.

The system should ensure that all activities will be monitories and will be compliant with ENISA’s policies and procedures (privacy statements, security policies etc).

2.6.6 Maintainability

The system must be easy to maintain and update after the project team delivers it. Appropriate documentation must be provided, to ensure that ENISA staff is aware how to use and maintain its components. Potential future developers must be able to continue the work without the need to contact the initial development team. The code, products, deployment and monitoring procedures must be documented on a level that permits the system to function and to be subsequently updated.

2.6.7 Scalability

The IT System will have a relatively constant number of users over the course of time, so the system will not need to handle significant growth in the foreseeable future. The IT System should be able to handle a constantly growing data storage.

2.6.8 Brand integrity and enhancement

The provider will ensure that all development work respects and consistently reflects the current ENISA Brand Guidelines.

2.7 ASSUMPTIONS AND CONSTRAINTS

The following assumptions and constraints were identified from the system’s perspective:

- The IT System will be developed on top of a security-sound platform, known on the market as being reliable, with a high-quality code base, having an active community of contributors or a reliable organisation to sustain its future development, being well documented and allowing the development of extensions and plugins;
- The chosen framework should have or allow the development of components to cover all functionalities described above;

- The IT System will follow the EU standards on website accessibility, design, programming languages, as well as security principles;
- The IT System will verify the user identity from an external user management system (EU Login, formally known as ECAS);
- The IT System will provide interoperability functionalities for future integration with other systems;
- The databases used will need to ensure data integrity checks and the ability to relate stored data;
- The IT Systems should be implemented in phases: the most critical functionalities will be implemented first, in order to sustain the urgent business processes, while less urgent functionalities could be delivered in subsequent iterations;
- The IT System will be hosted on ENISA infrastructure and system administration will be done following the same standards with the rest of the ENISA websites;
- The system will have complete documentation on all deliverables, potential training to the relevant users, as well as knowledge transfer to relevant ENISA staff;
- The project management will be done following a standard Agile methodology.

3. TECHNICAL REQUIREMENTS

3.1 SYSTEM ARCHITECTURE

3.1.1 Generic considerations

The IT System must be developed on top of a security-sound platform, established in the market as being reliable, with a high-quality code base. The platform should have an active community of contributors or a reliable organisation to sustain its future development, must be well documented and should allow the design and implementation of extensions and plugins.

The chosen framework should already possess or allow the development of components to cover all functionalities described Section 2. The IT System will follow the EU standards on website accessibility, design, programming languages, as well as security principles, as laid out in the IPG Rules[9].

The IT System will verify the user identity from an external user management system (preferably EU Login, formally known as ECAS). Also, it must provide interoperability functionalities for current and future integration with other systems, following common standards (e.g. GET/POST calls or Restful APIs).

The databases used will need to ensure data integrity checks and the ability to relate stored data.

The system will need to have complete documentation on all deliverables, potential training to the relevant users, as well as knowledge transfer of system administration and maintenance activities to relevant ENISA staff. Reuse of the existing ENISA frameworks is not mandatory, but would constitute an advantage, as it would reduce the administration burden for ENISA in the long term.

3.1.2 System overview

The major requirements for the IT System in support for the EU Cybersecurity Certification Framework are:

- Website and content management system for presentation of data and information
- Storage and workflow for requested candidate cybersecurity certification schemes from the EC and the ECCG
- Storage and workflow for requests to update current schemes
- Support for the design and development of candidate cybersecurity certification schemes
- Communications and collaboration features to support the feedback loop (consultation process) with ECCG and other stakeholders (i.e, Ad-hoc Working Group)
- Management of the content for the preparation and transmission of candidate schemes to EC
- Mechanism to receive feedback from EC and national authorities for the adopted cybersecurity certification schemes

[9] https://ec.europa.eu/ipg/about/rules/

- Mechanism to receive standards to be considered for the design of schemes
- Mechanism to receive information from manufacturers on conformity statements
- Notification mechanism and support for peer review processes
- Notification mechanism and support for mutual agreement processes (optional)
- Receipt, cataloguing and storage of self-asserted conformity claims and the resultant "EU statement of conformity"
- Ontology with (hierarchical) lists of terms for all data and content types
- Communication platform to engage ENISA with the EU-SDOs (CEN, CENELEC, ETSI).
- Support for the post-adoption lifecycle of the schemes (request feedback, participate in peer review of cybersecurity authorities etc.)
- Reporting functionalities (statistics and ad-hoc reports)
- Support for the automated identification of similarities between schemes and contributions of the various stakeholders of the promulgation of a scheme. (based on the concept of antiplagiarism software or service)
- Search and filtering for all data and information published in the website
- Ensure the alignment to storage management standards provided by AHWG, ECCG and ENISA
- Management of users, roles and permissions:
  - Authentication of EU Login users and retrieval of user details (full name, id, email address)
  - Support the creation and maintenance of user groups for the types of roles identified
  - Administration of user groups, which will translate into portal roles, as well as assignment of permissions to them

The system described here will need to operate in real time and to cater for an estimated 200 maximal concurrent users. This figure might increase in time, due to legislative changes or peaks in the number of requests by EC and the ECCG. The accessibility to anonymous or authenticated visitors will need to be 24 hours a day, 7 days a week, 365 days a year, excluding scheduled maintenance or pre-agreed outage periods. The system performance availability standard will be a minimum of 99.95%.

All services, supporting infrastructure and software engineering must be robust, resilient, stable, and established and maintained in accordance with the modern industry practices and standards for website development and maintenance.

It is likely that the system will evolve in time in terms of data structures, functionalities and interoperability with external services. Therefore, it has to be scalable and easily maintainable in the future. The development team should foresee the ability to scale both in terms of additional server power, as well in terms of component instances (CMS, database, other frameworks or services).

While building the user interfaces, the target users of the application should be taken under consideration:

- EU institutions
- Members of ECCG and SCCG
- National governments and authorities
- Manufacturers and providers of ICT products, ICT processes and ICT services
- Beneficiaries of ICT products, ICT processes and ICT services
- Global and international agencies and organisations
- Wider public and media

The quality of the projects' code needs to be tested and measured using dedicated tools such as CodeClimate, Codacy, or similar. Testing of the newly developed code should be conducted at different levels:

- Unit testing, at least for highly used and critical parts
- Functional testing, for the critical and most frequently used functionalities
- Integration & system testing, when it comes to the interoperability between platforms or integration of third-party components
- Usability and accessibility testing for the user interface
- Performance testing
- Security testing

3.1.3 System architecture

The IT System should rely on a modern content management system for the presentation, document management, collaboration, communication and integration with database structures – used in the storage and management of cybersecurity schemes, certificates, statements of conformity and other resources relevant to these processes.

Modern content management systems (CMSs) have built-in, strong document management capabilities and pluggable products for various communication and collaboration features. They also allow complex management of the system, layout, content, distinction of users, and allocation of roles and permissions. When certain functionalities are not available, developers either extend existing open source products for that CMS, or they build new ones from scratch. Therefore, it is expected that the upcoming system will be built on top of a CMS.

From a technical point of view, the overall requirements for this IT system are depicted in the figure below.

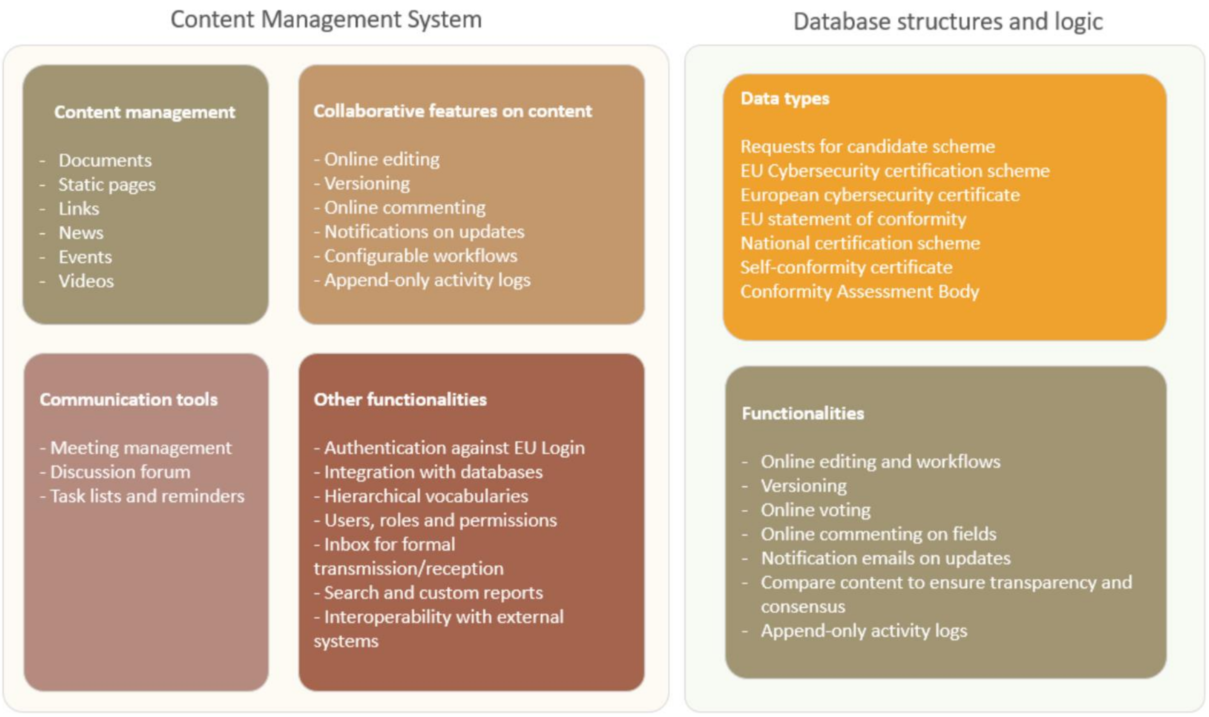

Content Management System
Content management
- Documents
- Static pages
- Links
- News
- Events
- Videos
Collaborative features on content
- Online editing
- Versioning
- Online commenting
- Notifications on updates
- Configurable workflows
- Append-only activity logs
Communication tools
- Meeting management
- Discussion forum
- Task lists and reminders
Other functionalities
- Authentication against EU Login
- Integration with databases
- Hierarchical vocabularies
- Users, roles and permissions
- Inbox for formal transmission/reception
- Search and custom reports
- Interoperability with external systems
Database structures and logic
Data types
Requests for candidate scheme
EU Cybersecurity certification scheme
European cybersecurity certificate
EU statement of conformity
National certification scheme
Self-conformity certificate
Conformity Assessment Body
Functionalities
- Online editing and workflows
- Versioning
- Online voting
- Online commenting on fields
- Notification emails on updates
- Compare content to ensure transparency and consensus
- Append-only activity logs

Figure 44: Required features of the IT System, organised by technology

An important aspect of the system is that most of the functionalities must be designed and implemented for restricted access to a complex set of roles. Therefore, proper tests should be designed to ensure that the restricted content cannot be accessed by users without the necessary set of roles, and that privileged operations cannot be executed by unauthorised users.

The architecture proposed will have to provide the flexibility to support ever-changing business (often legislatively driven) requirements. Its key feature should be that it separates out business logic, client access technology and centrally-held data into discrete layers with standard, open interfaces. It must be possible for the data to be exported in common formats, in order to integrate it in future versions of the frameworks used, or just reuse this data for other purposes (e.g. building reports).

More details about the different system components can be found in the next section.

3.1.4 Technology

ENISA currently uses Plone 4.x and 5.x for building most of its dynamic websites. To streamline future administration of the ENISA websites, it would make sense to have this IT system built on top of Plone 5. The more structured data can be stored in an external, relational database, such as MariaDB or Postgres, or in Json-based structures in Plone’s ZODB. This choice can be assessed at the time of detailed analysis of the development.

Plone 5 complies with the overall system requirements and allows building Python products for Plone for the implementation of the less standard structures and logic, such as handling the workflows of cybersecurity schemes.

3.1.5 Infrastructure services

3.1.5.1 Deployment

The deployment of the system could be made either on the existing ENISA infrastructure or on other platforms.

Aside from the production environment, a similar setup should be made for the development and acceptance server, where new versions of the application will be showcased and tested by the stakeholders, before going live. The project should adopt an iterative and agile approach and implement a continuous improvement process, making use of automated testing tools integrated in the development flow (continuous integration suite).

Continuous integration tools should be used for the automated testing of the backend (e.g. Travis, Jenkins), as well as for running the tests for the user interface (e.g. Selenium / PhantomJS).

The source code of the ENISA products could reside on private Gitlab repositories. Gitlab should therefore be used as support for release management, each release being accompanied by a change log and full traceability of the features developed.

3.1.5.2 Availability

The availability of the website and all its internal services will be measured on monthly basis, excluding maintenance periods agreed with ENISA. The requirements are:

Indicator	Typical	Guaranteed	Unit
Availability	99.3%	99.0%	Uptime/month
Response time		1 sec (first byte)	Seconds
Network time (taken by the server to answer to the request of a browser)	<= 3 sec		Seconds

Code performance should also be taken into account in the implementation phase of each project development. At least 95% of the pages should have a loading time less than or equal to to 7 sec/per page.

3.1.5.3 Data handling, backup and restore

The application must allow that all data stored by the system are properly backed up.

Data portability must be ensured, meaning that the application shall provide capabilities to export the data, so it can still be used by the customer, e.g. in the event of terminating the contract with the developer or host of the service.

All appropriate steps must be taken in order to ensure that data protection principles have been implemented. This can be done by choosing a secure framework for implementing the application, by implementing a secure deployment configuration and by implementing the necessary automated tests to ensure data access can be done only for properly authenticated users. Appropriate security policies should be put in place – handling of Intellectual Property, handling of classified documents, encryption of databases, encryption of data at transit and rest, etc.

The platform should provide reliable monitoring and logging mechanisms, in order to investigate data breaches and security incidents.

3.1.5.4 Logging

Regular log collection needs to be done for reviewing the user access into the application and for security reasons. In case of security incidents, systematically collected logs enrich the understanding of the nature of the incidents during their lifespan and afterwards, during the investigation.

Related to this application, the log events should at minimum include:

1. Application account information
   a. successful and failed application authentication attempts
   b. failed attempts to use restricted pages
   c. application account changes (e.g. roles being assigned to accounts)
2. Application operations
   a. application start-up and shutdown
   b. application failures
   c. major application configuration changes
   d. URLs requested and the type of response provided by the server
   e. application relevant transactions, for example:
      i. email messages recording the sender, recipients, subject name, and attachment names
      ii. requests from EC/ECCG being registered in the system

iii. changes in the publication workflow of documents

The details logged for each event may vary, but at minimum each event should capture:

- timestamp
- event, status, and/or error codes
- short and long descriptions of the event, as relevant to traceback potential issues
- user or system account associated with an event
- (when the information is available) device used (e.g. IPs, terminal session ID, web browser, etc.)

The conventional process to logs is that all actions relevant for the application need to be traceable by properly authenticated users. This method is called 'append-only logs', meaning that it should not be possible for users to tamper with the logs and delete certain interactions, without a trace that certain actions have been reverted.

3.2 DETAILED DESIGN

3.2.1 Content management system

The content management system will be the main access point to all system functionalities. End users should feel as they are interacting with a single platform, in a coherent sequence across devices and should remain agnostic to the different technologies used to build the entire IT System.

The chosen framework must support the ability to build content types with custom metadata, to revise existing content types and to create new ones along the way. The list of content types to be made available should be, at a minimum, the following:

- Links to internal and external pages
- Regular pages with static content
- Files (documents) of any type
- Folders
- Videos and images
- Events
- Meetings

The structure of the documents published in the portal is essential to fit multiple needs, exceeding the traditional metadata and simple file-upload capabilities. The CMS will offer typical document control functionalities:

- Online editing, with validation rules for fields
- Versioning capabilities
- Notifications on changes to subscribed users
- Customisable publishing workflows, to be tailored by portal administrators (drafting, revision, approval, etc.)
- Preview of the information before publishing
- Comments on versions, with the possibility to turn the comments 'on' or 'off'' on individual documents
- Moving of documents in folders
- Minimalistic undo capabilities (e.g. at a minimum the undo of the last operation for a limited period of time)

- Ability to compare content in files, to ensure transparency in the creation of schemes and consensus
- Append-only log of user activities which ensures a transparent traceability of user actions

The portal's user interface, accessible from an ENISA sub-domain (for example certification.enisa.europa.eu) will display content according to the rights of the logged user. The portal should be implemented with best practice security features and hold a Qualified Website Authentication Certificate (QWAC). Documents and other content (documentation, certificates, statements of conformity, etc.) will be organised in folder-like sections, either public or restricted to different classes of users. Individual and bulk download capabilities will be available to the users with 'view' access to the documents.

The contents' metadata should be based on the Dublin Core[10] set, enriched with properties relevant for this context.

The CMS will have to accommodate publishing the required information in a hierarchical structure, but also integrate pages that expose other data, possibly stored in databases:

- Requests for candidate cybersecurity certification schemes
- EU cybersecurity certification schemes and feedback received in the consultation processes, as well as those that are candidate schemes, those that are under revision and those that ENISA rejected to design
- Information on the national certification schemes
- Certificates, EU statements of conformity issued under the Cybersecurity Act, along with relevant documentation
- Self-conformity certificates
- List the Conformity Assessment Bodies
- Repository of links to cybersecurity information provided online by manufacturers and providers
- Discussion forum, with threaded discussion topics for groups and subgroups
- Message board - inbox for specialised communication in the different collaboration processes
- Meeting management
- Composition of the ad-hoc Expert Groups
- Calls for expression of interest for the ad-hoc Expert Groups

In addition to publishing the raw data, several dynamic pages need to be built for the custom display of the data and information, searches on different subsets of data, as well of predefined reports based on customisable templates. It must be possible for authorized users to select page types and templates from a list when they are creating pages.

3.2.2 Cybersecurity certification schemes

European Cybersecurity Certification Schemes (CSS) will be implemented with a complex structure, which makes it suitable for being stored and maintained in a database environment.

The following functionalities should be made available for this object type:

- *Add form*, with multiple steps and the possibility to have interim saved versions
- *Edit form*, with multiple steps and the possibility to have interim saved versions, which blocks the editing for other users
- *View page*, listing all fields in an intuitive manner and linking to related objects (see list below)

[10] Dublin Core Metadata Element Set http://www.dublincore.org/specifications/dublin-core/dces/

- *Publishing workflow* (draft, in review, in comments from stakeholders, voting, transmitted to EC, approved, in revision)
- *Consultation*, which allows posting comments on specific fields by the ADWG and ENISA. This functionality is part of the collaboration platform
- *Search and filtering* of schemes, which will include national schemes as well, further detailed under the sub-section "Reports" below

Schemes can be in one of the following states:

1. *Candidate* – following the request from EC or ECCG, ENISA creates a candidate scheme for review and comments
2. *Adopted* – following ENISA's transmission of a final candidate scheme to EC, the scheme is approved with an implementation act
3. *Rejected* – following a request outside the Union Rolling Working Programme from EC or ECCG, ENISA's management board rejects the request
4. *In assessment* – EC and ENISA regularly assess the efficiency and use of the adopted scheme and whenever European CSS
5. *Withdrawn* – expired or replaced scheme

The processes that govern the lifecycle of certification schemes are described in Section 2 and further summarised in the figure below.

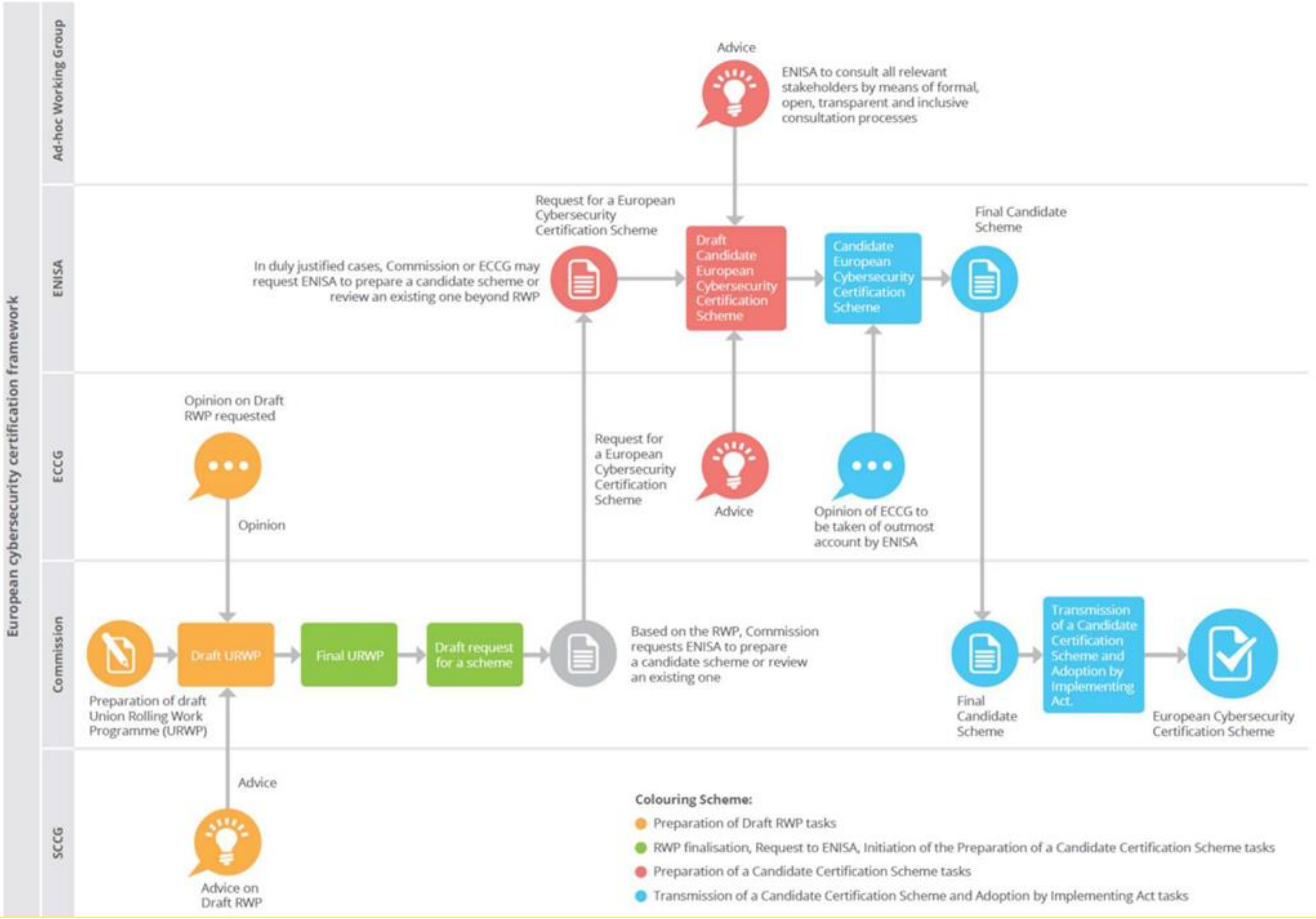

European cybersecurity certification framework
Ad-hoc Working Group
ENISA
ECCG
Commission
SCCG
Advice
ENISA to consult all relevant stakeholders by means of formal, open, transparent and inclusive consultation processes
Request for a European Cybersecurity Certification Scheme
In duly justified cases, Commission or ECCG may request ENISA to prepare a candidate scheme or review an existing one beyond RWP
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Final Candidate Scheme
Opinion on Draft RWP requested
Opinion
Request for a European Cybersecurity Certification Scheme
Advice
Opinion of ECCG to be taken of outmost account by ENISA
Draft URWP
Final URWP
Draft request for a scheme
Preparation of draft Union Rolling Work Programme (URWP)
Based on the RWP, Commission requests ENISA to prepare a candidate scheme or review an existing one
Final Candidate Scheme
Transmission of a Candidate Certification Scheme and Adoption by Implementing Act.
European Cybersecurity Certification Scheme
Advice
Advice on Draft RWP
Colouring Scheme:
● Preparation of Draft RWP tasks
● RWP finalisation, Request to ENISA, Initiation of the Preparation of a Candidate Certification Scheme tasks
● Preparation of a Candidate Certification Scheme tasks
● Transmission of a Candidate Certification Scheme and Adoption by Implementing Act tasks

Figure 45: Default workflow for EU cybersecurity schemes, from request to adoption.

The properties of European cybersecurity certification schemes known at this time are listed in the table below, but others may become necessary upon a more in-depth analysis at implementation time:

Name of property	Type	Mandatory	Purpose
Title	String, text only	yes	
abstract	String, text only	yes	The subject matter and scope of the certification scheme
types_covered	Multiple selection from list	yes	The type or categories of ICT products, ICT services and ICT processes covered
description	String, HTML elements allowed	yes	Description of the purpose of the scheme and description of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
references	Complex property, list of (type, link, title, organisation)	yes	References to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme
assurance_levels	Multiple selection from predefined list	no	Values: ‘basic’, ‘substantial’, ‘high’
conformity_self_assessment_allowed	boolean	yes	An indication of whether conformity self-assessment is permitted under the scheme
cab_specific_requirements	String, HTML elements allowed	no	Where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements
evaluation_criteria_methods	Complex property, list of (criteria, method, evaluatin_type)	yes	The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved
necessary_information	String, HTML elements allowed	no	Where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant
conditions_marks_labels	String, HTML elements allowed or List of String fields	no	Where the scheme provides for marks or labels, the conditions under which such marks or labels may be used
rules_mechanisms_compliance	String, HTML elements allowed	yes	Rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance

			with the specified cybersecurity requirements
conditions_upkeep	String, HTML elements allowed or List of String fields	no	Where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification
additional_rules_consequential	String, HTML elements allowed or List of String fields	yes	Rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme
rules_upcoming_vulnerabilities	String, HTML elements allowed or List of String fields	yes	Rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with
rules_rentention_by_cabs	String, HTML elements allowed or List of String fields	no	Where applicable, rules concerning the retention of records by conformity assessment bodies
related_schemes	Complex property, list of (scheme, type, categories_covered)	no	The identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels
content_format_certificate	File (content, title, size, content-type) or String, HTML elements allowed	yes	The content and the format of the European cybersecurity certificates to be issued
content_format_statement_conformity	File (content, title, size, content-type) or String, HTML elements allowed	yes	The content and the format of the EU statements of conformity to be issued
adoption_date	Date	no	The date the scheme was adopted by the EC
expiration_date	Date	no	The date the scheme is due to expire
period	Number, in months	yes	The period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes
maximum_validity_certificates	Number, in months	yes	Maximum period of validity of European cybersecurity certificates issued under the scheme
discosure_policy	String, HTML elements allowed or List of String fields	yes	Disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme
conditions_mutual_recognition	String, HTML elements allowed	no	Conditions for the mutual recognition of certification schemes with third countries
rules_peer_assessment	String, HTML elements allowed	no	Where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European

			cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59
format_procedures_providers	Complex property, list of (format, list of procedures)	yes	Format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55

As with other types of objects to be implemented in this system, logs of all actions done on CCSs will be kept in the system in the form of 'append-only' logs which will register at a minimum:

- User executing the action
- Precise date and time
- Name of the action
- Description of the action (optional)

After the definition of the candidate scheme by an ENISA user, a review process by the ECCG and the Ad-hoc Working Group begins, which allows the respective users to add comments on specific fields of the candidate scheme. These comments need to be stored in the system and displayed to authorised users in a manner that makes it easy to go through them and draw conclusions. During this time, authorised ENISA users can edit the scheme and make changes, either by creating a new version of the scheme or just by preserving the existing one.

The next optional step is for the users to vote (1-5) on the respective version of the candidate scheme. Final count of the votes will be weighted by country and displayed to reviewers in a report.

3.2.2.1 Related objects

- Ad-hoc Working group
- Feedback from the ECCG and the Ad-hoc Working Group
- Weighted voting on the versions
- European cybersecurity certificate
- EU statements of conformity
- Conformity Assessment Body
- Conformity self-assessment certificate
- National certification scheme

3.2.2.2 Reports

- Search of schemes based on their status (candidate, adopted, rejected, in assessment, withdrawn); unauthenticated users should only be allowed to search for adopted or withdrawn schemes
- Display comments and votes for a candidate scheme
- Searching and filtering of manufacturers of ICT products or services with certifications on a certain scheme
- Conformity self-assessment certificates declared under a certain scheme
- National certification schemes replaced by an EU scheme

3.2.3 Request for certification scheme

The request for a new candidate cybersecurity certification scheme arrives from the EC or the ECCG and needs to trigger the following processes:

- Setting up an ad-hoc working group
    - Upload relevant documents:
        - Publish Term of Requirement (ToR) document
        - Create a call for the expression of interest (CEI)
- Preparation of candidate schemes (described in the previous section)

This kind of request will be implemented as a formal message sent by the ECCG or the EC to ENISA via the Message board described in Section 3.10. Since the format for the request is not fixed, it is expected that the description of the upcoming scheme, its rules, technical requirements and other elements will be sent in a document format, as attachment to the message.

3.2.4 European cybersecurity certificates and EU statements of conformity

ENISA will be the source for data on all EU candidate cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity for all certified products on the European market. Therefore, this website will publish and make available through searches the data relevant to all these resources.

The content and format for the European cybersecurity certificates and the EU statements of conformity are set in the cybersecurity scheme under which they are issued. Aside from the specific fields, these data types will contain:

- text of the certificate or statement of conformity
- holder of the certificate or statement of conformity (natural or legal person who submitted the ICT products, ICT services or ICT processes for certification)
- assurance level specified in the European cybersecurity certification scheme
- date of issuance
- period of validity
- accreditation body
- technical documentation and links to relevant documentation on the holder’s website

3.2.4.1 Related objects

- European cybersecurity certification scheme
- Conformity Assessment Body

3.2.4.2 Reports

- Search and filtering through active, withdrawn and expired European cybersecurity certificates and EU statements of conformity
- Report on European cybersecurity certificates and EU statements of conformity issued under a specific scheme
- Report on European cybersecurity certificates and EU statements of conformity issued for an entity

3.2.5 National certification schemes

This data type will be simplified with respect to the European cybersecurity certification scheme, as the full information resides on the national websites. The structure will consist of standard metadata, status and links to the remote site for the text and procedures.

The functionalities for the national schemes will be the following:

- Internal library, accessible to ENISA, European Commission, ECCG, SCCG; the information for each country will be also accessible to the National Cybersecurity Certification Authorities

- National bodies and SCCG members will provide input to the data, usually at the beginning of elaboration of schemes
- Information should contain attributes based on requirements from Art.58[11]
- ENISA users will select the entries with potentially affected schemes
- Final draft of schemes includes schemes selected as overlapping

3.2.6 Conformity self-assessment

According to the CSA, a European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, services or processes. Conformity self-assessment shall be permitted only in relation to products, services and processes that present a low risk corresponding to assurance level 'basic'. Manufacturers or providers submit copies of the conformity self-assessments to the national cybersecurity certification authority and to ENISA, so it is conceivable that the submission to ENISA can be done directly through the system, with a final publication from an ENISA user.

The system should maintain a list of conformity self-assessments, each record containing:

- Details about the manufacturer or provider of ICT products, ICT services or ICT processes
- Statement of conformity
- Relevant technical documentation
- Scheme to which the self-assessment is made against
- Dates of submission and expiration

3.2.6.1 Related objects

- European cybersecurity certification scheme
- National certification scheme (if any)

3.2.7 Conformity Assessment Bodies (CABs)

In the process of implementation of cybersecurity certification schemes, manufacturers of ICT products or services submit applications to a conformity assessment body (CAB). These CABs are accredited by the national accreditation bodies and each MS can accredit one or more CABs. Their list may vary in time, in which case changes (add, restrict, suspend or revoke the accreditation of a CAB) must be notified to the EC and registered in the currently described IT system. To be noted that the accreditation will be issued to the CABs for a maximum of five years.

After the approval of a new scheme, the CABs accredited for that scheme should be added or removed progressively by the maintainers of the scheme.

The structure of this data type should contain:

- Name of the CAB
- Contact details
- Name of the accrediting NAB
- Scheme for which CAB is accredited (automatic link to the database of schemes)
- Link to the information about accreditation
- Date of accreditation
- Date of expiry of accreditation

[11] Article 58 - National cybersecurity certification authorities https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN#d1e3956-15-1

- EU Login Users which are members of the CAB

3.2.8 User groups (roles)

The system’s processes require different user groups to act together. Examples of these groups are ECCG, SCCG, SCCG candidates and secondees, Ad-hoc Working Groups, members of a National Accreditation Body, etc. As mentioned before, the user repository for this system will be the EU Login repository, which records several user details such as the name, email address and organisation.

The users having the role of the CMS administrator will be able to search for EU Login users and assign them different roles. Roles will be assigned acces either on the entire platform, or just in specific locations; for instance, a user from an Ad-hoc Working Group will have the rights to provide feedback on schemes of a certain type, and therefore have the local role of ‘ADWG_User’ on those schemes. It should be possible to grant and revoke users’ roles from the administration area of the portal.

The list of roles and their users must be browsable, through a specific page. It should be possible to see all roles (groups of users) and the users having that role at that point. When searching for a user, this page should present the roles that user has in the system and the location for each of them (entire system or specific section).

The table below summarises the user roles, as well as the use cases (described in detail in Section 2) in which each role is involved.

Entity	IT Role	Use Cases
European Commission	EC_User	Access to communication platform
		Publish Union rolling work programme
		Request certification scheme
		Access to propose cybersecurity certification schemes
		Formal approval of cybersecurity certification schemes
		Request revision of schemes
		Provide feedback for schemes
		Request for mutual agreement
		Formal peer review
		Access Meeting management
ENISA	Roles_Admin	Administration of roles and assignation of accounts to specific roles
	CSS_Admin	Administration and publication of cybersecurity certification schemes
	Certs_Statements_Admin	Administration of EU cybersecurity certificates and EU statements of conformity
	Com_Admin	Administration of communication platform and official publications

Entity	IT Role	Use Cases
	DraftSection_Admin	Administration of the drafting section
	ADWG_Secretary	Prepare a candidate scheme
		Review a candidate scheme
		Access to Content management system (CMS) drafting section
		Prepare reports
		Access Meeting management
	ENISA_User	Access to collaboration platform
		Access to CMS drafting section
		Access to communication platform
		Mutual recognition
Management Board of ENISA	Mgmt_Board_User	Approve requests to prepare a candidate scheme
		Transmit draft of proposed candidate scheme to EC
		Reject request for candidate scheme
European Cybersecurity Certification Group	ECCG_User	Request certification scheme
		Access to DMS drafting section
		Access to Communication Platform
		Provide feedback for schemes
		Approval of cybersecurity certification schemes
		Access Meeting management
Stakeholder Cybersecurity Certification Group	SCCG_User	Access to Communication Platform
		Access Meeting management
Manufacturers & Providers	Submitter_User	Submit an EU statement of conformity
Interested Parties	Complains_User	Provide feedback
The Public	NO_ROLE	Access to publicly available information on publication platform
		Search
European Standardisation Organisations (ESO)	ESO_User	Access to communication platform
		Access to collaboration platform
Ad hoc Working Group	ADWG_User	Provide feedback for schemes
		Provide voting for draft candidate certification scheme
		Access to collaboration platform

Entity	IT Role	Use Cases
		Access to communication platform
		Access Meeting management
National Cybersecurity Certification Authority	NCCA_user	Upload annual report
All Entities	All Roles	Login
All Entities	All Roles	Register
All Entities	All Roles	Logout

3.2.9 Lists of terms

Vocabularies are lists of terms (name, value) used throughout the system for categorising data and information. Typical uses include selection drop downs in search interfaces or when editing the fields of data records. It is essential for the system to allow the definition and maintenance of vocabularies, both programmatically (e.g. by uploading a Json file) or manually, by allowing properly authenticated users to edit the list through the web. Upon editing or deleting values, the system should perform checks to insure that data integrity is maintained, i.e. items used to tag the data are not deleted before the data corresponding records are deleted.

Examples of vocabularies are:

- List of countries
- Types and categories of ICT products, ICT services and ICT processes
- Assurance levels
- EU and international SDOs

All modern CMSs offer support for the maintenance of vocabularies, but further integration will be needed for their integration with the data structures.

3.2.10 Formal messages – Message board

As detailed in use cases from the functional requirements section, there are certain steps in the system's processes that require formal messages to be recorded and stored. For instance, the requests for new candidate cybersecurity certifications schemes from EC/ECCG or the transmission of candidate cybersecurity certification schemes from ENISA to the EC contain messages that must be formally recorded, as they trigger other actions in the system. Moreover, ENISA will co-chair and be the secretariat of SCCG, therefore is required to maintain a record of all correspondence relating to the SCCG.

In this context, the system must implement a mechanism to store and display these messages, as well as an interface to browse them by subject and by other filters. It must be possible to reference individual messages in other parts of the system, such as link a message to a candidate scheme. In some cases, receiving a message (e.g. request for new certification scheme) will trigger an entire process in the system.

The solution should be similar to an inbox of an email account; in fact, for the purpose of sending and receiving emails, one or more ENISA email addresses should be created. These addresses can be included in copy of the email correspondence that needs to be recorded, triggering the corresponding messages and their metadata to be stored in the system. In the case where such address is omitted from a relevant message, it should be possible to manually record the message in the system by properly authenticated users.

A component needs to be built (or adapted), in order to ensure the following functionality:

1. Secure storage and backup of all messages
2. Messages from the same thread must be recorded together
3. New messages can be added by manually filling out a form or by allowing the system to automatically register an email message
4. Possibility to tag messages by type/topic, either by using predefined texts in the subject of the email, or by manually tagging them as they arrive in the inbox
5. User interface for browsing messages by thread and for filtering by various tags
6. Possibility to restrict certain types of messages by default
7. Subscription to receive email notifications upon receiving a message; in some cases, the notifications to one or more user groups should be automatic
8. The addition of messages should create events in the system. Depending on the type of message, the events will be linked to scripts, thus triggering various activities to be executed (e.g. automatically send emails to user groups)

3.2.11 Discussion forum

This component is intended to facilitate free discussions between stakeholders, as part of the collaboration platform of this system. It should support defining multiple discussion topics, to which threaded messages can be posted. Topics should be restricted to certain user groups, or should be available to all authenticated users, as needed. A mechanism for moderation of discussions should be also implemented.

It should be possible to open topics on specific subjects, like a request for a candidate cybersecurity certification scheme or a specific cybersecurity certificate, in which case the topic should reference a link from the portal to the scheme or to the certificate. The threaded posts should allow simple HTML content with formatting and links, as well as attached files up to a certain size.

Strictly for purposes of exemplifying suitable modules from the known CMSs, the list below can be considered:

- Plone Collective Ploneboard[12], built on top of Dexterity
- Plone content type Discussion[13], part of the Plone core package and easily extendable
- Drupal Forum module[14], part of the Drupal core
- Drupal Advanced forum[15] builds on and enhances Drupal's core forum module

3.2.12 Meeting management

ENISA is required to co-chair and provide secretarial duties, as well as to maintain a record of all correspondence relating to the SCCG and a record of all meetings and decisions of the SCCG. Therefore, the inclusion of a meeting management component is relevant for this IT system.

The requirements for this are:

- Maintain records of the meetings, with their dates and locations

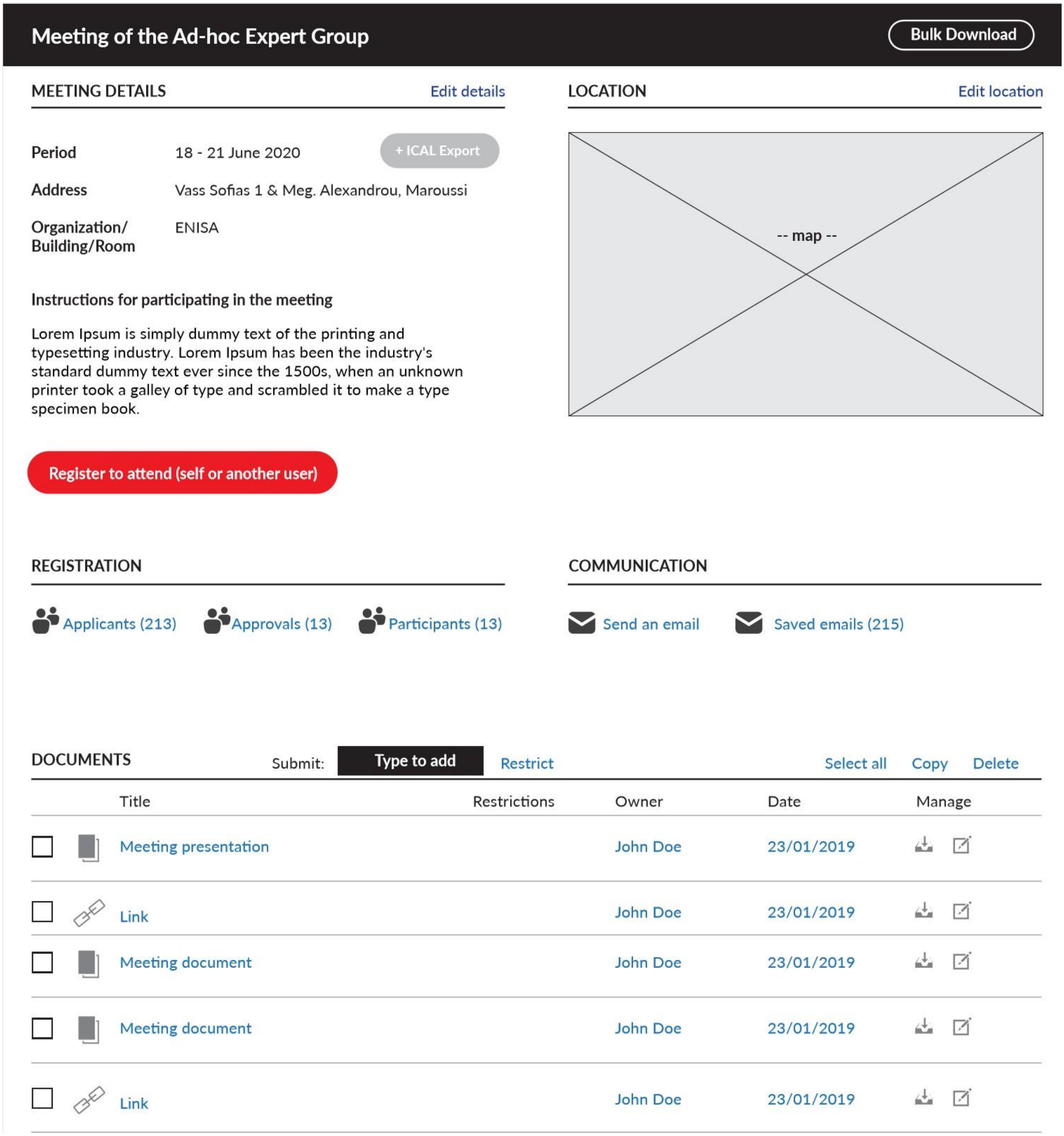
[12] Plone Collective Ploneboard https://github.com/collective/collective.ploneboard
[13] Plone Discussion https://github.com/plone/plone.app.discussion
[14] Drupal Forum module https://www.drupal.org/docs/7/core/modules/forum/overview
[15] Drupal Advanced forum https://www.drupal.org/project/advanced_forum

- Export of the meeting details in iCal format
- Maintain agendas, minutes and decisions taken during the meetings, along with the possibility to download the relevant documents
- Maintain a list of other documents and links
- Maintain a list of attendees, together with their affiliation. This entails the ability to generate reports with the participants, per role, organisation and country
- Offer instructions for participating in the meeting
- Ability for meeting administrators (ENISA users) to register participants
- Offer means to send mass emails to participants, with instructions and questions before the meeting
- Ability to restrict the content of the meeting materials to certain roles

In addition, other features would be useful for this component and should be implemented:

- Possibility for authenticated users to self-register for a meeting
- Possibility for meeting administrators to approve the self-registered attendees
- Interactive map with the meeting location
- Possibility to set a maximum number of participants

The wireframe below depicts the envisaged design for the meeting management tool.



Meeting of the Ad-hoc Expert Group

MEETING DETAILS

Period	18 - 21 June 2020
Address	Vass Sofias 1 & Meg. Alexandrou, Maroussi
Organization/ Building/Room	ENISA

Instructions for participating in the meeting

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

LOCATION

REGISTRATION

COMMUNICATION

DOCUMENTS

	Title	Restrictions	Owner	Date	Manage
□	Meeting presentation		John Doe	23/01/2019	⤓ ✎
□	Link		John Doe	23/01/2019	⤓ ✎
□	Meeting document		John Doe	23/01/2019	⤓ ✎
□	Meeting document		John Doe	23/01/2019	⤓ ✎
□	Link		John Doe	23/01/2019	⤓ ✎

Figure 46: Wireframe for the meeting management main interface

3.2.13 Data mining

Several parts of the cybersecurity certifications schemes, cybersecurity certificates or the statements of conformity need to be checked for potential duplication of content before being published or released. Therefore, the system must include a data mining component, intended to ensure and demonstrate consensus in the design of schemes amongst the AHWG and the ECCG.

For this purpose, a third-party component, built for antiplagiarism, should be used to find similarities between the texts of existing schemes, certificates and their technical documentation and signal potential overlaps.

A good list of such components can be found on Wikipedia[16], but other services might become available in the meantime. The difference in choosing the software should be made by the possibility to install the service locally as opposed to using it as a service (SaaS), the size of the database of texts and its relevance to the currently referred technical data, as well as the price of the service.

3.3 TIMELINE FOR IMPLEMENTATION

The IT Systems should be implemented in phases: the most critical functionalities will be implemented first, in order to sustain the urgent business processes, while less urgent functionalities could be delivered in subsequent iterations.

The implementation of this IT system is scheduled to take place over a year from the signing of the contract (T0). Four delivery phases are foreseen, with interim and final deliverables as follows:

1. Phase 1 [T0 + 3 months] – system in version 0.5, ready for adding content:
    a. Content management system in place with web design implemented
        i. Metadata for all content types
        ii. Content types for folder, link, article, document (file), event, news, video and image galleries
        iii. Lists of terms
        iv. User groups
    b. Message board (inbox of formal messages)
    c. Request for cybersecurity certification scheme
2. Phase 2 [T0 + 6 months] – system ready for launch in version 1:
    a. Cybersecurity certification schemes with collaboration features
    b. Adjustments to the content management system
    c. Meeting management
    d. National certification schemes
    e. Conformity Assessment Bodies
    f. Discussion forum
    g. Reports – first set
3. Phase 3 [T0 + 9 months] – system in third version:
    a. European cybersecurity certificates and EU statements of conformity
    b. Conformity self-assessment
    c. Reports – second set of reports
    d. Data mining
4. Phase 4 [T0 + 12 months] – final version of the system:
    a. All functionality completed and feedback from stakeholders implemented

[16] Wikipedia - Comparison of anti-plagiarism software https://en.wikipedia.org/wiki/Comparison_of_anti-plagiarism_software

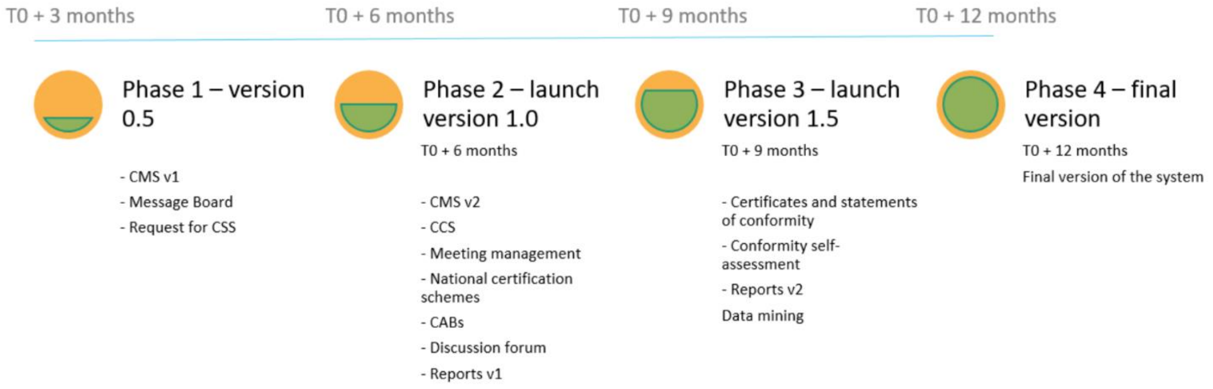


Figure 47: Proposed phases of the project and associated deliverables

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