Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D8.4

Standardisation Procedure Assessment Document

Document Identification	
Due date	31 March 2022
Submission date	31 March 2022
Revision	V1.0

Related WP	WP 8	Dissemination Level	PU
Lead Participant	GUF	Lead Author	Welderufael B. Tesfay
Contributing Beneficiaries	GUF, CYBER, UMA, POLITO, BRNO	Related Deliverables	D8.1/2/3

Abstract:

Deliverable 8.4 “Standardisation Procedure Assessment Document” presents an assessment of eight different Standards Development Organisations (SDOs) that have impact in the cybersecurity domain. The assessment is carried out using eight criteria developed through a mix of iterative expert discussions in Work Package 8 as well as some adapted from the World Trade Organisation principles. The deliverable also offers recommendations for different actors in cybersecurity, including the European Cybersecurity Competence Centre.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union’s Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This deliverable evaluates different existing Standards Development Organisations (SDOs) that are currently developing projects addressing cybersecurity-related aspects. The ultimate goal of this analysis is to allow both cybersecurity researchers and companies in the EU to better understand the operation of these organisations and to facilitate the process of deciding with which of them to collaborate or to associate. This document is intended to encourage participation in such organisations and to speed up the development of cybersecurity standards, which is usually a lengthy process, but cybersecurity issues are critical and need to be addressed swiftly.

More precisely, this document assesses eight standard organisations based on a methodology that defines eight evaluation criteria – openness, impact, governance, maturity, stability, effectiveness and relevance, coherence, and the development dimension. The assessed SDOs have been selected to cover a wide range of models, including organisations with national representation following the UN model, member-based consortia with no national restrictions as well as national standardisation bodies. After the analysis, the deliverable provides a summary with the key findings and a set of recommendations on how to better integrate cybersecurity into the procedures of standardisation bodies, especially in the future European Cybersecurity Competence Centre.

Document information

Contributors

Name	Partner
Welderufael B. Tesfay	GUF
Ruben Rios	UMA
Javier Lopez	UMA
Liina Kamm	CYBER
Antonio Lioy	POLITO
Petr Švenda	BRNO

Reviewers

Name	Partner
Antonio Lioy	POLITO
Mark Miller	CONCEPT
Stephan Krenn	AIT

History

Version	Date	Authors	Comment
0.01	2021-01-20	Welderufael B. Tesfay	ToC
0.02	2021-02-10	Welderufael B. Tesfay	Methodology section
0.03	2021-05-28	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda, Antonio Lioy	Contributions to Section 3
0.04	2021-08-30	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda, Antonio Lioy	Added summary table in Section 4
0.05	2021-09-20	Welderufael B. Tesfay, Ruben Rios, Petr Švenda	Section 4 content added
0.06	2021-10-27	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda, Antonio Lioy	Added summary table in Section 4
0.07	2021-11-03	Welderufael B. Tesfay	Addition of new assessment criteria based on WTO principles
0.08	2022-01-15	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda, Antonio Lioy	Expansion of Section 3 using newly added criteria
0.09	2022-01-31	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda	Internal review by contributors
0.10	2022-02-08	Welderufael B. Tesfay, Ruben Rios, Liina Kamm, Petr Švenda, Antonio Lioy	Address internal review feedback
0.11	2022-02-21	Liina Kamm	Internal review by WP leader
0.12	2022-02-22	Welderufael B. Tesfay	Address internal review by WP leader
0.13	2022-03-04	Mark Miller, Stephan Krenn	Review
0.14		Welderufael B. Tesfay	Address review
0.15	2022-03-20	Antonio Lioy	Second round review
0.16	2022-03-23	Welderufael B. Tesfay	Address reviews
0.17	2022-03-25	Liina Kamm	Review by WPL and PC
0.18	2022-03-27	Welderufael B. Tesfay	Address reviews
0.94	2022-03-30	Welderufael B. Tesfay	Finalisation
1.0	2022-03-31	Ahad Niknia	Final check , preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AENOR**	Asociación Española de Normalización y Certificación - Spanish Association for Standardisation and Certification
	ANSI	American National Standards Institute
	API	Application Programming Interface
B	**BOE**	Boletín Oficial del Estado - Official State Gazette
C	**CA**	Cooperation Agreement
	CEN	European Committee for Standardisation
	CENCENELEC	European Committee for Electrotechnical Standardisation
	CEPT	Conférence Européenne des Postes et des Télécommunications, i.e. European Conference of Postal and Telecommunications Administrations
	COPANT	Pan American Commission of Technical Standards
	CTN	Comité Técnico de Normalización - Normalisation Technical Committee
D	**DIN**	Deutsches Institut für Normung or German Institute for Standardisation
E	**EG**	ETSI Guide
	EN	European Norm
	EP	ETSI Project
	EPP	ETSI Partnership Project
	ES	ETSI Standard
	ESI	Electronic Signatures and Infrastructures
	ETSI	European Telecommunications Standards Institute
	EU	European Union
F	**FHIR**	Fast Healthcare Interoperability Resources
	FMG	FHIR management group
G	**GA**	General Assembly
	GDP	Gross Domestic Product
	GR	Group Report
	GS	Group Specification
H	**HL7**	Health Level Seven International
I	**IEC**	International Electrotechnical Commission
	ISG	Industry Specification Group
	ISO	International Organisation for Standardisation
	ITU	International Telecommunication Union
	ITTF	Information Technology Task Force

J	**JTC1**	Joint Technical Committee 1
L	**LOI**	Letter of Intent
M	**MoU**	Memorandum of Understanding
	NFV	Network Functions Virtualisation
N	**NIST**	National Institute of Standards and Technology
	NSO	National Standards Organisation
O	**OASIS**	Organisation for the Advancement of Structured Information Standards
	OECD	Organisation for Economic Co-operation and Development
	OP	Open Project
	OWG	Other Working Group
P	**PGB**	Project Governing Board
	PKI	Public-Key Infrastructure
Q	**QKD**	Quantum Key Distribution
S	**SAML**	Security Assertion Markup Language
	SMB	Standardization Management Board
	SC	Special Committee
	SDO	Standards Developing Organisation
	SME	Small and Medium Enterprise
	SR	Special Report
	STU	Standard for Trial Use
T	**TAG**	Technical Advisory Group
	TC	Technical Committee
	TMB	Technical Management Board
	TR	Technical Report
	TS	Technical Specification
	TSC	Technical Steering Committee
	TWP	Technical Working Procedures
U	**UNCTD**	United Nations Conference on Trade and Development
	UNE	Una Normal Española - Asociación Española de Normalización

	US	United States
W	**WG**	Working Group
	WSS	Web Services Security
	WTO	World Trade Organisation
X	**XACML**	eXtensible Access Control Markup Language

1 Introduction

There are numerous different standards developing organisations (SDOs) of different level and scope in the world. Most of them have their own organisation structure, membership criteria and fees. There are international standardisation organisations like ISO/IEC that cover a wide variety of topics, accept membership from all countries, and require payment for their standards. CEN/CENELEC is a European standardisation organisation that is somewhat similar to ISO/IEC but works on European standards (EN). HL7 is an international organisation that is focussed on electronic health information, allows membership from all countries and the standards are freely available. In addition, there are national standardisation organisations that govern the standardisation within one country with members from companies or institutions in that specific country.

This document looks at eight prominent standards developing organisations using eight assessment criteria. We give an overview of the differences and similarities of the organisations and offer recommendations to the European Commission and the European Cybersecurity Competence Centre to help shape their approach towards standardisation.

1.1 Problem Definition

Studies show that over the last decades, cybersecurity attacks and concerns have become prevalent. These threats and attacks often have detrimental effects to the welfare and brand of the company as well as to the privacy and safety of its users. Standardisation and certification of processes, products and information systems can help companies and developers to implement and deploy systems that are secure and private by design.

However, the attacks are evolving quickly and the technology cannot always be standardised in a timely manner. Moreover, different SDOs have different procedures and different turnaround times, therefore, it is difficult for an organisation developing a new technology, to know how and where to get it standardised.

This deliverable analyses the appropriateness of the existing standardisation procedures of eight standards developing organisations that are relevant for Europe and its cybersecurity goals:

- CEN/CENELEC,
- ISO/IEC JTC 1,
- ETSI,
- OASIS,
- HL7,
- BSI (German Federal Office for Information Security),
- UNE (National Standardisation Body of Spain), and
- Common Criteria.

In particular the deliverable assesses the work efforts and procedures of organisations in their development of cybersecurity standards and/or those work streams which include cybersecurity concerns in their standards. For all of the organisations, we assess the existing standardisation procedures, documenting their appropriateness for cybersecurity goals and their exploitation of open tools.

1.2 Document Structure

First, in Section 2 we describe the methodology and assessment criteria that we have developed and used for assessing and comparing the different standardisation organisations. Section 3 provides the results of our analysis of the selected standardisation organisations. Section 4 summarises the key observations in a

table that gives a comparative overview of the selected organisations. Furthermore, we give recommendations about standardisation activities that can be used by the European Commission and the European Cybersecurity Competence Centre to shape their viewpoint and course towards standardisation.

2 Methodology

In this section, we discuss the methodology we follow to develop our approach of assessing the appropriateness of the existing standardisation procedures for cybersecurity goals. This process is summarised on Figure 1. We first developed assessment criteria follow expert discussions within and the adaptation of existing principles from the World Trade Organisation (WTO). The WTO has developed a list of principles which also serve as basis in different areas, including in enacting regulations. We adapted three of these criteria into our assessment catalogue. Section 2.1 discusses these in more detail.

We selected the standardisation organisations that we focus on in this deliverable based on the following criteria. First, we looked at standardisation bodies involved with the security domain in the broad sense (including physical security and safety standards). We then shortlisted organisations to those still active and relevant to the cybersecurity field. Finally, we chose CEN/CENELEC and ISO/IEC JTC 1 as two of the largest organisations with national membership following the UN Model. We chose ETSI, OASIS, and HL7 that have member-based consortia with no national restrictions. We chose UNE (National Standardisation Body of Spain) and BSI (Bundesamt für Sicherheit in der Informationstechnik, German Federal Office for Information Security) as two examples of national standardisation organisations, and finally, we chose Common Criteria (CC) as the driving force for the widest available mutual recognition of secure IT products. In Deliverables 8.1 and 8.3, CEN/CENELEC, ISO/IEC JTC 1 and ETSI were revealed to be the SDOs with which CyberSec4Europe members have the most interactions. OASIS was brought to our attention by one of our reviewers and we decided to add this as it is relevant in the cybersecurity domain. The HL7 standard FHIR is used worldwide for digital health data and it was also adopted in Task 5.6 as per the suggestion of the standardisation work package. As for BSI and UNE, we decided to choose two national SDOs in which the deliverable authors are involved, because information about national SDOs is often harder to access and mostly in the language of the country in question.

After SDO selection, we analysed the SDOs based on the assessment criteria and documented the results, given in Section 3. In Section 4, we also present a table that gives a comparative overview of the SDOs.

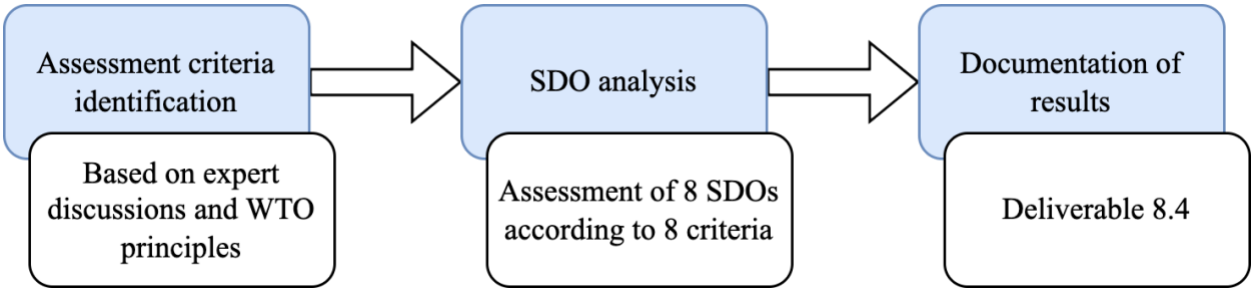

Figure 1: Assessment process

2.1 Assessment Criteria

In this subsection, we introduce the eight criteria used in this deliverable to assess the appropriateness of the existing standardisation procedures in the context of achieving the cybersecurity goals.

2.1.1 Openness

The openness criteria in itself entails a number of sub-criteria to analyse the procedures and practices of SDOs. The WTO defines the openness as a criterion fulfilling that "membership of an international standardizing body should be open on a non-discriminatory basis to relevant bodies of at least all WTO Members. This would include openness without discrimination with respect to the participation at the policy development level and at every stage of standards development." (WTO, 2000).

Furthermore, the European Interoperability Framework for pan-European eGovernment Services provides a more detailed definition of open standards including (EC, 2011):

- the standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.);
- the standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee;
- the intellectual property – i.e. patents possibly present – of (parts of) the standard is made irrevocably available on a royalty-free basis; and
- there are no constraints on the re-use of the standards.

In addition to the definitions by the WTO and European Interoperability Framework for pan-European eGovernment Services, openness can be checked against the following points.

(1) Openness to the public (participation, document availability, influence)
(2) Access to meetings (open for all, open for members, membership fees, membership tiers)

2.1.2 Impact

The impact criteria essentially analyses the contributions of results of the SDOs to the wellbeing of society. A closer look at the national and European Union (EU) level impact of the outcome of SDOs will be taken into consideration.

2.1.3 Governance

The governance criteria investigates how the SDOs are administered. This is further analysed using criteria such as organisational structures, voting rules, and commenting procedures on open projects. The voting rules maybe determined based on one member one vote rules, and membership tiers (e.g., those with prime membership).

2.1.4 Maturity of Procedures

Assessing the maturity of existing procedures aims to analyse if the SDO has self-checking mechanisms in place to ascertain that its existing procedures are up to the demand in relation to appropriateness.

2.1.5 Stability of Procedures

The stability of procedures criteria implores if the SDO is offering enough stability in its procedures, so that volunteers, especially those, who are not working on standardisation full time, can effectively participate. This means that the experts do not have to spend a too high share of their allocated time to update themselves on new procedures, and can rather spend their limited time budget on the actual standardisation projects.

2.1.6 Effectiveness and Relevance

The effectiveness and relevance principles are adapted from the WTO principles. These combined criteria assert that standards have to be adaptable to regulatory and market needs. In addition to adaptability of standards to market and regulatory needs, the criteria stipulates that the standards should take the scientific and technological advancements into account. Adaptability also entails that the standards have to foster innovations instead of inhibiting. This can be achieved by devising appropriate mechanisms with the purpose of identifying and reviewing standards that have become obsolete, inappropriate, or ineffective.

2.1.7 Coherence

The coherence principle of the WTO is used to check if SDOs have established mechanisms in place to avoid duplication of work in other similar efforts. Such mechanisms include the establishment of an effective liaison and channel of cooperation and coordination with SDOs working in similar projects.

2.1.8 Development Dimension

The development dimension principle demands that SDOs have effective remedies to encourage developing countries participation in the development of standards. While developing countries can contribute to the development of standards as well as create a conducive environment for early adoption of the standards, often their participation is limited primarily due to technical and financial challenges.

3 Analysis of SDOs

With the ever-growing sophistication and pervasiveness of cyber threats, the need to have safeguarding mechanisms becomes of paramount importance. Over the years, cyber threats have increased in their varieties and prevalence which calls for expeditious development of cybersecurity standards and guidelines. However, there are concerns that cybersecurity standards development is often moving at a slower pace compared to the speed at which the sophistication and pervasiveness of cyber-attacks are developing.

The aim of the analysis of SDOs in this section is, therefore, to methodically look at cybersecurity standards themselves and cybersecurity concerns in other relevant standards. This section documents the assessment of the existing standardisation procedures, to register their appropriateness for cybersecurity goals and their exploitation of open tools, and to suggest improvements.

3.1 Organisations with National Representation Following the UN Model

3.1.1 CEN/CENELEC

CEN is a European Standardisation Organisation, operating within the framework of EU Regulation 1025/2012. The members of CEN are joint producers and disseminators of market-driven European Standards (ENs) that serve the needs of business, industry, and other interested parties.

European standardisation is organised by and for the stakeholders concerned based on national representation (the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC)) and direct participation (the European Telecommunications Standards Institute (ETSI)), and is founded on the principles recognised by the World Trade Organisation (WTO) in the field of standardisation, namely coherence, transparency, openness, consensus, voluntary application, independence from special interests and efficiency (the founding principles) (EU, 2012).

CEN/CENELEC allows three levels of participation and involvement, namely:

1. National level
    1. Through the CEN National Standardisation Bodies/CENELEC National Committees
    2. Through the national trade associations representing different sectors of business and industry

2. European level
    1. Through European trade associations and federations
    2. Through European interest groups
    3. By contacting the CEN-CENELEC Management Centre in Brussels

3. International level
    1. Through the International Organisation for Standardisation (ISO)
    2. Through the International Electrotechnical Commission (IEC)
    3. JTC1

3.1.1.1 Openness

Standardisation activities of products and services in Europe is carried out mainly by European Standardisation Organisations: the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI).

CEN's National Members are the National Standardisation Bodies (NSBs) of the 27 European Union countries, United Kingdom, the Republic of North Macedonia, Serbia and Turkey and three countries of the European Free Trade Association (Iceland, Norway and Switzerland). There is one member per country.

As mentioned earlier, CEN/CENELEC allows three levels of participation and involvement. National level participation is mainly possible through the CEN National Standardisation Bodies/CENELEC National Committees and the national trade associations representing different sectors of business and industry. Similarly, European level participation is facilitated through European trade associations and federations, European interest groups as well as by contacting the CEN–CENELEC Management Centre in Brussels. Finally, international level is made possible through the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

Regarding document availability, many resources are available on the respective portals. However, during our research, we faced that some links appear to be broken. For example, “Part 1D” of the CEN-CENELEC Internal Regulations (https://boss.cen.eu/media/ref/IR1_E.pdf) does not lead to the intended resource.

CEN/CENELEC has a network of more than 200.000 technical experts from industry, associations, public administrations, academia, and societal organisations. In terms of stakeholders, the CEN/CENELEC system has: business, industry, and commerce; service providers; consumer, environmental, and societal organisations; public authorities and regulators; other public and private institutions.

CEN/CENELC seems to receive community (community refers to working group) membership coming through other entities, i.e., 34 national members, European organisations, associations and federations; governmental bodies and other authorities. The affiliates who are the national standards bodies/committees in countries that are cooperating with the European Union; relations and Memoranda of Understanding (MoU) with regions and countries outside the European Union and EFTA; and international cooperation with ISO (CEN) and IEC (CENELEC).

CEN-CLC/JTC 13 ‘Cybersecurity and data protection’ is the CEN and CENELEC horizontal technical committee that addresses these challenges. Its primary objective is to transport relevant international standards (especially from ISO/IEC JTC 1 SC 27) as European Standards (ENs) in the Information Technology (IT) domain. It also develops ‘homegrown’ ENs, where gaps exist, in support to EU regulations (RED, eIDAS, GDPR, NIS, etc.). These two streams of activities aim at creating a strategic portfolio of standards in Europe, which fits the European needs (CENELEC C. , 2022).

Consensus among all interested parties including industry, economic players, authorities and civil society is an essential characteristic of approving agreements in CEN/CENELEC procedures.

The degree of consensus is evaluated and measured at different stages, at different levels and in different ways during the development of a European Standard (EN). These include consensus at Working Group (WG) level, amongst the participants, evaluated by the WG Convenor with agreement from the WG, before submitting a draft to the Technical Committee (TC) Secretary for further processing; as well as consensus at CEN level, amongst the CEN National Members, measured in CCMC through the counting of the votes at the closure of the Enquiry and then assessed by the Technical Committee (CEN, CEN, 2017).

3.1.1.2 Impact

CEN and CENELEC have been contributing to EU wide policy on trade policies, standards and as connectivity and interoperability of products and technology across manufacturers, national borders, technical standards become the basic engine of global trades and relationships among national and international organisations (cencenelec, 2022). In addition to policy enactment support, CEN and CENELEC resources have been useful to design educational resources in the cybersecurity area (ICTSkills, 2022).

3.1.1.3 Governance

CEN and CENELEC each have their own respective governance bodies.

CENELEC Corporate Governing Bodies is composed of (CENELEC, 2022):

- The General Assembly (CENELEC/AG) is the supreme body of the CENELEC.
- The Administrative Board (CENELEC/CA) manages and administers the CENELEC’s business. It also responsible for the preparation of the agendas of the General Assembly meetings. Furthermore, the Administrative Board ensures the implementation of the decisions taken by the General Assembly.
- The Presidential Committee is the joint Corporate Body of CEN and CENELEC. Its role is to manage activities regarding the non-sector specific matters of common interest to both Associations. It is composed of the two Presidents of CEN and CENELEC, the two President Elects, the six Vice Presidents and the common Director General.

The Director General, the Technical Board, the Technical Committees and the Board of Appeal, as stipulated in the Internal Regulations are the other Corporate Bodies supporting the achievement of the scope of CENELEC. The CENELEC Technical Board is responsible for controlling the standards programme and promoting its speedy execution by the CEN-CENELEC Management Centre (CCMC), Technical Committees (TCs) and other bodies.

Similar to CENELEC, CEN Corporate Governing Bodies is composed of (CEN, 2022):

- General Assembly: is the supreme governing body of CEN and determines the CEN policy. The General Assembly is composed of the delegations from the National Standards Bodies (NSBs) of each of the Member countries of CEN and of selected CEN partners, who attend the AG as observers

(such as: Affiliates, Companion Standardization Bodies, CENELEC, ETSI, ISO, European Partner Organizations, the European Commission and the EFTA Secretariat).
- Administrative Board: manages and administers CEN's business by directing the work and coordinating the actions of all CEN bodies with the aim of executing the decisions taken by the General Assembly.
- The Presidential Committee is a joint Corporate Body of CEN and CENELEC. It manages and administers activities with respect to non-sector specific matters of common interest to both Associations.
- The CEN Technical Board controls the full standards programme and promotes its speedy execution by the Technical Committees (TC), the CEN-CENELEC Management Centre (CCMC), and other bodies.

The Director General, the Technical Board, the Technical Committees and the Board of Appeal, as stipulated in the Internal Regulations are the other Corporate Bodies supporting the achievement of the scope of CEN.

The CEN/CENELEC management center is headed by a Director General who is responsible for overall leadership and management of the organizations according to the strategic directions set by the governance. The Director General also represents CEN and CENELEC within the European Standardization System. Additionally, as highlighted above, both CEN and CENELEC have the Presidential Committees that serves as a joint Corporate Body of CEN and CENELEC.

3.1.1.4 Maturity of Procedures

CEN/CENELEC is regularly updating its various documents which in hindsight indicates that CEN/CENELE checks the maturity and viability of its procedures.

3.1.1.5 Stability of Procedures

The Stability of Procedures criteria answers if the CENE/CENELEC as an SDO is offering enough stability in its procedures, so that volunteers, especially those, who are not working on standardisation full time, can effectively participate. With regard to this, the internal regulations of CEN/CENELEC seems to be updated in January 2022 (InternalRegulations, 2022). This is its first update since it was last updated in 2017. The new release includes a latest update on Organisation and Structure released in January 2022 (ReferenceMaterial, 2022). Updates after five years interval could be an appropriate choice for two reasons: 1) to fit into dynamically changing environment, long interval updates could present a challenge; 2) five years interval might not create a steep learning curve as well as consume time of those with less resources including individuals and SMEs, as it gives enough time for adaptation and planning.

3.1.1.6 Effectiveness and Relevance

CEN/CENELEC is an independent association which is primarily market driven (CEN-CENELEC, 2022). It operates as a European Standardisation Organisation according to, and supportive of, the WTO principles. Furthermore, the Candidate Organisation to become a CEN and CENELEC national Member (i.e.: the Candidate Organisation) must be able to cope with the pace of the work of the CEN-CENELEC system in order to benefit fully from it, and not to slow down the progress of CEN and CENELEC, which is governed by market needs**.**

3.1.1.7 Coherence

In order to ensure coherence of the system it is important to avoid the development of conflicting standards. Likewise, it is also critical to avoid duplication of efforts among similar tasks in different SDOs. Hence, cooperation and coordination within the European system of CEN and/or CENELEC is essential to ensure

coherence. To achieve this, a Member shall implement the European standards by fulfilling two essential obligations:

a) giving the European standards “ENs” the status of national standards, and;
b) withdrawing any conflicting national standards.

This needs to avoid:

1. duplication and overlap with standardisation at European level (CEN-CENELEC) 'Internal coherence within the system'
2. duplication and overlap with standardisation at international level (ISO, IEC). 'External coherence with other systems'
3. duplication or conflict between sectors, within a Member’s work programme or collection of published standards, and with national legal requirements
4. be complementary to legal requirements

Regarding the relationship of CEN with other SDOs, conventions such as the Vienna Agreement have been agreed upon. The Vienna Agreement is essentially an agreement on technical cooperation between ISO and CEN including the exchange of technical information.

Its objectives include:

- to facilitate and recognise particular needs in Europe such as the European Single Market, which might demand the development of standards and help these standards be recognised at the international level; and
- the prioritisation of ISO work such that in some instances CEN needs to undertake work which is urgent in the European context, but less so in the international one.

There are two modes for collaboration and cooperation in the Vienna agreement, i.e., the mode under ISO lead and the mode under CEN lead, in which documents developed within one body are notified for the simultaneous approval by the other.

The Vienna agreement provides the following advantages:

- the agreement increases transparency of work ongoing in CEN to ISO members;
- it creates an opportunity to influence the content of CEN standards;
- avoidance of duplication of work and structures, thus allowing expertise to be focused and used in an efficient way to the benefit of international standardisation; and
- increasing the speed of elaboration, availability, and maintenance of standards through a need to establish consensus only once.

3.1.1.8 Development Dimension

CEN/CENELEC is supposed to fulfil the WTO principles and be governed by the EU regulation 1025/2012. However, our assessment could not find CEN/CENELEC’s plan to encourage participants from developing countries. This could be due to the continental nature of CEN/CENELEC.

3.1.2 ISO/IEC JTC 1

ISO and IEC Joint Technical Committee (JTC 1) for information technology, is a consensus-based, voluntary international standards group. Over 2000 experts from 163 countries develop mutually beneficial guidelines that enhance global trade while protecting intellectual property. Industries develop solutions for their markets and customers. ISO/IEC JTC 1 experts play a role in recommending baselines and standards for safety features, acceptable quality measures and testing, for example. When international bodies apply

those recommendations, it can facilitate global acceptance of products, speed up time-to-market for new products and reduce manufacturing costs.

3.1.2.1 Openness

As of February 2022, ISO has published 3299 standards, of which 513 are in the category of ISO/IEC JTC 1. Additionally, ISO has 581 projects under development (ISO, 2022). Out of the 581 projects, 35 are under responsibility of ISO/IEC JTC 1.

ISO/IEC JTC 1 has 42 subcommittees, of which subcommittee 27 (SC 27) deals with information security, cybersecurity and privacy protection.

SC 27 engages in active liaison relationships and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

Regarding membership, ISO has a maximum of one representative member per country i.e., the organisation most representative of standardisation in the respective field and country. Usually, these are national standardisations bodies, e.g., DIN in Germany. There are "participating" (with fee and right to vote) or "observing" membership types for technical committees. Observing members have the right to view documents, but not vote.

There are two types of drafts in the document development process, namely: working drafts that receive comments in working groups (WGs), composed by experts delegated by the participating members; and committee drafts that are commented by the participating national bodies, which are members of the respective committees or subcommittees. Work in a WGs is led by the "Convenor" who leads the activities of the WG as such the Convenor is responsible to lead management and organization of meeting agenda. The Convenor also looks after the interaction and the discussion pf works towards a consensus on the maturity of Working Drafts. After Working Draft is matured, it becomes a Committee Draft.

3.1.2.2 Impact

The results of ISO/IEC has been influential in fostering security in various industrial sectors, including in developing secured health health certificates in response to the Covid-19 (Price, 2021). The ISO/IEC 27001, 27701 for privacy, and the whole 27000 family as a success story of ISO are among the impactful outputs of the entire ISO family. These ISO outputs have also had a significant impact to industry and research in advancing security and privacy requirements, management of information and ICT security, cryptographic security mechanisms, secure aspects of identity management, etc.

3.1.2.3 Governance

As depicted in Figure 2 below, the ISO/IEC JTC 1 has Subcommittees, Working Groups, Study Groups, Special Working Groups and Advisory Boards. Additionally, it has an mechanism to interact with the Information Technology Task Force (ITTF) which is an entity jointly formed by ISO and IEC responsible for the planning and coordination of the work of JTC 1. JTC 1 has 22 Submcommittees (SC) focusing on various topics of standardization, of which SC 27 endeavors on Information security, cybersecurity and privacy protection. Additionally, JTC 1 previousld had 13 Working Groups (WGs) in its structure. Some of these have later converted in SCs.

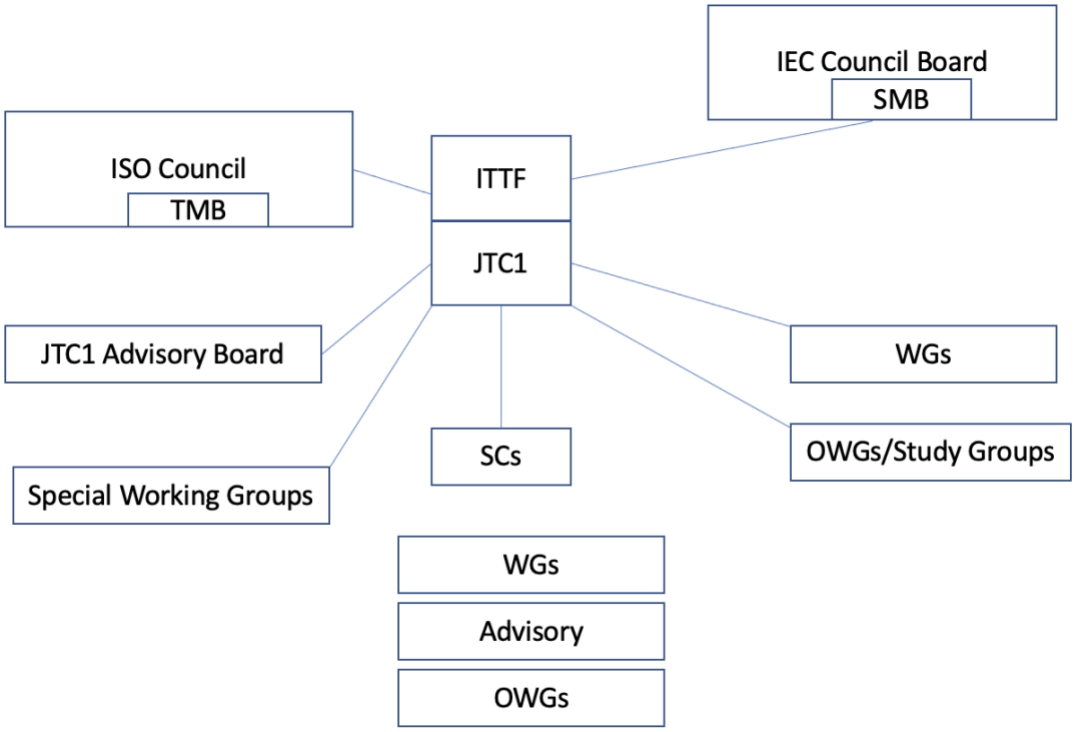

Figure 2: ISO/JTC 1 organisational structure (Wennblom, 2018)

3.1.2.4 Maturity of Procedures

SC 27 has committees and mechanisms that assess the maturity of existing procedures. This includes the Management advisory group that handles requirements from the members and member states and Operations that follows up the implementation of procedures or existing rules within the organisation. Likewise, JTC 1 has the JTC 1 advisory group (AG) which revises the JTC 1 supplements and the AG 17 which reviews meeting guidelines.

3.1.2.5 Stability of Procedures

When it comes to the stability of procedures, ISO/IEC has directives and its rules are updated every year. Similarly, JTC1 directive rules are updated every year. Lately, COVID-19 has affected the meeting procedures and rules. This has created a tendency into organising events and meeting virtually.

3.1.2.6 Effectiveness and Relevance

According to the ISO Strategy 2021-2030, ISO/IEC has identified goals including:

- Goal 2.1: Deliver ISO standards when the market needs them; and
- Goal 1.2: Innovate to meet users' needs.

The 12th edition ISO/IEC Directive Section 2.9 released in 2021 states that it implements a mechanism and procedures for the maintenance of deliverables. This helps identify obsolete standards and propose fitting remedies. Such mechanisms are given in the respective Supplements to the ISO/IEC Directives.

3.1.2.7 Coherence

Annex B of the ISO/IEC Directives, Part 1 (Procedures for the technical work), 17th edition, 2021, provides detailed rules of the liaison and work allocation facilitated within and to ISO/IEC including liaison between

- technical committees;
- liaison between ISO and IEC; as well as
- liaison with other organisations.

3.1.2.8 Development Dimension

ISO/IEC has a rule set called twinning aimed at encouraging participation of members from developing countries. Twinning serves as a linking/partnership mechanism between two national bodies for the purpose of capacity building between members of a developed and developing country. ISO and its members have developed the concept of twinning, by which an ISO member seeking to build its capacity may enter into an arrangement with an ISO member that is in a position to share its knowledge.

The objectives of twinning include:

- improve the standardisation infrastructures and capacities of the twinned partner;
- increase the participation of the twinned partner in the governance and technical work of ISO; and
- promote the exchange of experience between members, optimise the use of resources through cooperation, and develop long-term strategic partnerships.

Twinning partners need a written agreement using the ISO template. The agreement may not necessarily involve financial support. The lead partner provides training and guidance of capacity building to the twinned partner

The following steps are applied when implementing twinning:

- guidance on self-assessment (for the twinned partner);
- identifying a partner for the twinning arrangement;
- approval of nominated ISO member or individual; and
- negotiation of the twinning agreement.

After assessments, member decides for one of the four twinning modalities:

1. P-member twinning,
2. Leadership twinning:
    a. Convenor,
    b. Chair,
    c. Secretariat.

The lead partner has the important role of providing training, guidance and assistance to build the capacity of the twinned partner.

3.2 Organisations with Member-Based Consortia with No National Restrictions

3.2.1 ETSI

ETSI is a European Standards Organisation (ESO), set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) in response to proposals from the European Commission (ETSI, Official website,). ETSI is a European Standards Organization (ESO) also recognised as regional standards body dealing with telecommunications, broadcasting, and other electronic communications

networks and services. ETSI receives funding from the European Commission (EC) and the European Free Trade Association (EFTA).

ETSI is one of three bodies (along with CEN and CENELEC) whose standards are recognised as European Standards (ENs).

3.2.1.1 Openness

ETSI is open to organisations from all over the world. Bodies based in the CEPT area are eligible for Full membership, while bodies outside the CEPT area are eligible for Associate Membership. Associate members have the right to vote on all matters except in two situations, that is, where weighted national voting applies or where weighed individual voting by full members applies.

While participation is open, decisions are taken based on majority votes.

Annual fees and voting rights are tightly related and they are based on the class of the organisation and its annual turnout (more details at (ETSI, 2022). As a rule of thumb, the bigger the company, the more its voting rights.

To encourage participation, fees are kept to a minimum for SMEs, user and trade associations, micro-enterprises, universities, public research bodies and not-for-profit user associations.

3.2.1.2 Impact

ETSI is a well-established SDO, with its standards achieving recognition and widespread usage in the industry and governments, not only at European level but also worldwide.

Recent examples of impact achieved by ETSI work are in the sector of electronic signatures and related trust services (where its standards – created by the TC on Electronic Signatures and Infrastructures, ESI – form the basis of technical legislation across Europe) and of NFV (where its technical documents achieved recognition by industries across the world as the basis for product interoperability).

3.2.1.3 Governance

ETSI is governed by the General Assembly and the ETSI Board. The General Assembly has the following tasks:

- appointments;
- rules and regulations;
- membership;
- budget and financial matters;
- annual report;
- ainal point of approval; and
- appeals.

The ETSI Board has the following powers and duties

- work programme;
- application of financial resources;
- advice to General Assembly on finance/resource issues;
- creating/closing TCs, EPs, and SCs;
- appointing TC and EP Chairmen;
- standstill;
- resolving drafting problems;
- standardisation policy and performance;
- communication;

- resource framework for Technical Organisation;
- overseeing Technical Organisation;
- external relations;
- Technical Working Procedures (TWP); and
- disputes/appeals/complaints.

Technical work is organised in different groups:

- Special Committees (SC);
- Industry Specification Groups (ISG);
- Technical Committees (TC);
- ETSI Projects; and
- ETSI Partnership Projects.

It is worthwhile nothing that ETSI deals not only with the creation of official standards but also with providing widely accepted specifications for industrial products. The latter is the target of ISGs. A full list of active groups is available at https://www.etsi.org/committees.

In general, consensus is the preferred method for decisions within ETSI. However, when consensus cannot be reached, then voting procedures apply.

3.2.1.3.1 Voting rules

Two types of voting procedures exist.

- Weighted Individual Voting, where votes are cast by individual member organisations; and
- Weighted National Voting, where votes are cast by Head of National Delegation or National Standards Authority.

Vote weight is in accordance with the member's Units of Contribution (which is related to the annual association fee).

In Individual Voting, votes are cast by individual members. This procedure is used for:

- voting in a technical board
- approval of ETSI Standards and ETSI Guides
- election of officials to General Assembly
- election of Board members and Board Chairman
- selection of Director-General
- matters relating to the European Union (Full Members only)

A majority of 71% of cast votes is required (so to mimic wide consensus), for the validity of the vote a 50% quorum is required in the GA while there is no quorum in all other bodies.

In National Voting, a vote is cast by each Head of National Delegation (of course considering the views of national members). This procedure is used for:

- NSO Approval of ENs
- GA voting on changes to Statutes and Rules of Procedure
- GA voting on establishment of national weightings

National Voting is not available to countries of Associate Members but only to countries having a Full Member in the Administration, Other Governmental Bodies, or National Standards Organisations category which contributes to ETSI according to the country's Gross Domestic Product (GDP).

3.2.1.3.2 Commenting Procedures on Open Projects

Depending on the type of standard, different procedures for comments exist.

Technical Specifications (TS), Technical Reports (TR), Group Specifications (GS), Group Reports (GR) and Special Reports (SR) are not open for public comments. They are approved directly by the group that creates them (may be a Technical Committee or an Industry Specification Group).

ETSI Guides (EG) and ETSI Standards (ES) are drafted by a Technical Committee and then submitted for approval by the full ETSI membership. If the vote is successful, the ETSI Secretariat publishes the standard; if not, it is returned to the committee.

Most European Standards (EN) follow a procedure which comprises a Public Enquiry and a weighted national Vote. Once the Technical Committee has approved the draft, the ETSI Secretariat makes the document available to the NSOs, that carry out the Public Enquiry (which involves the national stakeholders) and then submit the national position on the standard. If the vote by the NSOs is successful, and if no substantial comments are received, the ETSI Secretariat finalises the draft and publishes the standard. Any technical comments received during Public Enquiry are considered by the Technical Committee, which may revise the draft and resubmit it to the Secretariat. If there are significant changes, the Secretariat may initiate another Public Enquiry; otherwise, the draft will be presented directly to a second vote. After a successful vote, the Secretariat publishes the standard.

3.2.1.4 Maturity of Procedures

ETSI does not have a specific procedure to assess the maturity of its procedures but the members may raise proposals for improvement.

3.2.1.5 Stability of Procedures

ETSI procedures are rather stable, as they have demonstrated to work well for several years. ETSI procedures are summarised at (ETSI, 2021).

3.2.1.6 Effectiveness and Relevance

ETSI has developed some very important standards, not only in the telecommunications area but also in the Digital Single Market: the standards about electronic signatures are a cornerstone of the EC regulations and have been widely adopted at national level.

Moreover, ETSI is also exploring and paving the way in several innovative areas: to cite a few, there are currently very active industrial standardisation groups related to NFV (Network Functions Virtualisation) and QKD (Quantum Key Distribution), that are hot topics nowadays.
The relevance of ETSI is also related to its bottom-up approach, where industries propose standardisation topics that are important for interoperability between different companies.

3.2.1.7 Coherence

ETSI has liaisons with several NSOs (National Standards Organisations) also outside the EU (a complete list is at https://www.etsi.org/about/our-partnerships). Additionally, ETSI has various forms of partnership with international and national organisations, fora and consortia. The work with partners can range from an informal exchange of information, to development of joint specifications and full cooperation. ETSI has developed different partnership models to meet the different needs of its committees and partners. Namely, ETSI has three different types of partnership agreement: Letter of Intent (LoI), Memorandum of Understanding (MoU), and Cooperation Agreement (CA), with increasing level of coordination. The complete list of partnership agreements is available at the following page: https://portal.etsi.org/webapp/AgreementView/AgreementSearch.asp (at the time of writing, there are 102 active agreements with external bodies across the world).

3.2.1.8 Development Dimension

While ETSI has no specific policy to support the involvement of developing countries, it does not put any obstacle towards their participation. This is demonstrated by the collaboration with some Asian partners, such as APKIC (Asia PKI Consortium) and EASC (Euro-Asian Council for Standardisation, Metrology and Certification).

3.2.2 OASIS

OASIS Open is a global, non-profit standards body founded in 1993 and now supported by organisations from around the world. The consortium behind OASIS works towards the development of open-source software and standards in very diverse ICT areas including cybersecurity, blockchain, cloud computing and IoT, among others.

3.2.2.1 Openness

The OASIS consortium is open to organisations and individuals from all over the world. To participate in technical committees, it necessary to become a member. OASIS offers three membership categories, which vary depending on the benefits offered to the organisations (Open, 2021). These categories are as follows:

- Contributor: provides unlimited participation in technical committees. Particularly suited for small government agencies, academic institutions, and non-profit associations.
- Sponsor: similar to the contributor membership but with additional visibility and marketing benefits.
- Foundational sponsor: receive maximum participation, visibility, and promotional benefits.

There is also an annual due associated with each membership category and the pricing depends on the type of organisation and the number of employees in the organisation. The annual dues in USD are presented in the table below:

Organisation type / size	Foundational	Sponsor	Contributor
Company employing more than 500 people	57.000	21.000	10.500
Company employing 100 – 500 people	55.000	18.000	9.700
Company employing 10 – 99 people	52.000	15.500	8.500
Company employing fewer than 10 employees	50.000	7.500	4.100
Academic Institution or Association	50.000	13.000	1.450
National government agency (OECD country)	50.000	13.000	(*[1])
National government agency (non-OECD country)	50.000	13.000	1.450
Local government agency	50.000	13.000	1.450

Table 1: Annual dues (in USD) for OASIS organisations (OASIS, 2021).

In addition to organisation membership, OASIS offers personal memberships. There are two types of personal memberships:

- Individual: for self-employed or unemployed individuals

[1] The annual due depends on the number of employees of the agency and correspond to the fees for companies.

- Individual/Associate: for individuals employed by organisations willing to sign the OASIS membership agreement and be bound by the policies of OASIS and no other employee participates in OASIS.

The benefits associated with these types of memberships are limited to participation in technical committees. There is also a cost associated with these memberships, which are 380 USD and 1,600 USD, per annum, respectively.

To join OASIS as an organisation, it is necessary to sign and submit the membership agreement. Personal members need to sign and submit an individual/associate membership agreement.

OASIS supports four types of open collaboration projects:

- Technical committees (TC): OASIS members collaborate towards the development of standard specifications that can later be approved and published by other SDOs like ISO, IEC, or ITU.
- Open projects (OP): provides support to open-source communities and is open to anyone without fees. The work is funded by organisations interested in the outputs of the project which contribute an annual sponsorship due depending on the size and type of the organisation, ranging from 25000 USD for big companies to 1000 USD for universities, non-profit and local or non-OECD governments.
- Foundation-as-a-service: groups that use their own processes and receive financial and legal support from OASIS.
- Technical advisory groups (TAG): represent the interests of American organisations and enable the US to have a voice in the global standards produced by ISO.

In addition to these types of projects, OASIS also considers the creation of member sections, which are groups that advances the interests of a specific community or technology. In member sections organisations or initiatives external to OASIS can be part of OASIS, while maintaining their identity and governance.

Most of the projects available under OASIS are TCs. Any work produced by these committees can be searched for and accessed by anyone, not only OASIS members, via (committee, 2021). In addition to the standard specification documents produced by the TC, which can be also searched for via (standards, 2021). There is other relevant information open to anyone: the list of members and their role in the TC, the emails exchanged by members of the TC, the e-mails received from external entities to the comments mailing list, the meeting minutes and ballots results. This principle of transparency is for all committees and subcommittees as stated in section 1.5 of the OASIS Committee Operations Process (operations, 2021).

All things considered, OASIS can be regarded as an open and fully transparent SDO where not only members can access standard specification documents produced by TC and they provide a simple mechanism for commenting on ongoing projects. Finally, meetings are only open to members but meeting minutes are typically shared as public documents by TCs.

3.2.2.2 Impact

OASIS is a global consortium with over 600 organisations and individual members in more than 60 countries. Among its members there are multinational companies such as IBM, Adobe Systems, Oracle and Microsoft, as well as organisations such as the US Department of Defence, US NIST and the European Union Publications Office, and also universities and research institutions.

According to the 2020 annual report, OASIS has a total of 59 active technical committees and 4 open projects. A total of 171 OASIS standards have been produced so far, some of which have been approved as international standards due to their formal working relationships and liaisons with other standards

organisations like ISO. OASIS has participated in the development of some standards widely used throughout the world. For example, some influencing standards in the scope of information security developed or participated by OASIS include:

- eXtensible Access Control Markup Language (XACML) for representing and evaluating access control policies;
- Web Services Security (WSS) for implementing security functions in messages implementing web services applications;
- Security Assertion Markup Language (SAML) for creating and exchanging security information between online partners; and
- PKCS #11 for the creation and manipulation of cryptographic tokens. OASIS continues to work on enhancing the standard which was originally created by RSA Security.

Moreover, OASIS has different types of liaisons with many organisations around the world, both public and private, involving many different sectors.

3.2.2.3 Governance

3.2.2.3.1 Organisational Structure

The technical work in OASIS is done through three types of committees, each of which has its own internal structure, and its member may pose different roles.

The technical committee roles are the following:

- Observer can attend to meetings and receive mails from the TC list but cannot participate of discussions, contribute to specifications or cast votes;
- Member can attend to meetings, participate of discussions and contribute to documents but cannot vote until some requirements are met;
- Voting members are TC members who have attended at least two consecutive TC meetings. Note that voting members can also lose their voting right if they miss two consecutive TC meetings; and
- Persistent non-voting members are TC members or voting members who do not wish to participate in ballots, make or second motions, or count for the purposes of calculating quorum (needed persons for decisions to be made).

The open projects roles are the following:

- Participant is any person or entity (not necessarily an OASIS member) that may provide comments on the project and report bugs on the code;
- Contributor is any person or entity (not necessarily an OASIS member) that in addition to providing comments and reporting bugs can submit pull requests to repository holding the code;
- Maintainer is a person (not necessarily an OASIS member) that serves as the principal editor of the project repository. The person with this role is decided by the project governing board; and
- Project governing board (PGB) is the entity in charge of guiding the project. It is composed of one member from each project sponsor and at least one expert representative from the community of contributors. The PGB can decide to create a technical steering committee.
- Chair is a member of the PGB that coordinates and manages project decision-making and logistics.

The member sections roles are the following:

- Steering committee which consists of members of OASIS elected to provide leadership and advance the mission of member section;
- Affiliated members are members who choose to affiliate with the member section;
- Participants are the persons who ultimately represent the affiliated members; and

- Affiliated technical committees are OASIS TCs interested in the work of the member section. Note that a TC cannot be affiliate with more than one member section.

Technical committees may have subcommittees (SC), which are aimed at producing recommendations on a specific topic for consideration by the parent TC. Similarly, member sections can create one or more subcommittees.

A summary table presenting the benefits and functions of TC and OP roles can be obtained from the OASIS Committee Operations Process (open, 2021).

3.2.2.3.2 Voting Rules

General voting rules for members of OASIS Committees are specified in the OASIS Committee Operations Process (open, 2021).

Whenever a committee needs to make a resolution, it is necessary to have a quorum (i.e., more than half of the members with voting rights) present. Typically, a simple majority vote (i.e., more votes in favour than against) is sufficient to make a decision. However, there may be some decisions in the committee that require a different voting scheme. For example, electing the chair of a committee or closing the committee requires a full majority vote (i.e., at least half of the members with the right to vote must agree) unless otherwise stated in the rules and policies of that specific type of committee.

Moreover, some committees may have special voting conditions or different voting rules. As mentioned above, in technical committees, members first need to obtain voting rights by attending two consecutive meetings (i.e., become a voting member) before they can participate in the decisions of the committee by casting a vote. Note that TC membership is per person and not per organisation. A voting member of a TC has a single vote. Organisations do not vote in TCs.

Individuals with personal memberships are not eligible to vote on OASIS Standards (Vote, 2021) .

3.2.2.3.3 Commenting Procedures on Open Projects

An OASIS specification must go through several steps before it is approved as an OASIS standard. After the submission of the specification for consideration it must complete a public review process.

During the public review process, the OASIS specification can be announced to different mailing lists, including the OASIS mailing list, to receive comments. Comments from outside the OASIS consortium must be sent via the archived public comment facility of the TC. Comments from OASIS members must be made to the TC general mailing list.

The TC must acknowledge the receipt of each comment and, at the end of the public review period which should be at least 60 days, it must publish a response to them in TC mailing list.

In case no comments are received or no changes are deemed necessary the specification can continue its standardisation process. If by full majority vote it is agreed that changes are needed, then the specification must be withdrawn to prepare a revised version.

3.2.2.4 Maturity of Procedures

OASIS provides a set of editorial resources and documentation for ensuring and verifying the quality and conformance of the specifications developed by OASIS members. These are accessible via (MBR, 2021)

and include checklists for verifying the editorial quality of the specifications, guidelines on the use of keywords or the writing of conformance clauses, and so on.

3.2.2.5 Stability of Procedures

OASIS offers a quick-reference guide for its members called the OASIS TC Handbook (Handbook, 2010). This guide is intended to provide a single resource to answer questions related to technical committees. The intended audience for this handbook is new members but also TC chairs and anyone in between.

Also, the TC process is publicly available in the OASIS website (TC, 2020) where a list of historical revisions of this policy. Since 2000, at the time of writing there have been 20 revisions of this policy, with the last one being carried out in July 2020.

3.2.2.6 Effectiveness and Relevance

OASIS Open includes among its members multinational companies, public organisations as well as universities and research institutions. OASIS members have developed some widely-used standards mostly driven by market needs.

As a matter of fact, Article 2 of OASIS Bylaws (Bylaws, 2020) states that one of the primary objectives of the organisation is "to provide an open venue to discuss market needs and directions, and to develop and refine information technology standards, specifications, code, policies, and methodologies".

3.2.2.7 Coherence

OASIS has different types of liaisons with governmental agencies, regional and international SDOs, and organisations from the health, energy and financial sectors. Among others, OASIS has established formal liaisons with ANSI, IEC, ISO, and ISO/IEC JTC 1. Current liaisons can be found at (LSN, 2021).

The liaison policy describes the process for establishing liaisons at an organisational level or at the technical committee level, as well as the policy for submitting OASIS standards for adoption by other SDOs. A special liaison policy is also in place for technical committees considering to submit their work as an American National Standard to ANSI.

Moreover, in 2020 OASIS Open launched the OASIS Open Europe Foundation (FDN, 2020) to serve as a collaboration point with European open-source projects and standards. More precisely, this sister organisation is aimed to participate in collaborative projects supported by the EU, organise events that promote open technologies, engage in and support European communities working to progress open-source and open standards, and offer educational, research and promotion services. However, at the time of writing there is still not much information on their website.

3.2.2.8 Development Dimension

Among OASIS members there are organisations from 60 different countries from all over the world, including developing countries (UN, 2021) in different continents such as Ghana, Egypt, Kenya and Uganda in Africa; Afghanistan, China, India, Malaysia, and Philippines in Asia; Jamaica, Mexico, Peru, Colombia, and Brazil in the Americas. A few of these countries are even included in the list of least developed countries released by the United Nations Conference on Trade and Development (UNCTAD).

We are not aware of any directives aimed at encouraging the participation of organisations or individual members from developing countries. There is, however, a distinction in the annual dues for national government agencies willing to become a contributor member. As shown in Table 1 from Section 3.3.2.1, national government agencies from a non-OECD country (OECD, 2020) participating as contributor

members will pay the lowest annual due (USD 1.450), while those from OECD countries pay an annual due which depends on the number of employees of the agency. The due in this case ranges from USD 4.100 to USD 10.500.

3.2.3 HL7

Created in 1987, HL7 (Health Level Seven International) works toward improving the electronic collection and exchange of healthcare data to improve the speed, quality, safety and cost of patient care. It is a not-for-profit organisation, which is a member-driven community. It is an American National Standards Institute (ANSI)-accredited Standards Developing Organisation. Health professionals and subject matter experts are working together to develop IT standards that help healthcare organisations reduce healthcare costs, streamline processes, lower development costs, and improve patient care.

HL7 has collaboration agreements with ISO/IEC, CEN/CENELEC. The HL7 model uses working groups (WG) of volunteers from around the world to develop the standards that are then balloted and voted on. There are nearly 40 WGs. HL7 V2, V3, HL7 CDA and HL7 FHIR (Fast Healthcare Interoperability Resources). FHIR (an API based standard) was introduced May 2012. A person can get involved via work groups, by becoming a voting member, taking part in connectathons or Developer Days.

HL7 is supported by members from over 50 countries, including over 500 corporate members representing healthcare providers, government stakeholders, payers, pharmaceutical companies, vendors/suppliers and consulting firms.

3.2.3.1 Openness

HL7 membership is meant for healthcare providers, government stakeholders, payers, pharmaceutical companies, vendors/suppliers, and consulting firms. The membership levels are the following.

1. Benefactor Membership. This is the highest level of membership, including the maximum number of voting members, greatest training discounts, and enhanced recognition for the organisation.
2. Gold Membership. This level offers additional benefits such as discounted training and increased access to HL7 experts.
3. Organisational Membership. This level offers the standard benefits of HL7 membership.
4. Individual Membership. This is meant for individuals who want to be involved with HL7 but whose organisations do not have a membership. There is also a student membership available for those who qualify.

There is a fairly complicated pricing scheme for each tier based on organisational revenue and category (state, local, federal, academic, professional). Details about the different membership levels and pricing can be accessed from the HL7 membership web page (HL7, 2022).

For the benefactor level, the prices range from $16,000 to $37,000 USD per year based on the annual (healthcare) revenue. For academic institutions, it is $16,000 USD per year.

For the gold level, the prices range from $1,850 to $28,400 USD per year based on the annual (healthcare) revenue. For academic institutions, it is $1,850 USD per year.

For the organisational level, the prices range from $1,500 to $23,000 USD per year based on the annual (healthcare) revenue. For academic institutions, it is $1,500 USD per year.

Individual membership is meant for people with a personal interest in the standards and the price is $775 USD per year.

HL7 is global, taking input from volunteers and members in over 50 countries across the world and have an official presence or affiliate in more than 30 countries.

They are geared towards interoperability of health data, so their standards and implementation guides are free of charge for everyone.

3.2.3.2 Impact

There are HL7 standards referenced in US Regulations, ANSI approved standards and ISO approved standards. HL7 standards are the most used health standards internationally. The FHIR standard (Fast Health Interop Resources) (FHIR, 2019)“is an interoperability standard intended to facilitate the exchange of healthcare information between healthcare providers, patients, caregivers, payers, researchers, and anyone else involved in the healthcare ecosystem. It consists of 2 main parts – a content model in the form of ‘resources’, and a specification for the exchange of these resources in the form of real-time RESTful interfaces as well as messaging and Documents”.

The FHIR standard is available free of charge at (Release4, 2019) The Copyright © 2011+ HL7, but is licensed under Creative Commons "No Rights Reserved" (CC0).

An Affiliate is an independent legal entity that represents its country and country affiliate members at HL7 International meetings and within its country/territory on HL7 matters. They participate in the standards development and governance processes, promote the relevance and fitness HL7 standards and procedures in its country/territory, distribute, translate and localise the HL7 Protocol Specifications as appropriate, administer HL7 Certification tests when suitable and promotes HL7 standards, educates, informs and supports current and potential users to promote consistent and widespread usage of the standards.

The current affiliates (February 2022) are Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, Hong Kong, India, Italy, Japan, Mexico, the Netherlands, New Zealand, Norway, Pakistan, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, United Arab Emirates, United Kingdom, the Ukraine. The current list of affiliates can be seen at (Leadership, 2022).

3.2.3.3 Governance

3.2.3.3.1 Organisational Structure

Figure 3 illustrates the detailed governance structure of HL7.

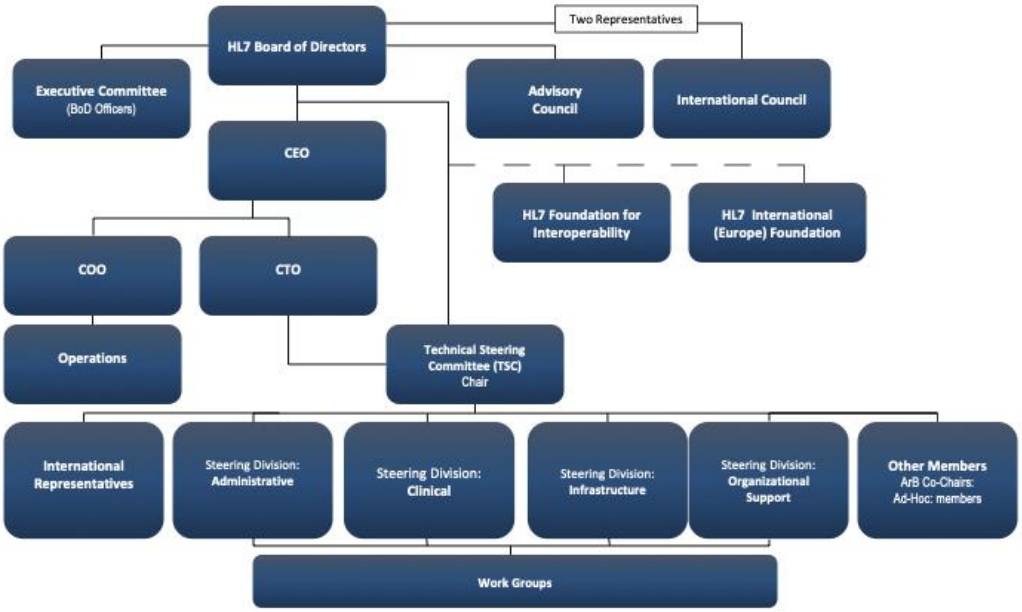

Figure 3: Governance structure of HL7 (Chart, 2022)

Health Level Seven members are organised into work groups and work groups are organised into steering divisions. HL7 members are encouraged to participate in all work groups in which they have an interest. Work groups are responsible for defining and developing the HL7 standards applicable to their domain. Each work group is chaired by two or more co-chairs.

There are currently around 50 working groups. WG meetings occur three times a year (one plenary). WGs have defined decision making processes that specify how they run meetings, debate and vote on issues.

The technical steering committee (TSC) provides technical direction to the HL7 organisation, oversees and coordinates the technical efforts contributed by the HL7 participants to ensure that the efforts of the working groups are focused on the overall mission.

3.2.3.3.2 FHIR

The TSC FHIR Management Group (FMG) provides day-to-day oversight of FHIR-related work group activities including performing quality analysis, monitoring scope and consistency with FHIR principles and aiding in the resolution of FHIR-related intra and inter-work group issues.

The FMG focusses on enabling that

- FHIR development is coordinated and consistent across the organisation;
- work groups have timely feedback and guidance and their development products are aligned with the broader goals of HL7 and its constituent communities;
- work groups act in a coordinated manner with quick resolution of disputes;
- work groups understand what is expected of them and have the breadth of domain knowledge, skills and tools necessary to perform their work.

The FMG, through its structure, processes and activities will make sure that

- the work group solutions do not diverge in resource and profile development;
- the work groups coordinate development activities as they should;
- the tools meet requirements of development;
- the development space is used correctly;
- the ballot processes meet the needs of work groups and/or community;
- the stakeholders are sure how to engage with the organisation; and
- the work groups are able to balance workload of FHIR and other activities.

3.2.3.3.3 Voting Rules

HL7 is a consensus driven SDO. As such, they are volunteer-driven, have uneven levels of participation with the commitment of most volunteers not being full-time. The projects are balloted with required resolution of negative ballots. Consensus standards are intended to meet the needs of the many and are prone to compromise.

A user signs up to participate in a specific ballot on a specification. There may be a cost associated with this if the user is not an HL7 member. A specification is subjected to review during a scheduled time window. Reviewers who have registered for the ballot can submit comments about the specification (raising issues and proposing changes). They also cast an overall vote indicating whether they believe the specification should be published in its current form. The relevant Work Group(s) then review the comments and address them through a process called reconciliation. Based on the response of the Work Group(s), the ballotter may choose to adjust their vote by withdrawing negative votes. The final determination of whether the specification can proceed to publication as a 'standard' is driven by the balance of affirmative votes received and varies depending on the type of ballot.

HL7 specifications can be balloted at one of four levels:

- For Comment ballots are used early in the development cycle to get feedback from the community. These ballots are meant to get guidance from the community outside those developing the specification. These never lead to the publication of the specification. This ballot is informative and does not end in a pass or fail.
- Informative ballots are used for content that is not intended to be binding on implementers. It is often used for specifications that guide internal HL7 processes or that give non-binding recommendations to the implementers. The result is non-binding.
- Standard for Trial Use (STU) ballots are used for content that is eventually intended to be binding on implementers. These ballots are conducted for content that is deemed ready to implement by the sponsoring work group, but where there has not yet been significant implementation experience. STU specifications are time-limited and give an opportunity for the community to exercise the specification in real-world implementation before the specification is locked down. STU specifications are also non-binding.
- Normative ballots are used for final review of specifications that are intended to be binding on the implementer community. The specifications that result from this process are considered authoritative. It is common for specifications to undergo multiple cycles before the community is satisfied and the specification can be published as an official standard.

3.2.3.4 Maturity of Procedures

As the organisation has been around since 1987 and their most widely-used standard (FHIR) was created in 2012, it is possible to say that the procedures are mature. The organisation seems active and meetings are taking place.

The current governance and operations manual was adopted in 2021. The working group decision making practices document is on version 5.2.1 and was adopted in 2019.

3.2.3.5 Stability of Procedures

As can be seen from the previous subsection, the procedures seem to be fairly stable. The HL7 electronic ballot charts (an appendix to the co-chair handbook) is from 2009 and the current WG decision making practices document was adopted in 2019.

3.2.3.6 Effectiveness and Relevance

The FHIR standard is widely used for communicating medical information between various information systems and is a cornerstone for implementing electronic health records worldwide (Noumeir, 2019). Mission: To provide standards that empower global health data interoperability. Vision: A world in which everyone can securely access and use the right health data when and where they need it.

The HL7 international strategic plan approved by the board of directors on September 17, 2019 states the following core strategic goals (Plan, 2019):

1. Establish HL7 FHIR as the primary standard for global health data interoperability.
2. Enhance and maintain quality of and accessibility to HL7 standards in current use.

3.2.3.7 Coherence

HL7 has liaison relationships with several different standardisation organisations, including CEN/TC 251, ISO and OASIS.

3.2.3.8 Development Dimension

HL7 had an International Mentoring Committee. It was established in order to formalise some of the pre-existing affiliate efforts to support fledgling HL7 affiliate chapters. It was moved to be a subcommittee of the International Council in 2018/2019 (WG, 2018). The mission of this council is to support the HL7 mission to create and promote its standards by helping to assure that the needs, issues and other input of the HL7 International Affiliates are recognised and effectively acted on by the HL7 organisation. The final project the International Mentoring Committee listed is the African Participation Outreach project. The objective of this project was to establish formal channels of communication and outreach to regions of the African continent with the end goal of raising awareness of HL7, increasing the use of HL7 on the continent, and eventually establishing HL7 affiliate organisations in Africa. This was moved to the International Council. It had an end date in May 2020 but is currently listed as awaiting approval.

3.3 National Standardisation Bodies

3.3.1 BSI

Federal Office for Information Security (Martin Schallbruch, 2018) (Bundesamt für Sicherheit in der Informationstechnik, BSI) is German federal agency responsible for the management of computer and communication security for the German government. The BSI is involved in the certification process according to the international Common Criteria, ITSEC and domestic Green book (IT-Grundschutzhandbuch), corresponding standardisation procedures (e.g., involvement in the ISO/IEC 15408/18045 Common criteria and evaluation methods and ISO/IEC 2700x information security standards series) as well as practical technical recommendations for IT security (e.g., BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths). Additionally, the BSI-produced Application Notes and

Interpretation of the Scheme (AIS) documents provide technical guidelines for the implementation of ITSEC and Common Criteria requirements.

3.3.1.1 Openness

Openness to the public
The BSI is a German federal agency and as such, it is not open for outside membership. The BSI-published standardisation documents are openly available on the BSI website free of charge. The documents are typically published both in German and English language. The documents, guidelines and recommendations (especially IT Baseline Protection Catalog) are created together with invited experts and open for public comments.

Access to meetings
BSI meetings are usually with restricted access to the agency employees and invited experts. There are no membership fees or tiers.

3.3.1.1.1 Commenting Procedures on Open Projects
The ongoing open projects are open for public comments. BSI documents to be included in IT-Grundschutz are first produced in the form of community drafts, which can be commented on for a period of four weeks or more. The public comments are checked by BSI and incorporated in the next version of the IT-Grundschutz (BSI, 2019).

3.3.1.2 Impact

The German BSI has significant impact at organisational, national as well as on the EU level.
The BSI standards and technical guidelines are primarily intended for national use by national agencies, organisations, manufacturers, distributors, and end-users in Germany.

BSI maintains IT-Grundschutz (baseline protection) catalogue of procedures for management system for information security (ISMS) based on the BSI-produced standards: BSI Standard 200-1 (general requirements for an ISMS), BSI Standard 200-2 (how to build ISMS based on one of three different approaches – basic, core and standard), BSI Standard 200-3 (all risk-related tasks) and BSI Standard 100-4 (covering Business Continuity Management). The older version of the IT-Grundschutz standard is available as BSI-Standard 100-x documents (Grundschutz, 2021). The certification based on the BSI baseline protection (IT-Grundschutz) is required for all organisations with customers in the public or legal sectors in Germany, resulting in wider impact of this set of documents.

The technical guidelines cover range of topics including certification, Common Criteria, Critical infrastructure, Cloud computing, IT crisis management, cryptography and electronic identity documents and are available in German and English language.

3.3.1.2.1 Organisations
The production of technical reports with minimum standards and recommendations influences the IT security handling in organisations in DACH countries via standards like IT-Grundschutz.

3.3.1.2.2 National
As the BSI is responsible for protection of federal government IT systems and is member of Accredited Common Criteria Recognition Arrangement (CCRA), its standardisation documents (BSI Standards 200-x within IT-Grundschutz) and recommendations are required for products eligible for use by German government.

3.3.1.2.3 EU Levels

The BSI is the one of the biggest producers of the certificates issued under Common Criteria scheme (together with France, US and recently Netherlands) within the Accredited Common Criteria Recognition Arrangement (CCRA). As a result, the IT security products certified by the BSI or BSI-accredited laboratories are influenced by the requirements and standards of the German government. This is especially true for the products with higher EAL levels than EAL4. The products are mutually recognised between EU countries only up to EAL4, but BSI-issued certificates are typically recognised also for the higher levels.

3.3.1.3 Governance

3.3.1.3.1 Organisational Structure

As a national body, the BSI's organisational structure is consisting of eight main divisions: Division Z (Central Tasks), Division TK (Technical Centres of Excellence), Division KM (Information Assurance Technology and IT Management), Division OC (Operational Cyber Security), Division SZ (St andardisation, Certification and Cybersecurity of Telecommunication Network), Division DI (Cyber Security for Digitisation and Electronic Identities), Division BL (Consulting for Federal, State and Local Governments) and Division WG (Cyber Security for the Private Sector and Society). Out of these, Division SZ and especially its Section SZ 13 (BSI Standards and IT-Grundschutz) are the most relevant for the standardisation process. The whole organisational structure as of 2020 is available on BSI website (BSI, 2020).

3.3.1.3.2 Voting Rules

As the BSI is a federal agency and not a consortium of independent members, there are no membership tiers or fees to participate. The voting rules are not published, decisions relevant to the prepared documents are made according to the internal agency rules.

3.3.1.3.3 Commenting Procedures on Open Projects

The public can comment on the open projects and resulting artifacts. Community drafts are open for comments for four weeks, other documents are open for variable commenting period, typically up to several months. The comments are processed by BSI employees and potentially included.

3.3.1.4 Maturity of Procedures

In the BSI organisational structure, there is Section SZ 14 (Expert Committee Work and Quality Management for Evaluation and Certification Processes)

3.3.1.5 Stability of Procedures

The BSI baseline catalogue (IT-Grundschutz) has been continuously developed for more than two decades now. While continuously evolving in the topics covered, the basic goals are stable, including community participation. The security certifications done by BSI according to Common Criteria scheme can be also considered stable as these need to synchronise with the wider Common Criteria procedures.

3.3.1.6 Effectiveness and Relevance

BSI standards are periodically maintained and updated. The BSI baseline catalogue (IT-Grundschutz) was lastly updated in February 2021, suite of BSI 200-x standards in year 2018. Selected BSI standards and guidelines are mandatory in Germany and actively used by the market participants primarily in DACH countries. BSI standards are thus both effective and relevenat.

3.3.1.7 Coherence

BSI standardisation documents are published either as or adapted from ISO/IEC standards (BSI 200-x standards) or as implementation guidance documents (AIS). The BSI 200-x standards specifically discuss the coherence to and differences to existing other standards, e.g., interaction between BSI 200-2 and ISO/IEC 27001 standard or BSI 200-3 vs. ISO/IEC 31000 standard. The BSI standards also explicitly mention the adaptation to changes made in ISO/IEC standards (e.g., adaptations of BSI 200-1 to updated ISO 27001 standard). Public review and commenting period can be also used to improve a coherence for the proposed standardisation document.

3.3.1.8 Development Dimension

As primarily national security advisory body, BSI is not primarily focused on encouraging the developing countries to participate.

3.3.2 UNE

UNE is a private, non-profit organisation recognised by the Spanish Public Administration as the National Standardisation Body in Spain. UNE is involved in the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), the European Telecommunications Standards Institute (ETSI), the Pan American Commission of Technical Standards (COPANT), as well as in the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU).

3.3.2.1 Openness

Any entity be it a natural or legal person, public or private, interested in standardisation can become a member of UNE. Currently, UNE is made up of more than 500 members with representatives of practically all the academic and business tissue in Spain. The members of UNE can be classified into:

- Honorary members: are designated by the General Assembly in recognition of outstanding services in the fulfilment of the aims of the Association;
- Corporate members: are professional business organisations representing the economic and industrial sectors, as well as state-level consumer and user associations;
- Affiliated members: are legal entities not recognised as corporate members. In particular, this category includes representatives of the Public Administrations that the current legislation establishes must be incorporated; and
- Individual members: are physical persons not being recognised in any of the previous groups.

To become a member - with the exception of honorary members - the person or entity must request it to the Board of Directors through a registration form, which implies the full acceptance of the Association Statutes and the Internal Regulations. If the request for admission is eligible, it will be provisionally approved by the Board of Directors, and finally ratified by the General Assembly.

Becoming a member of UNE implies the payment of annual dues, which are revised yearly and are subject to the budget of the association and the coefficient assigned to each member. For corporate members coefficients range from 8 to 1, for attached members they range from 1 to 0.2, and for individual members the coefficient is exactly 0.05. The annual dues result from multiplying a base due by the coefficient that corresponds to each member.

Among the benefits of being a member of UNE is to participate in the decisions of the association and contribute to its strategic lines, exercising the right to vote, as well as to attend the General Assembly and

participate of its Governing Bodies. Corporate and attached members can participate in the secretariats of the Normalisation Technical Committee (CTN) leading the work in these committees.

However, being a member is not a condition to participate in CTNs. Any entity with interest in the standardisation activities being performed within a given CTN can participate after submitting the form (Form, 2021) for entities; (Form2, 2021) for individuals). Typically, participation is subject to a fee that ranges between 500€ and 700€. This is the case for most corporate members and universities with the exception of SMEs, which pay a reduced fee (70% of the base fee), and business associations, for which the fee is higher, around 1200€. This amount is to be paid for each of the CTNs where the entity participates. UNE members are not required to pay CTN fees. Also, some particular CTNs have special access conditions. For example, universities are not required to pay a fee to participate in CTN 320, which is the CTN devoted to Cybersecurity and Personal Data Protection.

Only the members of a CTN may participate in the meetings. Exceptionally, other representatives may participate to a meeting, but this must be informed on time to the Secretariat. Also, the President may invite as observers, with voice but without vote, to entities that are considered relevant to some of the issues in the agenda of a particular session. Moreover, the Board of Directors may designate a person to attend certain meetings of the CTN.

The proposal for new standards within UNE is open to any entity. UNE provides an online form that can be used to propose a new standard at the national level. The form is very simple and consists of the very few short questions regarding the scope of the proposal, the motivation, possible applications and market of the future standard, etc. With the information provided in the form, UNE evaluates the proposal and decides whether a new project is established.

Both ongoing projects and standards can be searched for by anyone via (UNE, 2021) but for purchases one is redirected to AENOR's website.

UNE is also involved in offering courses and training in standardisation matters for its associated members and universities. Since 2016, free online webinars for professionals involved in technical standardisation committees. These webinars were initially intended only for people with management roles in the committees but now is open to other committee members. The topics covered in these webinars are aimed at helping committee members to get the grips of the association and make the most out of it. Past recorded webinars are also available to committee members.

Occasionally, UNE organises events to promote and publicise the work carried out by the association and the CTNs. These events are open and free to register. Moreover, UNE publishes a monthly magazine which is also freely accessible online (ENERO, 2022).

3.3.2.2 Impact

UNE is the official Spanish Standardisation Body recognised by the Spanish Public Administration and is involved in European (CEN, CENELEC) and international (ISO, IEC) organisations. UNE establishes the national position during the development of international standards and approves which members of a CTN can apply to participate in the meetings of the European and international bodies.

In its last annual report UNE states that 85% of the standards available have a European or international origin. Although this is the normal flow of standards, it is also possible that standards developed at the national level are raised for consideration to European or international standardisation bodies.

According to UNE, around 12% of the technical standards in their catalogue are cited in Spanish legislation thereby notably impacting organisations at the national level. For those members involved in the development of these standards, the support of legislation on them helps them to reduce the cost associated with their compliance and since most of the standards are adapted from European and international bodies, they can more easily reach markets outside Spain.

Also, since UNE participates in the Pan American Standards Commission (COPANT) it is one of the main entry points of international standards to Spanish-speaking countries in Latin America. UNE has 14 agreements in force with the standardisation bodies of Latin American countries.

3.3.2.3 Governance

3.3.2.3.1 Organisational structure

UNE is governed by the General Assembly, the Board of Directors, the Permanent Commission, and the President of the Association.

The standardisation activities carried out by UNE are developed through the National Technical Committees (CTNs). CTNs are comprised of a Chairperson, a Vice-chairperson – if deemed necessary, a Secretary and Committe members. Committee members act in representation of manufactures, services providers, administration, universities, and research centres, among others. The composition of CTNs aims for a balanced representation of all stakeholders involved in the field of activity of the CTN (UNE20RCT, 2020).

At the time of writing, there are over 200 committees, each of which have a different field of activity, relationships with other European and international bodies, and internal structure. CTNs can be divided into subcommittees (SC) and working groups (GT). Note that GT can hang directly from a CTN or a SC. At the proposal of UNE's technical services or one of its members, it may be possible to create Temporary Specific Groups (GET) in areas where the creation of a CTN is not advisable.

The technical committee devoted to Cybersecurity and Personal Data Protection is CTN320 (UNE320, 2020). Internally, this CTN is divided into six subcommittees:

- SC 1: Cybersecurity management systems;
- SC 2: Cryptography and security mechanisms;
- SC 3: Security assessment, testing and specifications;
- SC 4: Security controls and services;
- SC 5: Data protection, privacy, and identity management; and
- SC 6: Product security.

This CTN is the Spanish mirror of other European and international bodies and it is thus in line with their internal structure. In particular, there is a mapping with ISO/IEC/JTC1/SC 27 and ISO/PC 317 at the international level and CEN/CLC/JTC 13 at European level.

3.3.2.3.2 Voting Rules

As previously mentioned, each UNE member is assigned a coefficient which is basically determined by their turnover and in essence determine their annual dues and their voting rights. These voting rights are can be exercised for decisions regarding the governance of the Association.

The agreements of the CTN, which are fundamental for the creation of standards, will preferably be adopted by consensus. However, if voting is necessary, resolutions will be adopted by a simple majority of the votes present and represented, and abstentions will not be counted. Each member entity has one vote, regardless

of the number of representatives of the entity in the meeting. In the event of a tie, the Chairperson may use his/her vote to break the tie.

For decisions regarding national standard documents — approval for consideration, revision and proposals for publication, and cancellation, consensus will also be sought for. However, if consensus is not reached, the corresponding resolution will be adopted only if at least two-thirds of the votes cast by members are in favour of the proposal.

The CTNs will vote and comment on all documents generated by international and European organisations for which (a) they have been assigned responsibility, and for which (b) a national response is mandatory. Consensus will also be sought for in this case but, if voting is necessary, at least two-thirds of the votes cast by the members should be obtained otherwise the national position will be to abstain.

Both SCs and WGs meetings adhere to the same rules as CTNs.

3.3.2.3.3 Commenting Procedures on Open Projects

The development of new standards within UNE is a multi-step process that starts with the evaluation of the proposal. After that, the proposal is assigned to a suitable CTN that will work on the standard project. Once ready, the specification has been agreed upon including the views of all interested members, it is published for review.

To ensure that the final standard document is the result of consensus, UNE offers mechanisms so that anyone, even if they do not belong to the CTN that elaborates it, can issue their opinions or comments.

The availability of projects specifications is publicly announced in the Official State Gazette (BOE) and can be accessed through (Proyectos, 2022). From this website, anyone can search for projects in public review stage. Moreover, after registration, anyone can read, comment, and propose edits for a limited period of time, which according to the Procedural Guidelines for the Work of Technical Committees (COMITÉS, 2017) is fixed to a minimum of 20 days and a maximum of 60 days, depending on the type an extension of the document.

The CTN will also consider any observations made by representatives of other SDOs like CEN/CENELEC or ETSI, as well as accept their participation in meetings if so requested.

Any received comments will be compiled by the Secretary of the CTN and will be included in the history of the standard document. The Secretary will forward comments to all CTN members and make proposal on how to proceed with them (e.g., organise a CTN meeting to discuss them, approve the changes, etc.). In any case, the proponent will be informed of the decisions made by the CTN regarding the observations. The time to inform should be no longer than 2 months since the observations were received.

In case the specification needs to be modified, after consultation with the CTN, UNE's technical services will decide whether the changes introduced to the project are sufficiently important for it to be resubmitted for public review.

3.3.2.4 Maturity of Procedures

UNE has a procedure such that all of its standards must be revised at least every five years after their publication. This revision process may involve the confirmation of the standard for a new period of five years maximum, its partial modification, its cancellation, or its replacement by a new text.

3.3.2.5 Stability of Procedures

Standardisation activities in Spain were carried by the Spanish Association for Standardisation and Certification (AENOR), which was established in 1986. In 2016, the General Assembly of the AENOR agreed to modify its statutes and the separation of the standardisation and certification activities. In January 2017, finally divided into two different organisations: UNE for standardisation and AENOR International S.A.U. for certification.

The standardisation activities conducted at UNE where originally established by AENOR and thus their procedures. The CTN rules of procedure were revised by AENOR 4 times since its inception and once more when the creation of UNE was agreed in 2016. Since then, it has been revised twice, in 2019 and 2020, but only minor changes were introduced.

Also, the Procedural Handbook for CTNs works has not experienced many modifications in the last few years. The last revision of this document by AENOR was made in 2015 and after that it was reviewed by UNE in 2017 and 2021. Very few modifications have been made in newer versions of this procedure.

All things considered, we can say that the procedures defined by UNE are stable.

3.3.2.6 Effectiveness and Relevance

UNE is recognised as the National Standardisation Body in Spain and, as such, Spanish legislation turns to technical standards developed or adopted by UNE. Also, UNE has international relevance in Latin America due to its participation in the Pan American Standards Commission.

3.3.2.7 Coherence

UNE is involved in several organisations at the European and international level, including CEN/CENELEC, ETSI, COPANT as well as ISO, IEC and ITU. UNE has 14 agreements in force with the standardisation bodies of Latin American countries.

UNE has a Spanish-language catalogue of more than 33,500 standards, most of which adopt European and international norms developed with the contribution of the Spanish sectors.

3.3.2.8 Development Dimension

International cooperation is one of the activities carried out by the Spanish Association for Standardisation. This activity is developed through technical assistance projects aimed at strengthening the institutional capacities of the staff of organisations in countries with emerging economies, promoting the international policies of the European Union and Spain, and harmonizing the requirements for access to other markets.

In fact, UNE was included in the European Commission's list of entities to participate in twinning projects (UNE18Tw, 2018), which is an instrument of the European Union that promotes institutional cooperation with countries under the European Neighbourhood and Enlargement Policy, including EU pre-accession countries such as Albania, Serbian and Turkey, as well as southern Mediterranean countries (e.g., Morocco, Algeria, Egypt, Lebanon) and Eastern countries (e.g., Georgia, Moldova, Ukraine). UNE has worked within the framework of EU agreements with Mexico, Central America, and Georgia.

In addition to projects financed by the EU, UNE also works with other financing organisations to promote its development dimension.

As the Spanish mirror of ISO, UNE also adheres to its Action Plan for developing countries (ISO21APD, 2021).

3.4 Common Criteria

Common Criteria for Information Technology Security Evaluation (CC) is an international standard for computer security certification according to ISO/IEC 15408. The certification process is performed by testing laboratories complying with ISO/IEC 17025 and certification bodies approved against ISO/IEC 17065.

The certificates issued by certification bodies are mutually recognised to some extent based on the Common Criteria Mutual Recognition Arrangement (CC MRA), which was now known as Common Criteria Recognition Arrangement (CCRA) (CCRA, 2021). Evaluations up to evaluation assurance level (EAL) are mutually recognised worldwide, up to EAL 4 level within EU countries (and other members in the former ITSEC agreement), and evaluations with higher levels are typically recognised only based on the decision of the national government. The certificates up to EAL 7 are recognised among the Senior Official Group – Information Systems Security (SOG-IS, 15 European Countries) (CC, 2014).

3.4.1 Openness

3.4.1.1 Openness to the public

The CCRA consortium can contain only representatives of the signatory countries. A management committee consists of the senior representatives from each signatory's country. The members of CCRA have the role either as authorizing (producents of certificates, performing the evaluation) or consuming (consumers of certificates).

The Common Criteria standardisation and procedure documents as well as the resulting certificates, security targets (specification of a target of evaluation (ToE) of the certified product) and updates are openly available on the CC website free of charge.

The governmental organisations involved in creation of CC documents granted non-exclusive license to the ISO/IEC for use of CC documents in the development of the ISO/IEC 15408 international standard (which itself is available only for a fee). Common Criteria documents including the older versions are available at the Common Criteria portal (CCportal, 2021). The CC standards are prepared by the Common Criteria Technical Working Groups (TWGs) (CCWG, 2013).

Since 2014, technical documents can be prepared by international technical communities (iTCs) which are partially formed by members in Common Criteria Users Forum (CCUF). The CCUF management board is in turn in liaison with the Common Criteria Development Board (CCDB). The public can also openly contribute on the existing community Protection Profiles and supporting documents via standard GitHub pull requests (CCGithub, 2022).

3.4.1.2 Access to Meetings

Management committee meetings are restricted only to government organisations and government agencies representing their country. It is free of charge. The management committee may invite experts or technical advisers to attend meetings to advise on specific issues (CCRA, 2021)

Participants in international technical communities are enrolled via the Common Criteria Users Forum (CCUF). Membership in CCUF is free of charge (CCUF, 2022).

3.4.1.3 Commenting Procedures on Open Projects

The collaborative Protection Profiles are developed openly on GitHub with change requests moderated according to the iTC rules and with full git history of all changes. There is an additional three-week comment period.

3.4.2 Impact

The Common Criteria-produced standards have a wide impact on the national as well as international level. The standardisation documents used during the certification provide a common unifying framework and standard Protection Profiles further standardise the expected security functionality and assurance of the certified products. The number of CC-certified products in 2020 was the highest in the existence of the CC scheme. The number of members involved is mostly increasing over the time (currently with 31 members), but also with occasional decreases, most notably UK ceased to be a certificate producer in 2019.

3.4.3 Governance

3.4.3.1 Organisational Structure

The Common Criteria Recognition Arrangement (CCRA) is managed via the following structure of technical working groups (TWGs):

- Management committee (CCMC) – responsible for admittance of new members, compliance of new certification bodies, new versions of CC and overall scope of CCRA. Representatives by all signatories;
- Executive subcommittee (CCES) – responsible for the development of procedures for the conduct of business, assessment of technical compliance of new certification bodies, resolving technical disagreements. Representatives by all certificate authorising nations, participants from the consuming nations nominated by the management committee;
- CC Development Board (CCDB) – responsible for the development and maintenance of CC and CEM documents, liaison with ISO, initiative in specific technical areas. Representatives by all certificate authorising nations and selected participants with sufficient technical knowledge, observing participants from consuming nations nominated by the management committee; and
- Maintenance Board (CCMB) – responsible for the management of change proposals, based upon national CC and CEM development requirements.

The technical communities (TCs) are responsible for the production and subsequent maintenance of Protection Profiles. The international technical communities (iTCs) are formed to develop and maintain collaborative Protection Profiles (cPP). Some TCs/iTCs are formed by a specific national body, while others are formed by groups of vendors or parties interested in specific space. The cPPs are developed openly in machine-readable XML format using GitHub repositories (CCGithub, 2022).

3.4.3.2 Voting Rules

The voting procedure is different between Common Criteria Recognition Arrangement (CCRA) representatives and international technical communities (iTCs).

The voting process for CCRA is the following. Each country which has a representative in the management committee has one vote. Voting is typically attempted to be unanimous. Decisions are achieved by simple majority.

The voting process for iTCs is the following. The voting procedures are specified by a particular iTC, but typically they provide a three-week voting period, a minimum quorum of 25% or 50% of eligible

organisations/members and 2/3 majority of the votes (CCVoting, 2021). Larger iTCs have typically one vote per organisational members while smaller iTCs have one vote per person.

3.4.3.3 Commenting Procedures on Open Projects

The drafts are typically available for a defined period for public comments. CCRA proposals and mandatory documents are typically open for a one-month public comment period. ITC proposals are typically open for a three-week public comment period.

3.4.4 Maturity of Procedures

The CC reviews its procedures and develops new or updated procedures with the annual conference. The introduction of Protection Profiles was one of the major updates, enforced by the update to the recognition policy in 2012, which now favours products certified according to the PPs. The most recent Common Criteria Recognition Arrangement ratified in 2014 added focus on public-private collaboration and introduced a new type of governance and procedures named international technical communities. The change is targeted at higher participation of private organisations in the development of relevant security specifications for a particular technology domain.

3.4.5 Stability of Procedures

The Common Criteria scheme and related procedures were initially introduced in 1998, with the most recent Common Criteria Recognition Arrangement ratified in 2014 which implemented vision formulated in 2012.

It can be concluded that the basic procedures are now stable. The introduction of international technical communities as defined in 2014 was a substantial change in existing procedures. The iTCs resulted in sixteen new collaborative Protection Profiles till this date and with increased number in recent years. As the procedures have not changed significantly since 2014, this can be interpreted as sufficiently stable.

3.4.6 Effectiveness and Relevance

Common Criteria certification standards and corresponding certificates are produced and recognised formally by 31 national states and federations. By the end of 2021, there were seventeen countries authorising certificates under CC scheme (Certificate Authorizing Members) and an additional fourteen certificate consuming members. The additional members are occasionally added (last time Slovakia in 2019) or changed (UK from authorising to consuming member also in 2019).

The Common Criteria scheme is known to be relatively costly and time-consuming with the resulting effectiveness and possible improvements discussed as early as in 2004 (Hearn, 2004). The significant change leading to improved effectiveness and relevance was introduction of Protection Profile with significant adoption from around 2012.

Due to the detailed scrutiny and certification process, the standard CC scheme is not suited well for frequently changing products like software, specifically one developed in agile instead of waterfall development model. As a result, adapted version of CC called EUCC was drafted by Enisa (EUCC, 2020) focused specifically on the cybersecurity certification. EUCC is also aimed to be a successor to the existing SOG-IS EU scheme.

3.4.7 Coherence

The Common Criteria standards are defined as ISO/IEC standards with the corresponding editorial procedures to avoid duplication in other similar standards. Additionally, given the long history, prominence, and level of support on the governmental level, Common Criteria standards are well known within cybersecurity standardisation.

On the other hand, the relative complexity of the base CC standards leads to the creation of other domain-specific standards with partially overlapping goals. Preferably, such standards are simplified CC-inspired standards like EUCC (EUCC, 2020) or orthogonal standards focusing on a specific domain, which are then used to specify requirements (e.g., typically by a Protection Profile) on the products certified. Also, as the Common Criteria is primarily generic framework for certification, the risk for duplication of work in specific domain is decreased.

3.4.8 Development Dimension

The current set of Common Criteria consortium members consists mostly of developed countries. Two developing countries (India and Malaysia) are listed as certificate authorising members (out of seventeen), and three developing countries (Ethiopia, Indonesia, and Pakistan) are listed as certificate consuming members (out of fourteen). The developing countries might be involved in specific workgroups, international technical communities, or preparation of standards for a specific aspect of the CC-certified product, e.g., supply chain security.

4 Summary and Recommendations

In this section, we summarise the observations and findings of our study. We provide a sketch of the key findings, take-away messages and recommendations. Furthermore, Table 2 depicts a general comparison of different SDOs based on the criteria established in the beginning of this document.

4.1 Key Observations

During our analysis, we observed that many standard organisations allow free access to their standards, which greatly improves adoption. However, in some cases, we faced challenges in accessing relevant documents and finding the information even though these topics should be easily accessible for an interested party. In addition to these, we made the following observations:

- many organisations allow commenting on projects even if you are not a member;
- participation as individual member is possible in some SDOs and also affordable for small and medium sized enterprises or academic institutions;
- many organisations have liaisons with other organisations, which is supposed to reduce duplication of work;
- not all organisations take into account the development dimension. This is especially true for continental and national SDOs;
- some SDO rules and regulations (e.g., CEN/CENELEC) change seldom which indicates some sort of stability; and
- for ISO/IEC JTC 1, it takes almost half a year to put content into the new directives, while aproximately half a year later new directives may come up which leaves less time for sychronisation and stability.

SDO	Types of participation and membership	Access to meetings	Membership fees	Document availability	Voting rules	Impact level
CEN/ CENELEC	Blue-type Members	Open to members	Annual fee calculated by a combination of the country GNI, Population percentages, with a correction factor	Available for purchase Certain CEN and/or CENELEC Workshop Agreements (CWAs), are available free of charge under special arrangements	Simple majority where each member has one vote	Mainly European with international outreach
	Red-Type Members					
	Yellow-Type Members					
ISO/ IEC	Full members	Full voting rights	Unit value x n (n = number of units allocated)	Mainly available to buy	One country – one vote	Worldwide
	Correspondent members	Attend General Assembly without voting	Unit value x 2			
	Subscriber members	No voting	Unit value x 0.5			
OASIS	Contributor	Members only (minutes are open to anyone)	$1.450 - $10.500	Open to anyone	Simple majority vote (one vote per by individual). Some TC may apply different rules	Worldwide
	Sponsor		$13.000 - $21.000			
	Foundational Sponsor		$50.000 - $57.000			
	Personal (participation limited to TC)		$380 - $1.600			
ETSI	Members and associate members Not-for-profit bodies and Micro-Enterprises	Members only	Based on various factors (e.g. income, number of units)	Open to anyone	Vote depend on membership category and fee	Wordwide

SDO	Types of participation and membership	Access to meetings	Membership fees	Document availability	Voting rules	Impact level
	Governmental organisations Observers					
UNE	Honorary	Members only	-	On purchase	Consensus or simple majority vote (one vote per entity). Two thirds of votes for decisions on standard documents	Spanish-speaking countries
	Corporate		Depends on association budget			
	Affiliated					
	Individual		€500 - € 1.200			
	Non-members wishing to participate in TC					
Common Criteria	Certificate Authorizing Members	Members only, experts invited by Management Committee	Free of charge, but limited to gov organisations and agencies representing their country	Open to anyone	Each country one vote, simple majority, typically unanimous	Worldwide
	Certificate Consuming Members					
	International Technical Communities (iTC), Common Criteria Users Forum (CCUF)	Open to anyone	Free of charge		by iTC, typically 25% or 50% eligible organisations/members and 2/3 majority of the votes	
HL7	Individual	Members only	$775	Open to anyone	A user signs up to participate in a ballot. There may be a cost associated if the user is not an HL7 member.	Worldwide
	Organisational		$1,500-$23,000			
	Gold		$1,850-$28,400			
	Benefactor		$16,000-$37,000			
BSI	Germany governmental agency	Restricted to BSI and invited experts,	NA	Open to anyone	Non-public, internal procedures	Primarily German and EU, but some used

SDO	Types of participation and membership	Access to meetings	Membership fees	Document availability	Voting rules	Impact level
		public comments				world-wide

Table 2: Tabular summary of the analysis

4.2 Recommendations

The study and subsequent observation have led us to layout the following general recommendations.

- We recommend that the results of the work of SDOs (standards, technical reports) are made freely available to universities or independent cyber security researchers, as otherwise security research will be hindered. Putting standards behind paywalls often negatively impacts the accessiblity and outreach of the results to a wider audience. SDOs can follow a similar approach as “author’s copy” to make their resources available for free on the website of the authors or editors. More details are provided in Section 4.2.1.

- We recommend for the EU to support with more financing of standards development processes as well as encourage to enable free access of results of the SDOs. This would further encourage research and development processes to incorporate and disseminate standardisation results. Moreover, SMEs and private participants would be more encouraged to utilise standardisation results.

- We encourage the cyber security community of the EU (e.g., the European Cybersecurity Competence Centre) to make regular recommendations as to which standards to pick for financing by the EU. Affordability of standards is important for cyber security, especially for critical infrastructures.

- We recommend that Member States support the national standardisation organisations to include more international standards into the national standardisation collections to make them more easily accessible.

- The European Cybersecurity Competence Centre should also liase and work with SDOs in the development of relevant cyber security standardisations.

- SMEs and start ups often operate in the working language of their respective nations, therefore, translating the standardizations into European national languages can also increase in the uptake of standards in Europe.

4.2.1 Availability of Standardisation Documents

The question of accessibility of the standardisation documents and related issues can be discussed in the context of Open Access (OA) options as used for the publication of research articles. The OA recognises several different models: Gold OA (author pays for publication, immediately available), Green OA (free self-archiving for an author, paid access if readers access on publisher website), Hybrid OA (mix of freely available articles paid for by author and paid articles paid for by readers), Diamond OA (freely available articles without author paying for free access, source of income must be elsewhere – grants, advertisement) and so-called Black OA (unauthorised copies available online).

The relevant OA models to consider might be:

- Gold OA, where the author (e.g., governmental body) sponsors the creation of standardisation documents and makes them available online. An example of this approach is BSI 200-x standards sponsored by the German government and available on the BSI website and currently also Common Criteria ISO standards freely available at the CC consortium website.
- Green OA, where almost final drafts of a standard are freely available while definitive version must be paid for by a reader. This approach allows for easy accessibility of almost final information for researchers or interested buyers before purchase.
- Diamond OA, where publication is sponsored by a government or EU directly (similarly to Gold OA) or by payments collected from the vendors of compliant products.

Hybrid OA does not seem to be relevant as some documents would still not be freely available.

Bibliography

WTO. (2000). *Wolrd Trade Organisation: SECOND TRIENNIAL REVIEW OF THE OPERATION AND IMPLEMENTATION OF THE AGREEMENT ON TECHNICAL BARRIERS TO TRADE.* Committee on Technical Barriers to Trade.

EC. (2011). *European interoperability framework for pan-European egovernment services*. Retrieved February 2022, from Publications office of the European Union: https://op.europa.eu/en/publication-detail/-/publication/a4778634-27fa-43b4-9912-f753c4fdfc3f

EU. (2012, October 25). *Official journal of the European Union*. (REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL) Retrieved January 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025&from=EN

CEN. (2017, 11 09). *CEN*. Retrieved January 2022, from Guidance documents : https://boss.cen.eu/reference-material/guidancedoc/pages/fvuapvoting/

CENELEC, C. (2022). *www.cencenelec.eu*. Retrieved January 2022, from Digital society: https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/cybersecurity-and-data-protection/

CEN-CENELEC. (2022, January). Retrieved February 2022, from CEN-CENELEC Internal Regulations - Part 1:2022: https://boss.cen.eu/media/BOSS%20CENELEC/ref/ir1_e.pdf

Wennblom, P. (2018). Retrieved November 2021, from ISO/IEC Joint Technical Committee 1 ISO/IEC JTC 1: https://slideplayer.com/slide/14607623/

ETSI. ( ). Retrieved February 2022, from Official website: https://www.etsi.org/

OASIS. (2021). Retrieved February 2022, from https://www.oasis-open.org/categories-dues/

Open, O. (2021). Retrieved 2022, from Technical Committee Membership Benefits Matrix

committee, O. (2021). Retrieved 2022, from https://www.oasis-open.org/projects-committees/

standards, O. (2021). Retrieved 2022, from https://www.oasis-open.org/standards/

operations, O. (2021). Retrieved 2022, from https://www.oasis-open.org/policies-guidelines/oasis-committee-operations-process/

open, O. (2021). Retrieved 2022, from https://www.oasis-open.org/policies-guidelines/oasis-committee-operations-process/

Handbook, O. (2010). Retrieved 2022, from https://docs.oasis-open.org/TChandbook/

TC, O. (2020). Retrieved 2022, from https://www.oasis-open.org/policies-guidelines/tc-process-2017-05-26/

Bylaws, O. (2020). Retrieved 2022, from https://www.oasis-open.org/policies-guidelines/bylaws/

UN. (2021). Retrieved 2022, from https://unctad.org/system/files/official-document/ldc2021_en.pdf

OECD. (2020). Retrieved 2021, from https://www.oecd.org/about/members-and-partners/

Vote. (2021). Retrieved 2021, from https://www.oasis-open.org/join-2/

ETSI. (2021). (E. procedures, Producer) Retrieved February 2022, from https://www.etsi.org/events/714-how-does-etsi-make-standards

ISO. (2022). *Technical Committees*. Retrieved February 2022, from ISO/IEC JTC 1 Information technology: https://www.iso.org/committee/45020.html

cencenelec. (2022). Retrieved November 2021, from www.cencenelec.eu: https://www.cencenelec.eu/media/News/Policy_Opinions/PolicyOpinions/CEN-CLC_ResponseToTheEUTradePolicyReview.pdf

HL7. (2022). Retrieved from https://www.hl7.org/participate/membership/index.cfm?ref=nav
FHIR. (2019). Retrieved 2022, from https://www.hl7.org/implement/standards/product_brief.cfm?product_id=491
Release4. (2019). Retrieved 2022, from https://hl7.org/fhir/
Leadership. (2022). Retrieved from https://www.hl7.org/Special/committees/international/leadership.cfm
Chart. (2022). Retrieved 2022, from https://www.hl7.org/documentcenter/public/calendarofevents/2022HL7OrgChart.pdf
Noumeir, R. (2019). Active Learning of the HL7 Medical Standard. *Journal of digital imaging*, 354-361.
Plan. (2019). Retrieved 2022, from https://www.hl7.org/documentcenter/public/about/board-approved-strategic-goals-objectives.pdf
WG. (2018). Retrieved 2021, from https://www.google.com/url?client=internal-element-cse&cx=013068602079619598366:1md6bdavbtc&q=https://www.hl7.org/documentcenter/public/wg/intl/minutes/HL7%2520International%2520Council%2520Thursday%2520October%25204,%25202018%2520Minutes%2520(draft).docx
Martin Schallbruch, I. M. (2018). The Organisation of Cybersecurity in Germany. *Cybersecurity in Germany*.
BSI. (2019). Retrieved from https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Drafts/it-grundschutz-drafts_node.html
Grundschutz. (2021). Retrieved 2022, from https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
BSI. (2020). Retrieved 2022, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.pdf?__blob=publicationFile&v=1
Form. (2021). Retrieved 2022, from https://www.une.org/normalizacion_documentos/portal-une/FO-08a-Vocalia-entidad-UNE.pdf
Form2. (2021). Retrieved 2022, from https://www.une.org/normalizacion_documentos/portal-une/FO-08b-Vocalia-particular-UNE.pdf
UNE. (2021). Retrieved 2021, from https://www.une.org/encuentra-tu-norma/busca-tu-norma
ENERO. (2022). Retrieved 2022, from https://revista.une.org/
UNE20RCT. (2020). Retrieved 2021, from https://portal.aenormas.aenor.com/descargas/une/Reglamento-Comites-Tecnicos-de-Normalizacion-20170101.pdf
UNE320. (2020). Retrieved 2021, from https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite/?c=CTN%20320
Proyectos. (2022). Retrieved 2022, from https://srp.une.org/
COMITÉS. (2017). Retrieved 2021, from https://portal.aenormas.aenor.com/descargas/une/MANUAL-DE-PROCEDIMIENTO-2017-UNE.pdf
ISO21APD. (2021). Retrieved 2021, from https://www.iso.org/publication/PUB100374.html
UNE18Tw. (2018). Retrieved 2021, from https://www.une.org/la-asociacion/sala-de-informacion-une/noticias/proyecto-de-hermanamiento-twinning
CCRA. (2021). Retrieved from https://www.commoncriteriaportal.org/ccra/

CC. (2014). Retrieved 2022, from https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf
CCportal. (2021). Retrieved 2021, from https://www.commoncriteriaportal.org/cc/
CCWG. (2013). Retrieved 2021, from https://www.corsec.com/technical-communities-creating-common-criteria-protection-profiles/
CCGithub. (2022). Retrieved from https://github.com/commoncriteria
CCUF. (2022). Retrieved 2022, from https://www.ccusersforum.org/faqs/
CCVoting. (2021). Retrieved 2022, from https://www.ccusersforum.org/faq/should-approval-be-based-on-a-simple-majority-or-a-super-majority-or-some-other-criteria/
Hearn, J. (2004). Does the common criteria paradigm have a future? *IEEE Security & Privacy*, 64-65.
EUCC. (2020). Retrieved 2022, from https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme
ICTSkills. (2022). Retrieved 2022, from https://www.cencenelec.eu/areas-of-work/cen-sectors/digital-society-cen/ict-skills/
InternalRegulations. (2022). Retrieved February 2022, from https://boss.cen.eu/media/BOSS%20CENELEC/ref/ir1_e.pdf
ReferenceMaterial. (2022). Retrieved 2022, from https://boss.cenelec.eu/reference-material/refdocs/pages/
Price, A. (2021). Retrieved February 2022, from https://etech.iec.ch/issue/2021-06/iec-and-iso-standard-enables-secure-covid-health-certificates
ETSI. (2022). Retrieved February 2022, from https://www.etsi.org/membership/dues
CENELEC. (2022). *CENELEC Governance Structure*. Retrieved from https://www.cencenelec.eu/about-cenelec/structure-and-governance/
CEN. (2022). Retrieved from https://www.cencenelec.eu/about-cen/structure-and-governance/
LSN, O. (2021). Retrieved 2022, from https://www.oasis-open.org/liaisons/
FDN. (2020). Retrieved 2021, from https://www.oasis-open.eu/
MBR, O. (2021). Retrieved 2022, from https://www.oasis-open.org/member-resources/