Cyber Security for Europe

D8.5

Project Standards Matrix

Document Identification	
Due date	30th November 2022
Submission date	30th November 2022
Revision	1.0

Related WP	WP8	Dissemination Level	PU
Lead Participant	CYBER	Lead Author	Liina Kamm (CYBER)
Contributing Beneficiaries	ARCH, UMA, POLITO	Related Deliverables	D8.1, D8.2, D8.4

Abstract: The project standards matrix contains the mapping of the application areas and research challenges to existing cybersecurity standards and standardisation projects. The chosen topics are based on the areas covered by the project, but can be used by anyone who shares these interests. The aim is to connect experts to the standardisation process where they are needed. An expert from an application area can use the deliverable to narrow down the overwhelming list of available standards. This deliverable describes the methodology used to compile the matrix. The standards matrix is given as an annex to this deliverable and an interactive version in the form of an Excel is available on the project web page.

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

The initial goal of the project standards matrix was to study existing standards in the context of the project topics and to connect experts to the standardisation process where they are needed. During the project, the standards matrix was used for this purpose. The goal of this deliverable, however, is to report on the information that we gathered during the project and to give an overview of how different standards map to application areas and research challenges. The application areas have been chosen based on the project verticals, and the research challenges and requirements have been chosen mainly based on the project needs.

This deliverable discusses the motivation for this work, presents the methodology used for the mapping, includes the matrix in a static format, references the matrix as a filterable and sortable Excel sheet, and gives future plans for this resource. As this is an updated version of Deliverable 8.2 (Project Standards Matrix), we also discuss the evolution of this document.

Document information

Contributors

Name	Partner
Liina Kamm	CYBER
Dan Bogdanov	CYBER
Sandhra-Mirella Valdma	CYBER
Ruben Rios	UMA
Renáta Radócz	ARCH
Antonio Lioy	POLITO

Reviewers

Name	Partner
Stephan Krenn	AIT
Mark Miller	CONCEPT

History

0.1	2022-05-09	Liina Kamm	ToC and contents based on D8.2
0.2	2022-09-16	Liina Kamm	Coordinator high level review
0.3	2022-10-25	Liina Kamm	Document for first review
0.4	2022-11-14	Liina Kamm	Document for second review
0.9	2022-11-27	Liina Kamm	Document for quality management
1.0	2022-11-29	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Acronyms

List of Acronyms

C	**CD**	committee draft
D	**DIS**	draft international standard
	ECCC	European Cybersecurity Competence Centre
B	**ECSO**	European Cyber Security Organization
	EDPB	European Data Protection Board
	ETSI	European Telecommunications Standards Institute
G	**GDPR**	General Data Protection Regulation
I	**IALA**	International Association of Marine Aids to Navigation and Lighthouse Authorities
	IEC	International Electrotechnical Commission
	IoT	Internet of things
	ISO	International Organization for Standardization
	ISMS	information security management system
J	**JTC**	joint technical committee
N	**NIST**	National Institute of Standards and Technology
	NWIP	new work item proposal
P	**PDTS**	preliminary draft technical specification
	PII	personally identifiable information
S	**SC**	subcommittee
	SDO	standard development organisation
	SP	study period
T	**TR**	technical report
	TS	technical specification
W	**WD**	working draft
	WG	working group

1 Introduction

This deliverable presents the project standards matrix. This matrix contains privacy and cybersecurity standards from ISO/IEC, CEN/CENELEC, ETSI, ITU-T, IETF and OASIS that are relevant to the chosen application areas and research topics. All of these standards have been studied and mapped to the chosen topics.

The experts in cybersecurity are aware of the existence of standardisation and standards in their fields. However, it is not a trivial task to have an adequate overview of all the standard projects that could be relevant to each application area or topic. This deliverable has been compiled to direct the attention of experts to the standards and technical reports that could be relevant in their application area or research topic so that they can more quickly find the necessary information. We studied cybersecurity and privacy standards from ISO/IEC, CEN/CENELEC, ETSI, ITU-T, IETF and OASIS, and mapped them to the verticals and research topics of CyberSec4Europe.

All of the pilot cyber security competence centres and the European Cybersecurity Competence Centre (ECCC) include many capable specialists whose expertise can be a great benefit to the standardisation projects that are still being compiled. For this reason, during the project, we kept a list of ongoing standards projects from ISO/IEC in the matrices as CyberSec4Europe has a liaison relationship with ISO/IEC JTC 1/SC 27 WG 2 and WG 5. Using this relationship, CyberSec4Europe was and is able to contribute the research results and insights that have been gathered throughout the project to the standards under development. As was described in Deliverable 8.1 *Cybersecurity Standardization Engagement Plan*, many of the project partners are also involved in standardisation activities, so this can be another way of approaching disseminating the results of the project and ensuring that the bleeding-edge research reaches standardisation projects.

We have introduced the concept of the standards matrix (a mapping of standards and ongoing projects to application areas) to ISO/IEC JTC 1/SC 27 WG 5 and have proposed it as a standing document for the working group.

1.1 Document Structure

Section 2 of this deliverable talks about the expected benefits of this work. Section 3 discusses the methodology for compiling the standards matrices and also gives an overview of the main differences between this document and the initial version of the deliverable (D8.2 *Project Standards Matrix*). Section 4 includes the project standards matrix and Section 5 talks about the future of the matrix after the end of this project.

2 Expected Benefits and Impact

European economy. International standardisation (e.g., in ISO/IEC, but also CEN/CENELEC and ETSI) is one channel for technology dissemination for all kinds of organisations in the world. Companies and governments are coming together to contribute their best practices and agree on interoperability, compliance and certification.

Global technology companies are active in pushing their terminology and technological concepts into standardisation processes. The European technology companies, including the cybersecurity industry, should engage in the same practice. Especially as through European collaboration by multiple member states, there will be more impact in such activities.

Even though standardisation is a long-term strategy with no immediate return on investment, it will be instrumental in ensuring that European companies grow in size to compete on the global market.

European R&D. Researchers are envisioning the future with new technologies that promise cleaner environment, better security, more efficient work and better health. Through research activities, R&D forms the best practice for the future for both bleeding edge and existing technologies.

Thus, engaging in standardisation is a channel for global dissemination of research concepts. A standardised concept may be used by governments, companies and other organisations worldwide, proliferating EU research results. While it may not immediately be a source of citations or additional research funding, standardisation of research results will also inspire new research on the same topics, increasing research impact over a longer period.

CyberSec4Europe consortium. The CyberSec4Europe consortium has the unique opportunity to support pilot dissemination of research results and best practices from CyberSec4Europe partners through the liaison relation of the consortium. Through successful initial projects, we will teach new organisations to engage in the process.

3 Methodology

We have mapped cybersecurity standards to two categories of topics. First, much of the work in CyberSec4Europe (WP3, WP5) is done based on the needs of 7 application areas (verticals). The partners of CyberSec4Europe work on discovering the security and privacy requirements of typical use cases in these areas. Mapping standards to these verticals will help the people involved with these topics stay informed about the relevant standards that could be used when solving the security and privacy issues in their field. The verticals that CyberSec4Europe focuses on are the following (the summaries are taken from the CyberSec4Europe Description of Action).

- **Open banking**. This demonstration case addresses, when users are seeking to obtain account information, the risks and vulnerabilities emerging from social engineering and malware attacks. It also aims to provide protection for bank administration security policies as well as overcome weaknesses in the design and/or implementation of APIs in use and to prevent fraud and data loss in relation to the access and request of payment by third parties in an open banking environment.
- **Supply chain security assurance.** This demonstration case provides a blueprint for supply chain solutions for multiple sectors. One specific application will be for an energy use case involving transformers for power distribution, where the supply chain for the transformers will be critical to ensure proper operation of transformers as crucial components in power networks.
- **Privacy-preserving identity management.** This demonstration case enables an identity infrastructure to fulfil the need for strong privacy-preserving authentication with a distributed and scalable platform for privacy-preserving self-sovereign identity management. The platform will allow users to collect and manage attributes and claims from identity service providers, authenticate to service providers, provide consent for and control the personal data usage in a seamless and privacy-preserving fashion.
- **Incident reporting.** This demonstration case presents a platform that enables organisations or their entities to report incidents according to the different procedures and methods specified by applicable regulatory bodies. The platform will specifically support cybersecurity information data sharing in a bi-directional way, allowing for a centralised or a de-centralised approach, i.e. a peer-to-peer approach.
- **Maritime transport.** This demonstration case identifies the current cybersecurity challenges of the maritime sector and will design and develop a threat management system capable of continuously managing cybersecurity threats against Internet-connected critical cyber infrastructures in the maritime sector.
- **Medical data exchange.** This demonstration case allows the secure and trustworthy exchange of sensitive data between several kinds of players with different aims and claims, regarding the security, data protection and trust issues.
- **Smart cities.** This demonstration case connects the cyber security challenges of smart cities through the OASC organisation. It will deploy prototypes addressing cybersecurity challenges mainly related to privacy management in data exchanges among city stakeholders that will be elaborated with OASC during the first phase of the project.

Second, we have mapped other research challenges that have arisen in different work packages (e.g., WP3, WP5, WP7) of CyberSec4Europe, or those that span several work packages, to the main topics covered by

different standards. This way, experts who are working on solving these research challenges can have an overview of the applicable standards. The research challenges that we identified as relevant to the project are the following:

- authentication,
- machine learning and artificial intelligence (ML and AI),
- risk management,
- data de-identification,
- personally identifiable information (PII),
- Internet of things (IoT),
- information security management system (ISMS),
- General Data Protection Regulation (GDPR),
- access control/management,
- conformance testing (WP7),
- cloud services,
- security engineering (WP3),
- digital forensics,
- public key infrastructure (PKI),
- software development lifecycle (Task 3.3) (SDL (T3.3)),
- threat assessment/security evaluation,
- data sharing,
- secure multi-party computation (MPC), and
- biometrics.

We have included standards from ISO/IEC (The International Organization for Standardization/ International Electrotechnical Commission), CEN/CENELEC (The European Committee for Standardization/European Committee for Electrotechnical Standardization), ETSI (The European Telecommunications Standards Institute), ITU (International Telecommunications Union), IETF (Internet Engineering Task Force), and OASIS (The Organization for the Advancement of Structured Information Standards).

ISO/IEC was chosen because several partners of CyberSec4Europe are actively participating in ISO/IEC JTC 1/SC 27 and these standards are among the most used worldwide. As only standards developed by the CEN/CENELEC and ETSI are recognised as European Standards, we also included these standards in the deliverable. However, most of the CEN/CENELEC JTC 13 standards are mirrored from ISO/IEC standards, so these are not explicitly featured in the matrices. ITU-T, IETF and OASIS were added on the basis of relevant available content. Further information about the standardisation organisations can be found in Deliverable 8.4 (*Standardisation Procedure Assessment Document*), but also D8.1 and D8.3 (two versions of the *Cybersecurity Standardisation Engagement Plan*).

With the standard development organisations (SDOs) chosen, we started looking through the sections of those websites to identify their internal structure and recommendations for searching standards. We looked through all committees and working groups and finally selected the topics that were relevant for this deliverable. We also used keywords to search for all CyberSec4Europe verticals (open banking, supply

chain security, privacy-preserving identity management, incident reporting, medical data exchange, smart cities) and in addition, keywords like: security, secure, securing, cybersecurity, privacy, digital signatures, authentication, machine learning, artificial intelligence, internet of things, risk management, threat assessment, cryptographic, encryption, identity management, data de-identification, personally identifiable information, access management, vulnerability, incident management, threat information. The in-depth selection process by larger organisations was the following.

ETSI had divided their standards under different topics in the technology section and we looked through standards with the following topics: artificial intelligence, consumer IoT security, cybersecurity, digital signature, eHealth, Internet of things, maritime, quantum key distribution, quantum-safe cryptography, securing artificial intelligence, security algorithms, and smart cities. Also, we investigated standards prepared by ETSI committees and working groups: CYBER, eHEALTH, SET, SmartM2M, oneM2M, ETI, ENI, QKD, SAI, ESI, STAG, IN.

ISO had related topic sections like health informatics, financial services, banking, electronic fee collection, security management systems for the supply chain, Internet of things, information technology (e.g., 35.030 IT security, 35.240.40 IT applications in banking, 35.240.99 IT applications in other fields, 35.240.01 applications of information technology in general, 35.240.80 IT applications in health care technology). We also analysed separately the ISO/IEC 27000 and ISO 31000 series standards. We looked through the standards in the following technical committees: ISO/IEC JTC 1 Information technology (incl. ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, ISO/IEC JTC 1/SC 37 Biometrics), ISO/TC 8 Ships and marine technology, ISO/TC 68 Financial services, ISO/TC 215 Health informatics.

In CEN/CENELEC we analyse the standards of committees standardising artificial intelligence, cyber security and data protection, health informatics, and quantum technologies.

In IETF, we looked at security and privacy related working groups. In addition, the IETF webpage had a section named on security which listed several related standards.

For OASIS and ITU-T, we looked through the whole catalogue and selected the most relevant standards.

We also list four specific guidelines and standards that are not cybersecurity related but instead have surfaced as important vertical and task specific documents that need to be considered during research into these areas. These are

- the IALA Guideline 1082 – An Overview of AIS[1] (maritime transport vertical),
- the IALA Guideline 1117 – VDES Overview[2] (maritime transport vertical),
- the HL7® - FHIR® standard for health care data exchange[3] (the medical data exchange vertical), and

[1] https://www.iala-aism.org/product/an-overview-of-ais-1082/
[2] https://www.iala-aism.org/product/vhd-data-exchange-system-vdes-overview-1117/
[3] https://www.hl7.org/fhir/

- EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[4] (general guidance on the obligation of Data Protection by Design and by Default (Article 25 of GDPR)) (the privacy-by-design task).

3.1 Evolution of the Project Standards Matrix

The first version of this deliverable was originally submitted in the form of a static document. However, the authors felt that the matrix in this format lacked the desired usability, so we made the table containing the matrix also available both to project participants and on the web page. We feel that the improved usability also increased interest in this document and it quickly became one of our most downloaded resources on the project web page.

This deliverable more thoroughly maps different standards from different subcommittees of different SDOs. We have added standards from three new organisations: ITU-T, IETF and OASIS. We have also studied standards from other relevant subcommittees of ISO/IEC, CEN/CENELEC and ETSI.

Some of the ongoing standards projects listed in Deliverable 8.2 have meanwhile been published as standards, these are also included in the updated matrix. However, we omit ongoing projects from this version as this information would quickly become obsolete.

[4] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

4 Project Standards Matrix

The project standards matrix is included with this deliverable as a static table (PDF file) in Annex A. The project standards matrix is also available as an Excel file on the project web page[5]. This resource can be filtered, expanded and updated locally.

[5] Project standards matrix (spreadsheet) https://cybersec4europe.eu/wp-content/uploads/2022/11/Standards-matrix-1.0.xlsx

5 Further Work

We have introduced the project standards matrix (the Excel document) to ISO/IEC JTC 1/SC 27 WG 5 and we received very positive feedback. We hope to keep this alive as a standing document first in WG 5 and later, if this is successful, in the whole subcommittee. The nature of this standing document would be that it would keep the mapping of all the standards in the working group and later in the subcommittee to different selected application areas. This would help people from different areas to get started with standards in their chosen field and allow the subcommittee to communicate the standards better by giving hints as to which areas they could be useful for.

Even though not all of the standards that we have mapped will be in that living document, we envision that it will give a good overview of the standards and standards projects in the subcommittee and that the concept could be taken over by other subcommittees.

Annex A: Project Standards Matrix Table

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
	ISO and ISO/IEC Standards																											
2022	ISO/IEC TR 5895:2022 Cybersecurity — Multi-party coordinated vulnerability disclosure and handling	https://www.iso.org/standard/81807.html				x																			x		x	
2017	ISO 9564-1:2017 Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems	https://www.iso.org/standard/68669.html	x							x		x						x										
2016	ISO 9564-4:2016 Financial services — Personal Identification Number (PIN) management and security — Part 4: Requirements for PIN handling in eCommerce for Payment Transactions	https://www.iso.org/standard/61246.html	x							x								x										
2010	ISO/IEC 9798-1:2010 Information technology — Security techniques — Entity authentication — Part 1: General	https://www.iso.org/standard/53634.html								x																		
2019	ISO/IEC 9798-2:2019 IT Security techniques — Entity authentication — Part 2: Mechanisms using authenticated encryption	https://www.iso.org/standard/67114.html								x																		
2019	ISO/IEC 9798-3:2019 IT Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques	https://www.iso.org/standard/67115.html								x																		
2010	ISO/IEC 9798-6:2010 Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer	https://www.iso.org/standard/54529.html								x													x			x		
2022	ISO/IEEE 11073-40101:2022 Health informatics — Device interoperability — Part 40101: Foundational — Cybersecurity — Processes for vulnerability assessment	https://www.iso.org/standard/83502.html						x											x						x			
2022	ISO/IEEE 11073-40102:2022 Health informatics — Device interoperability — Part 40102: Foundational — Cybersecurity — Capabilities for mitigation	https://www.iso.org/standard/83503.html						x											x						x			
2015	ISO/IEEE 11073-00103:2015 Health informatics — Personal health device communication — Part 00103: Overview	https://www.iso.org/standard/64941.html						x																				
2005	ISO 11568-1:2005 Banking — Key management (retail) — Part 1: Principles	https://www.iso.org/standard/34937.html	x							x																		
2010	ISO/IEC 11770-1:2010 Information technology — Security techniques — Key management — Part 1: Framework	https://www.iso.org/standard/53456.html																										
2018	ISO/IEC 11770-2:2018 IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques	https://www.iso.org/standard/73207.html																										
2020	ISO/IEC 11770-5:2020 Information security — Key management — Part 5: Group key management	https://www.iso.org/standard/75295.html																										
2016	ISO/IEC 11770-6:2016 Information technology — Security techniques — Key management — Part 6: Key derivation	https://www.iso.org/standard/65275.html								x																		
2016	ISO 13491-1:2016 Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods	https://www.iso.org/standard/61137.html	x																									

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2017	ISO 13491-2:2017 Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions	https://www.iso.org/standard/72178.html	x																									
2019	ISO 13492:2019 Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption	https://www.iso.org/standard/73992.html	x																									
2019	ISO 13606-4:2019 Health informatics — Electronic health record communication — Part 4: Security	https://www.iso.org/standard/62306.html						x																				
2020	ISO/IEC 13888-1:2020 Information security — Non-repudiation — Part 1: General	https://www.iso.org/standard/76153.html								x																		
2010	ISO/IEC 13888-2:2010 Information technology — Security techniques — Non-repudiation — Part 2: Mechanisms using symmetric techniques	https://www.iso.org/standard/44736.html								x																		
2013	ISO/TS 14441:2013 Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment	https://www.iso.org/standard/61347.html						x																				
2002	ISO/IEC TR 14516:2002 Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services	https://www.iso.org/standard/31482.html																										
2010	ISO/TR 14742:2010 Financial services — Recommendations on cryptographic algorithms and their use	https://www.iso.org/standard/54951.html	x																									
2008	ISO/IEC 14888-1:2008 Information technology — Security techniques — Digital signatures with appendix — Part 1: General	https://www.iso.org/standard/44226.html			x					x																		
2008	ISO/IEC 14888-2:2008 Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms	https://www.iso.org/standard/44227.html			x					x																		
2022	ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model	https://www.iso.org/standard/72891.html																							x			
2022	ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components	https://www.iso.org/standard/72892.html																							x			
2022	ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components	https://www.iso.org/standard/72906.html																							x			
2022	ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities	https://www.iso.org/standard/72913.html																							x			
2022	ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	https://www.iso.org/standard/72917.html																							x			
2012	ISO/IEC 15443-1:2012 Security assurance framework Part 1: Introduction and concepts	https://www.iso.org/standard/59138.html		x								x																

			Verticals:							Research Challenges/Requirements in WP 5																			
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2012	ISO/IEC 15443-2:2012 Security assurance framework Part 2: Analysis	https://www.iso.org/standard/59140.html		x								x																
2012	ISO/IEC 15443-2:2012 Security assurance framework Part 2: Analysis	https://www.iso.org/standard/59140.html		x								x																
2017	ISO/IEC TR 15446:2017 Information technology — Security techniques — Guidance for the production of protection profiles and security targets	https://www.iso.org/standard/68904.html										x													x			
2020	ISO/TS 15638-4:2020 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 4: System security requirements	https://www.iso.org/standard/72094.html					x			x															x	x		
2002	ISO/IEC 15816:2002 Security information objects for access control	https://www.iso.org/standard/29139.html				x												x										
2022	ISO 16609:2022 Financial services — Requirements for message authentication using symmetric techniques	https://www.iso.org/standard/78305.html	x							x																		
2017	ISO 17090-5:2017 Health informatics — Public key infrastructure — Part 5: Authentication using Healthcare PKI credentials	https://www.iso.org/standard/67883.html						x															x					
2017	ISO/TS 17574:2017 Electronic fee collection — Guidelines for security protection profiles	https://www.iso.org/standard/70051.html	x									x					x	x										
2016	ISO/IEC 17825:2016 Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	https://www.iso.org/standard/60612.html																	x						x			
2022	ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation	https://www.iso.org/standard/72889.html																							x			
2016	ISO/IEC 18367:2016 Cryptographic algorithms and security mechanisms conformance testing	https://www.iso.org/standard/62286.html																	x									
2016	ISO/IEC 18370-1:2016 Information technology — Security techniques — Blind digital signatures — Part 1: General	https://www.iso.org/standard/62288.html			x					x																		
2005	ISO/TR 19038:2005 Banking and related financial services — Triple DEA — Modes of operation — Implementation guidelines	https://www.iso.org/standard/33733.html	x																									
2008	ISO 19092:2008 Financial services — Biometrics — Security framework	https://www.iso.org/standard/50145.html	x							x																x		x
2019	ISO/IEC 19086-4:2019 Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII	https://www.iso.org/standard/68242.html												x		x	x			x								
2017	ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications	https://www.iso.org/standard/64140.html	x	x	x	x	x	x	x												x							
2020	ISO 19299:2020 Electronic fee collection — Security framework	https://www.iso.org/standard/78357.html	x																									
2016	ISO/IEC 19592-1:2016 Information technology — Security techniques — Secret sharing — Part 1: General	https://www.iso.org/standard/65422.html																								x		

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2017	ISO/IEC 19592-2:2017 Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms	https://www.iso.org/standard/65425.html																								x		
2018	ISO/IEC TS 19608:2018 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	https://www.iso.org/standard/65459.html			x									x														
2020	ISO/IEC 19772:2020 Information security — Authenticated encryption	https://www.iso.org/standard/81550.html								x																		
2012	ISO/IEC 19790:2012 Security requirements for cryptographic modules	https://www.iso.org/standard/52906.html	x	x	x	x	x	x	x	x			x						x		x							
2010	ISO/IEC TR 19791:2010 Information technology — Security techniques — Security assessment of operational systems	https://www.iso.org/standard/52905.html																							x			
2009	ISO/IEC 19792:2009 Information technology — Security techniques — Security evaluation of biometrics	https://www.iso.org/standard/51521.html																							x			x
2018	ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements	https://www.iso.org/standard/71120.html																							x			
2018	ISO/IEC 19896-2:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	https://www.iso.org/standard/71121.html																							x			
2018	ISO/IEC 19896-3:2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	https://www.iso.org/standard/71122.html																							x			
2020	ISO/IEC 19989-1:2020 Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework	https://www.iso.org/standard/72402.html								x															x			x
2020	ISO/IEC 19989-2:2020 Information security — Criteria and methodology for security evaluation of biometric systems — Part 2: Biometric recognition performance	https://www.iso.org/standard/72403.html								x															x			x
2020	ISO/IEC 19989-3:2020 Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection	https://www.iso.org/standard/73721.html								x															x			x
2013	ISO/IEC 20008-1:2013 Anonymous digital signatures Part 1: General	https://www.iso.org/standard/57018.html			x					x																		
2013	ISO/IEC 20008-2:2013 Anonymous digital signatures Part 2: Mechanisms using a group public key	https://www.iso.org/standard/56916.html			x					x																		
2013	ISO/IEC 20009-1:2013 Anonymous Entity authentication Part 1: General	https://www.iso.org/standard/57079.html			x					x																		
2013	ISO/IEC 20009-2:2013 Anonymous Entity authentication Part 2: Mechanisms based on signatures using a group public key	https://www.iso.org/standard/56913.html			x					x																		
2022	ISO/IEC 20009-3:2022 Anonymous entity authentication Part 3: Mechanisms based on blind signatures	https://www.iso.org/standard/80615.html			x					x																		

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2017	ISO/IEC 20009-4:2017 Anonymous Entity authentication Part 4: Mechanisms based on weak secrets	https://www.iso.org/standard/64288.html			x					x																		
2017	ISO 20038:2017 Banking and related financial services — Key wrap using AES	https://www.iso.org/standard/64400.html	x																									
2019	ISO/IEC 20085-1:2019 IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques	https://www.iso.org/standard/70081.html																	x						x			
2020	ISO/IEC 20085-2:2020 IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus	https://www.iso.org/standard/70082.html																	x						x			
2018	ISO/IEC TS 20540:2018 Information technology — Security techniques — Testing cryptographic modules in their operational environment	https://www.iso.org/standard/68294.html																	x		x				x			
2018	ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques	https://www.iso.org/standard/69373.html	x		x	x	x	x	x				x	x			x											
2021	ISO/TR 21186-3:2021 Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards — Part 3: Security	https://www.iso.org/standard/79949.html					x		x	x															x	x		
2018	ISO 21188:2018 Public key infrastructure for financial services — Practices and policy framework	https://www.iso.org/standard/63134.html	x																				x					
2021	ISO/TR 21332:2021 Health informatics — Cloud computing considerations for the security and privacy of health information systems	https://www.iso.org/standard/70568.html						x																				
2010	ISO/TS 21547:2010 Health informatics — Security requirements for archiving of electronic health records — Principles	https://www.iso.org/standard/44479.html						x																		x		
2010	ISO/TR 21548:2010 Health informatics — Security requirements for archiving of electronic health records — Guidelines	https://www.iso.org/standard/44480.html						x																				
2008	ISO/IEC 21827:2008 Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)	https://www.iso.org/standard/44716.html																			x			x				
2006	ISO/TR 22221:2006 Health informatics - Good principles and practices for a clinical data warehouse	https://www.iso.org/standard/40783.html						x									x	x								x		
2013	ISO 22857:2013 Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data	https://www.iso.org/standard/52955.html						x																				
2021	ISO 23195:2021 Security objectives of information systems of third-party payment services	https://www.iso.org/standard/74853.html	x											x											x			
2021	ISO/IEC 23264-1:2021 Redaction of authentic data - Part 1: General	https://www.iso.org/standard/78341.html			x					x																		
2021	ISO 23323:2021 Ships and marine technology — Specification for software-based planned maintenance systems	https://www.iso.org/standard/75232.html					x																					

			Verticals:							Research Challenges/Requirements in WP 5																			
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2022	ISO/TS 23535:2022 Health informatics — Requirements for customer-oriented health cloud service agreements	https://www.iso.org/standard/75957.html						x												x								
2021	ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology	https://www.iso.org/standard/77678.html					x																					
2019	ISO/IEC 24761:2019 Information technology — Security techniques — Authentication context for biometrics	https://www.iso.org/standard/71163.html								x																		x
2022	ISO/IEC 24745:2022 Information security, cybersecurity and privacy protection — Biometric information protection	https://www.iso.org/standard/75302.html																										x
2017	ISO/IEC 24759:2017 Test requirements for cryptographic modules	https://www.iso.org/standard/72515.html																	x									
2019	ISO/IEC 24760-1:2019 A framework for identity management Part 1: Terminology and concepts	https://www.iso.org/standard/77582.html	x	x	x	x	x	x	x									x										
2015	ISO/IEC 24760-2:2015 A framework for identity management Part 2: Reference architecture and requirements	https://www.iso.org/standard/57915.html	x	x	x	x	x	x	x									x										
2016	ISO/IEC 24760-3:2016 A framework for identity management Part 3: Practice	https://www.iso.org/standard/57916.html	x	x	x	x	x	x	x									x										
2017	ISO 25237:2017 Health informatics — Pseudonymization	https://www.iso.org/standard/63553.html						x																				
2018	ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary	https://www.iso.org/standard/73906.html														x												
2022	ISO/IEC 27001:2022 Information security management	https://www.iso.org/standard/82875.html														x												
2022	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	https://www.iso.org/standard/75652.html														x												
2017	ISO/IEC 27003:2017 Information security management systems	https://www.iso.org/standard/63417.html														x												
2016	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	https://www.iso.org/standard/64120.html														x									x			
2022	ISO/IEC 27005:2022 Information security risk management	https://www.iso.org/standard/80585.html										x				x												
2015	ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	https://www.iso.org/standard/62313.html														x												
2020	ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing	https://www.iso.org/standard/77802.html														x												
2019	ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls	https://www.iso.org/standard/67397.html																							x			
2015	ISO/IEC 27010:2015 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications	https://www.iso.org/standard/68427.html																								x		

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2021	ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	https://www.iso.org/standard/78752.html														x												
2020	ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security	https://www.iso.org/standard/74046.html														x												
2014	ISO/IEC TR 27016:2014 Information technology — Security techniques — Information security management — Organizational economics	https://www.iso.org/standard/43756.html														x												
2015	ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	https://www.iso.org/standard/43757.html							x																			
2019	ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	https://www.iso.org/standard/76559.html												x		x				x								
2017	ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry	https://www.iso.org/standard/68091.html						x																				
2017	ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals	https://www.iso.org/standard/61003.html														x												
2021	ISO/IEC TS 27022:2021 Information technology — Guidance on information security management system processes	https://www.iso.org/standard/61004.html														x												
2012	ISO/IEC 27032:2012 Guidelines for cybersecurity	https://www.iso.org/standard/44375.html	x	x	x	x	x	x	x							x		x										
2015	ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts	https://www.iso.org/standard/63461.html	x	x		x	x	x	x			x								x	x				x			
2011	ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts	https://www.iso.org/standard/44378.html																			x							
2016	ISO/IEC 27035:2016 Information security incident management Part 1: Principles of incident management	https://www.iso.org/standard/60803.html				x										x									x			
2016	ISO/IEC 27035:2016 Information security incident management Part 2: Guidelines to plan and prepare for incident response	https://www.iso.org/standard/62071.html				x										x									x			
2020	ISO/IEC 27035-3:2020 Information security incident management - Part 3: Guidelines for ICT incident response operations	https://www.iso.org/standard/74033.html				x										x									x			
2021	ISO/IEC 27036-1:2021 Information security for supplier relationships Part 1: Overview and concepts	https://www.iso.org/standard/82905.html		x												x												
2022	ISO/IEC 27036-2:2022 Information security for supplier relationships Part 2: Requirements	https://www.iso.org/standard/82060.html		x												x												
2013	ISO/IEC 27036-3:2013 Information security for supplier relationships Part 3: Guidelines for information and communication technology supply chain security	https://www.iso.org/standard/59688.html		x												x												

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2016	ISO/IEC 27036-4 Information security for supplier relationships - Part 4: Guidelines for security of cloud services	https://www.iso.org/standard/59689.html		x												x				x								
2012	ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence	https://www.iso.org/standard/44381.html				x										x						x						
2015	ISO/IEC 27040:2015 Information technology — Security techniques — Storage security	https://www.iso.org/standard/44404.html																	x						x			
2015	ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method	https://www.iso.org/standard/44405.html				x						x							x						x			
2015	ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence	https://www.iso.org/standard/44406.html				x										x						x						
2015	ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes	https://www.iso.org/standard/44407.html				x																x						
2019	ISO/IEC 27050-1:2019 Information technology — Electronic discovery — Part 1: Overview and concepts	https://www.iso.org/standard/78647.html																				x						
2022	ISO/IEC 27099:2022 Public key infrastructure — Practices and policy framework	https://www.iso.org/standard/56590.html					x									x							x					
2020	ISO/IEC TS 27100:2020 Cybersecurity — Overview and concepts	https://www.iso.org/standard/72434.html														x												
2019	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance	https://www.iso.org/standard/72436.html														x						x						
2018	ISO/IEC 27103 Cybersecurity and ISO and IEC Standards	https://www.iso.org/standard/72437.html	x	x	x	x	x	x	x																			
2021	ISO/IEC TS 27110:2021 Cybersecurity — Cybersecurity framework development guidelines	https://www.iso.org/standard/72435.html														x												
2022	ISO/IEC 27400:2022 IoT security and privacy: Guidelines	https://www.iso.org/standard/44373.html	x	x			x	x	x						x		x				x							
2019	ISO/IEC TR 27550:2019 Privacy engineering for system life cycle processes	https://www.iso.org/standard/72024.html	x		x			x	x			x		x			x							x				
2021	ISO/IEC 27551:2021 Requirements for attribute-based unlinkable entity authentication	https://www.iso.org/standard/72018.html			x					x																		
2021	ISO/IEC 27555:2021 Establishing a PII deletion concept in organizations	https://www.iso.org/standard/71673.html	x		x			x	x					x		x	x											
2022	ISO/IEC 27556:2022 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	https://www.iso.org/standard/71674.html	x		x			x	x					x			x	x										
2021	ISO/IEC 27570:2021 Privacy guidelines for smart cities	https://www.iso.org/standard/71678.html							x		x		x	x			x	x			x							
2019	ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management	https://www.iso.org/standard/71670.html												x		x	x											
2016	ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002	https://www.iso.org/standard/62777.html						x										x								x		
2014	ISO 28004-2:2014 Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations	https://www.iso.org/standard/60905.html		x			x																					

			Verticals:							Research Challenges/Requirements in WP 5																			
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2018	ISO/IEC TS 29003:2018 Information technology — Security techniques — Identity proofing	https://www.iso.org/standard/62290.html			x					x				x														
2011	ISO/IEC 29100:2011 Privacy framework	https://www.iso.org/standard/45123.html	x		x		x	x						x			x											
2018	ISO/IEC 29101:2018 Privacy architecture framework	https://www.iso.org/standard/75293.html	x		x		x	x						x			x											
2011	ISO/IEC 29128:2011 Information technology — Security techniques — Verification of cryptographic protocols	https://www.iso.org/standard/45151.html																	x										
2017	ISO/IEC 29134:2017 Guidelines for privacy impact assessment	https://www.iso.org/standard/62289.html	x	x	x		x	x	x					x			x												
2016	ISO/IEC 29146:2016 A framework for access management	https://www.iso.org/standard/45169.html																x											
2018	ISO/IEC 29147:2018 Vulnerability disclosure	https://www.iso.org/standard/72311.html				x																x							
2017	ISO/IEC 29151:2017 Code of practice for personally identifiable information protection	https://www.iso.org/standard/62726.html	x		x	x		x	x					x															
2020	ISO/IEC 29184:2020 Information technology — Online privacy notices and consent	https://www.iso.org/standard/70331.html			x									x															
2015	ISO/IEC 29190:2015 Privacy capability assessment model	https://www.iso.org/standard/45269.html	x		x		x	x	x			x																	
2012	ISO/IEC 29191:2012 Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication.	https://www.iso.org/standard/45270.html								x																			
2019	ISO/IEC 30111:2019 Vulnerability handling processes	https://www.iso.org/standard/69725.html				x																x							
2020	ISO/IEC 30145-3:2020 Information technology — Smart City ICT reference framework — Part 3: Smart city engineering framework	https://www.iso.org/standard/76373.html							x																				
2019	ISO/IEC 30146:2019 Information technology — Smart city ICT indicators	https://www.iso.org/standard/70302.html							x																				
2021	ISO/IEC 30147:2021 Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	https://www.iso.org/standard/53267.html							x						x														
2021	ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts	https://www.iso.org/standard/71538.html						x																					
2021	IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle	https://www.iso.org/standard/76097.html						x																					
2021	ISO/TS 82304-2:2021 Health software — Part 2: Health and wellness apps — Quality and reliability	https://www.iso.org/standard/78182.html						x																					
	ETSI																												
2015	ETSI GS ISI 001-1 V1.1.2 Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=46042																	x		x				x				

			Verticals:							Research Challenges/Requirements in WP 5																			
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2015	ETSI GS ISI 001-2 V1.1.2 Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=46639																	x		x				x			
2015	ETSI GS ISI 002 V1.2.1 Information Security Indicators (ISI); Event Model A security event classification model and taxonomy	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=46638				x																						
2018	ETSI GS ISI 003 V1.2.1 Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50044				x													x			x			x			
2013	ETSI GS ISI 004 V1.1.1 Information Security Indicators (ISI); Guidelines for event detection implementation	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=41271				x													x									
2015	ETSI GS ISI 005 V1.1.1 Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=41272				x													x						x			
2018	ETSI GS ISI 007 V1.1.1 Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC)	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50920				x													x						x			
2018	ETSI GS ISI 008 V1.1.1 Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50045				x													x						x			
2012	ETSI GS INS 009 V1.1.1 Identity and access management for Networks and Services (INS); Security and privacy requirements for collaborative cross domain network monitoring	https://www.etsi.org/deliver/etsi_gs/INS/001_099/009/01.01.01_60/gs_INS009v010101p.pdf																x								x	x	
2020	ETSI TS 103 645 Cyber Security for Consumer Internet of Things: Baseline Requirements	https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf	x						x						x													
1998	ETSI TR 101 365 V1.1.1 Intelligent Network (IN); IN interconnect threat analysis	https://www.etsi.org/deliver/etsi_tr/101300_101399/101365/01.01.01_60/tr_101365v010101p.pdf																							x			
2014	ETSI TR 101 582 V1.1.1 Methods for Testing and Specification (MTS); Security Testing; Case Study Experiences	https://www.etsi.org/deliver/etsi_tr/101500_101599/101582/01.01.01_60/tr_101582v010101p.pdf	x		x			x		x		x													x	x		
2022	ETSI TS 102 165-1 V5.2.5 Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=63565																	x						x			
2009	ETSI TR 102 764 V1.1.1 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth	https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf						x																		x		
2019	ETSI TR 103 644 Increasing smart meter security	https://www.etsi.org/deliver/etsi_tr/103600_103699/103644/01.01.01_60/tr_103644v010101p.pdf							x																			
2015	ETSI TR 103 290 V1.1.1 Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment	https://www.etsi.org/deliver/etsi_tr/103200_103299/103290/01.01.01_60/tr_103290v010101p.pdf							x						x													
2019	ETSI TR 103 331 Structured threat information sharing	https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.02.01_60/tr_103331v010201p.pdf				x																						
2016	ETSI TR 103 303 V1.1.1 Protection measures for ICT in the context of Critical Infrastructure	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=44533						x	x						x						x							
2016	ETSI TR 103 304 Personally Identifiable Information (PII) Protection in mobile and cloud services	https://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf	x		x			x	x					x			x			x								

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2022	ETSI TR 103 305-1 V4.1.2 Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=64493																							x			
2018	ETSI TR 103 305-2 V2.1.1 Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=54742																							x			
2018	ETSI TR 103 305-3 V2.1.1 Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=54743													x										x			
2018	ETSI TR 103 305-4 V2.1.1 Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=54745																							x			
2018	ETSI TR 103 305-5 V1.1.1 Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=54744												x											x			
	ETSI TR 103 306 Global Cyber Security Ecosystem	https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.03.01_60/tr_103306v010301p.pdf	x	x	x	x	x	x	x			x										x						
2019	ETSI TR 103 370 V1.1.1 Practical introductory guide to Technical Standards for Privacy	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=47531			x			x	x					x														
	ETSI TS 103 458 Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements	https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf												x				x		x								
2020	ETSI TR 103 477 V1.2.1 eHEALTH; Standardization use cases for eHealth	https://www.etsi.org/deliver/etsi_tr/103400_103499/103477/01.02.01_60/tr_103477v010201p.pdf						x																				
2020	ETSI TS 103 485 V1.1.1 Mechanisms for privacy assurance and verification	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=47652			x			x						x														
	ETSI TS 103 532 Attribute Based Encryption for Attribute Based Access Control	https://www.etsi.org/deliver/etsi_ts/103500_103599/103532/01.01.01_60/ts_103532v010101p.pdf																x										
2019	ETSI TR 103 534-2 V1.1.1 SmartM2M; Teaching material; Part 2: Privacy	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf							x						x													
2019	ETSI TR 103 534-1 V1.1.1 SmartM2M; Teaching material; Part 1: Security	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf							x						x													
2021	ETSI TR 103 616 V1.1.1 Quantum-Safe Signatures	https://www.etsi.org/deliver/etsi_tr/103600_103699/103616/01.01.01_60/tr_103616v010101p.pdf			x					x																		
2019	ETSI TR 103 618 V1.1.1 Quantum-Safe Identity-Based Encryption	https://www.etsi.org/deliver/etsi_tr/103600_103699/103618/01.01.01_60/tr_103618v010101p.pdf			x					x																		
2022	ETSI TR 103 621 V1.2.1 Guide to Cyber Security for Consumer Internet of Things	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=66181							x						x													
2010	ETSI ES 202 642 V1.1.1 Human Factors (HF); Personalization of eHealth systems by using eHealth user profiles (eHealth)	https://www.etsi.org/deliver/etsi_es/202600_202699/202642/01.01.01_60/es_202642v010101p.pdf						x																		x		
2019	ETSI TS 103 645 V1.1.1 Cyber Security for Consumer Internet of Things	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=54761							x						x													
2021	ETSI TR 103 743 V1.1.1 Home Gateway Security Threat Analysis	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=59134							x																			
2021	ETSI TR 103 787-1 V1.1.1 Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=61738																										
2022	ETSI TR 103 838 V1.1.1 Cyber Security; Guide to Coordinated Vulnerability Disclosure	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=61976				x													x						x			
2021	ETSI TR 103 823 V1.1.2 Quantum-Safe Public-Key Encryption and Key Encapsulation	https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.02_60/tr_103823v010102p.pdf																										

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2022	ETSI TS 103 848 V1.1.1 Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=62605							x						x													
2021	ETSI TS 118 103 V3.13.0 oneM2M; Security solutions	https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/03.13.00_60/ts_118103v031300p.pdf							x						x													
2021	ETSI TS 119 461 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects	https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf			x	x				x		x		x			x	x										
2021	ETSI TS 119 495 V1.5.1 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking	https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.05.01_60/ts_119495v010501p.pdf	x																									
2016	ETSI EG 203 310 V1.1.1 Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection	http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=45962	x	x	x	x	x	x	x						x													
2017	ETSI GR QSC 004 Quantum-Safe Cryptography; Quantum-Safe threat assessment	https://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf	x		x		x	x																				
2021	ETSI GR SAI 002 V1.1.1 Securing Artificial Intelligence (SAI); Data Supply Chain Security	https://www.etsi.org/deliver/etsi_gr/SAI/001_099/002/01.01.01_60/gr_SAI002v010101p.pdf		x																								
2021	ETSI GR SAI 005 V1.1.1 Securing Artificial Intelligence (SAI); Mitigation Strategy Report	https://www.etsi.org/deliver/etsi_gr/SAI/001_099/005/01.01.01_60/gr_SAI005v010101p.pdf																	x						x			
2021	ETSI SR 003 809 V1.1.2 eHEALTH; The role of ICT to enable Health crisis management and recovery; Responding to the 2019 SARS-CoV-2 Pandemic	https://www.etsi.org/deliver/etsi_sr/003800_003899/003809/01.01.02_60/sr_003809v010102p.pdf						x																				
	CEN/CENELEC																											
2004	EN 12251:2004 Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:::::FSP_PROJECT,FSP_ORG_ID:23359,6232&cs=1F79FC64FE7552913761F85878E9F26CF						x		x				x				x										
2003	EN 14484:2003 Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:::::FSP_PROJECT,FSP_ORG_ID:21973,6232&cs=118AA3216C6187640DAA45F34FBDD4BCD						x									x											
2022	EN 17529:2022 Data protection and privacy by design and by default	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:63633,2307986&cs=11F70212	x	x	x	x	x	x	x					x			x				x			x				
2018	EN 419212-4:2018 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61440,6205&cs=14706465364CB67C7BD65620932DA52DE			x					x																		x
2018	EN 419212-5:2018 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61441,6205&cs=1C5C72F491FAABACC67A0C756547CD248			x				x	x																		
2015	EN 62056-1-0:2015 Electricity metering data exchange - The DLMS/COSEM suite - Part 1-0: Smart metering standardization framework	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:54211,1257151&cs=1D953							x																			
2017	EN 62320-2:2017 Maritime navigation and radiocommunication equipment and systems - Automatic identification system (AIS) - Part 2: AIS AtoN Stations - Operational and performance requirements, methods of testing and required test results	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:61292,1258049&cs=13A2FF9D032474534025FA9DB1653F404					x																					

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2014	EN 62351-3:2014 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:42838,1258723&cs=16546B193B1C98846206O2B46548DED8F							x																			
2020	EN IEC 62351-8:2020 Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:67696,1258723&cs=12EFBC9E790223EFD109786CDC16AF848							x																			
2021	EN IEC 63154:2021 Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:66863,1258049&cs=1844429470848D6474C74FE50D14EDF5D					x																					
2022	EN IEC 81001-5-1:2022 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:70468,1257161&cs=1B3ED8DD24520E8A975137B11147344EA						x																				
2021	CEN/TS 17631:2021 Personal identification - Biometric group access control	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP			x					x				x				x										x
2021	CEN/TS 17661:2021 Personal identification – European enrolment guide for biometric ID documents (EEG)	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:70154.6205&cs=173CE181D33D819F1FF7F7F312F76FA41			x					x				x				x										x
2005	CWA 50487:2005 SmartHouse Code of Practice	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:58365,1258281&cs=1A239017765F1BE96492E18B278FD6E32							x																				
	IETF standards																											
2015	Information-Centric Networking: Baseline Scenarios RFC 7476	https://datatracker.ietf.org/doc/rfc7476/							x						x													
2017	Requirements for Password-Authenticated Key Agreement (PAKE) Schemes RFC 8125	https://datatracker.ietf.org/doc/rfc8125/								x																		
2017	Research into Human Rights Protocol Considerations RFC 8280	https://datatracker.ietf.org/doc/rfc8280/															x											
2019	Network Virtualization Research Challenges RFC 8568	https://datatracker.ietf.org/doc/rfc8568/							x						x													
2019	Internet of Things (IoT) Security: State of the Art and Challenges RFC 8576	https://datatracker.ietf.org/doc/rfc8576/							x						x													
2019	Re-keying Mechanisms for Symmetric Keys RFC 8645	https://datatracker.ietf.org/doc/rfc8645/								x																		
2020	Randomness Improvements for Security Protocols RFC 8937	https://datatracker.ietf.org/doc/rfc8937/								x																		
2022	Hybrid Public Key Encryption RFC 9180	https://datatracker.ietf.org/doc/rfc9180/								x																		
	Vertical specific guidelines and standards																											
	IALA guideline 1082 - An Overview of AIS						x																					
	IALA Guideline 1117 VDES Overview						x																					
	HL7® - FHIR® standard for health care data exchange	https://www.hl7.org/fhir/						x																				
	OASIS Standards																											
2019	Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE) Version 2.0	https://docs.oasis-open.org/emergency/edxl-have/v2.0/cs02/edxl-have-v2.0-cs02.html						x																				

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2019	MQTT Version 5.0	http://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html							x						x													
2022	SAM Threshold Sharing Schemes Version 1.0	https://docs.oasis-open.org/sam/sam-tss/v1.0/os/sam-tss-v1.0-os.html			x			x	x		x				x													
2021	Common Security Advisory Framework Version 2.0	https://docs.oasis-open.org/csaf/csaf/v2.0/cs01/csaf-v2.0-cs01.html				x						x				x												
2017	CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2	http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/cs01/csaf-cvrf-v1.2-cs01.html				x						x				x												
2004	Application Vulnerability Description Language v1.0	https://www.oasis-open.org/committees/download.php/7145/AVDL%20Specification%20V1.pdf				x						x				x												
2021	CACAO Security Playbooks Version 1.0	https://docs.oasis-open.org/cacao/security-playbooks/v1.0/cs02/security-playbooks-v1.0-cs02.html				x						x				x												
2021	STIX™ Version 2.1	https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html				x						?				x						x						
2021	TAXII™ Version 2.1	https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html				x						?				x						x						
2020	Key Management Interoperability Protocol Specification Version 2.1	https://docs.oasis-open.org/kmip/kmip-spec/v2.1/os/kmip-spec-v2.1-os.html			x				x	x					x			x		x			x					
2020	Key Management Interoperability Protocol Profiles Version 2.1	https://docs.oasis-open.org/kmip/kmip-profiles/v2.1/os/kmip-profiles-v2.1-os.html			x				x	x					x			x		x			x					
2020	Key Management Interoperability Protocol Usage Guide Version 2.1	https://docs.oasis-open.org/kmip/kmip-ug/v2.1/kmip-ug-v2.1.html			x					x					x			x		x								
2020	PKCS #11 Cryptographic Token Interface Base Specification Version 3.0	https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/pkcs11-base-v3.0.html	x	x	x	x	x	x	x	x	x				x			x		x			x					
2020	PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0	https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/os/pkcs11-curr-v3.0-os.html	x	x	x	x	x	x	x	x	x				x			x		x			x					
2020	PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 3.0	https://docs.oasis-open.org/pkcs11/pkcs11-hist/v3.0/os/pkcs11-hist-v3.0-os.html	x	x	x	x	x	x	x	x	x				x			x		x			x					
2019	Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0	https://docs.oasis-open.org/dss-x/dss-core/v2.0/cs02/dss-core-v2.0-cs02.html	x	x	x	x	x	x	x	x																		
2019	Open Command and Control (OpenC2) Language Specification Version 1.0	https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html				x						x				x												
2019	Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0	https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html				x						x				x												
2019	Privacy Management Reference Model and Methodology (PMRM) Version 1.0	https://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html	x	x	x	x	x	x	x					x			x			x	x			x				
2019	Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0	https://docs.oasis-open.org/xspa/saml-xspa/v2.0/cs01/saml-xspa-v2.0-cs01.html			x			x		x								x										

			Verticals:							Research Challenges/Requirements in WP 5																			
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2017	Authentication Step-Up Protocol and Metadata Version 1.0	https://docs.oasis-open.org/trust-el/trust-el-protocol/v1.0/os/trust-el-protocol-v1.0-os.html			x					x		x						x										
2014	Basic Security Profile Version 1.1	http://docs.oasis-open.org/ws-brsp/BasicSecurityProfile/v1.1/cs01/BasicSecurityProfile-v1.1-cs01.pdf																										
2014	Electronic Identity Credential Trust Elevation Framework Version 1.0	http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/cs01/trust-el-framework-v1.0-cs01.pdf			x									x														
2013	eXtensible Access Control Markup Language (XACML) v3.0	https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html			x					x								x		x								
2015	XACML v3.0 Privacy Policy Profile Version 1.0	http://docs.oasis-open.org/xacml/3.0/privacy/v1.0/cs02/xacml-3.0-privacy-v1.0-cs02.html			x					x				x			x	x		x								
2012	Advanced Message Queuing Protocol (AMQP) Version 1.0 Part 5: Security	https://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-security-v1.0-os.html							x						x														
2011	Symmetric Key Services Markup Language (SKSML) Version 1.0	http://docs.oasis-open.org/ekmi/sksml/v1.0/cs02/SKSML-1.0-Specification.html	x	x	x	x	x	x	x						x					x								
2010	Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare v1.0	http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-os.html			x			x		x								x										
2009	Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare v1.0	http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-os.html			x			x		x								x										
2010	Service Provider Request Initiation Protocol and Profile Version 1.0	http://docs.oasis-open.org/security/saml/Post2.0/sstc-request-initiation-cs-01.html			x					x								x		x								
2009	Identity Metasystem Interoperability (IMI) v1.0	http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.html			x					x								x										
2008	Identity Provider Discovery Service Protocol and Profile	http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery-cs-01.html			x					x																		
2012	Approved Errata for SAML V2.0	https://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html			x					x								x		x								
2005	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf			x					x								x		x								
2005	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf			x					x								x		x								
2005	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf			x					x								x		x								
2005	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf			x					x								x		x								
2005	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf			x					x								x		x								
2005	Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf			x					x								x		x								
2005	Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf			x					x								x		x								

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
2005	Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0	https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf			x					x								x		x								
2006	Web Services Security: SOAP Message Security 1.1	https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf			x					x								x		x								
2009	Web Services Federation Language (WS-Federation) Version 1.2	https://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html			x					x								x		x								
2009	WS-SecurityPolicy 1.3	https://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.html			x					x								x		x								
2009	WS-SecureConversation 1.4	https://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.html			x					x								x		x								
2009	WS-Trust 1.4	https://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.html			x					x																		
	ITU-T Recommendations (specific)																											
	Y.4004 : Overview of smart oceans and seas, and requirements for their information and communication technology implementation	https://www.itu.int/rec/T-REC-Y.4004-202111-I					x		x			x			x													
	X.1060 : Framework for the creation and operation of a cyber defence centre	https://www.itu.int/rec/T-REC-X.1060-202106-I																			x	x						
	Y.4806 : Security capabilities supporting safety of the Internet of things	https://www.itu.int/rec/T-REC-Y.4806-201711-I							x		x	x		x	x					x								
	X.1641 : Guidelines for cloud service customer data security	https://www.itu.int/rec/T-REC-X.1641-201609-I												x						x								
	X.1642 : Guidelines for the operational security of cloud computing	https://www.itu.int/rec/T-REC-X.1642-201603-I													x					x								
	Y.2066 : Common requirements of the Internet of things	https://www.itu.int/rec/T-REC-Y.2066-201406-I.																										
	Y.4200 : Requirements for the interoperability of smart city platforms	https://www.itu.int/rec/T-REC-Y.4200-201802-I							x																			
	X.1500 : Revised structured cybersecurity information exchange techniques	https://www.itu.int/rec/T-REC-X.1500-201803-IIAmd12.									x	x						x		x		x						
	X.1362 : Simple encryption procedure for Internet of things (IoT) environments	https://www.itu.int/rec/T-REC-X.1362-201703-I											x	x	x													
	X.1363 : Technical framework of personally identifiable information handling system in Internet of things environment	https://www.itu.int/rec/T-REC-X.1363-202005-I											x	x	x													
	X.1365 : Security methodology for the use of identity-based cryptography in support of Internet of things (IoT) services over telecommunication networks	https://www.itu.int/rec/T-REC-X.1365-202003-I.											x	x	x													
	X.1258 : Enhanced entity authentication based on aggregated attributes	https://www.itu.int/rec/T-REC-X.1258-201609-I								x	x	x						x										
	X.1277 : Universal authentication framework	https://www.itu.int/rec/T-REC-X.1277-201811-I.								x	x	x						x										
	X.1054 : Information security, cybersecurity and privacy protection - Governance of information security	https://www.itu.int/rec/T-REC-X.1054-202104-I			x									x														
	ITU-T Recommendations series in general																											
	Y.4000-Y.4999: Internet of things and smart cities and communities								x						x													
	Y.4900-Y.4999: Evaluation and assessment								x			x			x	x		x										
	X.1000-X.1099: Information and network security										x																	
	X.1200-X.1299: Cyberspace security										x																	
	X.1250-X.1279: Identity management																											
	X.1600-X.1699: Cloud computing security																			x								

			Verticals:							Research Challenges/Requirements in WP 5																		
Year	Standard name	Link	Open Banking	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities	Authentication	ML and AI	Risk Management	Data de-identification	PII	IoT	ISMS	GDPR	Access control/ management	Conformance testing (WP7)	Cloud services	Security engineering (WP3)	Digital forensics	PKI	SDL (Task 3.3)	Threat assessment / Security evaluation	Data sharing	MPC	Biometrics
	X.1350-X.1369: Internet of things (IoT) security														x													