Cyber Security for Europe

D8.2

Project Standards Matrix

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	1.0

Related WP	WP8	Dissemination Level	PU
Lead Participant	CYBER	Lead Author	Liina Kamm (CYBER)
Contributing Beneficiaries	POLITO, AIT, GUF	Related Deliverables	D8.1

Abstract: The project standards matrix studies existing standards and ongoing standardisation projects in the context of the project topics and to connect experts to the standardisation process where they are needed. This deliverable contains the mapping of project topics to existing cybersecurity standards and standardisation projects. This will help the project partners to see which standards they need to consider in their work.

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 goal of the project standards matrix is to study existing standards and ongoing standardisation projects in the context of the project topics and to connect experts to the standardisation process where they are needed. This deliverable contains the mapping of project topics to existing cybersecurity standards and standardisation projects. The matrices in the document will allow the project partners to find the standards that are relevant to the verticals they are involved in, or to the topics that they are working on.

Document information

Contributors

Name	Partner
Liina Kamm	CYBER
Dan Bogdanov	CYBER
Sandhra-Mirella Valdma	CYBER

Reviewers

Name	Partner
Stephan Krenn	AFF
Antonio Lioy	POLITO
Ahad Niknia	GUF (high level review)

History

0.1	2019-01-09	Liina Kamm, Dan Bogdanov	v0.1 Draft for high level review
0.2	2020-01-13	Liina Kamm	v0.2 Minor editorial changes before the internal review
0.3	2020-01-29	Liina Kamm	v0.3 Incorporated comments from reviewers, corrected the template again
0.4	2020-01-30	Sandhra-Mirella Valdma	v0.4 Added references to standards (Annex 1)
1.0	2020-01-31	Liina Kamm	v1.0 Final version

List of Contents

List of Tables

List of Acronyms

CD	Committee Draft
DIS	Draft International Standard
ECSO	European Cyber Security Organization
EDPB	European Data Protection Board
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
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
JTC	Joint Technical Committee
NIST	National Institute of Standards and Technology
NWIP	New Work Item Proposal
PDTS	Preliminary Draft Technical Specification
PII	Personally Identifiable Infromation
SC	Subcommittee
SP	Study Period
TR	Technical Report
TS	Technical Specification
WD	Working Draft
WG	Working Group

1 Introduction

This deliverable presents the project standards matrices. These matrices contain privacy, and cybersecurity standards from ISO/IEC, CEN/CENELEC and ETSI that are relevant to the CyberSec4Europe verticals and research topics. All of these standards have been studied and mapped to the CyberSec4Europe 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 topic. This deliverable has been compiled foremost to direct the attention of the project partners to the standards and technical reports that could be relevant in their vertical or research topic so that they can more quickly find the necessary information. We studied cybersecurity and privacy standards from ISO/IEC, CEN/CENELEC and ETSI, and mapped their topics to the verticals and research topics of CyberSec4Europe.

On the other hand, all of the pilot competence centres include many capable specialists whose expertise can be a great benefit to the standardisation projects that are still being compiled. For this reason, we also included draft projects from ISO/IEC in the matrices. CyberSec4Europe has applied for liaison status in ISO/IEC JTC1/SC27 WG2 and WG5. If these requests are approved, CyberSec4Europe can contribute the research results and insights that have been gathered throughout the project to the standards that are under development. As 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.

Section 2 of this deliverable discusses the methodology for compiling the standards matrices. Section 3 includes the project standards matrices.

2 Methodology

We have mapped cybersecurity standards to two categories of topics. First, much of the work in CyberSec4Europe (WP4, WP5) is done based on the needs of 7 stakeholder 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 involved partners stay informed about the relevant standards that could be used when solving the security and privacy issues of their field. The tables in Section 3.1 describe these mappings. The verticals that CyberSec4Europe focuses on are the following (the summaries are taken from the CyberSec4Europe Description of Action).

- **E-commerce**. 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, WP7) of CyberSec4Europe to the main topics covered by different standards. This way, the partners who

are working on solving these research challenges can have an overview of the applicable standards. The tables in Section 3.2 describe these mappings. The research challenges that we identified as relevant to the project are the following (the parenthesis has the abbreviation that we use in the table header for layout considerations):

- authentication (Auth.),
- machine learning and artificial intelligence (ML and AI),
- risk management (Risk Mgmt.),
- data de-identification (Data De-ident.),
- personally identifiable information (PII),
- Internet of things (IoT),
- information security management system (ISMS),
- General Data Protection Regulation (GDPR),
- access control/management (Access Control/Mgmt.),
- conformance testing (WP7),
- cloud services,
- security engineering (WP3) (Security Eng. (WP3)),
- digital forensics,
- public key infrastructure (PKI), and
- software development lifecycle (Task 3.3) (SDL (T3.3)).

We have included standards from

- ISO/IEC JTC1/SC27 (Information security, cybersecurity and privacy protection) [1],
- CEN/CENELEC JTC 13 (Cybersecurity and Data Protection) [2], and
- ETSI privacy and security [3], [4].

ISO/IEC was chosen because several partners of CyberSec4Europe are actively participating in ISO/IEC JTC1/SC27 and these standards are among the most used worldwide. As only standards developed by the CEN/CENELEC and ETSI are recognized as European Standards, we also included these standards in the deliverable. However, most of the CEN/CENELEC JTC13 standards are mirrored from ISO/IEC standards, so these are not explicitly featured in the matrices. Further information about the standardisation organisations can be found in Deliverable 8.1.

In the mapping process, we have also taken into account ISO/IEC JTC1/SC27 standard projects, ETSI ongoing standard projects and one CEN/CENELEC JTC13 draft. We include these unfinished standards in the hope that CyberSec4Europe partners can comment and give additional practical insight on the standards in progress and, thereby, help improve them. A new ISO/IEC JTC1/SC27 standard project starts with a study period (SP), then goes on to become a new work item proposal (NWIP). After that there come the working draft (WD), committee draft (CD), draft international standard (DIS) and final draft international standard (FDIS). A preliminary draft technical specification (PDTS) preceeds the finalisation of a technical specification (TS).

Furthermore, we direct the attention of all partners to the document EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[1] which gives general guidance on the obligation of Data Protection by Design and by Default (Article 25 of GDPR), which requires data controllers to implement appropriate technical and organisational measures to protect the rights and freedoms of data subjects.

In addition, we found three specific guidelines and standards that are not cybersecurity related but instead have surfaced as important vertical specific documents that need to be considered during research into these areas. These are

- the IALA Guideline 1082 – An Overview of AIS[2] (maritime transport vertical),
- the IALA Guideline 1117 – VDES Overview[3] (maritime transport vertical), and
- the HL7® - FHIR® standard for health care data exchange[4] (the medical data exchange vertical).

2.1 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.

[1] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en
[2] https://www.iala-aism.org/product/an-overview-of-ais-1082/
[3] https://www.iala-aism.org/product/vhd-data-exchange-system-vdes-overview-1117/
[4] https://www.hl7.org/fhir/

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 Project Standards Matrix

We present this deliverable as several matrices for layout reasons. The project standards matrix is also available as a single matrix as an Excel file. The tables are the following.

1. Table 1 contains the mapping of ISO/IEC and ETSI standards to project verticals.
2. Table 2 contains the mapping of ongoing standard projects to project verticals.
3. Table 3 contains the mapping of ISO/IEC and ETSI standards to research challenges of the project.
4. Table 4 contains the mapping of ongoing standard projects research challenges of the project.

3.1 Standards Mapped to Project Verticals

Standard Number and Name	E-Commerce	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities
ISO/IEC 15443 Security assurance framework Parts 1 and 2 [5], [6]		x					
ISO/IEC 15816 Security information objects for access control [7]				x			
ISO/IEC 19790 Security requirements for cryptographic modules [8]	x	x	x	x	x	x	x
ISO/IEC 20008 Anonymous digital signatures Part 1, 2, 3 [9], [10]			x				
ISO/IEC 20009 Anonymous Entity authentication Part 1, 2, 4 [11], [12], [13]			x				
ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques [14]	x		x	x	x	x	x
ISO/IEC 24760 A framework for identity management Parts 1, 2, 3 [15], [16], [17]	x	x	x	x	x	x	x
ISO/IEC 27032 Guidelines for cybersecurity [18]	x	x	x	x	x	x	x
ISO/IEC 27035 Information security incident management Parts 1, 2 [19], [20]				x			
ISO/IEC 27036 Information security for supplier relationships, parts 1, 2, 3 [21], [22], [23]		x					

Standard Number and Name	E-Commerce	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities
ISO/IEC 27036-4 Information security for supplier relationships - Part 4: Guidelines for security of cloud services [24]		x					
ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence [25]				x			
ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence [26]				x			
ISO/IEC 27103 Cybersecurity and ISO and IEC Standards [27]	x	x	x	x	x	x	x
ISO/IEC TR 27550 Privacy engineering for system life cycle processes [28]	x		x			x	x
ISO/IEC 29100 Privacy framework [29]	x		x		x	x	
ISO/IEC 29101 Privacy architecture framework [30]	x		x		x	x	
ISO/IEC 29134 Guidelines for privacy impact assessment [31]	x	x	x		x	x	x
ISO/IEC 29147 Vulnerability disclosure [32]				x			
ISO/IEC 29151 Code of practice for personally identifiable information protection [33]	x		x	x		x	x
ISO/IEC 29190 Privacy capability assessment model [34]	x		x		x	x	x

Standard Number and Name	E-Commerce	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities
ISO/IEC 30111 Vulnerability handling processes [35]				x			
ETSI GS ISG ISI Series (Information security indicators, security event management) [36]				x			
ETSI TR 103 644 Increasing smart meter security [37]							x
ETSI TR 103 331 Structured threat information sharing [38]				x			
ETSI TR 103 304 Personally Identifiable Information (PII) Protection in mobile and cloud services [39]	x		x			x	x
ETSI TR 103 306 Global Cyber Security Ecosystem [40]	x	x	x	x	x	x	x

Table 1: Mapping of ISO/IEC and ETSI standards to project verticals

Standard Project Name (and number if available)	E-Commerce	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities
ISO/IEC CD 20009-3 Anonymous Entitiy authentication - Part 3 Mechanisms based on blind signatures [41]			x				
ISO/IEC DIS 23264-1 Redaction of authentic data - Part 1: General [42]			x				
ISO/IEC WD 23264-2 Redaction of authentic data - Part 2: Redactable signature schemes based on asymmetric mechanisms [43]			x				
ISO/IEC CD 27030 Guidelines for security and privacy in Internet of Things (IoT) [44]	x	x			x	x	x
ISO/IEC DIS 27035-3 Information security incident management - Part 3: Guidelines for ICT incident response operations [45]				x			
ISO/IEC CD 27099 Public key infrastructure — Practices and policy framework [46]					x		
ISO/IEC DIS 27551 Requirements for attribute-based unlinkable entity authentication [47]			x				
ISO/IEC CD 27555 Establishing a PII deletion concept in organizations [48]	x		x			x	x

Standard Project Name (and number if available)	E-Commerce	Supply Chain Security Assurance	Privacy-Preserving Identity Management	Incident reporting	Maritime Transport	Medical Data Exchange	Smart Cities
ISO/IEC WD 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences [49]	x		x			x	x
ISO/IEC PDTS 27570 Privacy guidelines for smart cities [50]							x
ISO/IEC WD 29115 Entity authentication assurance framework [51]			x				
ISO/IEC SP on Impact of artificial intelligence on privacy	x					x	x
ISO/IEC SP on Additional privacy-enhancing data de-identification standards	x			x	x	x	x
ISO/IEC SP on privacy for fintech services	x						
CEN/CENELEC JT013025 Data protection and privacy by design and by default	x	x	x	x	x	x	x
ETSI DTS/CYBER-0013 (TS 103 485) Privacy assurance and verification			x				
ETSI DTS/CYBER-0014 (TS 103 486) Identity Management and Discovery for IoT			x				

Table 2: Mapping of ongoing standard projects to project verticals.

3.2 Standards Mapped to Research Challenges

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC 15443 Security assurance framework Parts 1 and 2 [5], [6]			x												
ISO/IEC 15816 Security information objects for access control [7]									x						
ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing [52]										x					
ISO/IEC 19086-4 Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII [53]					x		x	x			x				
ISO/IEC 19790 Security requirements for cryptographic modules [8]	x			x						x		x			
ISO/IEC 20008 Anonymous digital signatures Part 1, 2, 3 [9], [10],	x														
ISO/IEC 20009 Anonymous Entitiy	x														

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
authentication Part 1, 2, 4 [11], [12], [13]															
ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques [14]				x	x			x							
ISO/IEC 21827 Systems Security Engineering — Capability Maturity Model® (SSE-CMM®) [54]												x			x
ISO/IEC 24759 Test requirements for cryptographic modules [55]										x					
ISO/IEC 24760 A framework for identity management Parts 1, 2, 3 [15], [16], [17]									x						
ISO/IEC 27001 Information security management [56]							x								
ISO/IEC 27002 Code of practice for information security controls [57]							x								
ISO/IEC 27003 Information security management systems [58]							x								

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC 27005 Information security risk management [59]			x				x								
ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [60]					x		x				x				
ISO/IEC 27032 Guidelines for cybersecurity [18]							x		x						
ISO/IEC 27035 Information security incident management Parts 1, 2 [19], [20]							x								
ISO/IEC 27036 Information security for supplier relationships, parts 1, 2, 3 [21], [22], [23]							x								
ISO/IEC 27036-4 Information security for supplier relationships - Part 4: Guidelines for security of cloud services [24]							x				x				
ISO/IEC 27037 Guidelines for identification, collection, acquisition							x						x		

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
and preservation of digital evidence [25]															
ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence [26]							x						x		
ISO/IEC TR 27550 Privacy engineering for system life cycle processes [28]			x		x			x							x
ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management [61]					x		x	x							
ISO/IEC 29100 Privacy framework [29]					x			x							
ISO/IEC 29101 Privacy architecture framework [30]					x			x							
ISO/IEC 29134 Guidelines for privacy impact assessment [31]					x			x							
ISO/IEC 29146 A framework for access management [62]									x						
ISO/IEC 29147 Vulnerability disclosure [32]													x		

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC 29151 Code of practice for personally identifiable information protection [33]					x										
ISO/IEC 29190 Privacy capability assessment model [34]			x												
ISO/IEC 30111 Vulnerability handling processes [35]													x		
ETSI GS ISG ISI Series (Information security indicators, security event management) [36]													x		
ETSI EN 303 645 Cyber Security for Consumer Internet of Things [63]						x									
ETSI TR 103 304 Personally Identifiable Information (PII) Protection in mobile and cloud services [39]					x			x			x				
ETSI TR 103 306 Global Cyber Security Ecosystem [40]			x									x			
ETSI TS 103 458 Application of Attribute Based Encryption (ABE) for					x				x		x				

Standard Number and Name	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements [64]															
ETSI TS 103 532 Attribute Based Encryption for Attribute Based Access Control [65]									x						

Table 3: Mapping of ISO/IEC and ETSI standards to research challenges of the project.

Standard Project Name (and number if available)	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC CD 20009-3 Anonymous Entitiy authentication - Part 3 Mechanisms based on blind signatures [41]	x														
ISO/IEC DIS 23264-1 Redaction of authentic data - Part 1: General [42]	x														
ISO/IEC WD 23264-2 Redaction of authentic data - Part 2: Redactable signature schemes based on asymmetric mechanisms [43]	x														
ISO/IEC CD 27030 Guidelines for security and privacy in Internet of Things (IoT) [44]						x		x				x			
ISO/IEC DIS 27035-3 Information security incident management - Part 3: Guidelines for ICT incident response operations [45]							x								
ISO/IEC CD 27099 Public key infrastructure — Practices and policy framework [46]							x							x	

Standard Project Name (and number if available)	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC WD TS 27100 Cybersecurity — Overview and concepts [66]							x								
ISO/IEC CD TS 27101 Cybersecurity — Framework development guidelines [67]							x								
ISO/IEC DIS 27551 Requirements for attribute-based unlinkable entity authentication [47]	x														
ISO/IEC CD 27555 Establishing a PII deletion concept in organizations [48]					x		x	x							
ISO/IEC WD 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences [49]					x			x	x						
ISO/IEC PDTS 27570 Privacy guidelines for smart cities [50]		x		x	x			x	x			x			
ISO/IEC WD 29115 Entity authentication assurance framework [51]	x														

Standard Project Name (and number if available)	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ISO/IEC SP on Impact of artificial intelligence on privacy		x	x		x		x								
ISO/IEC SP on Additional privacy-enhancing data de-identification standards				x	x		x								
ISO/IEC SP on privacy for fintech services	x	x							x		x				
ISO/IEC NWIP on Organizational Privacy Risk Management			x				x	x							
CEN/CENELEC JT013025 Data protection and privacy by design and by default					x			x				x			x
ETSI DTS/CYBER-0013 (TS 103 485) Privacy assurance and verification					x										
ETSI DTS/CYBER-0014 (TS 103 486) Identity Management and Discovery for IoT	x					x									
ETSI RTS/CYBER-0049 (TS 103 645) Securing Consumer IoT [68]						x									

Standard Project Name (and number if available)	Auth.	ML and AI	Risk Mgmt.	Data De-ident.	PII	IoT	ISMS	GDPR	Access Control/ Mgmt.	Conformance testing (WP7)	Cloud Services	Security Eng. (WP3)	Digital forensics	PKI	SDL (T3.3)
ETSI DTS/CYBER-0050 (TS 103 701) Cybersecurity assessment for consumer IoT products						x									

Table 4: Mapping of ongoing standard projects to research challenges of the project.

4 Further Work

This deliverable will have an updated version in Deliverable 8.5 at the end of the project. For that we will also include insights into how this deliverable has been used during the project and which of the standards projects we have been able to disseminate our results to.

For Deliverable 8.5, we will more thoroughly map out the skill sets of the consortium (and other competence centres). Using questionnaires, we will study partners' attitudes towards using standards during their work. We will also collaborate with Task 7.3 (Certification – methodologies, tools and infrastructures) and Task 3.8 (Conformity, Validation and Certification).

Contributions to existing standards will be proposed through liaisons with standardisation bodies. Standardisation activities from other competence centres will also be considered.

Research topics described in Deliverable 3.2 will also be mapped to standards. As the D3.2 was finalised at M11, Deliverable 8.2 does not yet hold this mapping.

5 References

[1] "Standards by ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection," [Online]. Available: https://www.iso.org/committee/45306/x/catalogue/ and https://www.din.de/en/meta/jtc1sc27.

[2] "CEN/CLC/JTC 13 - Cybersecurity and Data Protection," [Online]. Available: https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B.

[3] "ETSI standards," [Online]. Available: https://www.etsi.org/standards#page=1&search=&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-01-09&harmonized=0&keyword=&TB=824,,755&stdType=&frequency=&mandate=&collection=&sort=1.

[4] "ETSI TR 103 370 Practical introductory guide to Technical Standards for Privacy," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103370/01.01.01_60/tr_103370v010101p.pdf.

[5] "ISO/IEC 15443 Security assurance framework Part 1," [Online]. Available: https://www.iso.org/standard/59138.html.

[6] "ISO/IEC 15443 Security assurance framework Part 2," [Online]. Available: https://www.iso.org/standard/59140.html.

[7] "ISO/IEC 15816 Security information objects for access control," [Online]. Available: https://www.iso.org/standard/29139.html.

[8] "ISO/IEC 19790 Security requirements for cryptographic modules," [Online]. Available: https://www.iso.org/standard/52906.html.

[9] "ISO/IEC 20008 Anonymous digital signatures Part 1," [Online]. Available: https://www.iso.org/standard/57018.html.

[10] "ISO/IEC 20008 Anonymous digital signatures Part 2," [Online]. Available: https://www.iso.org/standard/56916.html.

[11] "ISO/IEC 20009 Anonymous Entity authentication Part 1," [Online]. Available: https://www.iso.org/standard/57079.html.

[12] "ISO/IEC 20009 Anonymous Entity authentication Part 2," [Online]. Available: https://www.iso.org/standard/56913.html.

[13] "ISO/IEC 20009 Anonymous Entity authentication Part 4," [Online]. Available: https://www.iso.org/standard/64288.html.

[14] "ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques," [Online]. Available: https://www.iso.org/standard/69373.html.

[15] "ISO/IEC 24760 A framework for identity management Part 1," [Online]. Available: https://www.iso.org/standard/77582.html.

[16] "ISO/IEC 24760 A framework for identity management Part 2," [Online]. Available: https://www.iso.org/standard/57915.html.

[17] "ISO/IEC 24760 A framework for identity management Part 3," [Online]. Available: https://www.iso.org/standard/57916.html.

[18] "ISO/IEC 27032 Guidelines for cybersecurity," [Online]. Available: https://www.iso.org/standard/44375.html.

[19] "ISO/IEC 27035 Information security incident management Part 1," [Online]. Available: https://www.iso.org/standard/60803.html.

[20] "ISO/IEC 27035 Information security incident management Part 2," [Online]. Available: https://www.iso.org/standard/62071.html.

[21] "ISO/IEC 27036 Information security for supplier relationships, part 1," [Online]. Available: https://www.iso.org/standard/59648.html.

[22] "ISO/IEC 27036 Information security for supplier relationships, part 2," [Online]. Available: https://www.iso.org/standard/59680.html.

[23] "ISO/IEC 27036 Information security for supplier relationships, part 3," [Online]. Available: https://www.iso.org/standard/59688.html.

[24] "ISO/IEC 27036-4 Information security for supplier relationships - Part 4: Guidelines for security of cloud services," [Online]. Available: https://www.iso.org/standard/59689.html.

[25] "ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence," [Online]. Available: https://www.iso.org/standard/44381.html.

[26] "ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence," [Online]. Available: https://www.iso.org/standard/44406.html.

[27] "ISO/IEC 27103 Cybersecurity and ISO and IEC Standards," [Online]. Available: https://www.iso.org/standard/72437.html.

[28] "ISO/IEC TR 27550 Privacy engineering for system life cycle processes," [Online]. Available: https://www.iso.org/standard/72024.html.

[29] "ISO/IEC 29100 Privacy framework," [Online]. Available: https://www.iso.org/standard/45123.html.

[30] "ISO/IEC 29101 Privacy architecture framework," [Online]. Available: https://www.iso.org/standard/75293.html.

[31] "ISO/IEC 29134 Guidelines for privacy impact assessment," [Online]. Available: https://www.iso.org/standard/62289.html.

[32] "ISO/IEC 29147 Vulnerability disclosure," [Online]. Available: https://www.iso.org/standard/72311.html.

[33] "ISO/IEC 29151 Code of practice for personally identifiable information protection," [Online]. Available: https://www.iso.org/standard/62726.html.

[34] "ISO/IEC 29190 Privacy capability assessment model," [Online]. Available: https://www.iso.org/standard/45269.html.

[35] "ISO/IEC 30111 Vulnerability handling processes," [Online]. Available: https://www.iso.org/standard/69725.html.

[36] "ETSI GS ISG ISI Series (Information security indicators, security event management)," [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ISI/001_099/003/01.02.01_60/gs_ISI003v010201p.pdf.

[37] "ETSI TR 103 644 Increasing smart meter security," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103644/01.01.01_60/tr_103644v010101p.pdf.

[38] "ETSI TR 103 331 Structured threat information sharing," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.02.01_60/tr_103331v010201p.pdf.

[39] "ETSI TR 103 304 Personally Identifiable Information (PII) Protection in mobile and cloud services," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf.

[40] "ETSI TR 103 306 Global Cyber Security Ecosystem," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.03.01_60/tr_103306v010301p.pdf.

[41] "ISO/IEC CD 20009-3 Anonymous Entity authentication - Part 3 Mechanisms based on blind signatures," [Online]. Available: https://www.iso.org/standard/78813.html.

[42] "ISO/IEC DIS 23264-1 Redaction of authentic data - Part 1: General," [Online]. Available: https://www.iso.org/standard/78341.html.

[43] "ISO/IEC WD 23264-2 Redaction of authentic data - Part 2: Redactable signature schemes based on asymmetric mechanisms," [Online]. Available: https://www.iso.org/standard/78342.html.

[44] "ISO/IEC CD 27030 Guidelines for security and privacy in Internet of Things (IoT)," [Online]. Available: https://www.iso.org/standard/44373.html.

[45] "ISO/IEC DIS 27035-3 Information security incident management - Part 3: Guidelines for ICT incident response operations," [Online]. Available: https://www.iso.org/standard/74033.html.

[46] "ISO/IEC CD 27099 Public key infrastructure — Practices and policy framework," [Online]. Available: https://www.iso.org/standard/56590.html.

[47] "ISO/IEC DIS 27551 Requirements for attribute-based unlinkable entity authentication," [Online]. Available: https://www.iso.org/standard/72018.html.

[48] "ISO/IEC CD 27555 Establishing a PII deletion concept in organizations," [Online]. Available: https://www.iso.org/standard/71673.html.

[49] "ISO/IEC WD 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences," [Online]. Available: https://www.iso.org/standard/71674.html.

[50] "ISO/IEC PDTS 27570 Privacy guidelines for smart cities," [Online]. Available: https://www.iso.org/standard/71678.html.

[51] "ISO/IEC WD 29115 Entity authentication assurance framework," [Online]. Available: https://www.iso.org/standard/73909.html.

[52] "ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing," [Online]. Available: https://www.iso.org/standard/62286.html.

[53] "ISO/IEC 19086-4 Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII," [Online]. Available: https://www.iso.org/standard/68242.html.

[54] "ISO/IEC 21827 Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)," [Online]. Available: https://www.iso.org/standard/44716.html.

[55] "ISO/IEC 24759 Test requirements for cryptographic modules," [Online]. Available: https://www.iso.org/standard/72515.html.

[56] "ISO/IEC 27001 Information security management," [Online]. Available: https://www.iso.org/standard/54534.html.

[57] "ISO/IEC 27002 Code of practice for information security controls," [Online]. Available: https://www.iso.org/standard/54533.html.

[58] "ISO/IEC 27003 Information security management systems," [Online]. Available: https://www.iso.org/standard/63417.html.

[59] "ISO/IEC 27005 Information security risk management," [Online]. Available: https://www.iso.org/standard/75281.html.

[60] "ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors," [Online]. Available: https://www.iso.org/standard/76559.html.

[61] "ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management," [Online]. Available: https://www.iso.org/standard/71670.html.

[62] "ISO/IEC 29146 A framework for access management," [Online]. Available: https://www.iso.org/standard/45169.html.

[63] "ETSI EN 303 645 Cyber Security for Consumer Internet of Things," [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf.

[64] "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," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf.

[65] "ETSI TS 103 532 Attribute Based Encryption for Attribute Based Access Control," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103500_103599/103532/01.01.01_60/ts_103532v010101p.pdf.

[66] "ISO/IEC WD TS 27100 Cybersecurity — Overview and concepts," [Online]. Available: https://www.iso.org/standard/72434.html.

[67] "ISO/IEC CD TS 27101 Cybersecurity — Framework development guidelines," [Online]. Available: https://www.iso.org/standard/72435.html.

[68] "ETSI RTS/CYBER-0049 (TS 103 645) Securing Consumer IoT," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.