Impulse

Identity Management in PUbLic SErvices

D3.4 Standards and related impacts and implications

Lead Authors: Madlen Schmudde, René Lindner
With contributions from: Francesca Morpurgo, Guillermo Otaduy, Iria Nuñez, Javier Gutiérrez Meana, Luca Boldrin, Xavier Martinez, Kais Dai, Jaime Loureiro Acuña
Reviewer: [Luca Boldrin (ICERT), Jesús Alonso (TREE)]

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	31-01-2023
Version:	1.0
Total number of pages:	56
Keywords:	Standard, CEN, ISO, standardization landscape, standardization activities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

Task 3.4 - *Analysis of existing relevant standards, and related impacts and implications* is one of the tasks of WP3 - *Multidisciplinary analysis of standards, legal and ethical implications*. The present deliverable D3.4 summarizes the main results of Task 3.4 which also form the basis for Task 7.6 - *Initiation of standardization activities*. This deliverable provides a general summary of the basic knowledge regarding standardization in order to bring the consortium on a uniform level in this respect. Nevertheless, the focus of this deliverable is on the standardization landscape which is relevant to the IMPULSE project.

In a first step, the methodology of the standards research conducted is described. With essential keywords provided by the consortium and already known relevant technical committees, a search for standards with a strong link to IMPULSE and consequently AI, blockchain, and eID was conducted. Not only formal standards were included in the standards overview but also so-called informal standards, which also are of high importance for the development of the technical solutions within IMPULSE. The standards found were evaluated by the partners in terms of their relevance to the project, with 397 out of 623 formal standards rated as relevant to the project. An overview of the relevant formal standards was provided in form of a dashboard which, besides providing a summary on relevant aspects regarding project related standards, allows consortium members to search for specific standards by using keywords.

Since the focus of this deliverable is on formal standards, the dashboard was also used within this deliverable to provide an overview of the standardization landscape related to IMPULSE. The different technical committees on international, European, and national level which are responsible for the development of the highlighted standards are described. Special focus was put on the European technical committees since European R&I projects like IMPULSE can also take the opportunity to contribute to ongoing standardization activities which is important in the context of Task 7.6 of IMPULSE. Therefore, active work items of CEN TC 224 - *Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment*, CEN-CLC/JTC 19 - *Blockchain and Distributed Ledger Technologies*, and CEN-CLC/JTC 21 - *Artificial Intelligence* are listed. Furthermore, nine formal standards were highlighted as highly relevant to the project, which is why they are described and examined regarding their relation to IMPULSE in more detail. Due to their great importance to the project and their relevance to other developers outside the IMPULSE consortium, these standards were listed on the IMPULSE website with some explanations.

In addition to formal standards, informal standards also play an important role in the development of the IMPULSE solution. Therefore, relevant organizations which develop these standards are also described. Out of 104 informal standards which were found on the organizations websites provided by the IMPULSE partners, 89 were rated as relevant to the project by the consortium. Six standards were categorized as highly relevant, which is why they are also examined in more detail regarding their content and their relevance to IMPULSE. These informal standards are also listed on the IMPULSE website.

All this information about standardization and the evaluation of standards have raised awareness within the IMPULSE consortium for the opportunities which standardization can provide for R&I projects. This is the essential basis for the initiation of standardization activities and therefore the integration of project result in standardization, which is what Task 7.6 of this project is about.

Document information

Grant agreement No.	**101004459**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	www.impulse-h2020.eu		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D3.4	**Title**	Standards and related impacts and implications
Work package	**Number**	WP3	**Title**	Multidisciplinary analysis of standards, legal and ethical implications
Task	**Number**	T3.4	**Title**	Analysis of existing relevant standards and related impacts and implications

Date of delivery	**Contractual**	M24	**Actual**	M24
Status	version 1.0		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	DIN, CEL, ALiCE, GRAD, TREE, ICERT			
Responsible author	**Name**	Madlen Schmudde		
	Partner	DIN	**E-mail**	madlen.schmudde@din.de

Summary **(for dissemination)**	*The main aim of this task is to create a well-grounded documentation of the current technical standards related to the IMPULSE project, mainly to be used as framework for the co-creative design of IMPULSE and the piloting to ensure the compliance with the prior art. Therefore, a collection of relevant standardisation activities with focus on standards regarding digital identification and authentication will be initially conducted. This flows into a deep examination of standards concerning data privacy and data protection, for example, storing, transfer, change or deletion of personal data by ETSI/CEN and ISO to identify and document the requirements on a secure handling of personal data in the context of GDPR. This will also include a concise overview about related standards in the field of digital preservation, information security and trustworthiness of digital transactions and records (e.g. ISO TC46, ISO-27k, CCDS etc.) due to the possibility to store digital identities in IMPULSE but also the related content itself and so the need to preserve confidentiality, integrity and availability. Regarding the fact that IMPULSE is blockchain-based it is necessary to analyse the standardisation of ISO/TC 307 too, where the main worldwide standards for blockchain are under construction. To achieve also national standards and best practices relevant for the implementation of IMPULSE and/or the piloting, the analysis will identify in collaboration with the pilots the relevant guidelines for analysation of relevance and impacts like possible objections compared to international standards including the management of this gap by adopting the international standards. The final documentation will be used as framework for the co-creative design of IMPULSE as mentioned but also – in collaboration with the co-creative design process and the design of IMPULSE itself – (i) to close the gaps between building blocks of IMPULSE and the standards before implementation of basic system and pilot but also (ii) to identify needs for further changes in the scope of standardisation to enable the utilisation of disruptive technologies for public services like a blockchain-based eID solution.*
Keywords	*Standard, CEN, ISO, standardization landscape, standardization activities*

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
24-11-2021	**0.1**	**Madlen Schmudde**	**Structure and first draft**
05-2022	**0.2**	**Madlen Schmudde**	**Integration of the input from partners**
08-12-2022	**0.3**	**Madlen Schmudde**	**Update and further completion**
21-12-2022	**0.4**	**Madlen Schmudde**	**Integration of input from partners, Addition of Executive Summary and Summary and Conclusion**
19-01-2023	**1.0**	**Madlen Schmudde**	**Integration of the comments from the internal review and language enhancement**

Table of contents

List of tables

List of figures

Abbreviations and acronyms

AI	*Artificial Intelligence*
ANSI	*American National Standards Institute*
ASME	*American Society of Mechanical Engineers*
ASTM	*American Society for Testing and Material*
BC	*Blockchain*
BSI	*British Standards Institution, Federal Office for Information Security*
CEN	*European Committee for Standardization*
CEN-CLC/JTC	*CEN-CENELEC Joint Technical Committee*
CENELEC	*European Committee for Electrotechnical Standardization*
CWA	*CEN Workshop Agreement*
DID	*Decentralized Identifier Documents*
DIF	*the Decentralized Identity Foundation*
DIN	*German Institute for Standardization*
DKE	*German Commission for Electrotechnical, Electronic, and Information Technologies of DIN and VDE*
DLT	*Distributed Ledger Technology*
EBSI	*European Blockchain Services Infrastructure*
EFTA	*European Free Trade Association*
eID	*electronic IDentification*
eIDAS	*electronic IDentification, Authentication and trust Services*
EN standard	*European standard*
ESI	*Electronic Signatures and Infrastructures*
ESSIF	*European self-sovereign identity framework*
ETSI	*European Telecommunications Standards Institute*
EU	*European Union*
GDPR	*General Data Protection Regulation*
ICS	*International Classification for Standards*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
IP	*Identity Provider*
ITU	*International Telecommunication Union*
IWA	*International Workshop Agreement*
JTC	*Joint Technical Committee*
NIST	*National Institute of Standards and Technology*
NSB	*National Standardization Body*
R&I	*Research and Innovation*
SAI	*Securing Artificial Intelligence*
SC	*Subcommittee*
SDO	*Standards Developing Organization*
SSI	*Self Sovereign Identity*
TC	*Technical Committee*
TR	*Technical Report*
TS	*Technical Specification*
UK	*United Kingdom*
UL	*Underwriter Laboratories*
UMTS	*Universal Mobile Telecommunications System*
UNE	*Spanish Association for Standardization*
US	*United States*
VDI	*Association of German Engineers*
VDMA	*Mechanical Engineering Industry Association*
W3C	*World Wide Web Consortium*
WG	*Working Group*
WP	*Work Package*

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101004459

1 Introduction

1.1 Background and Objective

Standardization[1] is of great importance both at national and European level. Although European standardization activities are in the foreground in the H2020-funded research project IMPULSE, international and also relevant national standards are presented, as a transnational harmonization of standardization documents is considered highly relevant and is the basis for the common economic area in the European Union.

The IMPULSE project is about improving digital public services by combining two disruptive technologies, Blockchain and Artificial Intelligence (AI), on electronic identities (eID). Thus, it is essential to ensure the applicability, trust, and compliance of electronic identity management solutions for access to public services. Therefore, it is a necessity that the IMPULSE solutions are compliant with standards, technical specifications, and procedures. This is a crucial aspect to guarantee that the developed system is working properly and the project results are trustworthy. For this reason, IMPULSE has integrated standardization as an essential element in the project. Regarding the working structure of IMPULSE (Figure 1) standardization is integrated in two work packages, namely WP3 and WP7, in two tasks.

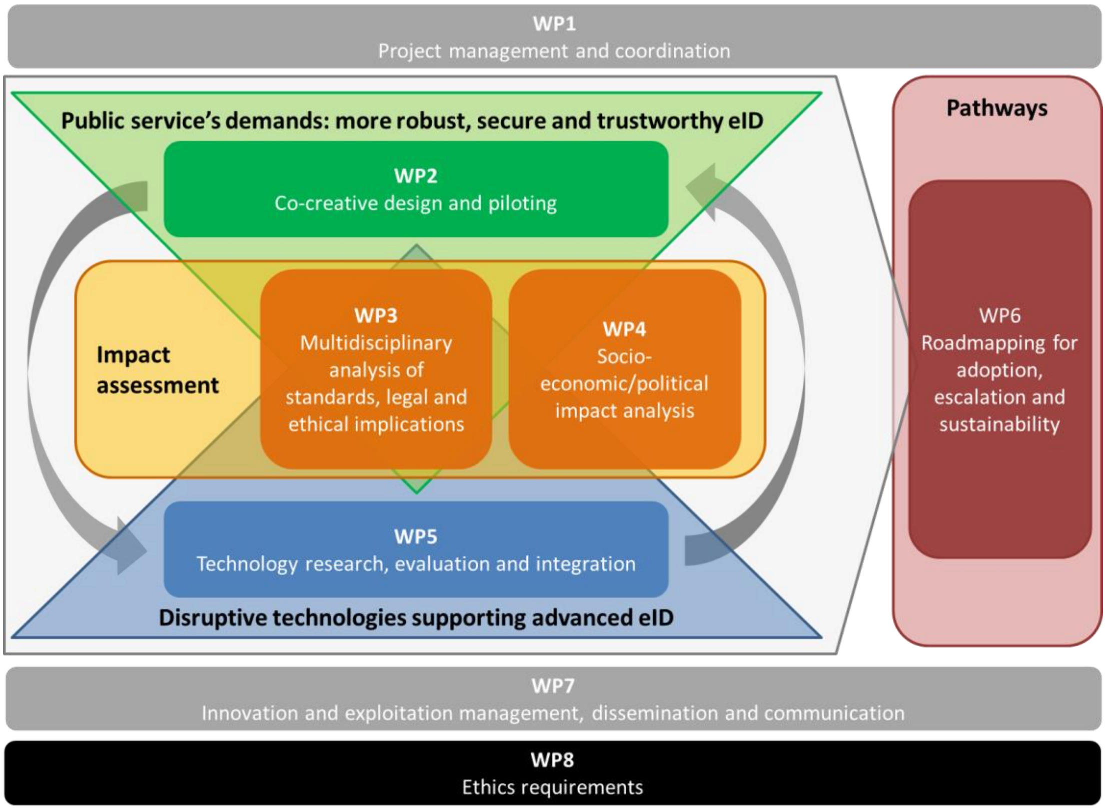

WP1
Project management and coordination
Public service's demands: more robust, secure and trustworthy eID
WP2
Co-creative design and piloting
Impact assessment
WP3
Multidisciplinary analysis of standards, legal and ethical implications
WP4
Socio-economic/political impact analysis
WP5
Technology research, evaluation and integration
Disruptive technologies supporting advanced eID
Pathways
WP6
Roadmapping for adoption, escalation and sustainability
WP7
Innovation and exploitation management, dissemination and communication
WP8
Ethics requirements

Figure 1: The working structure of IMPULSE

In WP 3 - *Multidisciplinary analysis of standards, legal and ethical implications* Task 3.4 - *Analysis of existing relevant standards, and related impacts and implications* is integrated. The objective of this task is to create a well-grounded documentation of the current standards and standardization documents related to the IMPULSE project. This will provide an overview of the state of the art of the standardization landscape that is relevant for IMPULSE and therefore ensure the compliance of the project's results with what is already on the market. The knowledge about existing standards is of importance for the IMPULSE consortium to align their products, processes, services, and solutions to the current state of the art. The present deliverable D3.4, belonging to Task 3.4, delivers an overview of the standardization landscape and highlights the most relevant standards for IMPULSE as well as their impact and implication.

[1] Standardization covers all types of standardization documents and is used here in a general manner.

Besides the necessity to know what is going on regarding standardization, this knowledge also provides the opportunity to raise awareness for the needs regarding standardization in this area. Therefore, this deliverable supports the activities in Task 7.6 - *Initiation of standardization activities*, a part of WP7 - *Innovation and exploitation management, dissemination, and communication*.

In general, this standardization overview serves as the basis for further standardization activities in IMPULSE. Knowing about existing standardization documents makes it possible to build up on existing knowledge and avoid unnecessary duplication of work. In addition, existing gaps in standardization can be better identified and impulses for new standardization activities can be developed.

1.2 Document structure

In contrast to patents, knowledge about standardization is less pronounced, especially in the area of research and innovation. For this reason, the basic principles of standardization are presented in this report (see clause 2) as well as the different facets of standardization at international (subclause 2.2), European (subclause 2.3) and national level (subclause 2.4). Subsequently, the various types of standardization documents (subclause 2.1), the function of standardization in the context of research projects (subclause 2.5), and the process for creating a CWA (subclause 2.1) are presented in more detail. The results of the standardization research for IMPULSE are presented by explaining the approach for the standards research (clause 3) and finally giving an overview of the related standardization landscape (clause 4). Besides a general overview of the standardization landscape of IMPULSE (clause 4.1) the relevant international (subclause 4.2), European (subclause 4.3) and national standardization activities (subclause 4.4) are examined. The standards highlighted as highly relevant for the project are focused on more closely especially with regard to the IMPULSE project (subclause 4.5). So-called informal standards also have a strong relation to IMPULSE (subclause 4.6) and therefore, the relation of selected informal standards to IMPULSE is described (subclause 4.7).

2 Standardization

2.1 General

Within the IMPULSE project the standardization part can support technology development as well as ethical implications and social aspects. Therefore, it is important to clarify what a standard actually is. In general, a standard is a consensus-based document that is approved by a recognized body. It provides rules, guidelines or characteristics for activities or their results, reflecting the state-of-the art. It should be based on the consolidated results of science, technology and experience, and aim to promote optimal community benefits.[2] Standardization as an important strategic tool is used to agree on terminologies, methodologies, requirements, characteristics, etc. in specific areas to make a product, process, or service fit for its purpose. Thus, standardization can drive innovative outcomes by agreeing on common product requirements such as interoperability, quality or safety, and provide guidelines for achieving them. Standardization can support the creation of a generic language, which is understandable for everyone and thus helps to create a common understanding. The result of the standardization process is a document, which provides rules, guidelines or characteristics for activities or their results. The benefits of these documents and their applications vary and depend on the different types of documents (Figure 2). The differences between these types of documents lie in their development procedure together with the degree of consensus which has to be reached, and the openness to participation.

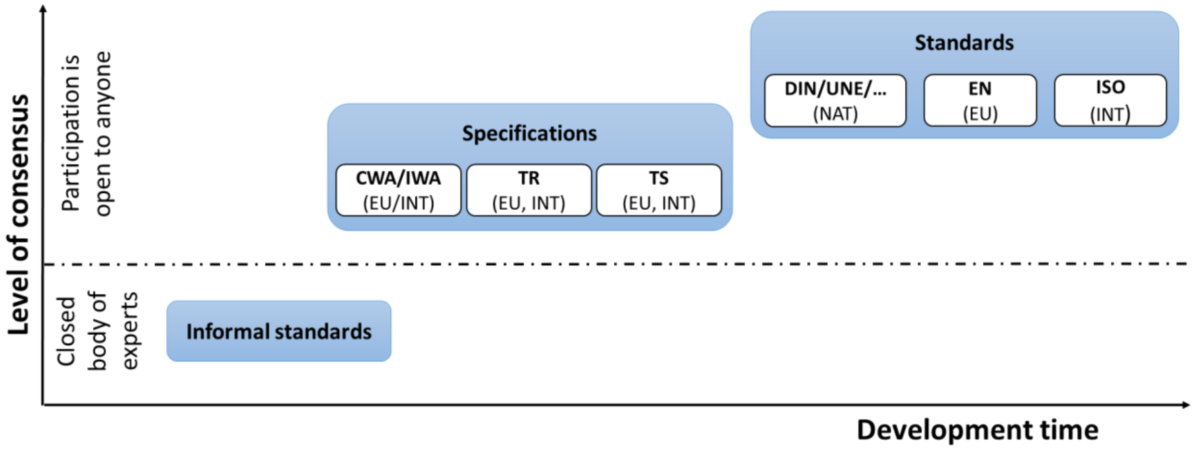
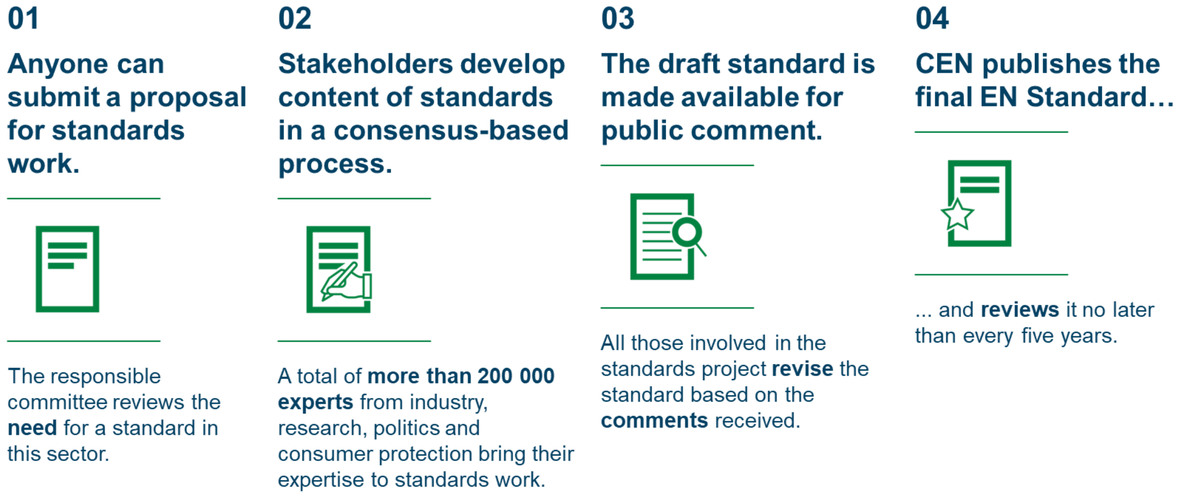


Figure 2: Types of standardization documents

According to Figure 2, **standards** in the narrower sense are developed within the formal standardization system where all interested parties have to be included in the development process of the document and consensus, meaning the general agreement of all participants and the lack of sustained objection to central content, must be reached. The main objective of the consensus is to take into account the views of all interested parties concerned and to dispel any counter-arguments. The development of a standard is shown in Figure 3.

[2] CEN/CENELEC, „EN 45020:2006: Standardization and related activities - General vocabulary," 2006



01

Anyone can submit a proposal for standards work.

The responsible committee reviews the **need** for a standard in this sector.

02

Stakeholders develop content of standards in a consensus-based process.

A total of **more than 200 000 experts** from industry, research, politics and consumer protection bring their expertise to standards work.

03

The draft standard is made available for public comment.

All those involved in the standards project **revise** the standard based on the **comments** received.

04

CEN publishes the final EN Standard…

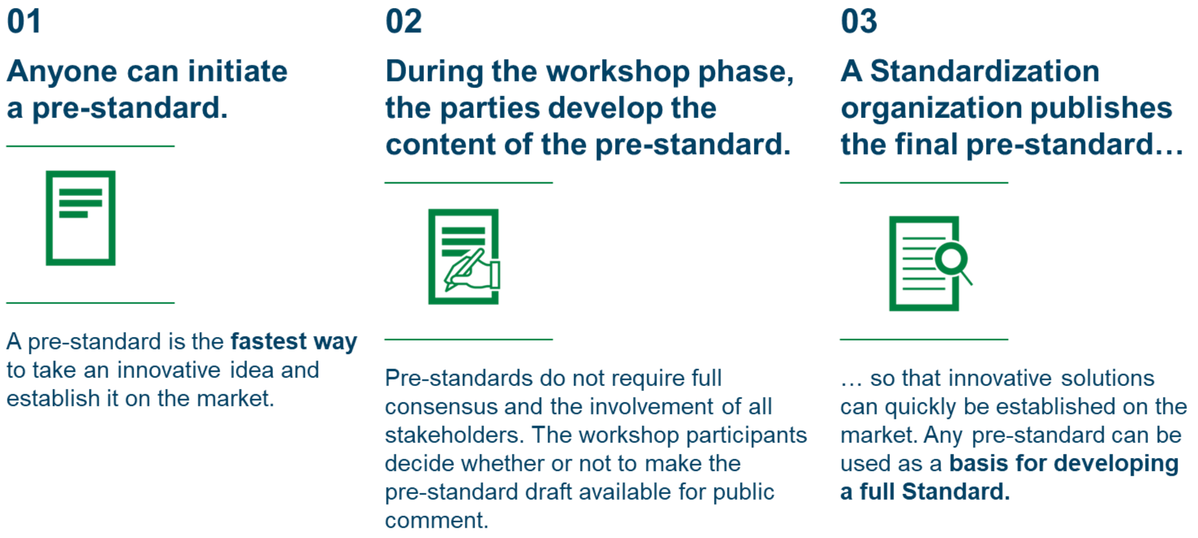
... and **reviews** it no later than every five years.

Figure 3: Development of a standard

First of all, anyone who has identified a need for a standard can submit a standardization proposal. The associated standards committee evaluates the need and checks whether standardization activities are already taking place or if standards covering the described need already exist. If a need is identified, a standard is then developed in a standards committee. Attention is paid to a balanced composition of these committees with all interested parties concerned (science, consumers, industry, ...) in order to guarantee the neutrality of the documents. When a finished draft has been approved by the standards committee, it is released for commenting by the public. The comments are finally discussed and then the final standard is published by consensus. Due to the high level of transparency and the involvement of the public, the development time increases so that national standards usually require 18 months to develop. The development of European and international standards takes more than two years due to the national standards bodies having form an opinion in their respective mirror committees and vote on whether they support the European or international standard.[3] Due to the high degree of consensus, standards have a high level of acceptance in society. There are various types of existing standards, focusing on different topics of interest, e.g. terminology or testing.

In contrast to a standard created with consensus, the standardization activities in research projects focus on the creation of **specifications** or so-called pre-standards. A specification is a publicly available document that describes products, systems or services by defining characteristics and requirements. It is characterized by the fact that, compared to a standard, a consensus is not absolutely necessary and the involvement of all interested parties is not obligatory. The creation of a specification, e. g. CWA is shown in Figure 4.

[3] https://www.iso.org/developing-standards.html



01

Anyone can initiate a pre-standard.

A pre-standard is the **fastest way** to take an innovative idea and establish it on the market.

02

During the workshop phase, the parties develop the content of the pre-standard.

Pre-standards do not require full consensus and the involvement of all stakeholders. The workshop participants decide whether or not to make the pre-standard draft available for public comment.

03

A Standardization organization publishes the final pre-standard…

… so that innovative solutions can quickly be established on the market. Any pre-standard can be used as a **basis for developing a full Standard.**

Figure 4: Development of a specification

Again, anyone can submit an application to develop a specification. A standardization organization checks internally whether standards conflicting with the application exist. If no conflicting standards exist, the standardization organization publishes the business plan for public comment and a call for cooperation from interested organizations. In contrast to standards, specifications are created in workshops (temporary committee) with a standardization organization acting as a secretary. This committee also decides whether a draft should be published for comment and once a specification has successfully been adopted by the committee, it is published by a standardization organization. There are different types of specifications. A Workshop Agreement on European (CWA) or international (IWA) level is developed in a temporary workshop which is designed to meet an immediate need and forms the basis for future standardization activities lead by a national standardization body. Even if there are not as strict rules for developing a specification as there are for standards, it is important to ensure the coherence of the standardization regulations to protect the credibility of international, European, and national standardization. The workshop is open for direct participation to anyone with an interest in the development of the agreement but no full consensus is needed. The development of a Workshop Agreement is fast and flexible, on average between 10 and 12 months and therefore also attractive for research projects. The different national standardization organizations each have their own name for these spcifications that have been developed in workshops, e.g., a nationally created pre-standard by DIN (Germany) is called DIN SPEC (e.g., DIN SPEC 91392). Specifications can also be developed within standards committees if, for example , no final consensus can be reached. These documents are then referred to as CEN or ISO TS (Technical Specifications). A TS on European level may not conflict with a European standard but conflicting national standards may continue to exist. Technical Reports (TR) are informal documents that are developed and approved by a technical committee. A TR provides information on technical content and standardization work.

Regarding the development time, the fastest ones are the **informal standards** (see Figure 2), also called industry, consortia or de-facto-standards. Among other things, they are characterized by the fact that not all interested parties need to be included in the creation process. These closed group of experts can be, e. g. industry-specific consortia that have been formed from different companies. Although these documents have some characteristics of a standardization document such as defined procedures or documentation rules, consortia standards are often not freely accessible and are developed in private. Such informal standards are considered separately from the formal ones in this deliverable.

Every country participating in the European and international standardization world of CEN, CENELEC, ISO, and IEC follows the so called delegation principle. National standardization bodies, such as DIN in Germany, UNE in the Spain or BSI in the UK send representatives to the European or international standardization committees of CEN, CENELEC, ISO, and IEC to represent their national interests (Figure 5).

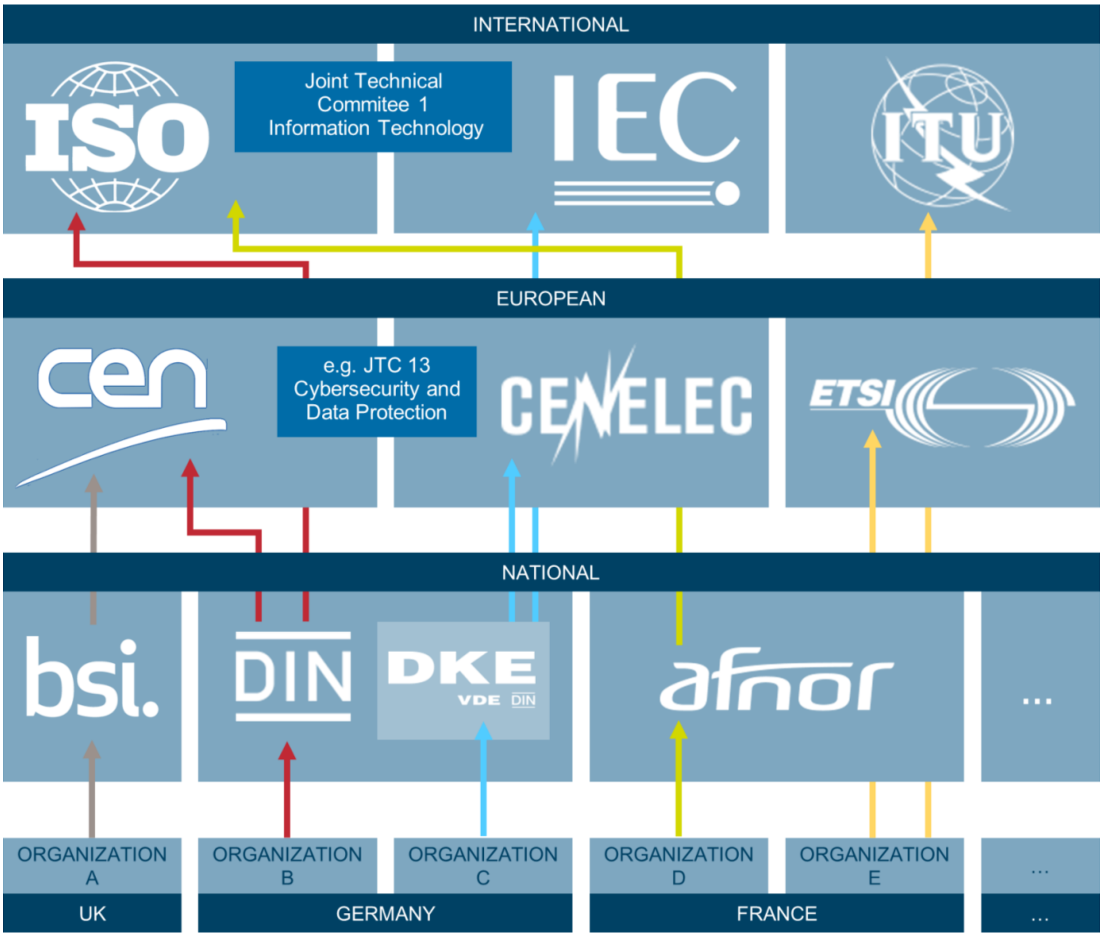


Figure 5: Overview of the organizational structure of the standardization world

An essential aspect of standardization work is to ensure that documents do not contradict each other, especially since European and international standardization has gained significantly in importance, as reflected in DIN’s statistics, which show that European and international standards account for 90% of all standardization projects nowadays. The following clauses give a brief description of the framework of formal standardization on international, European, and national level. Furthermore, on the relevance of standardization in R&I project is considered.

2.2 International standardization level

The international standardization organizations ISO[4] (International Organization for Standardization), IEC[5] (International Electrotechnical Commission), and ITU[6] (International Telecommunication Union) are responsible for organizing international standardization work. ISO is responsible for all non-electronic and IEC for electrotechnical standardization activities while the ITU is in charge of standardization activities in the field of telecommunications on an international level.

ISO and IEC are made up of the national standardization organizations, with DIN and DKE representing German interests on an international level. The ITU, on the other hand, is a special unit of the United Nations, whose 191 member states develop recommendations together with companies from the private sector and other regional and national organizations. Only when they are adopted by normative organizations such as ISO, ANSI (USA) or ETSI as well as by national regulatory authorities such as the Federal Network Agency in Germany do they acquire the character of standards.

The so-called delegation principle applies to ISO and IEC, meaning that the national standardization organizations send their experts to the international standardization bodies. Here, the work is discussed in a

[4] www.iso.org
[5] https://www.iec.ch/
[6] https://www.itu.int

national mirror committee, existing results are discussed, a national opinion is developed and the final draft standards are agreed upon. Only when a sufficiently large majority of the national standardization organizations has voted for a draft standard is it accepted and published as an international standard (ISO). International specifications are referred to as IWA as well as ISO TS or IEC TS, depending on the type of creation.

In contrast to European standardization, there is no obligation to adopt international standards in national standards. However, since internationally applicable standards are relevant for international trade or for global stakeholders, conflicting national or European standards should be avoided. There is the possibility of incooperating international standards in European and national standards and there are also parallel creation processes of standards at international and European level. The resulting documents have the characteristics and names listed in Table 1, depending on the background.

Table 1: Names of international standards depending on their adoption level.

Name	Description
ISO XXXXX	International standard neither nationally nor European adopted
DIN ISO XXXXX	International standard only nationally (Germany) adopted
DIN EN ISO XXXXX	International standard adopted on European and national level

2.3 European standardization level

The main goal of standardization at European level is to harmonize the national standards of the member states of the European Union (EU). This includes on the one hand the uniform transfer of international standards and on the other hand the creation of European standards. The European standardization organizations CEN[7] (European Committee for Standardization), CENELEC[8] (European Committee for Electrotechnical Standardization) and ETSI[9] (European Telecommunications Standards Institute) are responsible for the organization of European standardization work. CEN is responsible for all non-electronic activities and CENELEC for electrotechnical standardization activities, while ETSI is responsible for the standardization activities in the field of telecommunications at European level.

There is a particularly close cooperation between CEN and CENELEC, which are made up of national standardization organizations from the EU and EFTA (European Free Trade Association) member states, e.g. Germany's interests being represented by DIN and DKE, as well as the states seeking membership. In contrast, the members of ETSI are directly European companies, institutes and organizations.

The so-called delegation principle applies to CEN and CENELEC, meaning that the members, the national standardization bodies, send their national experts to a European standardization body at CEN or CENELEC. In a national committee, known as the mirror committee, the work and existing results are discussed and a national opinion is developed. This committee then votes on the final draft standards. Only when a sufficiently large majority of the national standardization organizations has voted for a draft standard is it accepted and published as a European standard (EN standard).

European standards must automatically be adopted by the member states of the EU and opposing national standards withdrawn. As a result of this adoption obligation, the EN standards in Germany then become DIN EN standards (e.g. DIN EN 16575). European specifications are referred to as CWA as well as CEN TS or CENELEC TS, depending on the type of creation. The obligation to adopt the national standards of the member countries does not apply to specifications, but is possible (e.g. DIN CEN/TS 17045).

For IMPULSE in particular, aspects of standardization play an important role. Both the national and the European research framework program Horizon 2020 address the topic of standardization in a series of calls for proposals.

[7] www.cen.eu

[8] www.cenelec.eu

[9] www.etsi.org

2.4 National standardization level

On the national level, there are different structures and standardization bodies in different countries, as e. g. British Standards Institute (BSI), German Institute for Standardization (DIN), Spanish standardization body (UNE). In general, each country has a recognized national standardization body (NSB) which represents the national opinion at international / European level. Each national standardization body can develop national standards as long as there is no EN standard existing on a particular area. There are situations in which it is possible to complement EN standards with additional national standards, for instance to set more detailed requirements suiting to specific needs of the member state.

An important country outside of Europe, which must be taken into account in the context of standardization are the USA. The United States (US) standardization landscape differs somehow from the European approach. The American National Standards Institute (ANSI) is a private, non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the US. The organization also coordinates US standards with international standards. ANSI accredits standards that are developed by representatives of other standards organizations, government agencies, consumer groups, companies, and others.[10] It works as kind of umbrella organization by coordinating 240 Standards Developing Organizations (SDOs), such as Underwriter Laboratories (UL), American Society of Mechanical Engineers (ASME), Institute of Electrical and Electronics Engineers (IEEE). Many of them develop standards for the US-market and provide certification or accreditation services as well, e. g. UL. The American Society for Testing and Material (ASTM), which is an ANSI-accredited standards developer,[11] is another important national standardization body in the US. Some standards are implemented in the federal laws, others are viewed more as guidelines for industry. This is the case for many of the standards developed by US-SDOs.

The IMPULSE consortium includes the participation of one national standardization body – DIN.

2.5 Standardization in research projects

It is crucial for an R&I project to know the state of the art in the areas relevant for or connected to the project. Since standards reflect this state of the art in a specific area it is essential for R&I projects to have an overview of the standardization landscape related to the project. This knowledge enables the project to adapt its results such as products, services, etc. to the current needs. R&I projects need to consider what is being developed within other relevant activities. Irrespective of the technical merits of the R&I project developments, these efforts will be inconsequential if developed in isolation and the market decides to follow another path. Furthermore, the knowledge about related standards also enables the R&I project to overcome additional challenges and go beyond the current state of the art. On the one hand, an overview of the related standardization landscape offers an R&I project the advantages described above. On the other hand, awareness is raised on where standardization is still needed. This opportunity can be used by the R&I project to implement project results in already ongoing standardization activities or by developing new standards out of project results.

[10] https://ansi.org/american-national-standards/ans-introduction/overview

[11] https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/ANSI%20Accredited%20Standards%20Developers/DEC2022ASD.pdf

3 Methodology of the Standards Research for IMPULSE

To provide an overview of the standardization landscape related to IMPULSE a standards research was conducted. The approach for the standards research is summarized in Figure 6. It is divided into three main phases; the actual standards search (phase I), the standards analysis (phase II), and the result dissemination (phase III). The procedure in the three phases is described in the following.

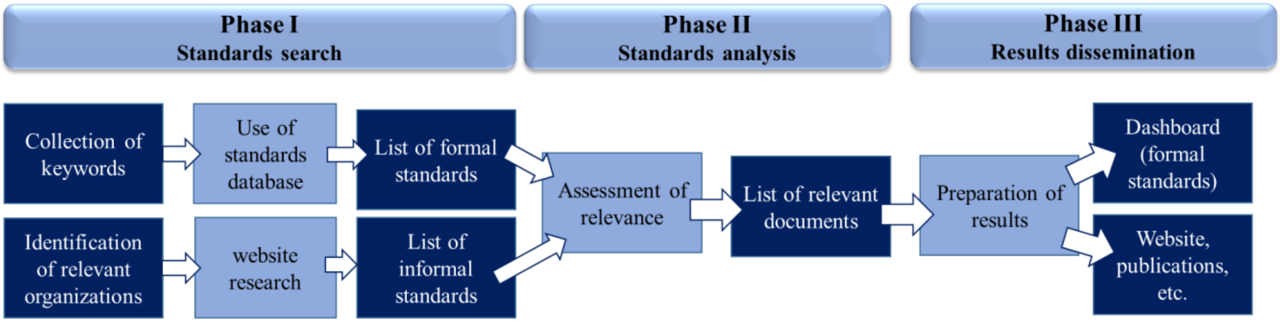


Figure 6: Methodology of standards research

In order to do a search for standards relevant for IMPULSE (**phase I**), keywords were provided by the partners of the different work packages of the project. The keywords are listed in Table 2. Besides keywords, the names of relevant technical committees (TC) and organizations, which are also listed in Table 2 were supplied. The keywords, TC's, and organizations were used to identify standardization documents and further TC's related to the IMPULSE project.

Table 2: From the WP's supplied keywords, TC's and organizations for the standards research.

Keywords
artificial intelligence (AI)
blockchain
decentralized identity
DID controller
DID document
DID subject
disruptive technology
EBSI
eID
eIDAS
electronic identification
ESSIF
holder
issuer
registration authority
self sovereign identity
self-sovereign type of blockchain
Verifiable Credential
Verifiable Presentation
verifier
Technical Committees
CEN-CLC/JTC 19/WG 01 - Blockchain and Distributed Ledger Technologies - Decentralised identity management
CEN/TC 331/WG 02 - Postal services - New digital postal services
ETSI ESI - Electronic Signature Initiative
ETSI ISG - Permissioned Distributed Ledger
ISO TC 307 - Blockchain and distributed ledger technologies

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity, and privacy protection
ISO/TC 46 - Information and documentation
ISO/TC 154 - Processes, data elements and documents in commerce, industry, and administration
ITU-T - Digital Currency Global Initiative
Organizations
Bitkom
Cloud Signature Consortium
DIF Decentralized Identity Foundation
Hyperledger Identity
ToIP Trust over IP
W3C Credentials Community Group
W3C Decentralized Identifier Working Group
W3C Verifiable Credentials Working Group

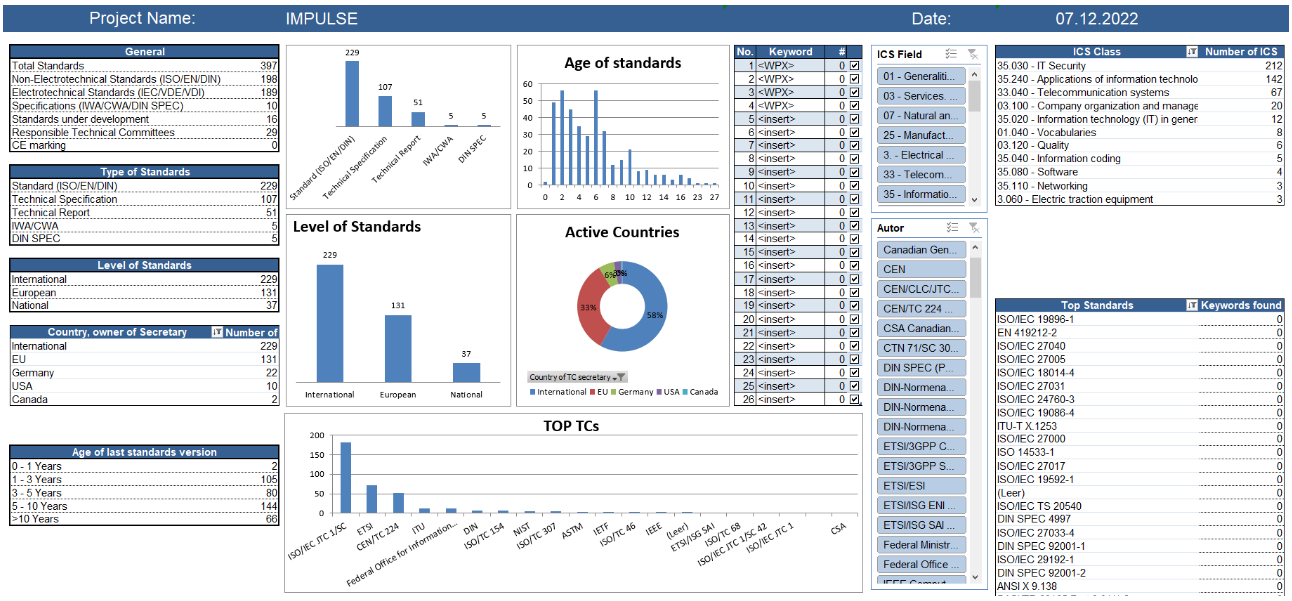
For the standard search, mainly the search engine PERINORM was used to find formal standards. PERINORM is a bibliographic database which includes databases from 29 countries as well as data from European and international standardization bodies with around 2,4 million records worldwide.[12] Beside the standards of European national organizations like e. g. DIN, UNE or BSI and Non-European national organizations e. g. from Brazil, USA or South Africa, the database also includes standards from the European organizations CEN, CENELEC, ETSI, and international organizations such as ISO, IEC, and ITU. Regulations, technical documents, and reports on these levels have been considered for the analysis. In case of national standards, it has to be stated that due to language barriers mostly those providing at least an English title have been considered. All the hits from the PERINORM research using the different keywords resulted in a list of 559 standards whereof 8 were informal standards.

Besides the keywords and TCs used in the PERINORM research, sources for informal standards from organizations which are no standardization body were suggested from the different WPs. Browsing the websites of the organizations which were referred to by the WPs 102 informal standards were collected. Those standards were provided separately from the formal standards in a list of informal standards.

For both, formal and informal standards, an analysis and assessment of the standards relevant and important to the IMPULSE project was conducted by the consortium (**phase II**). The identification of those standards was carried out by filtering the list of standards with keywords relevant for the specific work package and an individual evaluation based on the title as well as the abstract of the standards. Mainly project partners involved in WP3, WP4 and WP5 have identified relevant standards. This way 382 formal and 95 informal standards were highlighted as relevant for IMPULSE. In individual meetings with IMPULSE partners from one organization (UC, GRAD, ICERT, ALiCE) or city case (ARH, RVK) awareness was raised of the relevant standards. Furthermore, those meetings were used to clarify questions regarding standardization and input to standards rated as highly relevant was collected.

The overview of the relevant formal standards (**phase III**) was spread in the form of a dashboard (Figure 7) among the work packages, whereas the informal standards were provided in a simple list. Both kind of standards are listed in Table 11 (A.1) and Table 12 (A.2), whereas standards highlighted as highly relevant are discussed in more detail in clause 4.5 and clause 4.7.

[12] https://www.perinorm.com/home/default.aspx?ReturnUrl=%2fdefault.aspx



Project Name: IMPULSE   Date: 07.12.2022

General	
Total Standards	397
Non-Electrotechnical Standards (ISO/EN/DIN)	198
Electrotechnical Standards (IEC/VDE/VDI)	189
Specifications (IWA/CWA/DIN SPEC)	10
Standards under development	16
Responsible Technical Committees	29
CE marking	0

Type of Standards	
Standard (ISO/EN/DIN)	229
Technical Specification	107
Technical Report	51
IWA/CWA	5
DIN SPEC	5

Level of Standards	
International	229
European	131
National	37

Country, owner of Secretary	Number of
International	229
EU	131
Germany	22
USA	10
Canada	2

Age of last standards version	
0 - 1 Years	2
1 - 3 Years	105
3 - 5 Years	80
5 - 10 Years	144
>10 Years	66

No.	Keyword	#	
1	<WPX>	0	☑
2	<WPX>	0	☑
3	<WPX>	0	☑
4	<WPX>	0	☑
5	<insert>	0	☑
6	<insert>	0	☑
7	<insert>	0	☑
8	<insert>	0	☑
9	<insert>	0	☑
10	<insert>	0	☑
11	<insert>	0	☑
12	<insert>	0	☑
13	<insert>	0	☑
14	<insert>	0	☑
15	<insert>	0	☑
16	<insert>	0	☑
17	<insert>	0	☑
18	<insert>	0	☑
19	<insert>	0	☑
20	<insert>	0	☑
21	<insert>	0	☑
22	<insert>	0	☑
23	<insert>	0	☑
24	<insert>	0	☑
25	<insert>	0	☑
26	<insert>	0	☑

ICS Class	Number of ICS
35.030 - IT Security	212
35.240 - Applications of information technolo	142
33.040 - Telecommunication systems	67
03.100 - Company organization and manage	20
35.020 - Information technology (IT) in gener	12
01.040 - Vocabularies	8
03.120 - Quality	6
35.040 - Information coding	5
35.080 - Software	4
35.110 - Networking	3
3.060 - Electric traction equipment	3

Top Standards	Keywords found
ISO/IEC 19896-1	0
EN 419212-2	0
ISO/IEC 27040	0
ISO/IEC 27005	0
ISO/IEC 18014-4	0
ISO/IEC 27031	0
ISO/IEC 24760-3	0
ISO/IEC 19086-4	0
ITU-T X.1253	0
ISO/IEC 27000	0
ISO 14533-1	0
ISO/IEC 27017	0
ISO/IEC 19592-1	0
(Leer)	0
ISO/IEC TS 20540	0
DIN SPEC 4997	0
ISO/IEC 27033-4	0
DIN SPEC 92001-1	0
ISO/IEC 29192-1	0
DIN SPEC 92001-2	0
ANSI X 9.138	0

Figure 7: Dashboard with the relevant standards for the IMPULSE project

A first version of the dashboard with all relevant standards was provided in October 2021. The dashboard is an Excel template, which was developed specifically for the research of standards and provides an overview of the main information regarding the relevant standards. It can be used to search for specific standards by keywords or to get an overview of the standards within a specific ICS field or developed by a specific TC. This dashboard was shared within the whole IMPULSE consortium.

Since the development of standards does not stand still, a standards research was performed in summer 2022 by using the provided keywords and TC's. That way, a list of newly published standards including 64 formal standards was created. After the evaluation by the IMPULSE partners seven relevant formal standards were added to the dashboard and a new version containing 389 formal standards was made available to the consortium in November 2022. Additionally, two relevant informal standards were added, bringing the list of informal standards to 97 items. The following overview of the IMPULSE standardization landscape is based on the updated dashboard version.

To disseminate the result of the IMPULSE project regarding standardization a publication with the title "Analyzing the Standardization Landscape for Identity Management in Public Services - A Standards Review for the IMPULSE project" was prepared and submitted in February 2022 at JASIST (Journal of the Association for Information Science and Technology). Since it is a bit out of the journal's scope it was rejected for publication in July 2022. Nevertheless, the reviewers advised to submit this paper in another journal. This process is still ongoing.

To raise awareness outside of the IMPULSE consortium that standards play an important role in R&I projects, standards which are highly relevant for IMPULSE are summarized on the IMPULSE website with some general information and the two important categories of standards (formal and informal standards) for IMPULSE.[13] On the website a post on "What does the standardization landscape for identity management in public services look like?" can be found, explaining standardization activities in an R&I project, using the example of IMPULSE.[14]

[13] https://www.impulse-h2020.eu/standards/

[14] https://www.impulse-h2020.eu/2022/03/30/what-does-the-standardization-landscape-for-identity-management-in-public-services-looks-like/

4 Overview of the IMPULSE Standardization Landscape

4.1 General

This clause gives an overview of the standardization landscape related to the IMPULSE project. Using this knowledge, it is possible to assess results from the IMPULSE project have the potential to initiate new standardization activities. Furthermore, standardization is a significant instrument to support both dissemination and exploitation of the project results. By considering the topic of standardization at an early stage of the project, the interoperability of the project results with products already on the market is ensured. The planned standardization activities in WP7 will foster a sustainable transfer of project results to the market by providing e.g. standardization documents or input to already ongoing standardization activities. As a whole, standardization has a positive effect on the entire innovation process, from fundamental research to marketing of new products. For this reason, an overview of the standardization landscape in general as well as details on which standardization bodies and organizations are already active in the relevant fields for IMPULSE, is given in this clause of the deliverable. Furthermore, standards, formal and informal, highlighted as highly relevant for the IMPULSE project are looked at more closely. Within this deliverable the term *relevant standard* means a standard which is relevant to the IMPULSE project.

To provide an overview of the standardization landscape related to IMPULSE the results of the standards research, the dashboard (see clause 3), are used as a basis. The dashboard contains 389 formal standards (out of 615) which were highlighted as relevant or highly relevant for the project by the IMPULSE partners. Since the dashboard only focuses on the formal standards, the 97 relevant informal standards (out of 112) are listed separately. The number of highlighted relevant and highly relevant standards out of the provided standards list is visualized in Figure 8.

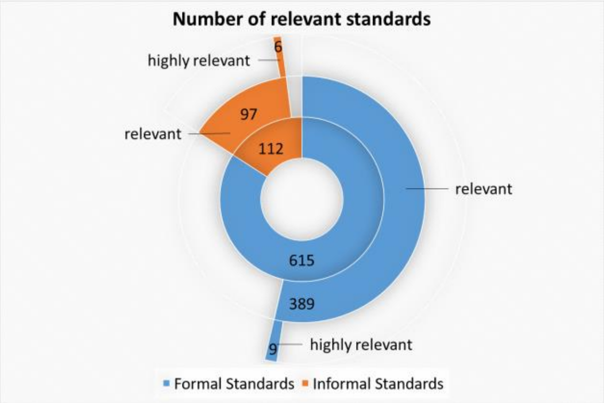
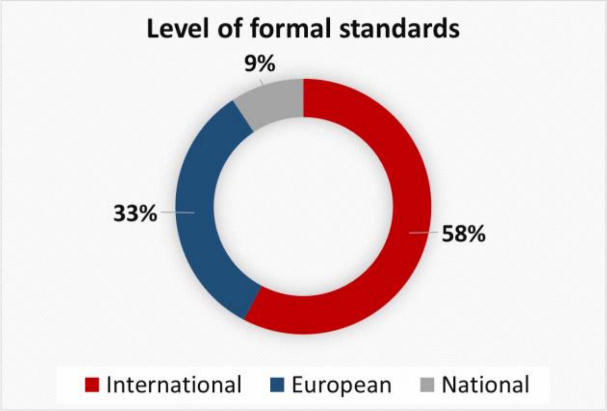


Figure 8: Number of relevant standards

The dashboard was used to provide some general information on the standards relevant to the IMPULSE project. In Figure 9 the origin of these is visualized. The majority (58%) of the standards were developed on international level, whereas 33% originated on European level and the minority of 9% on national level (Figure 9). The most important countries regarding the origin of the national standards are Germany and the US since more than half of these standards were developed in the former country and around one quarter in the latter (Figure 10).



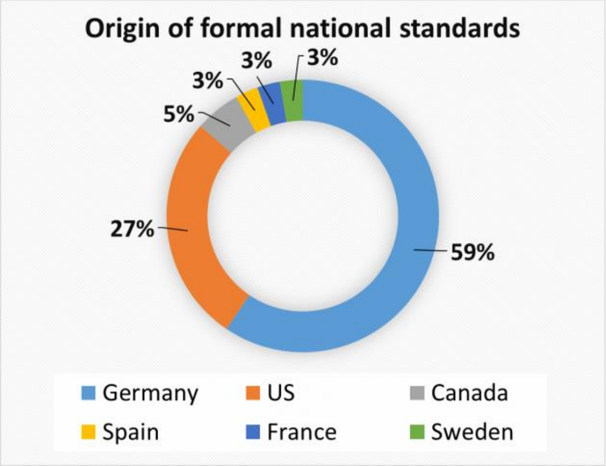


Figure 9: Level of relevant standards

Figure 10: Origin of national standards

There are different types of standardization documents which are included in the dashboard. More than half of these documents (58%) are standards like ISO- / EN- or national standards but more than one quarter (27 %) are technical specifications and one eighth (13%) are technical reports. The remaining documents are specifications like CWA's or DIN SPEC's. In the last 5 years, around half of those formal standards have been published.

The standards relevant for the IMPULSE project cover a wide range of different areas. Based on the ICS (International Classification for Standards) fields, an overview of the different areas can be given (Figure 11). For this overview only ICS fields which are assigned to at least 3 standards are presented in Figure 11. The identified standards are part of five different ICS fields, whereas *33 - Telecommunications. Audio and video engineering* and *35 - Information technology* are the most present ones. It is important to keep in mind, that one standard can be part of different ICS fields. This means that the 397 formal standards identified as relevant are in total 482 times classified in ICS fields. Nevertheless, there are three mainly relevant subcategories. Nearly half (44%) of the standards are classified as *IT Security* (35.030), which is by far the most prominent field. The field *Application of information technology* (35.240) is the second most important field in which nearly one third (29%) of the standards are categorized. One-seventh of the standards are part of ICS field *Telecommunication Systems* (33.040).

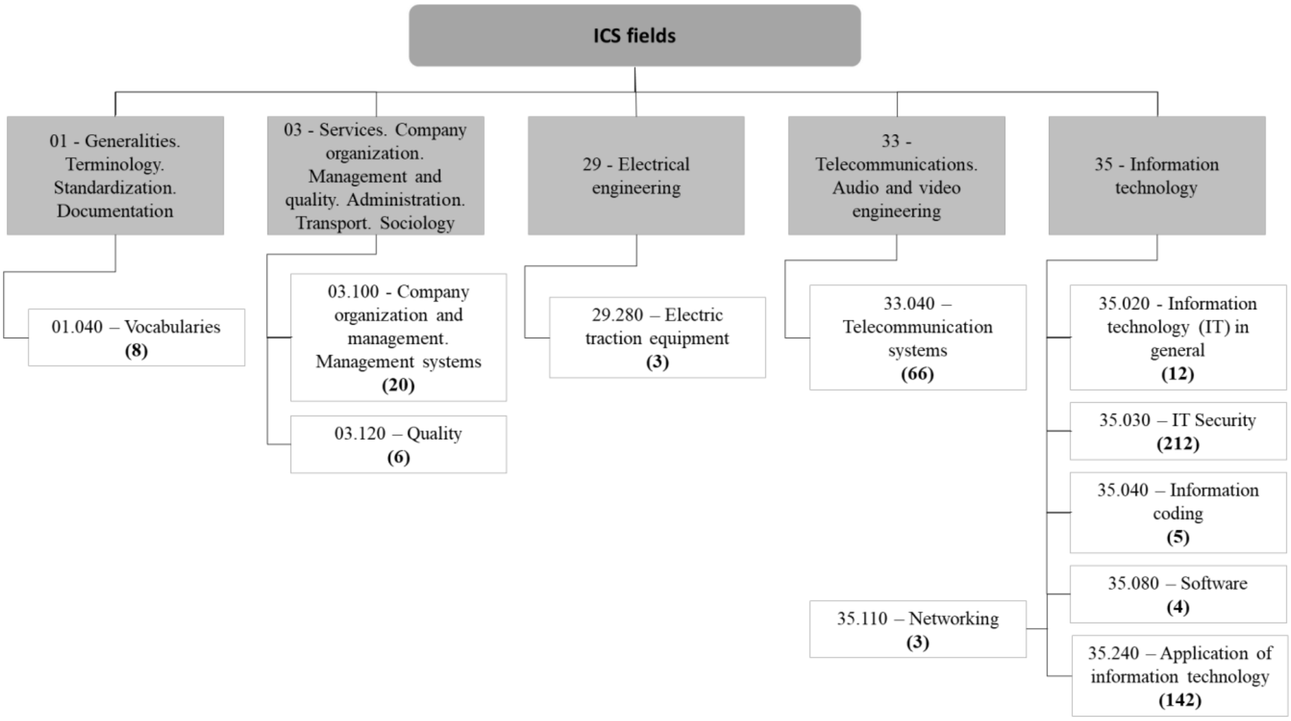

ICS fields
01 - Generalities. Terminology. Standardization. Documentation
03 - Services. Company organization. Management and quality. Administration. Transport. Sociology
29 - Electrical engineering
33 - Telecommunications. Audio and video engineering
35 - Information technology
01.040 – Vocabularies (8)
03.100 - Company organization and management. Management systems (20)
03.120 – Quality (6)
29.280 – Electric traction equipment (3)
33.040 – Telecommunication systems (66)
35.020 - Information technology (IT) in general (12)
35.030 – IT Security (212)
35.040 – Information coding (5)
35.080 – Software (4)
35.110 – Networking (3)
35.240 – Application of information technology (142)

Figure 11: Overview of the number of standards in the different ICS fields

4.2 Standardization activities on international level

During the assessment of the relevance of the preselected standards, 229 international standards were classified as relevant for the IMPULSE project. The main technical committees, which are responsible for these standards are listed in Table 3 and are described in the following.

Table 3: Relevant standard setting organizations and TC's on international level.

ISO/IEC JTC 1	Information Technology
ISO/TC 154	Processes, data elements and documents in commerce, industry and administration
ISO/TC 307	Blockchain and distributed ledger technologies
ISO/TC 46	Information and documentation
ISO/TC 68	Financial services
ITU-T	International Telecommunication Union Telecommunication Standardization Sector

The **ISO/IEC JTC1 – Information Technology**[15] founded in 1987 is a joint technical committee from ISO and IEC focusing on the development of ICT standards for business and consumer applications.[16] It has already published around 3300 ISO/IEC standards, whereas nearly 500 are currently under development.[17] Regarding the relevant international standards for IMPULSE 185 of them were developed by this JTC.

ISO/IEC JTC1 is composed of 22 sub committees whereas the relevant ones are described in the following.[18]

The *ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection* published 162 standards relevant for this project. It was created in 1989 and DIN is holding the secretariat for this SC. The scope of this JTC is to develop standards for the protection of information and ICT including generic methods, techniques, and guidelines to address both security and privacy aspects. So far it has published 227 ISO standards and 63 are under development. This JTC has 53 participating and 34 observing members.[19]

The *ISO/IEC JTC 1/SC 37 – Biometrics* published 14 of the international standards deemed relevant to IMPULSE. This SC was created in 2002 and the secretariat is held by ANSI. The focus is on standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. These generic human biometric standards include common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. The application of biometric technologies to cards and personal identification (ISO/IEC JTC 1/SC 17) as well as biometric data protection techniques, biometric security testing, evaluations and evaluations methodologies (ISO/IEC JTC 1/SC 27) are not part of the work in this SC. So far 135 ISO standards were published by this SC and 21 are under development. The JTC has 29 participating and 21 observing members.[20]

The remaining relevant international standards were published by *ISO/IEC JTC 1/SC 17 - Cards and security devices for personal identification*, *ISO/IEC JTC 1/SC 29 - Coding of audio, picture, multimedia and hypermedia information*, *ISO/IEC JTC 1/SC 41 - Internet of things and digital twin* and *ISO/IEC JTC 1/SC 42 - Artificial intelligence*. There are also a couple of standards developed by *ISO/IEC JTC 1/SC 17* which are becoming more and more relevant for the EU digital identity wallet and therefore also for IMPULSE, like ISO/IEC 18013-5:2021 - *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application* and ISO/IEC 23220-1 - Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems (under development).

[15] https://jtc1info.org/
[16] https://jtc1info.org/sd-2-history/
[17] https://www.iso.org/committee/45020.html
[18] https://jtc1info.org/about/committees/
[19] https://www.iso.org/committee/45306.html
[20] https://www.iso.org/committee/313770.html

Furthermore, the for the IMPULSE project relevant international standards were published by ISO/TC 154, ISO/TC 307, ISO/TC 46, and ISO/TC 68. **ISO/TC 154 - Processes, data elements and documents in commerce, industry and administration** aims to standardization and registration of business and administration processes and supporting data used for information interchange between and within individual organizations as well as support for standardization activities in the field of industrial data.[21] Standardization of blockchain technologies and distributed ledger technologies is done in **ISO/TC 307 - Blockchain and distributed ledger technologies**. This TC was created in 2016 and in its short time of existence has already published 9 ISO standards and 7 are under development.[22] **ISO/TC 46 - Information and documentation** deals with standardization of practices relating to libraries, documentation and information centres, publishing, archives, records management, museum documentation, indexing and abstracting services, and information science.[23] **ISO/TC 68 – Financial services** is responsible for standardization in the field of banking, securities, and other financial services.[24]

Besides standards on ISO level, 13 relevant standards were published by **ITU**. ITU is the United Nations specialized agency for information and communication technologies. Independently from the UN, it was founded in 1865 to facilitate international connectivity in communication networks. Among the allocation of global radio spectrum and satellite orbits, it develops technical standards that ensure that networks and technologies interconnect.[25] The **ITU-T** (ITU Telecommunication Standardizing Sector) develops standards which are critical to the interoperability of ICT's.[26]

The IMPULSE partner InfoCert is a participant in the following for IMPULSE relevant international standardisation committees: ISO/IEC JTC 1/SC 17, ISO/TC 154, and ISO/TC 307.

4.3 Standardization activities on European level

As already mentioned in clause 2.3 the standardization activities on European level are strongly connected to the ones on international level. 131 standards that are important for the project were developed at European level. The responsible TC's are listed in Table 4.

Table 4: Relevant TC's on European level.

ETSI TC ESI	ETSI Technical Committee Electronic Signatures and Infrastructures
ETSI ISG SAI	ETSI Industry Specification Group on Securing Artificial Intelligence
ETSI 3GPP	ETSI 3rd Generation Partnership Project
CEN TC 224	Personal identification and related personal devices with secure element, systems, operations, and privacy in a multi sectorial environment
CEN-CLC/JTC 19	Blockchain and Distributed Ledger Technologies
CEN-CLC/JTC 21	Artificial Intelligence

The European Standards Organisation **ETSI** (European Telecommunications Standards Institute) deals with standardization in the fields of telecommunication, broadcasting, and other electronic communication networks and services.[27] Regarding standards relevant for IMPULSE on European level, the majority, namely 76 standards, were published by ETSI.

[21] https://www.iso.org/committee/53186.html
[22] https://www.iso.org/committee/6266604.html
[23] https://www.iso.org/committee/48750.html
[24] https://www.iso.org/committee/49650.html
[25] https://www.itu.int/en/about/Pages/default.aspx
[26] https://www.itu.int/en/ITU-T/about/Pages/default.aspx
[27] https://www.etsi.org/about

The ETSI Technical Committee Electronic Signatures and Infrastructures (**ETSI TC ESI**) published 70 of them. The work from TC ESI addresses the requirements of digital signatures, including formats and procedures and policies for creation and validation, as well as trust services supporting the authenticity of transactions. This TC is highly relevant for the work at IMPULSE as it supports the eIDAS (electronic IDentification, Authentication and trust Services) Regulation as well as the general requirements of the international community to provide trust and confidence in electronic transactions.[28, 29]

The remaining standards were published by the ETSI Industry Specification Group on Securing Artificial Intelligence (**ISG SAI**) and the ETSI 3rd Generation Partnership Project (**ETSI 3GPP**). The ETSI ISG SAI, created in 2019, works alongside a landscape of huge growth in AI, creating standards to preserve and improve the security of Artificial Intelligence.[30, 31] 3GPP is a partnership project bringing together national Standards Development Organizations (SDOs) from around the globe initially to develop technical specifications for the 3rd generation of mobile, cellular telecommunications, UMTS.[32]

TC ESI works in collaboration with CEN TC 224 to provide standards for digital signatures. The **CEN TC 224 - Personal identification and related personal devices with secure element, systems, operations, and privacy in a multi sectorial environment** is responsible for 52 of the European standards rated as relevant by the IMPULSE partners. The aim of this TC is the development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations, and privacy in a multi sectorial environment.[33]

Besides those standards there are 5 CWA's and 1 EU regulation which were also rated as relevant.

There are two TC's on European level which could also be relevant to the IMPULSE topics, even if no standards from them were highlighted by the IMPULSE partners. The reason for that is that both TC's are quite new and thus have not yet published any standards.

On the basis of a white paper from 2018 the **CEN-CLC/JTC 19 - Blockchain and Distributed Ledger Technologies** was created. This JTC works in close contact with ISO/TC 307 while focusing on supporting the EU Digital Single Market.[34, 35] At the beginning of 2021 **CEN-CLC/JTC 21 - Artificial Intelligence** was established with the intention to adopt international standards available or under development and to produce standardization deliverables addressing the European market.[34, 36]

The IMPULSE partner InfoCert is a participant in the following to IMPULSE relevant European standardisation committees: ETSI TC ESI, CEN TC 224, and CEN-CLC/JTC 19.

[28] https://www.etsi.org/committee-activity/activity-report-esi?highlight=WyJlc2kiXQ==

[29] https://www.etsi.org/committee/esi

[30] https://www.etsi.org/committee/sai?highlight=WyJldHNpIiwiZXRzaSdzIiwiJ2V0c2kiLCJldHNpJ3NkaXJlY3RvciIsIidldHNpJ3MiLCJldHNpJyIsImV0c2knc2NvbnZlbnRpb25hbCIsImV0c2knc3N0YW5kYXJkaXphdGlvbiIsImV0c2knc21hY2hpbmUtdG8tbWFjaGluZSIsImlzZyIsImlzZydzIiwic2FpIiwiZXRzaSBpc2ciLCJldHNpIGlzZyBzYWkiLCJpc2cgc2FpIl0=

[31] https://www.etsi.org/newsroom/press-releases/1650-2019-10-etsi-launches-specification-group-on-securing-artificial-intelligence?highlight=WyJldHNpIiwiZXRzaSdzIiwiJ2V0c2kiLCJldHNpJ3NkaXJlY3RvciIsIidldHNpJ3MiLCJldHNpJyIsImV0c2knc2NvbnZlbnRpb25hbCIsImV0c2knc3N0YW5kYXJkaXphdGlvbiIsImV0c2knc21hY2hpbmUtdG8tbWFjaGluZSIsImlzZyIsImlzZydzIiwic2FpIiwiZXRzaSBpc2ciLCJldHNpIGlzZyBzYWkiLCJpc2cgc2FpIl0=

[32] https://www.etsi.org/committee/1418-3gpp

[33] https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:6205&cs=1E59B4D3EFD280E27AAC0C16CC13CD4FD

[34] https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/emerging-technologies/

[35] https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:2702172&cs=148F2B917E4B67BCFD6FE36CE0EA923AC

[36] https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:2916257&cs=11D701467243B7C63DEF4702C86E0138A

For IMPULSE especially the standardization activities on CEN level are interesting since the development of a CWA or the implementation of project results via a liaison with a TC at CEN level is targeted. Therefore, the following Table 5 to Table 7 give an overview of the current work items within CEN TC 224, CEN-CLC/JTC 19, and CEN-CLC/JTC 21.

Table 5: Current work items of CEN TC 224.

Standard No.	Title.	Status
prCEN/TS 17489-5 (WI=00224269)	Secure and interoperable European Breeder Documents - Part 5: Trust establishment and management processes	Preliminary
prEN ISO/IEC 2382-37 rev (WI=00224274)	Biometrics multilingual vocabulary based upon the English version of ISO/IEC 2382-37:2012	Under Drafting
(WI=00224275)	Personal identification – Usage of biometrics in breeder documents	Preliminary
(WI=00224271)	Personal identification – European guide for verification applications based on ID documents (EVG)	Preliminary
(WI=00224273)	Digital Presentation Attack in biometric systems	Preliminary
(WI=00224270)	Secure and interoperable European Breeder Documents — Part 2: Data model	Under Drafting
(WI=00224272)	European Digital Identity Wallets standards Gap Analysis	Under Drafting
(WI=00224266)	Personal identification —Use of biometric verification data across EU countries and scenarios	Under Drafting

Table 6: Current work items of CEN-CLC/JTC 19.

Standard No.	Title.	Status
prCEN/CLC/TS XXXX (WI=JT019002)	Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. – Part 1: Generic Reference Framework.	Under Drafting

Table 7: Current work items of CEN-CLC/JTC 21.

Standard No.	Title.	Status
prCEN/CLC/TR 17894 (WI=JT021001)	Artificial Intelligence Conformity Assessment	Under Drafting
prCEN/CLC/TR XXXX (WI=JT021002)	Artificial Intelligence - Overview of Al Tasks and functionalities related to natural language processing	Under Drafting
prCEN/TR XXX (WI=JT021007)	Data Governance and data quality for AI in the European context	Preliminary
prCEN/TR XXX (WI=JT021009)	AI Risks - Check List for AI Risks Management	Preliminary
prEN ISO/IEC 22989 (WI=JT021004)	Information technology - Artificial intelligence - Artificial intelligence concepts and terminology	Under Drafting
prEN ISO/IEC 23053 (WI=JT021005)	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	Under Drafting
prEN XXX (WI=JT021008)	Artificial Intelligence trustworthiness characterization	Preliminary

4.4 Standardization activities on national level

Regarding the standardization activities on national level, it must be pointed out that only standards with at least an English title were considered. Other standards were excluded due to the language barrier. Nevertheless, 37 national standards were highlighted as relevant for IMPULSE project. An overview of the nations which developed these standards is given in Table 8.

Table 8: Relevant national standardization bodies.

Germany	BSI - Federal Office for Information Security
	DIN - German Institute for Standardization
US	NIST - National Institute of Standards and Technology
	ANSI - American National Standards Institute
Canada	CSA Group - Canadian Standards Association Group
Spain	UNE - Spanish Association for Standardization
France	AFNOR - French Standardization Association
Sweden	SIS - Swedish Institute for Standards

The majority of the highlighted standards, namely 23 were developed in **Germany,** although the German standardization body DIN is not the main publisher with 7 standards, but the Federal Office for Information Security (BSI) with 13 standards. The BSI is the Federal Cyber Security Authority in Germany, which shapes the information security in digitization through prevention, detection and reaction for government, business and society.[37] In addition, there is one standard each from the Association of German Engineers (VDI) and the Mechanical Engineering Industry Association (VDMA). The second highest proportion of national standards, 10, is from the **US**. These were published by the National Institute of Standards and Technology (NIST), which is part of the **US**. Department of Commerce[38] and the American National Standards Institute (ANSI), a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system.[39] The remaining relevant standards were published by the **Canadian** Standards Association Group (CSA Group), the **Spanish** Association for Standardization (UNE), the **French** Standardization Association (AFNOR), and the **Swedish** Institute for Standards (SIS).

4.5 Highly relevant formal standards

Standards which are used within IMPULSE e.g. for developing the IMPULSE solution or whose topics are strongly related to IMPULSE were highlighted as highly relevant standards. Nine standards were identified as highly relevant for IMPULSE (Table 9). Their content and relevance for IMPULSE are described in the following.

Table 9: Standards rated as highly relevant by the WP's.

Document No.	Title	Date of Publication
CEN/TS 16921	Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems	2016-03
DIN SPEC 4997	Privacy by Blockchain Design: A standardized model for processing personal data using blockchain technology	2020-04

[37] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=A075659575DD9293CD44FA999E3741DC.internet471

[38] https://www.nist.gov/about-nist

[39] https://www.ansi.org/about/introduction

ETSI GR SAI 001 V 1.1.1	Securing Artificial Intelligence (SAI) - AI Threat Ontology	2022-01
ETSI GR SAI 002 V 1.1.1	Securing Artificial Intelligence (SAI) - Data Supply Chain Security	2021-08
ETSI TS 119 182-1	Electronic Signatures and Infrastructures (ESI) - JAdES digital signatures - Part 1: Building blocks and JAdES baseline signatures	2021-03
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	2018-11
ISO/IEC 27001	Information technology - Security techniques - Information security management systems - Requirements	2022-10
ISO/IEC 30107 series	Information technology — Biometric presentation attack detection	Since 2022-01
UNE 71207-1	Digital Enabling Technologies - Distributed Identities Management Model on Blockchain and other Distributed Ledger Technologies. Part 1: Reference Framework	2020-12

CEN/TS 16921 - Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems

This technical specification primarily focuses on biometric aspects of portable verification and identification systems for law enforcement and border control authorities. The recommendations given here will balance the needs for security, ease of access and data protection. This technical specification extends the ISO standards by emphasizing specific European needs.[40] Since this specification focuses on the personal identification using mobile biometric identification systems it is probably the most relevant standard for facial recognition and document verification services. These services are used within the IMPULSE project to identify citizens who request an enrolment process that leads to the issuance of a credential that proves the citizen’s identity. That is why this TS is considered as highly relevant for the IMPULSE project.

DIN SPEC 4997 - Privacy by Blockchain Design: A standardized model for processing personal data using blockchain technology

This DIN SPEC establishes general principles for and methods of handling personal data in BC/DLT systems. It specifies technical and organizational measures for data protection while taking into account the principles of privacy by design as well as specifications that are inspired by legal frameworks, such as the GDPR.[41] This specification provides a standardized model for processing personal data using blockchain technology, which is a must-read standard in order to design a new decentralised eID model compliant with the current standards. Therefore, it is extremely relevant for IMPULSE.

ETSI GR SAI 001 - Securing Artificial Intelligence (SAI) - AI Threat Ontology

The document defines what an Artificial Intelligence (AI) threat is and defines how it can be distinguished from any non-AI threat. The model of an AI threat is presented in the form of an ontology to give a view of the relationships between actors representing threats, threat agents, assets and so forth. The ontology described in the present document applies to AI both as a threat agent and as an attack target.[42] This standard is used to discover security vulnerabilities and attacks to IMPULSE AI systems based on threat modelling. In this context and as an example, a forgery simulator (AI threat/attack agent) has been developed in order to train/test the ID document verification module (system design). Specific metrics are obtained to assess the model and provide feedback.

[40] https://standards.iteh.ai/catalog/standards/cen/936c835a-9724-478f-9dab-dfcd79244767/cen-ts-16921-2016

[41] https://www.beuth.de/de/technische-regel/din-spec-4997/321277504

[42] https://www.etsi.org/deliver/etsi_gr/SAI/001_099/001/01.01.01_60/gr_SAI001v010101p.pdf

ETSI GR SAI 002 - Securing Artificial Intelligence (SAI) - Data Supply Chain Security

The document summarizes the methods currently used to source data for training AI, along with a review of existing initiatives for developing data sharing protocols. It then provides a gap analysis on these methods and initiatives to scope possible requirements for standards for ensuring integrity and confidentiality of the shared data, information, and feedback.[43] In the context of ID documents' verification module, there is a need to collect photos of ID documents (provided by volunteers from different countries) in order to train an AI based forgery detection model. In this sense, TREE provided a multi-language form to obtain labelled dataset (photos of front/back sides of ID cards and the biodata page of passports). During this process, TREE team followed this standard's recommendations in term of data sources, data curation, training/testing and deployment of the forgery detection solution. Mechanisms to preserve integrity through cybersecurity hygiene and supply chain security has been followed. It is important to note, that a legal framework has been deployed during data collection/processing (privacy notice to participants) and in total respect of GDPR regulations.

ETSI TS 119 182-1 - Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures

The document is intended to cover digital signatures supported by PKI and public key certificates, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, among other, applicable requirements from Regulation (EU) No 910/2014 [i.1].[44] This document specifies a JSON format for AdES signatures (JAdES signatures) built on JSON Web Signatures (JWS) as specified in IETF RFC 7515. It is used in IMPULSE to build a profile for the Verifiable Credential signature.

ISO/IEC 20889 - Privacy enhancing data de-identification terminology and classification of techniques

This document provides a description of privacy-enhancing data de-identification techniques, to be used to describe and design de-identification measures in accordance with the privacy principles in ISO/IEC 29100.[45] This is a fundamental standard for IMPULSE due to its relevance to the technical specifications of the project. In fact, the standard deals with Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity, and confidentiality of information and Security aspects of identity management, biometrics, and privacy which is highly relevant for IMPULSE.

ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements

This document specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.[46] This standard is already implemented in most of the companies working on the technical side of the IMPULSE project. It provides security requirements to be considered for information security management in IMPULSE.

ISO/IEC 30107 series - Information technology — Biometric presentation attack detection

Part 1: Framework

The purpose of ISO/IEC 30107-1 is to provide a foundation for presentation attack detection (PAD) through defining terms and establishing a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed, and communicated for subsequent decision making and performance assessment activities. This foundation is intended to not only introduce and frame the topics of presentation attacks and PAD but also to benefit other standards projects.[47]

[43] https://www.etsi.org/deliver/etsi_gr/SAI/001_099/002/01.01.01_60/gr_SAI002v010101p.pdf
[44] https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010101p.pdf
[45] https://www.iso.org/standard/69373.html
[46] https://www.iso.org/standard/82875.html
[47] https://www.iso.org/standard/53227.html

Part 2: Data formats

ISO/IEC 30107-2:2017 defines data formats for conveying the mechanism used in biometric presentation attack detection and for conveying the results of presentation attack detection methods. The attacks considered in the ISO/IEC 30107 series take place at the sensor during the presentation and collection of the biometric characteristics. Any other attacks are outside the scope of this document.[48]

Part 3: Testing and reporting

ISO/IEC 30107-3:2017 establishes: principles and methods for performance assessment of presentation attack detection mechanisms; reporting of testing results from evaluations of presentation attack detection mechanisms; a classification of known attack types (in an informative annex).[49]

Part 4: Profile for testing of mobile devices

This document is a profile that provides requirements for testing biometric presentation attack detection (PAD) mechanisms on mobile devices with local biometric recognition.[50]

These standards provide information on how to evaluate the security regarding biometrics. In the IMPULSE project the metrics described in this document are used.

UNE 71207-1 - Digital Enabling Technologies - Distributed Identities Management Model on Blockchain and other Distributed Ledger Technologies. Part 1: Reference Framework

This standard defines a reference framework for the management of decentralized identities oriented to people, physical and legal, which includes the description of an approach based on life cycles and the relationship of the main actors that participate in them, as well as the interrelationships among them.[51] The purpose of the IMPULSE project is not to design a new identity model, but to use an existing one. The UNE 71307-1 standard directly tackles the management of digital identities in a decentralised manner. Therefore, this standard is used in IMPULSE to follow the best practices for decentralised identity management. The GRAD team is a member of the CTN 71/SC 307 Committee in UNE (Blockchain and distributed ledger technologies) which developed this standard. The main contributions from the IMPULSE partner to this standard relate to security and privacy aspects of the use of DLTs/blockchain networks in the context of digital identity.

4.6 Informal standardization activities

Besides the official standardization organisation relevant so called informal standards (see clause 2.1) are developed by other standard setting organisations. In the context of the IMPULSE project 97 informal standards were rated as relevant for the project.

The majority of those standards (37) were developed within the World Wide Web Consortium (**W3C**). Within the international community of member organizations, full-time staff, and the public the goal is to develop Web standards.[52] The standards from W3C define an Open Web Platform for application development enabling the developers to build interactive experiences. Technical specifications and guidelines are developed within W3C by focusing on the consensus about the content to ensure high technical and editorial quality.[53] In the context of Self Sovereign Identity (SSI), W3C is the most acknowledged standardization organisation. It is hosting different working groups such as the *Decentralized Identifier WG* and the *Verifiable Credentials WG* to develop standards for the core elements of the decentralized identity.[54]

Another important actor in the field of relevant standards for IMPULSE is the Decentralized Identity Foundation (**DIF**) which developed 14 informal standards rated as relevant. This engineering-driven organization focuses on developing foundational elements necessary to establish an open ecosystem for

[48] https://www.iso.org/standard/67380.html
[49] https://www.iso.org/standard/67381.html
[50] https://www.iso.org/standard/75301.html
[51] https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0064986
[52] https://www.w3.org/Consortium/
[53] https://www.w3.org/standards/
[54] https://www.w3.org/groups/wg/

decentralized identity and ensures interoperability between all participants.[55] DIF aims to advance the interests of the decentralized identity community, including performing research and development to advance "pre-competitive" technical foundations towards established interoperable, global standards.[56]

The Internet Engineering Task Force (**IETF**) is another developer of informal standards relevant for IMPULSE. This organisation published 10 of the relevant informal standards. The scope of IETF is the development of technical documents that influence the way people design, use and manage the internet[57] within a large open international community.[58]

Within the **OpenID Foundation** 9 of the relevant informal standards were published. This non-profit international standardization organization includes individuals as well as companies which are active in 10 working groups.[59]

Further relevant standards (4) were published by the Institute of Electrical and Electronics Engineers (**IEEE**). IEEE is the world's largest technical professional organization and a leading developer of international standards in the field of telecommunication, information technology, and power-generation products and services.[60]

The remaining informal standards rated as relevant for IMPULSE are from OASIS Open, The Open Group Architecture Forum, Kantara Initiative or cannot be assigned to a specific organization. **OASIS Open** is a non-profit standards body offering projects a path to standardization and de jure approval for reference in international policy and procurement.[61] **The Open Group Architecture Forum** develops standards for enterprise architectures and certification for enterprise IT and business architecture.[62] At **Kantara Initiatives**, ID systems and credential service providers are assessed against privacy and security standards.[63]

4.7 Highly relevant informal standards

Regarding the informal standards it is important to keep in mind that some of the mentioned standards are at an early stage of development. This also means that they represent the most advanced documents in the industry. During the standards assessment six informal standards were highlighted as highly relevant for IMPULSE (Table 10).

Table 10: Informal standards rated as highly relevant by the WP's.

Title	Date of Publication
Decentralized Identifiers (DIDs) v1.0	2022-07-19
JSON-LD 1.1	2020-07-16
OpenId Specifications for Verifiable Credential Issuance	2022-10-27
OpenId Specifications for Verifiable Presentations	2022-09-06
Verifiable Credentials Data Model 1.1	2022-03-03
Verifiable Credentials JSON Schema Specification	2019-12-11

Decentralized Identifiers (DIDs) v1.0

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DID's have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.

[55] https://identity.foundation/
[56] https://identity.foundation/governance/about
[57] https://www.ietf.org/about/mission/
[58] https://www.ietf.org/about/who/
[59] https://openid.net/foundation/
[60] https://www.ieee.org/about/at-a-glance.html
[61] https://www.oasis-open.org/org/
[62] https://www.opengroup.org/architecture-forum
[63] https://kantarainitiative.org/

Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party.[64] This informal standard could become the first new identifier the W3C would approve since the URL. This document specifies the algorithms and guidelines for resolving DIDs and dereferencing DID URL's. It is the basis of the technology stacks on which IMPULSE will implement its services. Nevertheless, even if the document can fit on a strictly security aspect, on privacy issues its adoption should be assessed with caution.

JSON-LD 1.1

JSON is a useful data serialization and messaging format. This specification defines JSON-LD 1.1, a JSON-based format to serialize Linked Data. The syntax is designed to easily integrate into deployed systems that already use JSON and provides a smooth upgrade path from JSON to JSON-LD. It is primarily intended to be a way to use Linked Data in Web-based programming environments, to build interoperable Web services, and to store Linked Data in JSON-based storage engines.[65] This informal standard is used within IMPULSE for the REST APIs.

OpenId Specifications for Verifiable Credential Issuance

This specification defines an API designated as Credential Endpoint that is used to issue verifiable credentials and corresponding OAuth 2.0 based authorization mechanisms that the Wallet uses to obtain authorization to receive verifiable credentials.[66] This informal standard is used by ESSIF to provide guidelines for the process of issuing Verifiable Credentials. In the IMPULSE project we follow these guidelines for the issuance of EBSI Verifiable Authorisations and EBSI Verifiable Identities.

OpenId Specifications for Verifiable Presentations

This specification defines a mechanism on top of OAuth 2.0 [RFC6749] for presentation of claims via verifiable credentials, supporting W3C formats as well as other credential formats. This allows existing OpenID Connect RPs to extend their reach towards claim sources asserting claims in this format. It also allows new applications built using verifiable credentials to utilize OAuth 2.0 or OpenID Connect as integration and interoperability layer towards credential holders.[67] This informal standard is used by ESSIF to provide guidelines for the process of creating Verifiable Presentations. In the IMPULSE project we follow these guidelines for the verifiable presentations of EBSI Verifiable Authorisations and EBSI Verifiable Identities.

Verifiable Credentials Data Model 1.1

Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.[68] This informal standard provides a mechanism to express the credentials used on the decentralized eID management approach in a way that is cryptographically secure, privacy respecting, and machine-verifiable. In the IMPULSE project this is essential for the user identification.

Verifiable Credentials JSON Schema Specification

The [VC_DATA_MODEL] specifies the models used for Verifiable Credentials and Verifiable Presentations, and explains the relationships between three parties: issuer, holder, and verifier. A critical piece of infrastructure out of the scope of those specifications is the Credential Schema. This specification provides a mechanism to express a Credential Schema and the protocols for evolving the schema.[69] The Identity Verifiable Credentials used in IMPULSE will need to be compliant with this specification.

[64] https://www.w3.org/TR/did-core/#:~:text=Abstract,the%20controller%20of%20the%20DID.
[65] https://www.w3.org/TR/json-ld11/
[66] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[67] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[68] https://www.w3.org/TR/vc-data-model/
[69] https://w3c-ccg.github.io/vc-json-schemas/v1/index.html#:~:text=The%20Credential%20Schema%20is%20a,data%20in%20a%20known%20way.

5 Summary and Conclusion

Generally, the present deliverable gives an overview of the standardization landscape related to the IMPULSE project and therefore summarizes the results of Task 3.4 - *Analysis of existing relevant standards, and related impacts and implications*. This is important for the project since it enables the development of solutions which are compliant with the latest standards. Therefore, a standards database in form of a dashboard was created which includes 389 standards which could be somehow relevant for the project. On the one hand, this dashboard offers the opportunity to search for specific standards. On the other hand, the overview this dashboard gives provides the opportunity to identify standardization gaps and is therefore the basis for Task 7.6 - *Initiation of standardization activities* of WP7. Within this deliverable, the dashboard was used to describe the standardization activities on international, European, and national level related to IMPULSE. Besides the formal standards, which are included in the dashboard, relevant informal standardization activities are also analyzed. A specific focus was laid on standards, formal and informal ones, highlighted as highly relevant for the project. Nine formal and six informal standards were categorized as highly relevant for the project since these standards are used for the development of the IMPULSE solution. Due to the great importance of these standards for the project they are also presented on the IMPULSE website to raise awareness of them outside the consortium as well. Furthermore, this deliverable offers an overview of the TC's which are working on standards related to IMPULSE. Since the interaction with relevant standardization committees is targeted in Task 7.6, an overview of current work items of the TC's interesting to IMPULSE on European level is provided. Through all the work done within Task 3.4 the awareness for standardization was raised throughout the consortium and the basis was laid for Task 7.6.

Annex A Relevant standards

A.1 Formal Standards rated as relevant by the consortium

Table 11: Formal standards rated as relevant by the consortium.

Document No.	Title	Date of Publication
ANSI X 9.138	Distributed Ledger Technologies Terminology	2020
ANSI/ATIS 1000035	Next Generation Network (NGN) Identity Management (IdM) Framework	2009
ANSI/ATIS 1000045	ATIS Identity Management: Mechanisms and Procedures Standard	2012
ANSI/INCITS/ISO/IEC 11770-4 AMD 1	Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets - Amendment 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)	2019
BASI/TR 03105 Part 3.3 V1.2	Conformity Tests for Official Electronic ID Documents - Part 3.3: Test Plan for eID-Cards withAdvanced Security Mechanisms - EAC 2; Version 1.2	2020-02
BASI/TR 03105 Part 3.4*BASI/TR 03105 Teil 3.4	Test plan for eID-cards with eSign-application acc. to BSI TR-03117; Version 1.0	2010-04
BASI/TR 03105 Part 5.2 V2.0*BASI/TR 03105 Teil 5.2	Test plan for eID and eSign compliant smart card readers with EACv2; Version 2.0	2015-05
BASI/TR 03105 Part 5.3 V2.0*BASI/TR 03105 Teil 5.3	Test plan for eID and eSign compliant terminal software with EACv2; Version 2.0	2015-05
BASI/TR 03110-1 V2.20*TR-03110-1	Advanced security mechanisms for machine readable travel documents - Part 1: eMRTD with BAC/PACEv2 and EACv1; Version 2.20	2015-02
BASI/TR 03110-2 V2.21	Advanced security mechanisms for machine readable travel documents and eIDAS token - Part 2 - Protocols for electronic IDentification, authentication and trust services (eIDAS); Version 2.21	2016-12
BASI/TR 03110-3 V2.21	Advanced security mechanisms for machine readable travel documents and eIDAS token - Part 3: Common specifications; Version 2.21	2016-12
BASI/TR 03110-4 V2.21	Advanced security mechanisms for machine readable travel documents and eIDAS token - Part 4 - Applications and document profiles; Version 2.21	2016-12
BASI/TR 03119 V1.41	Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control; Version 1.41	2020-01
BASI/TR 03130-1 V2.4.0	eID-Server - Part 1: Functional specification; Version 2.4.0	2021-08
BASI/TR 03130-2 V2.1.2	eID-Server - Part 2: Security Framework for eID-Server operations; Version 2.1.2	2017-10
BASI/TR 03130-3 V1.1	eID-Server - Part 3: eIDAS-Middleware-Service for eIDAS-Token; Version 1.1	2020-02
BASI/TR 03130-4 V1.2*TR-03130	eID-Server - Part 4: Conformance test specification; Version 1.2	2021-03

Document No.	Title	Date of Publication
CAN/CIOSC 101	Ethical design and use of automated decision systems	2019-10
CAN/CIOSC 103-1	Digital Trust and Identity - Part 1: Fundamentals	2020-09
CEN/TR 419010	Framework for standardization of signatures - Extended structure including electronic identification and authentication	2017-05
CEN/TR 419040	Rationalized structure for electronic signature standardization - Guidelines for citizens	2018-05
CEN/TR 419200	Guidance for signature creation and other related devices	2017-05
CEN/TR 419210	Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)	2019-03
CEN/TS 15291	Identification card system - Guidance on design for accessible card-activated devices	2006-01
CEN/TS 15480-1	Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics	2012-10
CEN/TS 15480-2	Identification card systems - European Citizen Card - Part 2: Logical data structures and security services	2012-06
CEN/TS 15480-3	Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface	2014-04
CEN/TS 15480-4	Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use	2012-03
CEN/TS 15480-5	Identification card systems - European Citizen Card - Part 5: General Introduction	2013-04
CEN/TS 16428	Biometrics Interoperability profiles - Best Practices for slap tenprint captures	2012-10
CEN/TS 16634	Personal identification - Recommendations for using biometrics in European Automated Border Control	2014-04
CEN/TS 16921	Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems Personenidentifikation	2016-03
CEN/TS 17051	Full body photography Photographie du corps entier	2017-05
CEN/TS 17261	Biometric authentication for critical infrastructure access control - Requirements and Evaluation	2018-12
CEN/TS 17262	Personal identification - Robustness against biometric presentation attacks - Application to European Automated Border Control	2018-12
CEN/TS 17489-1	Personal identification - Secure and interoperable European Breeder Documents - Part 1: Framework overview	2020-08
CEN/TS 17631	Personal identification - Biometric group access control	2021-06
CEN/TS 419221-1	Protection Profiles for TSP cryptographic modules - Part 1: Overview	2016-07
CEN/TS 419221-2	Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup	2016-07
CEN/TS 419221-3	Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services	2016-07
CEN/TS 419221-4	Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup	2016-07

Document No.	Title	Date of Publication
CEN/TS 419221-6	Conditions for use of EN 419221-5 as a qualified electronic signature or seal creation device	2019-03
CEN/TS 419261	Security requirements for trustworthy systems managing certificates and time-stamps	2015-03
CWA 15263:2005	Analysis of privacy protection technologies, privacy-enhancing technologies (PET), privacy management systems (PMS) and identity management systems (IMS), the drivers thereof and the need for standardization	2005-04
CWA 15264-1	Architecture for a European interoperable eID system within a smart card infrastructure	2005-04
CWA 15264-3	User Requirements for a European interoperable eID system within a smart card infrastructure	2005-04
CWA 15535-1	Multi-application multi-issuer citizen card scheme standardisation - Part 1: Business model agreement	2006-04
CWA 17025-108	Business Interoperability Interfaces for Public Procurement in Europe - Architecture - Part 108: Use of Digital Signature and Other Trust Services	2016-05
DIN EN ISO/IEC 17030	Conformity assessment - General requirements for third-party marks of conformity (ISO/IEC DIS 17030:2021); German and English version prEN ISO/IEC 17030:2021	2021-02
DIN SPEC 13266	Guideline for the development of deep learning image recognition systems	2020-04
DIN SPEC 16597	Terminology for blockchains; Text in English	2018-02
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English	2020-04
DIN SPEC 92001-1	Artificial Intelligence - Life Cycle Processes and Quality Requirements - Part 1: Quality Meta Model; Text in English	2019-04
DIN SPEC 92001-2	Artificial Intelligence - Life Cycle Processes and Quality Requirements - Part 2: Robustness	2020-12
DIN/TS 31648	Criteria for Trusted Transactions - Records Management and Evidence Retention in DLT and Blockchain	2021-04
EN 1332-1	Identification card systems - Human-machine interface - Part 1: Design principles for the user interface	2009-07
EN 1332-2	Identification card systems - Man-machine interface - Part 2: Dimensions and location of a tactile identifier for ID-1 cards	1998-05
EN 1332-3	Identification card systems - User Interface - Part 3: Key pads	2020-07
EN 1332-4	Identification card systems - Man-machine interface - Part 4: Coding of user requirements for people with special needs	2007-06
EN 1332-5	Identification card systems - Man-machine interface - Part 5: Raised tactile symbols for differenciation of application on ID-1 cards	2006-03
EN 15320	Identification card systems - Surface transport applications - Interoperable Public Transport Applications - Framework	2007-12
EN 1545-1	Identification card systems - Surface transport applications - Part 1: Elementary data types, general code lists and general data elements	2015-04

Document No.	Title	Date of Publication
EN 1545-2	Identification card systems - Surface transport applications - Part 2: Transport and travel payment related data elements and code lists	2015-04
EN 17054	Biometrics multilingual vocabulary based upon the English version of ISO/IEC 2382-37:2012	2019-05
EN 319411-1 V 1.3.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements	2021-05
EN 319412-1 V 1.4.4	Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures	2021-05
EN 319412-2 V 2.2.1	Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons	2020-07
EN 319412-3 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons	2020-07
EN 419211-2	Protection profiles for secure signature creation device - Part 2: Device with key generation	2013-07
EN 419211-2	Protection profiles for secure signature creation device - Part 2: Device with key generation	2013-07
EN 419211-3	Protection profiles for secure signature creation device - Part 3: Device with key import	2013-10
EN 419211-4	Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application	2013-11
EN 419211-5	Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application	2013-12
EN 419212-1	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions	2017-09
EN 419212-2	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services	2017-12
EN 419212-3	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols	2017-09
EN 419212-4	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols	2018-04
EN 419212-5	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService	2018-04
EN 419221-5	Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services	2018-05
EN 419231	Protection profile for trustworthy systems supporting time stamping	2019-08
EN 419241-1	Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements	2018-07

Document No.	Title	Date of Publication
EN 419241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing	2019-02
EN 419251-1	Security requirements for device for authentication - Part 1: Protection profile for core functionality	2013-03
EN 419251-2	Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application	2013-03
EN 419251-3	Security requirements for device for authentication - Part 3: Additional functionality for security targets	2013-03
ETSI GR SAI 004 V 1.1.1	Securing Artificial Intelligence (SAI) - Problem Statement	2020-12
ETSI TR 119000 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - The framework for standardization of signatures: overview	2016-04
ETSI TR 119001 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - The framework for standardization of signatures - Definitions and abbreviations	2016-03
ETSI TR 119100 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Guidance on the use of standards for signature creation and validation	2016-03
ETSI TR 119112 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Most significant differences between AdES/ASiC ENs and previous TSs	2019-04
ETSI TR 119124-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Testing Conformance and Interoperability - Part 1: Overview	2016-06
ETSI TR 119134-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Testing Conformance and Interoperability - Part 1: Overview	2016-06
ETSI TR 119144-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Testing Conformance and Interoperability - Part 1: Overview	2016-06
ETSI TR 119164-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) - Testing Conformance and Interoperability - Part 1: Overview	2016-06
ETSI TR 119300 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Guidance on the use of standards for cryptographic suites	2016-03
ETSI TR 119400 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Guidance on the use of standards for trust service providers supporting digital signatures and related services	2016-03
ETSI TR 119411-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2	2018-05
ETSI TR 119460 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Survey of technologies and regulatory requirements for identity proofing for trust service subjects	2021-02
ETSI TR 119500 V 1.1.1	Business Driven Guidance for Trust Application Service Providers	2019-02
ETSI TR 119530 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Registered Electronic Mail (REM) - Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-based systems	2019-02

Document No.	Title	Date of Publication
ETSI TR 133924 V 16.0.0*3GPP TR 33.924 Version 16.0.0 Release 16	Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - LTE - Identity management and 3GPP security interworking - Identity management and Generic Authentication Architecture (GAA) interworking (3GPP TR 33.924 version 16.0.0 Release 16)	2020-08
ETSI TS 119101 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for applications for signature creation and signature validation	2016-03
ETSI TS 119102-1 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation	2018-08
ETSI TS 119102-2 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 2: Signature Validation Report	2019-02
ETSI TS 119122-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES	2017-01
ETSI TS 119124-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Testing Conformance and Interoperability - Part 2: Test suites for testing interoperability of CAdES baseline signatures	2016-06
ETSI TS 119124-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Testing Conformance and Interoperability - Part 3: Test suites for testing interoperability of extended CAdES signatures	2016-06
ETSI TS 119124-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Testing Conformance and Interoperability - Part 4: Testing Conformance of CAdES baseline signatures	2016-06
ETSI TS 119124-5 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - CAdES digital signatures - Testing Conformance and Interoperability - Part 5: Testing Conformance of extended CAdES signatures	2016-06
ETSI TS 119132-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES	2021-01
ETSI TS 119134-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Testing Conformance and Interoperability - Part 2: Test suites for testing interoperability of XAdES baseline signatures	2016-06
ETSI TS 119134-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Testing Conformance and Interoperability - Part 3: Test suites for testing interoperability of extended XAdES signatures	2016-06
ETSI TS 119134-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Testing Conformance and Interoperability - Part 4: Testing Conformance of XAdES baseline signatures	2016-06
ETSI TS 119134-5 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - XML Advanced Electronic Signature (XAdES) Testing Compliance & Interoperability - Part 5: Conformance Testing for XAdES Baseline Profile	2012-04

Document No.	Title	Date of Publication
ETSI TS 119134-5 V 2.1.1	Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Testing Conformance and Interoperability - Part 5: Testing Conformance of extended XAdES signatures	2016-06
ETSI TS 119142-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)	2016-12
ETSI TS 119144-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PDF Advanced Electronic Signature (PAdES) Testing Compliance & Interoperability - Part 2: Test Suite for PAdES interoperability test events	2012-03
ETSI TS 119144-2 V 2.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Testing Conformance and Interoperability - Part 2: Test suites for testing interoperability of PAdES baseline signatures	2016-06
ETSI TS 119144-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Testing Conformance and Interoperability - Part 3: Test suites for testing interoperability of additional PAdES signatures	2016-06
ETSI TS 119144-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Testing Conformance and Interoperability - Part 4: Testing Conformance of PAdES baseline signatures	2016-06
ETSI TS 119144-5 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - PAdES digital signatures - Testing Conformance and Interoperability - Part 5: Testing Conformance of additional PAdES signatures	2016-06
ETSI TS 119164-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) Testing Compliance & Interoperability - Part 2: Test Suite for ASiC interoperability test events	2012-03
ETSI TS 119164-2 V 2.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) - Testing Conformance and Interoperability - Part 2: Test suites for testing interoperability of ASiC baseline containers	2016-06
ETSI TS 119164-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) - Testing Compliance and Interoperability - Part 3: Test suites for testing interoperability of ASiC containers other than baseline	2016-06
ETSI TS 119164-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) - Testing Compliance and Interoperability - Part 4: Testing Conformance of ASiC baseline containers	2016-06
ETSI TS 119164-5 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC) - Testing Compliance and Interoperability - Part 5: Testing Conformance of additional ASiC containers	2016-06
ETSI TS 119172-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Signature Policies - Part 1: Building blocks and table of contents for human readable signature policy documents	2015-07
ETSI TS 119172-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Signature Policies - Part 2: XML format for signature policies	2019-12
ETSI TS 119172-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Signature Policies - Part 3: ASN.1 format for signature policies	2019-12

Document No.	Title	Date of Publication
ETSI TS 119172-4 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Signature Policies - Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists	2021-05
ETSI TS 119182-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - JAdES digital signatures - Part 1: Building blocks and JAdES baseline signatures	2021-03
ETSI TS 119192 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - AdES related Uniform Resource Identifier	2021-05
ETSI TS 119312 V 1.3.1	Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites	2019-02
ETSI TS 119403-2 V 1.2.4	Electronic Signatures and Infrastructures (ESI) - Trust Service Provider Conformity Assessment - Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates	2020-11
ETSI TS 119403-3 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Trust Service Provider Conformity Assessment - Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers	2019-03
ETSI TS 119412-1 V 1.4.1	Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures	2020-07
ETSI TS 119431-1 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers - Part 1: TSP service components operating a remote QSCD / SCDev	2021-05
ETSI TS 119431-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers - Part 2: TSP service components supporting AdES digital signature creation	2018-12
ETSI TS 119432 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Protocols for remote digital signature creation	2020-10
ETSI TS 119441 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy requirements for TSP providing signature validation services	2018-08
ETSI TS 119442 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Protocol profiles for trust service providers providing AdES digital signature validation services	2019-02
ETSI TS 119495 V 1.5.1	Electronic Signatures and Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking	2021-04
ETSI TS 119511 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques	2019-06
ETSI TS 119512 V 1.1.2	Electronic Signatures and Infrastructures (ESI) - Protocols for trust service providers providing long-term data preservation services	2020-10
ETSI TS 119524-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Electronic Registered Delivery Services - Part 1: Testing conformance	2019-02
ETSI TS 119524-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Electronic Registered	2019-02

Document No.	Title	Date of Publication
	Delivery Services - Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers	
ETSI TS 119534-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Registered Electronic Mail Services - Part 1: Testing conformance	2019-02
ETSI TS 119534-2 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Registered Electronic Mail Services - Part 2: Test suites for interoperability testing of providers using same format and transport protocols	2019-02
ETSI TS 119612 V 1.2.1	Electronic Signatures and Infrastructures (ESI) - Trusted Lists	2014-04
ETSI TS 119612 V 2.2.1	Electronic Signatures and Infrastructures (ESI) - Trusted Lists	2016-04
ETSI TS 119614-1 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Trusted Lists - Part 1: Specifications for testing conformance of XML representation of Trusted Lists	2016-06
ETSI TS 119615 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Trusted lists - Procedures for using and interpreting European Union Member States national trusted lists	2021-05
ETSI TS 124175 V 16.0.0*3GPP TS 24.175 Version 16.0.0 Release 16	Universal Mobile Telecommunications System (UMTS) - LTE - 5G - Management Object (MO) for multi-device and multi-identity in the IP Multimedia Subsystem (IMS) (3GPP TS 24.175 version 16.0.0 Release 16)	2020-11
EUV 910/2014*EUReg 910/2014*UEReg 910/2014*eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	2014-07
EUV910/2014DG		2017-07
FprCEN/TS 17661	Personal identification - European enrolment guide for biometric ID documents (EEG)	2021-04
ISO 14533-1	Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)	2014-12
ISO 14533-2	Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)	2021-08
ISO 14533-3	Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)	2017-09
ISO 14533-4	Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)	2019-08
ISO 15836-1	Information and documentation - The Dublin Core metadata element set - Part 1: Core elements	2017-05

Document No.	Title	Date of Publication
ISO 15836-2	Information and documentation - The Dublin Core metadata element set - Part 2: DCMI Properties and classes	2019-12
ISO 19626-1	Processes, data elements and documents in commerce, industry and administration - Trusted communication platforms for electronic documents - Part 1: Fundamentals	2020-03
ISO 19626-2	Processes, data elements and documents in commerce, industry and administration - Trusted communication platform for electronic documents - Part 2: Applications	2021-02
ISO 20415	Trusted mobile e-document framework - Requirements, functionality and criteria for ensuring reliable and safe mobile e-business	2019-10
ISO 20614	Information and documentation - Data exchange protocol for interoperability and preservation	2017-11
ISO 22739	Blockchain and distributed ledger technologies - Vocabulary	2020-07
ISO/DIS 23257	Blockchain and distributed ledger technologies - Reference architecture	2020-09
ISO/DIS 24165-1	Digital token identifier (DTI) - Registration, assignment and structure - Part 1: Method for registration and assignment	2021-02
ISO/DIS 24165-2	Digital token identifier (DTI) - Registration, assignment and structure - Part 2: Data elements for registration	2021-02
ISO/IEC 11770-1	Information technology - Security techniques - Key management - Part 1: Framework	2010-12
ISO/IEC 11770-2	IT Security techniques - Key management - Part 2: Mechanisms using symmetric techniques	2018-10
ISO/IEC 11770-3 AMD 1	Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques - Amendment 1: Blinded Diffie-Hellman key agreement	2017-11
ISO/IEC 11770-4 AMD 2	Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets - Amendment 2: Leakage-resilient password-authenticated key agreement with additional stored secrets	2021-02
ISO/IEC 11770-5	Information security - Key management - Part 5: Group key management	2020-11
ISO/IEC 11770-6	Information technology - Security techniques - Key management - Part 6: Key derivation	2016-10
ISO/IEC 11770-7	Information security - Key management - Part 7: Cross-domain password-based authenticated key exchange	2021-07
ISO/IEC 13888-1	Information security - Non-repudiation - Part 1: General	2020-09
ISO/IEC 13888-2 Technical Corrigendum 1	Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques; Technical Corrigendum 1	2012-12
ISO/IEC 13888-3	Information security - Non-repudiation - Part 3: Mechanisms using asymmetric techniques	2020-09
ISO/IEC 14888-2 Technical Corrigendum 1	Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms; Technical Corrigendum 1	2015-10
ISO/IEC 14888-3	IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms	2018-11

Document No.	Title	Date of Publication
ISO/IEC 15408-2	Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components	2008-08
ISO/IEC 15408-3	Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components	2008-08
ISO/IEC 15946-1	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General	2016-07
ISO/IEC 15946-5	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation	2017-08
ISO/IEC 17825	Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	2016-01
ISO/IEC 17922	Information technology - Security techniques - Telebiometric authentication framework using biometric hardware security module	2017-09
ISO/IEC 18014-1	Information technology - Security techniques - Time-stamping services - Part 1: Framework	2008-09
ISO/IEC 18014-2	Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens	2021-09
ISO/IEC 18014-3	Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens	2009-12
ISO/IEC 18014-4	Information technology - Security techniques - Time-stamping services - Part 4: Traceability of time sources	2015-04
ISO/IEC 18031 AMD 1	Information technology - Security techniques - Random bit generation - Amendment 1: Deterministic random bit generation	2017-02
ISO/IEC 18032	Information security - Prime number generation	2020-12
ISO/IEC 18033-1	Information technology - Security techniques - Encryption algorithms - Part 1: General	2021-09
ISO/IEC 18033-2 AMD 1	Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers; Amendment 1: FACE	2017-11
ISO/IEC 18033-3 AMD 1	Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers - Amendment 1: SM4	2021-06
ISO/IEC 18033-4 AMD 1	Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers - Amendment 1: ZUC	2020-08
ISO/IEC 18033-5 AMD 1	Information technology - Security techniques - Encryption algorithms - Part 5: Identity-based ciphers - Amendment 1: SM9 mechanism	2021-02
ISO/IEC 18033-6	IT Security techniques - Encryption algorithms - Part 6: Homomorphic encryption	2019-05
ISO/IEC 18045	Information technology - Security techniques - Methodology for IT security evaluation	2008-08
ISO/IEC 18367	Information technology - Security techniques - Cryptographic algorithms and security mechanisms conformance testing	2016-12
ISO/IEC 18370-1	Information technology - Security techniques - Blind digital signatures - Part 1: General	2016-11
ISO/IEC 18370-2	Information technology - Security techniques - Blind digital signatures - Part 2: Discrete logarithm based mechanisms	2016-07

Document No.	Title	Date of Publication
ISO/IEC 19086-4	Cloud computing - Service level agreement (SLA) framework - Part 4: Components of security and of protection of PII	2019-01
ISO/IEC 19592-1	Information technology - Security techniques - Secret sharing - Part 1: General	2016-11
ISO/IEC 19592-2	Information technology - Security techniques - Secret sharing - Part 2: Fundamental mechanisms	2017-10
ISO/IEC 19772	Information security - Authenticated encryption	2020-11
ISO/IEC 19785-2 AMD 1	Information technology - Common Biometric Exchange Formats Framework - Part 2: Procedures for the operation of the Biometric Registration Authority - Amendment 1: Addditional registrations	2010-04
ISO/IEC 19790	Information technology - Security techniques - Security requirements for cryptographic modules	2012-08
ISO/IEC 19792	Information technology - Security techniques - Security evaluation of biometrics	2009-08
ISO/IEC 19795-1	Information technology - Biometric performance testing and reporting - Part 1: Principles and framework	2021-05
ISO/IEC 19795-2 AMD 1	Information technology - Biometric performance testing and reporting - Part 2: Testing methodologies for technology and scenario evaluation - Amendment 1: Testing of multimodal biometric implementations	2015-04
ISO/IEC 19795-4	Information technology - Biometric performance testing and reporting - Part 4: Interoperability performance testing	2008-06
ISO/IEC 19795-5	Information technology - Biometric performance testing and reporting - Part 5: Access control scenario and grading scheme	2011-03
ISO/IEC 19795-6	Information technology - Biometric performance testing and reporting - Part 6: Testing methodologies for operational evaluation	2012-02
ISO/IEC 19795-7	Information technology - Biometric performance testing and reporting - Part 7: Testing of on-card biometric comparison algorithms	2011-01
ISO/IEC 19896-1	IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements	2018-02
ISO/IEC 19896-2	IT security techniques - Competence requirements for information security testers and evaluators - Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers	2018-08
ISO/IEC 19896-3	IT security techniques - Competence requirements for information security testers and evaluators - Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators	2018-08
ISO/IEC 19989-1	Information security - Criteria and methodology for security evaluation of biometric systems - Part 1: Framework	2020-09
ISO/IEC 19989-2	Information security - Criteria and methodology for security evaluation of biometric systems - Part 2: Biometric recognition performance	2020-10
ISO/IEC 19989-3	Information security - Criteria and methodology for security evaluation of biometric systems - Part 3: Presentation attack detection	2020-09

Document No.	Title	Date of Publication
ISO/IEC 20008-1	Information technology - Security techniques - Anonymous digital signatures - Part 1: General	2013-12
ISO/IEC 20008-2 AMD 1	Information technology - Security techniques - Anonymous digital signatures - Part 2: Mechanisms using a group public key; Amendment 1	2021-02
ISO/IEC 20009-1	Information technology - Security techniques - Anonymous entity authentication - Part 1: General	2013-08
ISO/IEC 20009-2	Information technology - Security techniques - Anonymous entity authentication - Part 2: Mechanisms based on signatures using a group public key	2013-12
ISO/IEC 20009-4	Information technology - Security techniques - Anonymous entity authentication - Part 4: Mechanisms based on weak secrets	2017-08
ISO/IEC 20085-1	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	2019-10
ISO/IEC 20085-2	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	2020-03
ISO/IEC 20543	Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408	2019-10
ISO/IEC 20547-4	Information technology - Big data reference architecture - Part 4: Security and privacy	2020-09
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	2018-11
ISO/IEC 20897-1	Information security, cybersecurity and privacy protection - Physically unclonable functions - Part 1: Security requirements	2020-12
ISO/IEC 21878	Information technology - Security techniques - Security guidelines for design and implementation of virtualized servers	2018-11
ISO/IEC 23000-21 DAM 1	Information technology - Multimedia application format (MPEG-A) - Part 21: Visual identity management application format - Amendment 1: Conformance and reference software	2020-03
ISO/IEC 23264-1	Information security - Redaction of authentic data - Part 1: General	2021-03
ISO/IEC 2382	Information technology - Vocabulary	2015-05
ISO/IEC 24727-6	Identification cards - Integrated circuit card programming interfaces - Part 6: Registration authority procedures for the authentication protocols for interoperability	2010-12
ISO/IEC 24745	Information technology - Security techniques - Biometric information protection	2011-06
ISO/IEC 24759	Information technology - Security techniques - Test requirements for cryptographic modules	2017-03
ISO/IEC 24760-1	IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts	2019-05
ISO/IEC 24760-2	Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements	2015-06

Document No.	Title	Date of Publication
ISO/IEC 24760-3	Information technology - Security techniques - A framework for identity management - Part 3: Practice	2016-08
ISO/IEC 24761	Information technology - Security techniques - Authentication context for biometrics	2019-10
ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary	2018-02
ISO/IEC 27001 Technical Corrigendum 2	Information technology - Security techniques - Information security management systems - Requirements; Technical Corrigendum 2	2015-12
ISO/IEC 27002 Technical Corrigendum 2	Information technology - Security techniques - Code of practice for information security controls; Technical Corrigendum 2	2015-11
ISO/IEC 27003	Information technology - Security techniques - Information security management systems - Guidance	2017-03
ISO/IEC 27004	Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation	2016-12
ISO/IEC 27005	Information technology - Security techniques - Information security risk management	2018-07
ISO/IEC 27006 AMD 1	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems; Amendment 1	2020-03
ISO/IEC 27007	Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing	2020-01
ISO/IEC 27009	Information security, cybersecurity and privacy protection - Sector-specific application of ISO/IEC 27001 - Requirements	2020-04
ISO/IEC 27010	Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications	2015-11
ISO/IEC 27011 Technical Corrigendum 1	Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations; Technical Corrigendum	2018-09
ISO/IEC 27013	Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	2015-12
ISO/IEC 27014	Information security, cybersecurity and privacy protection - Governance of information security	2020-12
ISO/IEC 27017	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	2015-12
ISO/IEC 27018	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	2019-01
ISO/IEC 27021 DAM 1	Information technology - Security techniques - Competence requirements for information security management systems professionals - Amendment 1: Addition of ISO/IEC 27001: 2013 clauses or subclauses to competence requirements	2020-10

Document No.	Title	Date of Publication
ISO/IEC 27031	Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity	2011-03
ISO/IEC 27032	Information technology - Security techniques - Guidelines for cybersecurity	2012-07
ISO/IEC 27033-1	Information technology - Security techniques - Network security - Part 1: Overview and concepts	2015-08
ISO/IEC 27033-2	Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security	2012-08
ISO/IEC 27033-3	Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues	2010-12
ISO/IEC 27033-4	Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways	2014-03
ISO/IEC 27033-5	Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	2013-08
ISO/IEC 27033-6	Information technology - Security techniques - Network security - Part 6: Securing wireless IP network access	2016-06
ISO/IEC 27034-1 Technical Corrigendum 1	Information technology - Security techniques - Application security - Part 1: Overview and concepts; Technical Corrigendum 1	2014-01
ISO/IEC 27034-2	Information technology - Security techniques - Application security - Part 2: Organization normative framework	2015-08
ISO/IEC 27034-3	Information technology - Application security - Part 3: Application security management process	2018-05
ISO/IEC 27034-5	Information technology - Security techniques - Application security - Part 5: Protocols and application security controls data structure	2017-10
ISO/IEC 27034-6	Information technology - Security techniques - Application security - Part 6: Case studies	2016-10
ISO/IEC 27034-7	Information technology - Application security - Part 7: Assurance prediction framework	2018-05
ISO/IEC 27035-1	Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management	2016-11
ISO/IEC 27035-2	Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response	2016-11
ISO/IEC 27035-3	Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations	2020-09
ISO/IEC 27037	Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence	2012-10
ISO/IEC 27038	Information technology - Security techniques - Specification for digital redaction	2014-03

Document No.	Title	Date of Publication
ISO/IEC 27039	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)	2015-02
ISO/IEC 27040	Information technology - Security techniques - Storage security	2015-01
ISO/IEC 27041	Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method	2015-06
ISO/IEC 27042	Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence	2015-06
ISO/IEC 27043	Information technology - Security techniques - Incident investigation principles and processes	2015-03
ISO/IEC 27701	Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines	2019-08
ISO/IEC 29100 AMD 1	Information technology - Security techniques - Privacy framework - Amendment 1: Clarifications	2018-06
ISO/IEC 29101	Information technology - Security techniques - Privacy architecture framework	2018-11
ISO/IEC 29109-5	Information technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 - Part 5: Face image data	2019-05
ISO/IEC 29115	Information technology - Security techniques - Entity authentication assurance framework	2013-04
ISO/IEC 29128	Information technology - Security techniques - Verification of cryptographic protocols	2011-12
ISO/IEC 29134	Information technology - Security techniques - Guidelines for privacy impact assessment	2017-06
ISO/IEC 29146	Information technology - Security techniques - A framework for access management	2016-06
ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure	2018-10
ISO/IEC 29150 Technical Corrigendum 1	Information technology - Security techniques - Signcryption; Technical Corrigendum 1	2014-03
ISO/IEC 29151	Information technology - Security techniques - Code of practice for personally identifiable information protection	2017-08
ISO/IEC 29184	Information technology - Online privacy notices and consent	2020-06
ISO/IEC 29190	Information technology - Security techniques - Privacy capability assessment model	2015-08
ISO/IEC 29191	Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication	2012-12
ISO/IEC 29192-1	Information technology - Security techniques - Lightweight cryptography - Part 1: General	2012-06
ISO/IEC 29192-2	Information security - Lightweight cryptography - Part 2: Block ciphers	2019-11
ISO/IEC 29192-3	Information technology - Security techniques - Lightweight cryptography - Part 3: Stream ciphers	2012-10

Document No.	Title	Date of Publication
ISO/IEC 29192-4 AMD 1	Information technology - Security techniques - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques; Amendment 1	2016-02
ISO/IEC 29192-5	Information technology - Security techniques - Lightweight cryptography - Part 5: Hash-functions	2016-08
ISO/IEC 29192-6	Information technology - Lightweight cryptography - Part 6: Message authentication codes (MACs)	2019-09
ISO/IEC 29192-7	Information security - Lightweight cryptography - Part 7: Broadcast authentication protocols	2019-07
ISO/IEC 30107-1	Information technology - Biometric presentation attack detection - Part 1: Framework	2016-01
ISO/IEC 30107-2	Information technology - Biometric presentation attack detection - Part 2: Data formats	2017-12
ISO/IEC 30107-3	Information technology - Biometric presentation attack detection - Part 3: Testing and reporting	2017-09
ISO/IEC 30107-4	Information technology - Biometric presentation attack detection - Part 4: Profile for testing of mobile devices	2020-06
ISO/IEC 9796-2	Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms	2010-12
ISO/IEC 9796-3	Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms	2006-09
ISO/IEC 9798-1	Information technology - Security techniques - Entity authentication - Part 1: General	2010-07
ISO/IEC 9798-3	IT Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques	2019-01
ISO/IEC 9798-4 Technical Corrigendum 2	Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function; Technical Corrigendum 2	2012-07
ISO/IEC 9798-5	Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques	2009-12
ISO/IEC 9798-6	Information technology - Security techniques - Entity authentication - Part 6: Mechanisms using manual data transfer	2010-12
ISO/IEC DIS 15408-4	Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities	2020-05
ISO/IEC DIS 15408-5	Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements	2020-05
ISO/IEC DIS 18033-7	Information technology - Security techniques - Encryption algorithms - Part 7: Tweakable block ciphers	2021-07
ISO/IEC DIS 20009-3	Information security - Anonymous entity authentication - Part 3: Mechanisms based on blind signatures	2021-02
ISO/IEC DIS 20897-2	Information security, cybersecurity and privacy protection - Physically unclonable functions - Part 2: Test and evaluation methods	2021-03

Document No.	Title	Date of Publication
ISO/IEC DIS 22989	Information technology - Artificial intelligence - Artificial intelligence concepts and terminology	2021-06
ISO/IEC DIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	2021-06
ISO/IEC DIS 27070	Information technology - Security techniques - Requirements for establishing virtualized roots of trust	2020-12
ISO/IEC DIS 27552	Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines	2018-12
ISO/IEC DIS 27555	Information security, cybersecurity and privacy protection - Guidelines on personally identifiable information deletion	2020-12
ISO/IEC FDIS 27551	Information security, cybersecurity and privacy protection - Requirements for attribute-based unlinkable entity authentication	2021-06
ISO/IEC TR 15443-1	Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts	2012-11
ISO/IEC TR 15443-2	Information technology - Security techniques - Security assurance framework - Part 2: Analysis	2012-11
ISO/IEC TR 15446	Information technology - Security techniques - Guidance for the production of protection profiles and security targets	2017-10
ISO/IEC TR 19791	Information technology - Security techniques - Security assessment of operational systems	2010-04
ISO/IEC TR 19795-3	Information technology - Biometric performance testing and reporting - Part 3: Modality-specific testing	2007-12
ISO/IEC TR 20004	Information technology - Security techniques - Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	2015-12
ISO/IEC TR 27016	Information technology - Security techniques - Information security management - Organizational economics	2014-03
ISO/IEC TR 27023	Information technology - Security techniques - Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	2015-07
ISO/IEC TR 27103	Information technology - Security techniques - Cybersecurity and ISO and IEC Standards	2018-02
ISO/IEC TR 27550	Information technology - Security techniques - Privacy engineering for system life cycle processes	2019-09
ISO/IEC TR 29144	Information technology - Biometrics - The use of biometric technology in commercial Identity Management applications and processes	2014-07
ISO/IEC TR 29149	Information technology - Security techniques - Best practices for the provision and use of time-stamping services	2012-03
ISO/IEC TR 30176	Internet of Things (ioT) - Integration of IoT and DLT/Blockchain: Use Cases	2021-04
ISO/IEC TS 19249	Information technology - Security techniques - Catalogue of architectural and design principles for secure products, systems and applications	2017-10
ISO/IEC TS 19795-9	Information technology - Biometric performance testing and reporting - Part 9: Testing on mobile devices	2019-12
ISO/IEC TS 20540	Information technology - Security techniques - Testing cryptographic modules in their operational environment	2018-05

Document No.	Title	Date of Publication
ISO/IEC TS 27006-2	Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems	2021-02
ISO/IEC TS 27008	Information technology - Security techniques - Guidelines for the assessment of information security controls	2019-01
ISO/IEC TS 27022	Information technology - Guidance on information security management system processes	2021-03
ISO/IEC TS 27034-5-1	Information technology - Application security - Part 5-1: Protocols and application security controls data structure, XML schemas	2018-04
ISO/IEC TS 27100	Information technology - Cybersecurity - Overview and concepts	2020-12
ISO/IEC TS 27110	Information technology, cybersecurity and privacy protection - Cybersecurity framework development guidelines	2021-02
ISO/IEC TS 27570	Privacy protection - Privacy guidelines for smart cities	2021-01
ISO/IEC TS 29003	Information technology - Security techniques - Identity proofing	2018-03
ISO/IEC TS 30104	Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements	2015-05
ISO/TR 18128	Information and documentation - Risk assessment for records processes and systems	2014-03
ISO/TR 23244	Blockchain and distributed ledger technologies - Privacy and personally identifiable information protection considerations	2020-05
ISO/TR 23455	Blockchain and distributed ledger technologies - Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	2019-09
ISO/TR 23576	Blockchain and distributed ledger technologies - Security management of digital asset custodians	2020-12
ITU-T F Supplement 4	Overview of convergence of artificial intelligence and blockchain	2021-04
ITU-T X Supplement 7*ITU-T X.1250 Series Supplement 7	ITU-T X.1250 series - Supplement on overview of identity management in the context of cybersecurity	2009-02
ITU-T X.1250	Baseline capabilities for enhanced global identity management and interoperability	2009-09
ITU-T X.1252	Baseline identity management terms and definitions	2021-04
ITU-T X.1253	Security guidelines for identity management systems	2011-09
ITU-T X.1255	Framework for discovery of identity management information	2013-09
ITU-T X.1257	Identity and access management taxonomy	2016-03
ITU-T X.1403	Security guidelines for using distributed ledger technology for decentralized identity management	2020-09
ITU-T X.402	Information technology - Message Handling Systems (MHS): Overall architecture	1999-06
ITU-T Y Supplement 62	Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects	2020-07
ITU-T Y.4560	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities	2020-08

Document No.	Title	Date of Publication
ITU-T Y.4561	Blockchain-based data management for supporting Internet of things and smart cities and communities	2020-08
ITU-T Y.4907	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities	2020-08
NIST SP 800-63B	Digital Identity Guidelines: Authentication and Lifecycle Management	2017-12
NIST SP 800-79-2	Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)	2015-07
NISTIR 7284	Personal Identity Verification Card Management Report	2006-01
NISTIR 8014	Considerations for Identity Management in Public Safety Mobile Networks	2015-03
NISTIR 8202	Blockchain Technology Overview	2018-10
NISTIR 8301	Blockchain Networks - Token Design and Management Overview	2021-02
prEN 1105	Identification card systems - General concepts applying to systems using IC cards in inter-sector environments - Rules for inter-application consistency	1995-10
SS 614331:2011	Identification Cards - Electronic ID Certificate	2011-12
UNE 71307-1:2020	Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework	2020-12
VDI 6225 Blatt 1	Biomimetics - Biomimetic information processing	2012-09
VDMA 66430-1	Only German: XML-basiertes Kommunikationsprotokoll für Industrieroboter und prozessorgesteuerte Peripheriegeräte (XIRP)	2006-07
XP Z77-101	Guide of good practices in matters of governance of ethical approaches within organizations	2021-08
EN ISO/IEC 24760-1	IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts (ISO/IEC 24760-1:2019)	2022-06
ETSI GR ENI 018 V 2.1.1	Experiential Networked Interlligence (ENI) - Introduction to Artificial Intelligence Mechanisms for Modular Systems	2021-08
ETSI GR SAI 001 V 1.1.1	Securing Artificial Intelligence (SAI) - AI Threat Ontology	2022-01
ETSI GR SAI 002 V 1.1.1	Securing Artificial Intelligence (SAI) - Data Supply Chain Security	2021-08
ETSI TS 119461 V 1.1.1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects	2021-07
ISO/IEC TR 24027	Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making	2021-11
ISO/IEC TR 24030	Information technology - Artificial intelligence (AI) - Use cases	2021-05

A.2 Informal Standards rated as relevant by the consortium

Table 12: Informal standards rated as relevant by the consortium.

Titel	**Date of Publication**
[PKCS11-Base-v3.0]	
[PKCS11-Current-v3.0]	
[PKCS11-Historical-v3.0]	
[PKCS11-Profiles-v3.0]	
[trust-el-framework-v1.0]	
[Trust-El-Protocol-v1.0]	
ActivityPub	23.01.2018
Aries RFC 0013: Overlays	
Aries RFC 0103: Indirect Identity Control	
Aries RFC 0104: Chained Credentials	
Aries RFC 0167: Data Consent Lifecycle	
Aries RFC 0231: Biometric Service Provider	
Aries RFC 0281: Aries Rich Schemas	
At least one DIF-approved Secure Data Storage v0.9 Implementation	
Authorization Capabilities for Linked Data v0.3	29.12.2020
BBS+ Signature Scheme	16.08.2021
BBS+ Signatures 2020	13.06.2021
CBOR-LD 1.0	21.05.2021
Citizenship Vocabulary v0.3	29.12.2020
Confidential Storage 0.1	12.08.2021
Credential Handler API 1.0	23.06.2021
Credential Manifest	
Credential Manifest	
Cryptographic Hyperlinks	31.10.2020
Data Privacy Vocabulary (DPV)	28.07.2021
Decentralized Identifier Resolution (DID Resolution) v0.2	31.08.2021
Decentralized Identifiers (DIDs) v1.0	03.08.2021
DID Authentication Profile for SIOP	
DID Implementation Guide v1.0	01.09.2021
DID Method Rubric v1.0	07.09.2021
DID Specification Registries	31.08.2021
did:web Method Specification	26.07.2021
DIDComm JS Lib	
DIDComm JS Lib	
DKMS (Decentralized Key Management System) Design and Architecture V4	29.03.2019
draft technical specification	20.02.2018
Element	
Encrypted Data Vaults 0.1	09.07.2020
Engineering Privacy for Verified Credentials	29.12.2020
ERC-20	

Titel	**Date of Publication**
Ethereum Improvement Proposals (EIPs)	
JSON Web Algorithms	01.05.2015
JSON Web Encryption (JWE)	01.05.2015
JSON Web Key (JWK)	01.05.2015
JSON Web Message	01.01.2015
JSON Web Signature (JWS)	01.05.2015
JSON Web Token (JWT)	01.05.2015
JSON-LD 1.1	16.07.2021
KERI - Key Event Receipt Infrastructure	
Linked Data Cryptographic Suite Registry	29.12.2021
Linked Data Proofs 1.0	03.06.2021
OAuth 2.0	
OAuth 2.0 Form Post Response Mode	27.04.2015
OAuth 2.0 Multiple Response Type Encoding Practices	25.02.2014
OpenID 2.0 to OpenID Connect Migration 1.0	16.04.2015
OpenID Connect Core 1.0 incorporating errata set 1	08.11.2014
OpenID Connect Credential Provider	20.04.2021
OpenID Connect Discovery 1.0 incorporating errata set 1	08.11.2014
OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1	08.11.2014
Peer DID Method Specification	13.07.2021
Presentation Exchange	
Revocation List 2020	20.11.2021
Self-Issued OpenID Connect Provider DID Profile v0.1 (DEPRECATED)	
Self-Issued OpenID Provider v2	
Sidetree Protocol	
Sidetree v1.0.0	
Signing HTTP Messages	10.04.2020
The did:key Method v0.7	26.07.2021
The Plain CBOR Representation v1.0	29.06.2021
The Security Vocabulary	12.08.2021
The Trust Over IP Stack	
TOGAF, The Open Group Architecture Framework	
Traceability Vocabulary v0.0	31.08.2021
Universal Wallet 2020	19.08.2021
Use Cases and Requirements for Decentralized Identifiers	16.06.2021
User-Managed Access (UMA) 2.0	18.08.2016
VC JSON Schemas	11.12.2019
Verifiable Claims Use Cases 1.0	
Verifiable Credentials Data Model 1.1	09.11.2021
Verifiable Credentials JSON Schema Specification	11.12.2019
Verifiable Credentials Use Cases	18.04.2021
Verifiable Presentation Request Specification v0.1	20.04.2021
WACI PeX	

Titel	**Date of Publication**
Web Authentication: An API for accessing Public Key Credentials Level 2	08.04.2021
Web Cryptography API	26.01.2017
WebKMS v0.7	20.04.2021
Well Known DID Configuration	
OpenID Specifications	
OpenID for Verifiable Presentations	06.09.2022
OpenID for Verifiable Credential Issuance	27.10.2022
IEEE Standard for General Requirements for Cryptocurrency Exchanges	2020-11-04
IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management	2021-01-18
IEEE Standard for Data Format for Blockchain Systems	2020-12-23
IEEE Standard for DevOps: Building Reliable and Secure Systems Including Application Build, Package, and Deployment	2021-02-09
A Universally Unique IDentifier (UUID) URN Namespace	2005-07
System for Cross-domain Identity Management: Core Schema	2015-09
System for Cross-domain Identity Management: Protocol	2015-09
Authenticated Identity Management in the Session Initiation Protocol (SIP)	2018-02