



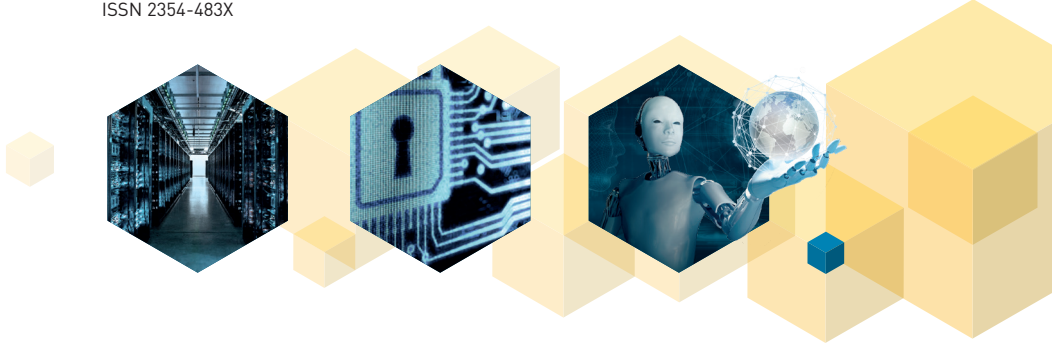
IILNAS

STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 3.0 · September 2020
ISSN 2354-483X





STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 3.0 · September 2020

ISSN 2354-483X

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services



Agence pour la Normalisation et
l'Economie de la Connaissance

Foreword

Technical standardization and standards play an important role in the support of economic development. Nowadays, almost every professional sector relies on standards to perform its daily activities and provide services in an efficient manner. They can provide, for example, good practices for services and product development, governance, quality assessment, safety, trustworthiness, etc. Even if the application of standards remains voluntary, they offer a real added value in order to comply with legislation. Standards are therefore considered as a source of benefits in all sectors of the economy and this is particularly true in the Information and Communication Technology (ICT) sector, which supports all other economic developments.

Indeed, the ICT sector has gained more and more importance in society as a whole in the few last decades. The rapid evolution of these technologies and their usage in our daily lives are defining a new paradigm in which ICT has an increasing role. The ability of all “things” to be connected, to communicate with one another and to collect information is deeply changing the world as we know it and we are probably only at the beginning of this transformation wherein ICT become Smart. In this context, technical standardization plays a key role, for example to connect all Smart ICT components, to make them interoperable and prevent vendor lock-in, to support the integration of multiple data sources of Smart ICT technologies or to guarantee the security and safety of the next digital world.

The Grand-Duchy of Luxembourg has clearly understood the importance of the digital economy and has engaged since several years in an ambitious innovation strategy for the ICT sector, considering that the development of a trusted and sustainable economy will notably rely on a data-driven approach. The “*Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services*” (ILNAS) fully supports this development through the “Luxembourg Standardization Strategy 2020-2030”¹, signed by the Minister of the Economy, which identifies the ICT sector as key to fostering growth, along with the construction and aerospace sectors. In this context, ILNAS has developed “Luxembourg’s policy on ICT technical standardization 2020-2025”², which aims to promote and strengthen the use of technical standards by the national market, to reinforce the positioning of Luxembourg in the global ICT standardization landscape, particularly through a stronger involvement of national stakeholders in the relevant standardization technical committees, and to pursue the development of research and education programs in the Smart ICT standardization area. In order to carry out this policy, ILNAS benefits notably from the support of the Economic Interest Group “*Agence pour la Normalisation et l’Économie de la Connaissance*” (ANEC G.I.E. – Standardization Department).

In this frame, ILNAS is already actively involved in the domain of education about standardization, and two educational programs have been developed through a fruitful collaboration with the University of Luxembourg. The first one was the University certificate “Smart ICT for Business Innovation” which was delivered twice (2015-2016 and 2018-2019) and which has led to the creation of a new Master’s degree “Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions”³ that will start in February

2021. This diploma will allow national stakeholders to gain familiarity with Smart Secure ICT technologies, notably from a standardization and Technopreneurship point of view, in order to seize the future business opportunities offered in this innovative area.

In parallel, ILNAS has also launched different research activities in the Smart Secure ICT domain, which are directly contributing to the success of its education about standardization developments. On the one hand, ILNAS and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg launched a research program “Technical Standardisation for Trusted Use in the Field of Smart ICT” (2017-2020)⁴, involving three PhD students respectively working on Cloud Computing, Internet of Things and Big Data/Artificial Intelligence. This program largely considers technical standardization and Digital Trust aspects of these Smart ICT technologies and has already resulted in the publication of a White Paper “Data Protection and Privacy in Smart ICT” in October 2018 and three technical reports, in October 2019, on the gaps between scientific research and technical standardization in the three aforementioned Smart ICT areas. On the other hand, ILNAS has published a series of White Papers and reports⁵ in order to inform the market about technical standardization developments in Smart ICT. In this framework, White Papers on “Internet of Things”, “Blockchain and Distributed Ledger Technologies” or “Digital Trust for Smart ICT” have been published in recent years, as well as a National Technical Standardization Report on the IoT in 2020. For its part, the Standards Analysis “Smart Secure ICT Luxembourg” is regularly updated in order to provide to the national market an overview of the recent Smart Secure ICT developments from a technical standardization perspective. The document has evolved over recent years to focus on Smart Secure ICT, following the national market’s interests.

This Standards Analysis “Smart Secure ICT Luxembourg” is intended to serve as a practical tool to discover the latest standardization developments in Smart ICT related technologies, such as the Internet of Things, Cloud Computing, Artificial Intelligence, and Blockchain, as well as Digital Trust related standards for those technologies. It is also directly answering the objectives set by the “National Cybersecurity Strategy III”⁶ in terms of standardization needs for digital infrastructure protection. Therefore, the present document will allow national stakeholders to identify relevant standardization technical committees and fora and consortia in the Smart Secure ICT area, with the ultimate objective to offer them guidance for a potential future involvement in the standards development process and allow them to discover the services provided by ILNAS at the national level regarding technical standardization.

Jean-Marie REIFF, Director
Jean-Philippe HUMBERT, Deputy Director
ILNAS

¹ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf>

² <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/policy-on-ict-technical-standardization-2020-2025.pdf>

³ <https://mtech.uni.lu/>

⁴ <https://smartict.gforge.uni.lu/>

⁵ <https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/normalisation-recherche.html#white-papers>

⁶ <https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en.pdf>

Executive summary

The Standards Analysis “Smart Secure ICT Luxembourg” is meant as a practical guide to all national stakeholders regarding standardization activities in selected Smart ICT domains: the Internet of Things, Cloud Computing, Artificial Intelligence and Blockchain, as well as standards developments related to these technologies in the Digital Trust area. This document is intended to help the national market identify stakes and interests in technical standardization. It encourages their participation in Smart ICT standardization technical committees, with the aim to have them benefit from the related knowledge in order to build secure Smart ICT environments in their business. This Standards Analysis also provides information on the cybersecurity standardization landscape, including an overview of Digital Trust technical committees as well as relevant fora and consortia. This monitoring directly meets the standardization objective of the “National Cybersecurity Strategy III”, by offering technical standardization tracks on which the national market can rely to develop national digital confidence and contribute to the protection of the digital infrastructure. Moreover, different opportunities, presented in this Standards Analysis, are available to enable national stakeholders to take advantage of standards and standardization.

In this context, this Standards Analysis is designed to develop an information and exchange network for Smart Secure ICT standardization knowledge in the Grand Duchy of Luxembourg. Currently, 85⁷ experts are registered through ILNAS as national delegates in the ICT sector. Among them, 71 are directly involved in Smart ICT and Digital Trust related technical committees⁸, such as in Internet of Things: 19; Cloud Computing: 11; Artificial Intelligence: 24; Blockchain: 17, Digital Trust: 42.

In the frame of the “Luxembourg Standardization Strategy 2020-2030” and “Luxembourg’s policy on ICT technical standardization 2020-2025”, ILNAS has the objective to encourage national experts to develop their normative culture in Smart ICT and to take advantage of technical standardization for their business. In that sense, ILNAS develops annually, with the support of ANEC G.I.E., an implementation plan for ICT technical standardization, which focuses on strengthening Smart ICT technical standardization in order to support the related economic development. ILNAS priorities notably consist in the management of the national Smart ICT technical committees, in the promotion of the use of technical standards as well as in making national organizations aware of the relevant standardization activities in their area of work. In this frame, ILNAS aims at fostering national involvement in Smart ICT technical standardization, which will contribute to a better consideration of national interests in international Smart ICT technical standardization.

In summary, this Standards Analysis provides information on the Smart ICT standardization development at the international and European levels to support national stakeholders in the identification of technical committees and standards relevant for their business. Firstly, it introduces basic components of Smart ICT technologies as well as Digital Trust requirements for Smart ICT, and secondly, it presents related standardization activities performed at the international, European and national levels. It is intended to facilitate the involvement of national stakeholders in such activities, allowing them to take advantage of standards and standardization for their economic development. It also aims at helping the national market in the identification of relevant cybersecurity standardization activities, to support the implementation of the “National Cybersecurity Strategy III” through a monitoring of standardization technical committees and fora and consortia working in the Digital Trust area.

⁷ National register of standardization delegates – July 2020

⁸ Please note that some experts are participating in more than one technical committee

Table of contents

1	INTRODUCTION	11
2	TECHNICAL STANDARDIZATION AND STANDARDS	13
2.1	Standardization Objectives and Principles.....	13
2.2	Standardization Landscape	14
3	SMART SECURE ICT LANDSCAPE	19
3.1	Introduction, Definition and Interactions between Smart ICT Components	19
3.2	Economic Overview	20
3.3	Smart Secure ICT in Luxembourg	21
4	SMART SECURE ICT STANDARDS WATCH	25
4.1	Internet of Things (IoT).....	25
4.1.1	Characteristics.....	26
4.1.2	IoT Standardization Technical Committees	27
4.2	Cloud Computing	34
4.2.1	Characteristics.....	34
4.2.2	Cloud Computing Standardization Technical Committees.....	36
4.3	Artificial Intelligence (AI) and Big Data.....	40
4.3.1	Artificial Intelligence	40
4.3.2	Big Data	41
4.3.3	Artificial Intelligence and Big Data Standardization Committees	43
4.4	Blockchain and Distributed Ledger Technologies	48
4.4.1	Characteristics.....	48
4.4.2	Blockchain and Distributed Ledger Technologies Standardization Technical Committee	49
4.5	Digital Trust in Smart ICT	53
4.5.1	Basic Components of Digital Trust.....	53
4.5.2	Digital Trust Standardization Related Technical Committees.....	54
4.6	Fora and Consortia Related to Digital Trust.....	64
4.6.1	3GPP - 3rd Generation Partnership Project.....	64
4.6.2	BSI - Bundesamt für Sicherheit in der Informationstechnik	65
4.6.3	CSA - Cloud Security Alliance.....	65
4.6.4	EC-Council - International Council of E-Commerce Consultants	65
4.6.5	EuroCloud	66
4.6.6	GIAC - Global Information Assurance Certification.....	66
4.6.7	IEEE SA - Institute for Electrical and Electronic Engineers Standards Association	66
4.6.8	IETF - Internet Engineering Task Force.....	67
4.6.9	GSMA - GSM Association.....	67
4.6.10	IIC - Industrial Internet Consortium	67

4.6.11	ISACA - Information Systems Audit and Control Association.....	68
4.6.12	(ISC) ² - International Information System Security Certification Consortium.....	68
4.6.13	ISECOM - Institute for Security and Open Methodologies	68
4.6.14	NIST - National Institute of Standards and Technology.....	69
4.6.15	OASIS - Organization for the Advancement of Structured Information Standards.....	69
4.6.16	OCF - Open Connectivity Foundation.....	69
4.6.17	OMG - Object Management Group	70
4.6.18	oneM2M	70
4.6.19	OWASP - The Open Web Application Security Project	70
4.6.20	PCI-SSC - PCI Security Standards Council.....	71
4.6.21	SNIA - Storage Networking Industry Association.....	71
4.6.22	TCG - Trusted Computing Group.....	71
4.6.23	W3C - World Wide Web Consortium.....	72
5	PROMISING STANDARDIZATION AREAS	73
5.1	Brain Computer Interface	73
5.2	Digital Twin	74
5.3	Quantum Computing	76
6	OPPORTUNITIES FOR THE NATIONAL MARKET	77
6.1	Information about Standardization	78
6.1.1	Smart ICT Workshops and Information Sessions	78
6.1.2	Awareness Sessions.....	79
6.1.3	Smart ICT Standards Watch	79
6.1.4	Publications and Dissemination	79
6.1.5	Free Consultation of Standards	81
6.1.6	Smart ICT Standardization Research Results	81
6.2	Training in Standardization	82
6.2.1	Training on Smart ICT Standardization.....	82
6.2.2	Project of Professional “Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions”	82
6.3	Involvement in Standardization	83
6.3.1	Becoming a National Delegate in Standardization.....	83
6.3.2	Comment Standards under Public Enquiry.....	84
6.3.3	Propose New Standards Projects	85
6.3.4	Monitor the Standardization Work Performed by the European Multi-Stakeholder Platform on ICT Standardization (MSP).....	85
7	CONCLUSIONS.....	87
8	APPENDIX - SMART SECURE ICT STANDARDS AND PROJECTS.....	91
8.1	Internet of Things	91
8.1.1	Published Standards	91

8.1.2	Digital Trust related Published Standards.....	96
8.1.3	Standards Under Development (Under Study)	97
8.1.4	Digital Trust related Standards Under Development (Under Study).....	101
8.2	Cloud Computing	102
8.2.1	Published Standards	102
8.2.2	Digital Trust related Published Standards.....	105
8.2.3	Standards Under Development (Under Study)	106
8.2.4	Digital Trust related Standards Under Development (Under Study).....	107
8.3	Artificial Intelligence and Big Data	107
8.3.1	Published Standards	107
8.3.2	Digital Trust related Published Standards.....	110
8.3.3	Standards Under Development (Under Study)	111
8.3.4	Digital Trust related Under Development Standards (Under Study).....	113
8.4	Blockchain and Distributed Ledger Technologies	114
8.4.1	Published Standards	114
8.4.2	Digital Trust related Published Standards.....	115
8.4.3	Standards Under Development (Under Study)	115
8.4.4	Digital Trust related Under Development Standards (Under Study).....	117
AUTHORS AND CONTACTS		119

1 INTRODUCTION

The Information and Communication Technology (ICT) sector is a keystone of the global economy. It provides pervasive support to all other sectors of activity. The concept of Smart ICT relies on the integration and implementation of emerging and innovative tools or techniques to strengthen societal, social, environmental and economic needs. The Internet of Things, Cloud Computing, Artificial Intelligence and Blockchain are some examples of them. As systems become more and more intricate, the growth of the Smart ICT sector is now driven by the ability of its component parts to interoperate (“to talk to each other”). Standards can allow this interoperability between different products from different manufacturers, while offering solutions to ensure an adequate level of trustworthiness in their operation.

ILNAS works on the development of this key sector for the economy, from the technical standardization perspective. The Institute undertakes several activities in order to develop a network of experts, support the transfer of knowledge and education about Smart ICT standardization to national stakeholders, and strengthen their participation in related technical committees⁹. To enhance these activities also at the academic level, ILNAS is notably working with the University of Luxembourg to develop standards-related education and research. The University certificate “*Smart ICT for Business Innovation*”, organized in 2015-2016 and in 2018-2019, with the aim to provide standards-based knowledge on recent emerging Smart ICT technologies to national ICT professionals, was a first step in this collaboration with academia. The course, offered for two semesters, was implemented successfully, and was of great interest to participants from multiple industries of different sectors.

In line with the University certificate, ILNAS and the University of Luxembourg are also implementing a research program whose objective is to analyze and extend standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, the Internet of Things and Artificial Intelligence/Big Data. In this context, three PhD students are performing research activities in the above-mentioned Smart ICT domains. Some of the first results of this collaboration are the publication of a White Paper “Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization” in October 2018¹⁰, the award “Security Project of the Year”, received by the research team during the Information Security Day 2019¹¹, and the publication of three technical reports, in October 2019, on the gaps between scientific research and technical standardization in the three aforementioned Smart ICT domains. One objective of this program is to rely on the research results to develop new academic courses on ICT technical standardization, notably through the planned professional Master Program “*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*” expected to be launched in February 2021.

In relation with the above-mentioned developments, this Standards Analysis “Smart Secure ICT Luxembourg” concentrates on standards development of recognized Standards Development Organizations (SDOs) within the Smart ICT landscape, such as the Internet of Things, Cloud Computing, Artificial Intelligence and Blockchain, together with Digital Trust related standards development. It aims to serve as a supporting tool to maintain a secure and trustworthy Smart ICT environment through technical standardization. For this purpose, this analysis provides a brief overview of the technical background of Smart ICT technologies as well as details on the technical committees working in these domains. To answer the objectives of the “National Cybersecurity Strategy III” in terms of standardization needs for digital infrastructure protection, the document also provides an introduction of common Digital Trust issues for Smart ICT technologies together with related technical standards

⁹ Note: In this report, the term “standardization technical committee” is generic and covers “technical committees”, “subcommittees”, “working groups”, etc.

¹⁰ ILNAS & University of Luxembourg, White Paper “Data Protection and Privacy in Smart ICT - Scientific Research And Technical Standardization”, 2018 - <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf>

¹¹ https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team

development. Moreover, information on relevant fora and consortia in the cybersecurity domain is provided, as well as a list of relevant standards in all these areas with the purpose of helping national stakeholders in building and maintaining secure Smart ICT environments.

As mentioned earlier, the purpose of this Standards Analysis is to inform national stakeholders about the major standardization activities and technical committees related to Smart Secure ICT with the objective to offer them guidance for a potential future involvement in the standards development process. It also provides a support to the current and future development of ILNAS standardization at the national level (i.e., in research and education).

This Standards Analysis is organized as follows. The objectives of technical standardization and introduction to its landscape at the national, European and international levels have been included in Chapter 2. Chapter 3 proposes a definition of Smart ICT, provides an economic overview of ICT and introduces the main interactions between the Smart ICT domains included in this analysis. Chapter 4 further details each of these Smart ICT domains by providing some basic concepts and presenting relevant technical committees. Requirements of Digital Trust for Smart ICT are also detailed in this chapter, together with related technical committees and fora and consortia. Chapter 5 introduces some promising new ICT technologies, which have recently draw the attention of standardization organizations. A summary of existing standardization developments is provided in order to inform national stakeholders of upcoming opportunities in these areas. Chapter 6 presents opportunities related to standardization for national stakeholders. It also introduces the way ILNAS supports the national economy through technical standardization. Chapter 7 provides a summary of this Standards Analysis and reiterates the commitment of ILNAS to assist national entities with their involvement in technical standardization. Finally, lists of both published standards and projects are included in the Appendix (Chapter 8) for each Smart ICT domain, as well as related Digital Trust standards.

2 TECHNICAL STANDARDIZATION AND STANDARDS

Standardization corresponds to the definition of voluntary technical or quality specifications with which current or future products, production processes or services may comply. Standardization is organized by and for the stakeholders concerned based on national representation (CEN, CENELEC, ISO and IEC) and direct participation (ETSI and ITU-T), and is founded on the principles recognized by the World Trade Organization (WTO)¹² in the field of standardization, namely coherence, transparency, openness, consensus, voluntary application, independence from special interests and efficiency. In accordance with these founding principles, it is important that all relevant interested parties, including public authorities and small and medium-sized enterprises, are appropriately involved in the national, European and international standardization process¹³.

Technical standards provide an effective economic tool for achieving various objectives, such as mutual understanding, reduction of costs, elimination of waste, improvement of efficiency, achievement of compatibility between products and components or access to knowledge about technologies¹⁴. The application of the fundamental principles stated by the WTO throughout the development of technical standards, also guarantees the legitimacy of these documents. In addition, technical standards play an important role for innovation. As pointed out by the European Commission (EC) in its communication Europe 2020 Flagship Initiative¹⁵, “they enable the dissemination of knowledge, the interoperability between new products and services for a platform for further innovation”. It is all the more relevant in the current context, in which the world tends to become digitalized and everything becomes connected. Technical standardization is thus a keystone to ensure interoperability of complex ICT systems and it will contribute to minimize the barriers that may still exist to build the future of the digital world.

2.1 Standardization Objectives and Principles

As stated in the Regulation (EU) N°1025/2012 on European standardization, and according to the World Trade Organization (WTO), standardization is based on founding principles, which are observed by the formal standards bodies for the development of international standards:

Transparency

All essential information regarding current work programs, as well as on proposals for standards, guides and recommendations under consideration and on the results should be made easily accessible to all interested parties.

Openness

Membership of an international standards body should be open on a non-discriminatory basis to relevant bodies.

Impartiality and Consensus

All relevant bodies should be provided with meaningful opportunities to contribute to the elaboration of an international standard so that the standard development process will not give privilege to, or favor the interests of, a particular supplier, country or region. Consensus procedures should be

¹² WTO, “Second triennial review of the operation and implementation of the agreement on technical barriers to trade – Annex,” 2000 - <http://docsonline.wto.org/imrd/directdoc.asp?DDFDocuments/t/G/TBT/9.doc>

¹³ Based on: Regulation (EU) N°1025/2012 of the Parliament and of the Council - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF>

¹⁴ CEN-CENELEC, “Standards and your business,” 2013 - https://www.cencenelec.eu/news/publications/Publications/Standards-and-your-business_2013-09.pdf

¹⁵ European Commission, “Europe 2020 Flagship Initiative, Innovation Union, COM(2010) 546,” 2010 - https://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf

established that seek to take into account the views of all parties concerned and to reconcile any conflicting arguments.

Effectiveness and Relevance

International standards need to be relevant and to effectively respond to regulatory and market needs, as well as scientific and technological developments in various countries. They should not distort the global market, have adverse effects on fair competition, or stifle innovation and technological development. In addition, they should not give preference to the characteristics or requirements of specific countries or regions when different needs or interests exist in other countries or regions. Whenever possible, international standards should be performance based rather than based on design or descriptive characteristics.

Coherence

In order to avoid the development of conflicting international standards, it is important that international standards bodies avoid duplication of, or overlap with, the work of other international standards bodies. In this respect, cooperation and coordination with other relevant international bodies is essential.

Development dimension

Constraints on developing countries, in particular, to effectively participate in standards development, should be taken into consideration in the standards development process. Tangible ways of facilitating developing countries participation in international standards development should be sought.

Standardization is an efficient economic tool offering the possibility to pursue various objectives, such as:

- Management of diversity;
- Convenience of use;
- Performance, quality and reliability;
- Health and safety;
- Compatibility;
- Interchangeability;
- Security;
- Trustworthiness;
- Environmental protection;
- Product protection;
- Mutual understanding;
- Economic performance;
- Trade;
- Etc.

2.2 Standardization Landscape

In Europe, the three recognized European Standardization Organizations (ESO), as stated in Regulation (EU) No 1025/2012¹⁶, are:

- European Committee for Standardization (CEN);
- European Committee for Electrotechnical Standardization (CENELEC);
- European Telecommunications Standards Institute (ETSI).

At the international level, the three recognized standardization organizations are:

- International Organization for Standardization (ISO);
- International Electrotechnical Commission (IEC);
- International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).

¹⁶ Regulation (EU) N°1025/2012 of the Parliament and of the Council - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF>

This standardization frame allows cooperation between standardization organizations at the same level, or at different levels but on the same topics:

- CENELEC and IEC are specialized in electrotechnical standards;
- ETSI and ITU-T are focused on telecommunications standards;
- CEN and ISO are in charge of the standards in other sectors.

European and International Standardization Bodies		Date of Creation	Number of Members	Number of publications
ISO	International Organization for Standardization	1946	165	23,311
IEC	International Electrotechnical Commission	1906	89	10,700
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector	1865	271 ¹⁷	5,671
CEN	European Committee for Standardization	1961	34	17,309
CENELEC	European Committee for Electrotechnical Standardization	1973	34	7,590
ETSI	European Telecommunications Standards Institute	1988	933 ¹⁷ (65 countries)	36,477

Table 1: Figures of European and International Standardization Organizations¹⁸

At national levels, one or several national standards bodies protect the interests of the country within each of the European and international standardization organizations (e.g.: in Germany, on the one hand DIN is the member of ISO and CEN, and on the other hand DKE is member of IEC, CENELEC and ETSI). In Luxembourg, ILNAS – the only official national standards body – is member of the European and international standardization organizations CEN, CENELEC, ETSI, ISO, IEC and ITU-T.

Several bridges exist between the national, European and international standardization organizations in order to facilitate the collaboration and coordination of standardization work in the different fields (Figure 1).

¹⁷ ITU-T and ETSI have a specific way of working compared to the other recognized organizations, as they work through the direct participation of industry stakeholders

¹⁸ Source: Websites of organizations














	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
 International level			 
 European level			
 National level			

Figure 1: Interactions between the Standardization Organizations

Indeed, in order to ensure transparency in the work and avoid the duplication of standards, agreements have been established between international and European standardization organizations.

In 1991, ISO and CEN signed the Vienna Agreement¹⁹, which is based on the following guiding principles:

- Primacy of international standards and implementation of ISO Standards at European level (EN ISO);
- Work at European level (CEN), if there is no interest at international level (ISO);
- When a given project undergoes parallel development, procedures are in place ensuring standardization documents of common interest are approved by both (ISO and CEN) organizations.

Similarly, CENELEC and IEC signed the Dresden Agreement in 1996 with the aim of developing intensive consultations in the electrotechnical field. This agreement has been replaced by the Frankfurt Agreement²⁰ in 2016 with the aim to simplify the parallel voting processes, and increase the traceability of international standards adopted in Europe thanks to a new referencing system. It is intended to achieve the following guiding principles:

- Development of all new standardization projects by IEC (as much as possible);
- Work at European level (CENELEC), if there is no interest at international level (IEC);
- When a given project undergoes parallel development, ballots for relevant standardization documents are organized simultaneously at both (IEC and CENELEC) organizations.

Under both agreements, 33% of all European standards ratified by CEN, as well as 74% of those ratified by CENELEC, are respectively identical to ISO or IEC standards²¹. In that respect, the European and international organizations do not duplicate work.

¹⁹ Agreement on technical co-operation between ISO and CEN (Vienna Agreement) - http://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230458/01_Agreement_on_Technical_Cooperation_between_ISO_and_CEN_%28Vienna_Agreement%29.pdf?nodeid=4230688&vernum=-2

²⁰ IEC-CENELEC Agreement on Common planning of new work and parallel voting (Frankfurt Agreement) - ftp://ftp.cencenelec.eu/CENELEC/Guides/CLC/13_CENELECGuide13.pdf

²¹ CEN CENELEC in figures – 2020 Q2 - https://www.cencenelec.eu/stats/CEN_CENELEC_in_figures_quarter.htm

Similarly, ITU-T and ETSI have agreed on a Memorandum of Understanding (MoU) in 2000, lastly renewed in 2016²², that paves the way for European regional standards, developed by ETSI, to be recognized internationally.

Agreements also exist between the standards organizations to facilitate their cooperation. For example, ISO and IEC have the possibility to sign conventions to create Joint Technical Committees (JTC) or Joint Project Committees (JPC) when an area of work overlaps the two organizations (e.g.: ISO/IEC JTC 1 for the Information Technology domain).

ISO, IEC and ITU have also established the World Standards Cooperation (WSC) in 2001, a high-level collaboration system intending to strengthen and advance the voluntary consensus-based international standards system and to resolve issues related to the technical cooperation between the three organizations²³. Similarly, the cooperation between CEN and CENELEC aims to create a European standardization system that is open, flexible and dynamic.

❖ ISO and IEC Standardization Committees

ISO is the world's dominant developer and publisher of International Standards in terms of scope. It has around 23,300 standards published and more than 4,700 standards under development²⁴. ISO is in charge of developing International Standards for all industry sectors.

IEC prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as “electrotechnology”.

To prevent an overlap in standardization work related to information technology, ISO and IEC formed a Joint Technical Committee in 1987 known as ISO/IEC JTC 1 *Information technology*. It has taken a leading role in Smart ICT standardization in the last few years with the creation of working groups and technical subcommittees directly responsible for the development of International Standards in the Smart ICT area.

❖ CEN and CENELEC Standardization Committees

CEN and CENELEC are two official European Standards Organizations (ESOs) closely collaborating through a common CEN-CENELEC Management Centre since 2010. They are notably in charge of developing ICT standards at the European level. Even if most of the ICT-related topics are being tackled at the international level by ISO/IEC JTC 1, complying with the “Vienna Agreement” set up between CEN and ISO, as detailed above, CEN has technical committees and additional other groups active in different areas of the ICT sector directly under its supervision.

The standardization activities of CEN and CENELEC are detailed in an annual common Work Program, which was published in December 2019 for the year 2020²⁵. They are active in several ICT-related areas covering both digital society and smart technologies: e-Signatures, Intelligent Transport Systems, Smart Grids, Smart Metering, Internet of Things, Smart Homes, Smart Cities, Advanced Manufacturing, Artificial Intelligence, Blockchain and Distributed Ledger Technologies, Cybersecurity and Data Protection, etc.

²² Renewed memorandum of understanding between ETSI and ITU - <https://www.itu.int/en/ITU-T/extcoop/Documents/mou/MoU-ETSI-ITU-201605.pdf>

²³ <http://www.worldstandardscooperation.org/>

²⁴ <https://www.iso.org/iso-in-figures.html>

²⁵ https://www.cencenelec.eu/News/Publications/Publications/CEN-CENELEC_WP_2020_EN.pdf

❖ ETSI - European Telecommunications Standards Institute

ETSI is a leading standardization organization for ICT standards fulfilling European and global market needs²⁶. The European Union officially recognizes ETSI as an ESO. In this Standards Analysis, specific technical committees of ETSI are detailed due to their particular importance for the Smart Secure ICT area – e.g.: Internet of Things (ETSI/TC SmartM2M) or Digital Trust (e.g.: ETSI/TC ESI and ETSI/TC CYBER).

❖ ITU-T - International Telecommunication Union - Telecommunication Standardization Sector

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) is an “intergovernmental public-private partnership organization” which brings together experts from around the world to develop international standards known as ITU-T Recommendations, which cover defining elements in the global infrastructure of ICT. It is currently composed of 11 Study Groups working on different aspects of ICT.

²⁶ <https://www.etsi.org/about>

3 SMART SECURE ICT LANDSCAPE

3.1 Introduction, Definition and Interactions between Smart ICT Components

Information and Communication Technology (ICT) has progressively gained importance in recent decades, becoming a foundation for all sectors of the economy. The fast growing connectivity, storage, software and hardware capabilities have strongly affected society in all its aspects. The way of doing business as well as daily lives of citizens now strongly rely on ICT. This trend shows no signs of slowing and the sector still offer great promises, opportunities and challenges.

Dynamism in ICT based technology is driving innovation processes. New tools and technologies are now adopted in ICT business to enhance its effectiveness in the governmental and industrial sector. These technologies add more smartness and are closely interconnected with each other. They are also referred to as Smart ICT technologies. For example, Cloud Computing, the Internet of Things, and Artificial Intelligence are already offering previously unimagined possibilities for innovation and business development. As mentioned earlier in the introduction, building and maintaining (digital) trust is also essential in the Smart ICT area. In addition to traditional security techniques, recent emerging technology, such as Blockchain, can for example add transparency in the transactions of components of Smart ICT, which could eliminate the need for some intermediaries in interactions or transactions. For the sake of a high-level understanding of Smart ICT, a definition is proposed here:

Smart ICT definition

“Smart ICT corresponds to a holistic approach of ICT development, integration and implementation, where a range of emerging or innovative tools and techniques are used to maintain, improve or develop products, services or processes with the global objective to strengthen different societal, social, environmental and economic needs. It includes, through related interconnected ecosystems, advanced ICT such as Cloud Computing, Big Data and Analytics, Internet of Things, Artificial Intelligence, Robotics, and new ways of gathering data, such as social media and crowdsourcing²⁷”.

Although many concepts come to mind when talking about Smart ICT, this Standards Analysis concentrates on components that are considered as some of the most important to build Smart ICT systems while taking into account Digital Trust related aspects: the Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI) and Blockchain.

In order to better understand how these Smart ICT technologies interact, a scenario illustrating how data is generated in various environments, and transferred as well as processed intelligently for its efficient utilization by multiple applications is provided below:

- The Internet of Things collects enormous amount of data or information from various environments. Communication networks including telecommunications help to distribute collected data to specific destinations.
- Big Data stores, analyzes and provides mechanisms for operating and understanding the large amount of collected data.
- Cloud Computing supports these environments by providing the processing power and infrastructure used by Big data and analytics tools to produce/extract value from the data collected.

²⁷ Definition proposed by ILNAS based on NICTA (National ICT Australia Ltd), Tzar C. Umang (Chief ICT Specialist of the Department of Science and Technology – Smarter Philippines Program) and exchanges with Pr. François Coallier (Chairman of the subcommittee ISO/IEC JTC 1/SC 41 “Internet of Things and related technologies”).

- Artificial Intelligence, corresponding to a set of techniques aimed at approximating some aspects of human or animal cognition without human intervention, allows, for example, the automation of processes in relation with the analysis of (Big) data. Data based learning is the highly applied approximation approach in AI. AI is now offered as a service through the Cloud.
- Blockchain tracks the records of smart devices (for example used by IoT systems) to make interactions more transparent and trustworthy.
- To utilize Smart ICT technology as efficiently as possible, building and maintaining Digital Trust among stakeholders is extremely important. Different components of Digital Trust are important for Smart ICT technology adoption, such as privacy, data and information security and interoperability. Standards, in that context, are produced as a tool offering a set of good practices allowing for creating, maintaining and strengthening Digital Trust (e.g., by setting appropriate information management systems, making Smart ICT interoperability possible, providing guidelines for data protection, etc.).

A technological introduction of the above-mentioned Smart ICT technologies including Digital Trust is provided in Chapter 4. It proposes, in particular, an overview of standardization technical committees active in these technologies. Technical standardization can indeed support national stakeholders in building and maintaining the Smart Secure ICT environment, creating Digital Trust.

3.2 Economic Overview

The ICT sector is now more than ever an important part of the global economy. Beyond the investments in Smart ICT technologies that continue to increase, companies also largely investing in cybersecurity solutions to ensure a high level of Digital Trust in their technologies and services. Nowadays, one of the major challenges is indeed to prevent or mitigate increasingly frequent cyber-attacks, whose costs deal major damage to the economy.

Worldwide revenues for IT services crossed the \$1 trillion mark in 2018 according to IDC²⁸. In the same time, companies' investment in IT was growing all over last years. However, mainly due to the COVID-19 pandemic, Gartner estimates that global IT spending will be decreased by 7.3% for this year as compared to 2019, reaching \$3.5 trillion²⁹. Another analysis provided by IDC³⁰ forecast that ICT spending will remain flat compared to 2019, with a decrease of 3% of the spending in traditional ICT, compensated by a growth of 16% of the spending in new technologies. According to the 2019 EU Industrial R&D Investment Scoreboard³¹, Research & Development global investment into R&D in 2018 increased by 8.9% over the previous year, with a total of €823.4 billion invested by companies analyzed in the study (accounting for approximately 90% of the world's business-funded R&D). This growth was mainly driven by the sectors of ICT services (+16.9%) and ICT producers (+8.2%). Moreover, the coming trends show that the sector is still innovating with the development of Smart ICT technologies such as Artificial Intelligence, Digital twin, Edge computing, Blockchain, Smart spaces, Quantum computing, etc.^{32,33}

The development of Smart ICT technologies, which are increasingly interconnected, represents great opportunities for the economy, but also brings new threats. Nowadays, cyber defense appears as one

²⁸ <https://www.idc.com/getdoc.jsp?containerId=prUS45011519>

²⁹ <https://www.gartner.com/en/newsroom/press-releases/2020-07-13-gartner-says-worldwide-it-spending-to-decline-7-point-3-percent-in-2020>

³⁰ <https://www.idc.com/promo/global-ict-spending/forecast>

³¹ The 2019 EU Industrial R&D Investment Scoreboard - <https://iri.jrc.ec.europa.eu/scoreboard/2019-eu-industrial-rd-investment-scoreboard>

³² Gartner Top 10 Strategic Technology Trends for 2020 - <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/>

³³ Deloitte Tech Trends 2020 - <https://www2.deloitte.com/us/en/insights/focus/tech-trends.html>

of the main challenges for companies and countries considering the cost of cybercrime for the global economy. The Center for Strategic and International Studies (CSIS) estimated³⁴ that the global cost of cybercrime may be as much as \$600 billion in 2017, meaning nearly one percent of the global GDP. Another prediction from Cybersecurity Ventures forecasts that cybercrime will cost the world \$6 trillion annually by 2021³⁵. At the same time, worldwide spending on information security is forecast to reach \$123.8 billion in 2020, representing an increase of 2.4% compared to 2019 (this figure is largely impacted by the COVID-19 pandemic since Gartner was forecasting a growth of 8.7%, compared to 2018, in December 2019)³⁶.

At the European level, the ICT sector has been directly responsible for 5.16% of the GVA³⁷ (Gross Value Added), with a market value of €734 billion in 2018³⁸, but it contributes far more to overall productivity growth. This is not only due to the high levels of dynamism and innovation inherent to the sector, but also due to the enabler role this sector plays, in changing how other sectors do business. At the same time, the social impact of ICT has become significant. This is supported by European statistics of 2019, with 89% (Luxembourg: 95%) of households having a broadband connection³⁹, 85% (Luxembourg: 93%) of individuals using the Internet on a regular basis⁴⁰ of which 75% (Luxembourg: 86%) used a mobile device to connect to the Internet away from home or work⁴¹.

The European Commission also promotes research and innovation in the ICT sector, through innovative Public-Private Partnerships and through the Horizon 2020 research funding program that encompass a large range of ICT-related topics and capabilities, like sustainable use of natural resources, development of secure and efficient mobility, revolution of health services, cybersecurity, societal impact of the digital transformation, etc. The Horizon 2020 Work Program from 2018 to 2020 focuses on EU political priorities and attributes one of the largest budgets (EUR 1.8 billion) to the focus area dedicated to ICT, namely “Digitising and transforming European industry and services”. This focus area will “*address the combination of digital technologies (5G, high-performance computing, artificial intelligence, robotics, big data, Internet of Things, etc.) with innovations in other technological areas, as emphasized in the Digital Single Market strategy. [...] In addition, a particular emphasis will be put on cybersecurity and on addressing the societal impact of the digital transformation*”⁴². ICT will remain at the heart of the next funding program of the European Commission, Horizon Europe, which will be launched on the 1st of January 2021. It will be part of one of the clusters (Digital Industry & Space) in Pillar 2 “Global Challenges & European Industrial Competitiveness”.

3.3 Smart Secure ICT in Luxembourg

ICT is considered a key economic sector in the Grand Duchy of Luxembourg. Within the Coalition Agreement of the Government⁴³, the follow-up of Smart ICT development constitutes an important aspect since they represent great opportunities for the Economy. At the same time, it is important to mitigate threats related to their overall adoption. The Government works to make the country one of the leaders of the ICT sector and has adopted strategies in order to accelerate developments in different

³⁴ <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>

³⁵ Cybersecurity Ventures 2019 Official Annual Cybercrime Report - <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

³⁶ Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020 - <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>

³⁷ Gross value added is the value of output less the value of intermediate consumption; it is a measure of the contribution to GDP made by an individual producer, industry or sector (source: OECD)

³⁸ Source: Eurostat - National accounts aggregates by industry (up to NACE A*64) - code: nama_10_a64

³⁹ Source: Eurostat - Households with broadband access - code: TIN00073

⁴⁰ Source: Eurostat - Individuals regularly using the internet - code: TIN00091

⁴¹ Source: Eurostat - Individuals using mobile devices to access the internet on the move - code: TIN00083

⁴² http://europa.eu/rapid/press-release_MEMO-17-4123_en.htm

⁴³ <https://gouvernement.lu/dam-assets/documents/actualites/2018/12-decembre/Accord-de-coalition-2018-2023.pdf>

areas, such as 5G, Artificial Intelligence or High Performance Computing (HPC), while taking into account cybersecurity related challenges. In this context, the “National Cybersecurity Strategy III”⁴⁴, last updated in May 2018, provides the way forward in order to ensure maximum security for all stakeholders.

This program ensures continuity in the ICT sector’s growth in the country. Indeed, since the last decade, multiple actions have been initiated to foster the positioning of Luxembourg in the ICT landscape. One was the creation of the Ministry for Digitalisation in 2018, which is, for example, responsible for:

- The implementation of the "Digital Lëtzebuerg" action plan and the monitoring of the ICT sector (competence shared with the Minister of the Economy and the Minister for Communications and Media);
- The promotion of the ICT sector (competence shared with the Minister of Economy);
- The development and implementation of an Internet of Things plan;
- The development of a national strategy in the field of Artificial Intelligence (in consultation with the Minister for Communications and Media and the Minister of Economy).

Through the national policy pursued in recent years, Luxembourg aims to accompany the transition to a digital economy and society. Indeed, several initiatives have been launched to consolidate and expand the country’s ICT capabilities. For example:

- The launch of "Digital Lëtzebuerg"⁴⁵ in 2014, which is a multidisciplinary government initiative working with public, private and academic players to harness digitalization for positive transformation.
- The Digital4Education initiative⁴⁶, unveiled in 2015 by the Minister of Education, Childhood & Youth, which aims at developing digital skills & know-how fit for the 21st century.
- The strategic study on the “Third Industrial Revolution”⁴⁷, presented in November 2016, which proposes concrete actions and tools, including a range of strategic measures and projects, to prepare the country, its society and its economy to begin the process of the "Third Industrial Revolution".
- The “National Cybersecurity Strategy III”⁴⁸, lastly updated in May 2018, which intends to provide an environment conducive to digital development, while ensuring maximum security for all stakeholders. This strategy notably highlights the importance of monitoring standards development in order to take into account internationally recognized practices in the cybersecurity area.
- The “5G strategy for Luxembourg”⁴⁹, published in November 2018, which sets the objective of the country to develop the infrastructure supporting 5G deployment.
- The document “Artificial Intelligence: a Strategic Vision for Luxembourg”⁵⁰, published in May 2019, which defines three main ambitions for the country: to be among the most advanced digital societies in the world, especially in the EU; to become a data-driven and sustainable economy; to support human-centric AI development.
- The “Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg”⁵¹, published in May 2019. It provides an approach to accelerate the

⁴⁴ <https://hpcn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf>

⁴⁵ <https://gouvernement.lu/en/dossiers/2014/digital-letzebuerg.html>

⁴⁶ <https://men.public.lu/dam-assets/catalogue-publications/dossiers-de-presse/2014-2015/digital-4-education.pdf>

⁴⁷ <http://www.troisiemerevolutionindustrielle.lu/etude-strategique/>

⁴⁸ <https://hpcn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf>

⁴⁹ https://digital-luxembourg.public.lu/sites/default/files/2018-11/Digital-Luxembourg_Strategy5G_V1_WEB.pdf

⁵⁰ https://digital-luxembourg.public.lu/sites/default/files/2019-05/AI_EN.pdf

⁵¹ <https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-economie/The-Data-driven-Innovation-Strategy.pdf>

digitalization-enabled transformation of Luxembourg's industry across key strategic sectors, boosting productivity across the entire Luxembourg economy.

All these developments have allowed Luxembourg to establish a competitive ICT sector. The country ranks 10th out of the 28 EU Member States in the "European Commission Digital Economy and Society Index" (DESI) 2020⁵². The country is particularly strong in terms of connectivity (ranks 3rd), human capital (ranks 8th) and use of the Internet (ranks 12th). Luxembourg is also well placed in the cybersecurity landscape, ranking 11th in the Global Cybersecurity Index 2018⁵³, which is a composite index published by the ITU to measure the commitment of countries to cybersecurity in order to raise cybersecurity awareness. The ICT sector was composed of 2 426 companies in 2017 (6.3% of the total number of companies) and represented 4.55% of the total employment of the first quarter of 2020⁵⁴.

⁵² <https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg>

⁵³ https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

⁵⁴ Source: STATEC

4 SMART SECURE ICT STANDARDS WATCH

The objective of this Standards Analysis “Smart Secure ICT Luxembourg” is to facilitate the involvement of the national stakeholders in the technical standardization process. To achieve this goal, this chapter introduces basic concepts of Smart ICT technologies, such as the Internet of Things (IoT), Cloud Computing, Artificial Intelligence and Blockchain as well as the main standardization technical committees active in these areas. In addition, the chapter also highlights the importance of Digital Trust in Smart ICT and introduces related technical standardization committees towards above-mentioned Smart ICT technologies, along with a list of fora and consortia active in the Digital Trust area.

In addition, lists of standards both published and under development for the selected Smart ICT technologies and related Digital Trust are provided in the Appendix. This overview of standards and projects at the international and European levels is intended to help national stakeholders in building secure and trustworthy environments in Smart ICT technologies through technical standardization. In particular, this Standards Analysis focuses on ISO/IEC, CEN, CENELEC, ETSI and ITU-T standardization developments.

4.1 Internet of Things (IoT)

The Internet of Things (IoT) refers to business processes and applications of sensed data, information and content generated from an interconnected world by the means of connected devices that exist in the internet infrastructure⁵⁵. In the IoT ecosystem, systems are composed of networked entities. The entities could be IoT devices, information resources or people, which can be easily interconnected to interact with the physical world.⁵⁶ In summary, it describes a world where anything can be connected and can interact in an intelligent fashion. Table 2 provides definitions of the IoT provided by different standard development organizations (SDOs).

SDO	IoT Definition
ISO/IEC ⁵⁷	“IoT is an infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world”
ITU-T ⁵⁸	“A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”
IEEE ⁵⁹	“Internet of Things envisions a self-configuring, adaptive, complex network that interconnects ‘things’ to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely

⁵⁵ ILNAS White Paper Internet of Things (IoT) - <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf>

⁵⁶ ILNAS National Technical Standardization Report on Internet of Things (IoT) - <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/national-technical-standardization-report-iot-june-2020.pdf>

⁵⁷ ISO/IEC 20924:2018, Information technology - Internet of Things (IoT) - vocabulary, <https://www.iso.org/obp/ui/#iso:std:iso-iec:20924:ed-1:v1:en:term:3.2.1>

⁵⁸ ITU-T Y.2060 (06/2012), Overview of the Internet of things - <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=en>

⁵⁹ IEEE, Towards a definition of the Internet of Things (IoT) - https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

SDO	IoT Definition
	<p>identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.”</p>

Table 2: IoT definitions

4.1.1 Characteristics

The IoT is a complex system with a number of characteristics that can be defined from the perspectives of IoT components used, services provided, usability, and security. Some of the general and key characteristics are highlighted in Table 3.

Characteristic	Description
Smart data collection and smart handling	<p>The IoT is able to distribute sensors widely and collect data quickly and effectively to form a new way of collaboration among connected devices. Smart data processing of such collected data is a key IoT feature. The different kinds of data produced by physical devices of IoT systems can be stream, batch, and asynchronous data. Such data can be processed and used for system feedback, allowing for process improvement, fault detection and incorporation of real-world context into business workflows.</p>
Interconnectivity	<p>The IoT is able to interconnect anything (physical or virtual things) with the help of global information and communication infrastructure. Communication infrastructure⁶⁰ refers to backbone of the communications system upon which various broadcasting and telecommunication services are operated. This can be built from copper cable, fiber, or wireless technologies utilizing the radio frequency spectrum, such as microwave and satellite.</p>
Things-related services	<p>The IoT is capable of providing things-related services within the constraints of things, such as privacy protection and semantic consistency between physical and their associated virtual objects. In order to provide things-related services within the constraints of things, both technologies in physical world and information world are required.</p>

⁶⁰ <http://www.blackwellreference.com>

Characteristic	Description
Heterogeneity / diversity	The devices in the IoT should be heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks. Diversity is another characteristic of the IoT. Identifiers in the physical world and the information world are different. In the physical world, the identifiers of physical things of the IoT devices may be different according to applied technologies.
Dynamic changes	The state of devices changes dynamically (for instance, sleeping and waking up, connected and/or disconnected) as well as the context of devices, including location and speed. Moreover, the number of devices can change dynamically.
Enormous scale	The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the number of devices connected to current internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be management of the generated data and its interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Table 3: IoT Basic Characteristics⁶¹


4.1.2 IoT Standardization Technical Committees

Many organizations are actively involved in IoT technical standardization. It is widely acknowledged that many standardization challenges need to be addressed for further spread of the IoT. Issues include, but are not limited to, security, privacy, interfaces, data structures, and architecture. Because the IoT covers everything from pure technical level up to business processes and even political decisions, there is no single standard (not even at the interface level) and, as a result, the world of IoT standards is completely fragmented⁶². The urgent need for standardization and necessary improvements in interoperability are critical success factors for accelerated adoption of IoT systems⁶³. This section provides an overview of the IoT related technical committees currently active in the recognized standardization organizations to fill the gap in IoT standardization. In addition, standards and projects of these technical committees, in the IoT and Digital Trust areas, are listed in the Appendix (Section 8.1).

⁶¹ ILNAS White Paper Internet of Things (IoT) - <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf>

⁶² OECD Digital Economy Outlook 2015" - <http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm>

⁶³ McKinsey Global Institute "The Internet of Things: mapping the value beyond the hype" - [https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking the potential of the Internet of Things Executive summary.pdf](https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking%20the%20potential%20of%20the%20Internet%20of%20Things%20Executive%20summary.pdf)

ISO/IEC JTC 1/SC 41 INTERNET OF THINGS AND RELATED TECHNOLOGIES			
GENERAL INFORMATION			
Creation date	2017	Secretariat	KATS (Republic of Korea)
Chairperson	Mr. François Coallier	Committee Manager	Ms. Jooran Lee
Scope	Standardization in the area of Internet of Things and related technologies. <ul style="list-style-type: none"> - Serve as the focus and proponent for JTC 1's standardization program on the Internet of Things and related technologies, including Sensor Networks and Wearables technologies. - Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications. 		
Structure	WG 3 IoT Architecture WG 4 IoT Interoperability WG 5 IoT Applications JWG 3 IEC Smart Energy Roadmap Managed by SyC Smart Energy JWG 17 System interface between industrial facilities and the smart grid Managed by TC 65 AG 6 JTC 1/SC 41 Advisory Group AG 20 Sectorial Liaison Group (SLG 1) on Industrial IoT (IIoT) AG 21 Sectorial Liaison Group (SLG 2) on Utilities IoT AG 22 Liaison Coordination Group (LCG) on IoT Trustworthiness AG 25 Advisory Group on IoT use cases AHG 14 Ad hoc group on Business Plan AHG 15 Communication and outreach AHG 23 Ad hoc group on IoT Personnel positioning management system (PPMS) AHG 26 Trustworthiness interoperability		
Webpage	https://www.iec.ch/dyn/www/f?p=103:7:0:::FSP_ORG_ID,FSP_LANG_ID:20486,25		
STANDARDIZATION WORK			
Published standards	27	Projects	19
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (26)	Australia, Austria, Belarus, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Israel, Italy, Japan, Republic of Korea, Luxembourg , Malaysia, Netherlands, Norway, Russian Federation, Singapore, Spain, Sweden, Switzerland, United Kingdom, United States		
O-Members (13)	Argentina, Iceland, Iran, Ireland, Kenya, Mexico, Pakistan, Republic of the Philippines, Poland, Portugal, Romania, Saudi Arabia, Slovakia		
Luxembourg's involvement (17)	<ul style="list-style-type: none"> - Mr. Shyam Wagle (Chairman) ANEC G.I.E. - Mr. Johann Amsenga INCERT GIE - Mr. Philippe Bovy KPMG Luxembourg S.C. - Mr. Matthias Brust University of Luxembourg - Mr. Arunas Buknys FANUC Europe S.A. - Mr. Vincent Cady Tarkett S.A. - Mr. Sankalp Ghatpande University of Luxembourg - Mr. Konrad Grohs FANUC Europe S.A. - Mr. Abdallah Ibrahim University of Luxembourg - Mr. Jean Lancrenon ANEC G.I.E. - Ms. Maria Rita Palattella LIST - Mr. Benoit Poletti INCERT GIE - Mr. Cyrille Rousseau CORAX IP S.à.r.l - Mr. Nader Samir Labib University of Luxembourg - Mr. Claude Schanet ANSSI - Mr. Ridha Soua University of Luxembourg - Mr. Muhammad Wasim University of Luxembourg 		

COMMENTS

ISO/IEC JTC 1/SC 41 “Internet of Things and related technologies” has been established according to the Resolution 12 of the 31st Meeting of ISO/IEC JTC 1 in November 2016. It is currently developing standards to build IoT foundations and exploring new areas of work relating to other emerging technologies.

The detail of IoT standards and projects developed by ISO/IEC JTC 1/SC 41 can be found in the Appendix (Section 8.1).

ISO/IEC JTC 1/SC 31 AUTOMATIC IDENTIFICATION AND DATA CAPTURE TECHNIQUES



GENERAL INFORMATION

Creation date	1996	Secretariat	ANSI (United States)
Chairperson	Mr. Henri Barthel	Committee Manager	Mr. Eddy Merrill
Scope	Standardization of data formats, data syntax, data structures, data encoding, and technologies for the process of automatic identification and data capture and of associated devices utilized in inter-industry applications and international business interchanges and for mobile applications.		
Structure	WG 1 Data carrier WG 2 Data and structure WG 4 Radio communications WG 8 Application of AIDC standards		
Webpage	https://www.iso.org/committee/45332.html		

STANDARDIZATION WORK

Published standards	127	Projects	23
---------------------	-----	----------	----

INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT

P-Members (25)	Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Japan, Kazakhstan, Republic of Korea, Luxembourg , Mauritania, Netherlands, Peru, Russian Federation, Slovakia, South Africa, Sweden, Switzerland, United Kingdom, United States		
O-Members (25)	Argentina, Belarus, Bosnia and Herzegovina, Colombia, Czech Republic, Ghana, Hong Kong, Hungary, Indonesia, Islamic Republic of Iran, Italy, Kenya, Malaysia, New Zealand, Pakistan, Philippines, Poland, Romania, Serbia, Singapore, Slovenia, Spain, Thailand, Turkmenistan, Ukraine		
Luxembourg's involvement (4)	- Mr. Benoit Poletti (Chairman)	INCERT G.I.E.	
	- Mr. Clément Gorlt	INCERT G.I.E.	
	- Mr. Abdelkrim Nehari	INCERT G.I.E.	
	- Mr. Shyam Wagle	ANEC G.I.E.	

COMMENTS

Technologies such as bar coding and radiofrequency identification (RFID) provide quick, accurate and cost-effective ways to identify, track, acquire and manage data and information about items, personnel, transactions and resources. These are known as the automatic identification and data capture (AIDC) technologies.


The focus is on efficient implementations of the standards. Governmental bodies in a growing number of countries mandate AIDC technologies, for example in the pharmaceutical and medical device sectors or in the area of fighting against illicit trade in the tobacco industry. There are however still requirements for new technology standards, specifically new barcodes and additional cryptography standards to secure information stored in RFID tags.

ISO/IEC JTC 1/SC 31, Automatic identification and data capture techniques, is responsible for almost 150 published or in-progress standards in this area. These standards address bar code symbologies (how a bar code is created and read), RFID air interface (how an RFID tag is read), real-time locating systems, and mobile item identification (which explains how a device such as a phone is used to read and access data as well as providing standards to define how the data associated with the technology are stored and read).


The work that has been done to date has enabled major changes in the world with barcodes used everywhere, and RFID technology fast becoming adopted by many sectors. The growth of the Internet of Things (IoT) has awakened interest in the technologies based on the SC 31 technology standards. Standards for Radio Frequency identification, Real-Time Locating System, and barcodes will be important to the fast and efficient adoption of the IoT concepts.


SC 31 has also published a standard in the IoT area to specify the common rules applicable for unique identification that are required to ensure full compatibility across different identities: ISO/IEC 29161:2016, Information technology -- Data structure -- Unique identification for the Internet of Things.


The detail of IoT standards and projects developed by ISO/IEC JTC 1/SC 31 can be found in the Appendix (Section 8.1).

ISO/IEC JTC 1/SC 25 INTERCONNECTION OF INFORMATION TECHNOLOGY EQUIPMENT			
GENERAL INFORMATION			
Creation date	1990	Secretariat	DIN (Germany)
Chairperson	Mr. Rainer Schmidt	Committee Manager	Mr. Marco Peter
Scope	<p>Standardization of microprocessor systems, interfaces, protocols, architectures and associated interconnecting media for information technology equipment and networks to support embedded and distributed computing environments, storage systems and other input/output components.</p> <p>Standards for home and building electronic systems in residential and commercial environments to support interworking devices (IoT-related) and applications such as energy management, environmental control, lighting, and security.</p> <p>Cabling system standards for information and communication technology (ICT), in all types of residential, commercial and industrial environments for the design, planning and installation, test procedures, automated infrastructure management systems and remote powering.</p> <p>NOTE: JTC 1/SC 25 standards reference IEC standards for cables, waveguides and connectors.</p>		
Structure	<p>WG 1 Home electronic systems</p> <p>WG 3 Customer Premises Cabling</p> <p>WG 4 Interconnection of Computer Systems and Attached Equipment</p> <p>PT 40G Channels in support of 40Gbit/s</p> <p>PT TT Project Team Taxonomy and Terminology</p> <p>JWG 10 Industrial Cabling Managed by IEC/TC 65/SC 65C</p> <p>AHG 1 Bonding adhoc</p> <p>JPT 1 Joint modelling task group linked to IEC/TC 46/SC 46C, IEC/TC 48/SC 48B</p>		
Webpage	https://www.iec.ch/dyn/www/f?p=103:7:0:::FSP_ORG_ID:3399		
STANDARDIZATION WORK			
Published standards	230	Projects	17
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (29)	Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Lebanon, Mexico, Netherlands, Norway, Poland, Russian Federation, Singapore, Spain, Sweden, Switzerland, United Kingdom, United States		
O-Members (18)	Argentina, Bosnia and Herzegovina, Croatia, Cuba, Ghana, Greece, Hungary, Iceland, Indonesia, Kenya, Malaysia, New Zealand, Pakistan, Republic of the Philippines, Romania, Serbia, Turkey, Ukraine		

Luxembourg's involvement (0)	No registered delegate
COMMENTS	
<p>Homes are increasingly equipped with home systems conforming to the Home Electronic System (HES) architecture and implementing protocols specified in the ISO/IEC 14543 series. These protocols support competitive markets with products from various sources implementing protocols specified in this series. Standards for remote access and management of home equipment are being developed. Products meeting these specifications have been well received by the market and enable smart grids to interact with intelligent homes. Extensions of cloud-based services connected to home devices for home applications creating an IoT environment are expanding the market for standards developed by JTC 1/SC 25. SC 25 is also developing standards to address concerns for cybersecurity (data security), privacy, and the safety of connected devices and appliances in homes.</p> <p>The detail of IoT standards and projects developed by ISO/IEC JTC 1/SC 25 can be found in the Appendix (Section 8.1).</p>	

CEN/TC 225 AIDC TECHNOLOGIES			
GENERAL INFORMATION			
Creation date	1989	Secretariat	TSE (Turkey)
Chairperson	Mr. Claude Tételin	Secretary	Ms. Aysegül Ibrsim
Scope	Standardization of data carriers for automatic identification and data capture, of the data element architecture therefore, of the necessary test specifications and of technical features for the harmonization of cross-sector applications. Establishment of an appropriate system of registration authorities, and of means to ensure the necessary maintenance of standards.		
Structure	WG 4 Automatic ID applications		
Webpage	http://standards.cen.eu/dyn/www/f?p=204:7:0:::FSP_ORG_ID:6206&cs=1E12277AECC001196A7556B8DBCDF0A1C		
STANDARDIZATION WORK			
Published standards	28	Projects	1
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
Members (34)	34 members of CEN/CENELEC		
Luxembourg's involvement (0)	No registered delegate		
COMMENTS			
<p>CEN/TC 225 takes into account the technical specifications, standards and regulations currently available or being prepared at international levels to prepare standards for Europe. In particular, the technical work in ISO/IEC JTC 1/SC 31 (Automatic Identification and Data Capture (AIDC) techniques) and ISO/IEC JTC 1/SC 27 (Privacy) are taken into account. CEN/TC 225 delivers EN standards and technical reports to:</p> <ul style="list-style-type: none"> - Guide the deployment of AIDC systems in public and private enterprises within Europe; - Ensure the deployments are secure and protect personal privacy issues identified by the European regulation on Data protection; - Provide guidelines for the unique identification of all types of objects supporting the free global movement of goods, enhanced health and safety aspects in industries and in governmental sector. <p>The detail of IoT standards and projects developed by CEN/TC 225 can be found in the Appendix (Section 8.1).</p>			

ETSI/TC Smart M2M SMART MACHINE-TO-MACHINE COMMUNICATION			
GENERAL INFORMATION			
Creation date	N/A		
Chairperson	Mr. Enrico Scarrone		
Scope	<p>TC Smart M2M primarily provides specifications for M2M services and applications. Much of the work focuses on aspects of the Internet of Things (IoT) and Smart Cities. TC Smart M2M supports European policy and regulatory requirements including mandates in the area of M2M and the Internet of Things. TC Smart M2M work includes the identification of EU policy and regulatory requirements on M2M services and applications to be developed by SmartM2M, and the conversion of the oneM2M specifications into European Standards.</p> <p>The activities of TC Smart M2M include the following:</p> <ul style="list-style-type: none"> - Be a center of expertise in the area of M2M and Internet of Things (IoT) to support M2M services and applications; - Maintain ETSI M2M published specifications; - Produce specifications as needed for regulatory purposes; - Transpose the output of oneM2M to TC SmartM2M. <p>TC Smart M2M will aim at referring to existing work done elsewhere, or encouraging existing groups to fulfil Smart M2M requirements. The TC will undertake necessary work that is not being provided for elsewhere.</p>		
Structure	N/A		
Webpage	http://portal.etsi.org/portal/server.pt/community/SmartM2M		
STANDARDIZATION WORK			
Published standards	86	Projects	12
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
Members (106)	106 members organizations		
Luxembourg's involvement (2)	<p>- Skylane Optics - FBConsulting S.A.R.L.</p> <p>Note: ILNAS, with the support of ANEC G.I.E. is also monitoring the developments of the ETSI/TC SmartM2M.</p>		
COMMENTS			
<p>ETSI's Smart Machine-to-Machine Communications committee (TC SmartM2M) is developing standards to enable M2M services and applications and certain aspects of the IoT. The committee's focus is on an application-independent 'horizontal' service platform with architecture capable of supporting a very wide range of services including smart metering, smart grids, eHealth, city automation, consumer applications and car automation.</p> <p>The detail of IoT standards and projects developed by ETSI/TC SmartM2M can be found in the Appendix (Section 8.1).</p>			

ITU-T/SG 20 INTERNET OF THINGS, SMART CITIES AND COMMUNITIES			
GENERAL INFORMATION			
Chairperson	Mr. Nasser Saleh Al Marzouqi		
Scope	<p>Study Group 20 is responsible for studies relating to Internet of Things (IoT) and its applications, and smart cities and communities (SC&C). This includes studies relating to big data aspects of IoT and SC&C, e-services and smart services for SC&C. The lead study group roles include:</p> <ul style="list-style-type: none"> - Internet of things (IoT) and its applications; 		

	<ul style="list-style-type: none"> - Smart cities and communities, including its e-services and smart services; - Internet of things identification.
Structure	<p>WP1/Q1 End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C</p> <p>WP1/Q2 Requirements, capabilities, and use cases across verticals</p> <p>WP1/Q3 Architectures, management, protocols and Quality of Service</p> <p>WP1/Q4 e/Smart services, applications and supporting platforms</p> <p>WP2/Q5 Research and emerging technologies, terminology and definitions</p> <p>WP2/Q6 Security, privacy, trust and identification for IoT and SC&C</p> <p>WP2/Q7 Evaluation and assessment of Smart Sustainable Cities and Communities</p> <p>Other groups under SG 20:</p> <p>JCA-IoT and SC&C Joint Coordination Activity on Internet of Things and Smart Cities and Communities</p> <p>FG-DPM Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities</p>
Webpage	https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx
STANDARDIZATION WORK	
Published standards	83
Projects	89
NATIONAL INVOLVEMENT	
Luxembourg's involvement	Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ITU-T/SG 20.
COMMENTS	
<p>The objective of SG 20 is to standardize requirements of IoT technologies. It was initially focused on IoT applications in Smart Cities and Communities (SC&C). This SG is now composed of two working parties including seven different study questions dealing with different aspects of IoT standardization. It develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study group is the standardization of end-to-end architectures for IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.</p> <p>The detail of IoT standards and projects developed by ITU-T/SG 20 can be found in the Appendix (Section 8.1).</p>	

4.2 Cloud Computing

Cloud Computing enables ubiquitous access to shared pools of services and system resources, which can be rapidly provisioned with minimal management effort over the Internet. The current advancement of Cloud Computing is closely related to virtualization. The ability to pay on demand and scale quickly when required is largely a result of Cloud service providers being able to pool resources that could be divided into multiple users. Among multiple definitions of Cloud Computing, ITU-T, ISO/IEC and National Institute of Standards (NIST) definitions are listed in Table 4 to better understand the concept of Cloud Computing.

SDO / Organization	Definition
ITU-T Y.3500 and ISO/IEC 17788 ⁶⁴	Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand
NIST ⁶⁵	Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

Table 4: Definitions of Cloud Computing

4.2.1 Characteristics

Nowadays, anything as a service (XaaS) is considered to categorize the service capabilities offered in Cloud Computing. However, Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) remain the main fundamental services provided in Cloud Computing. Furthermore, four deployments models, namely, Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud are commonly used in practice.

Considering its rapid implementation across multiple sectors, any list of Cloud Computing characteristics can be very long. Some fundamental characteristics of Cloud Computing are summarized in Table 5. Fundamental characteristics, services and deployment models of Cloud Computing are also highlighted in Figure 2.

Characteristic	Explanation
Broad Network Access	The physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms.

⁶⁴ ITU-T Y.3500 | ISO/IEC 17788, Information technology - Cloud computing - Overview and vocabulary - https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3500-201408-1!!PDF-E&type=items | http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip

⁶⁵ NIST Special Publication 800-145, The NIST Definition of Cloud Computing - <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Characteristic	Explanation
Measured Service	The metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed. The customer may only pay for the resources that they use.
Multi-tenancy	Physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another.
On-demand Self-service	A cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider.
Rapid Elasticity and Scalability	Physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the cloud service customer, physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements.
Resource Pooling	A cloud service provider's physical or virtual resources can be aggregated in order to serve one or more cloud service customers.

Table 5: Characteristics of Cloud Computing⁶⁶

⁶⁶ ITU-T Y.3500 | ISO/IEC 17788, Information technology - Cloud computing - Overview and vocabulary - https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3500-201408-I!!PDF-E&type=items | http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip

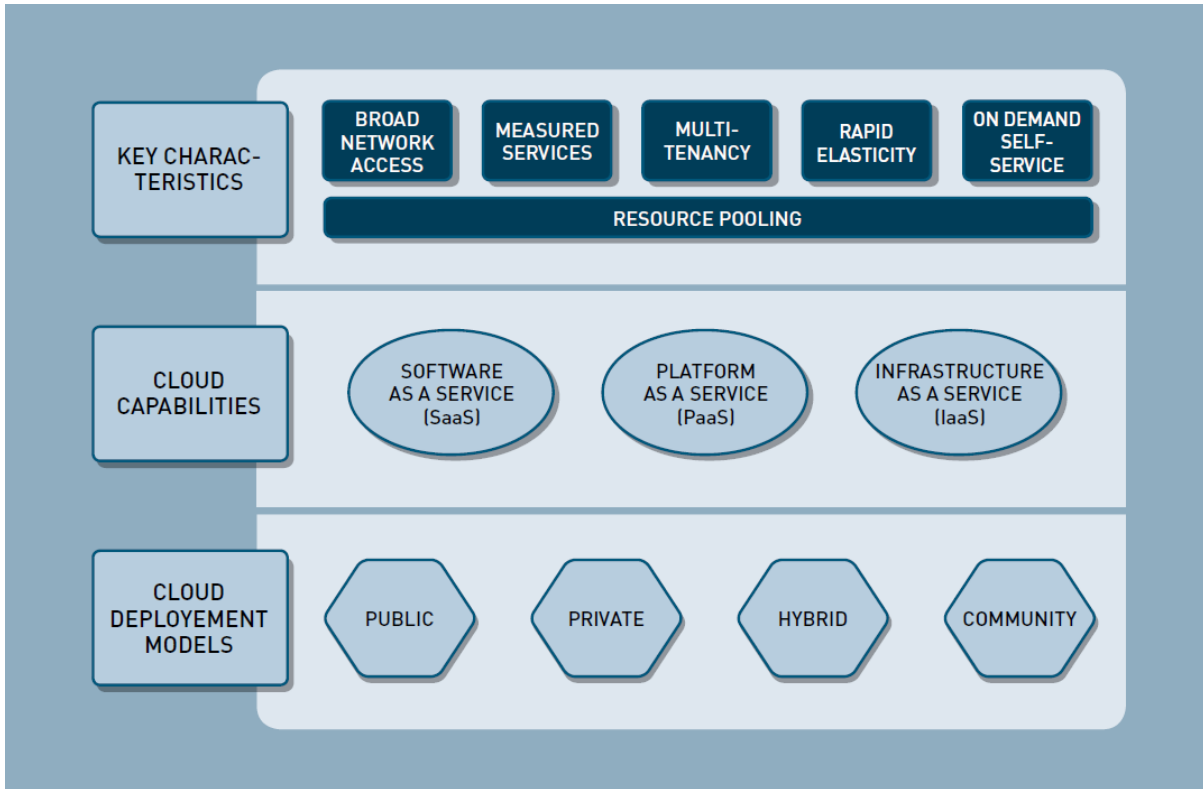



Figure 2: Visual Model of ISO/IEC Cloud Computing Definition⁶⁷

4.2.2 Cloud Computing Standardization Technical Committees

The standards landscape for Cloud Computing is extensive since many standards developing organizations are active in the Cloud Computing domain and many standards and specifications have been developed. This section provides an overview of the Cloud Computing related technical committees and standards currently active in the recognized standardization organizations. In addition, standards and projects of these technical committees, in the Cloud Computing and Digital Trust areas, are listed in the Appendix (Section 8.2).

ISO/IEC JTC 1/SC 38 CLOUD COMPUTING AND DISTRIBUTED PLATFORMS			
GENERAL INFORMATION			
Creation date	2009	Secretariat	ANSI (United States)
Chairperson	Mr. Steve Holbrook	Committee Manager	Mr. Bill Ash
Scope	Standardization in the areas of Cloud Computing and Distributed Platforms including: <ul style="list-style-type: none"> - Foundational concepts and technologies; - Operational issues; - Interactions among Cloud Computing systems and with other distributed systems. SC 38 serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in these areas.		

⁶⁷ Figure based on the Cloud Computing definition given in ISO/IEC 17788:2014, Information technology -- Cloud computing -- Overview and vocabulary

Structure	AG 1	Communications committee
	AG 2	JTC 1/SC 38 Officers group
	AG 3	Multi-cloud
	AG 4	Cloud service connectivity
	AG 5	Long-term standards roadmap
	CG 1	Liaison coordination group for JTC 1/SC 27
	CG 2	Liaison coordination group for JTC 1/SC 41
Webpage	CG 3	Liaison coordination group for JTC 1/SC 42
	WG 3	Cloud Computing Fundamentals (CCF)
	WG 5	Data in cloud computing and related technologies
https://www.iso.org/committee/601355.html		
STANDARDIZATION WORK		
Published standards	21	Projects 7
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT		
P-Members (28)	Australia, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Luxembourg , Netherlands, Panama, Poland, Russian Federation, Singapore, Slovakia, Spain, Sweden, Switzerland, United Kingdom, United States	
O-Members (21)	Argentina, Austria, Bosnia and Herzegovina, Czech Republic, Hong Kong Special Administrative Region of China, Hungary, Indonesia, Kenya, Mexico, Norway, Pakistan, Philippines, Portugal, Romania, Serbia, South Africa, Trinidad and Tobago, Turkey, Ukraine, Uruguay, Zambia	
Luxembourg's involvement (11)	<ul style="list-style-type: none"> - Mr. Shyam Wagle (Chairperson) ANEC G.I.E. - Mr. Matthias Brust University of Luxembourg - Mrs. Myriam Djerouni LUXITH G.I.E. - Mr. Michael Feddema KPMG Luxembourg S.C. - Mr. Laurent Fisch Laurent Fisch Luxlegal S.à r.l. - Mrs. Shenglan Hu POST Telecom PSF S.A. - Mr. Abdallah Ibrahim University of Luxembourg - Mr. Andreas Kremer ITTM - Mr. Chao Liu University of Luxembourg - Mr. Qiang Tang LIST - Mr. Muhammad Wasim University of Luxembourg 	
COMMENTS		
<p>ISO/IEC JTC 1/SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in the Cloud Computing area. With the progression of service oriented architecture specification and the publication of ISO/IEC 17788 and 17789, standards presenting a taxonomy, terminology and vocabulary, from the Cloud Computing collaboration with ITU-T/SG 13, SC 38 is turning its focus to identifying other standardization initiatives in these rapidly developing areas.</p> <p>Based on an understanding of the market/business/user requirements for Cloud Computing standards and a survey of related standardization activities within ISO/IEC JTC 1 and other standards setting organizations, new Cloud Computing standardization initiatives will be proposed and initiated. ISO/IEC JTC 1/SC 38 will address the public and private sector needs for standards that answer end-user requirements and facilitate the rapid deployment of Cloud Computing. To this end, ISO/IEC JTC 1 SC 38 has recently published technical reports covering billing modes in Cloud Computing (ISO/IEC TR 23613:2020) and the rapidly developing Edge Computing paradigm (ISO/IEC TR 23188:2020), among others.</p> <p>In parallel, projects related to Cloud Computing security are under the direct responsibility of ISO/IEC JTC 1/SC 27. In this frame, several International Standards have already been published, like ISO/IEC 27017:2015 or ISO/IEC 27018:2019, which respectively define a code of practice for information security controls based on ISO/IEC 27002 for cloud services and for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO/IEC JTC 1/SC 27 also developed the fourth part of ISO/IEC 19086-4:2019, concerning the security and privacy aspects of the SLA framework and technology.</p> <p>The detail of Cloud Computing standards and projects developed by ISO/IEC JTC 1/SC 38 can be found in the Appendix (Section 8.2).</p>		

**ITU-T/SG 13
FUTURE NETWORKS, WITH FOCUS ON IMT-2020, CLOUD COMPUTING AND
TRUSTED NETWORK INFRASTRUCTURES**



GENERAL INFORMATION

Chairperson	Mr. Leo Lehmann																																				
Scope	<p>ITU-T Study Group 13 is responsible for studies relating to the requirements, architectures, capabilities, and APIs as well as softwarization and orchestration aspects of converged future networks (FN), specifically focusing on IMT-2020 non-radio related parts. This also includes IMT- 2020 project management coordination across all ITU-T study groups and release planning and implementation scenarios. It is responsible for studies relating to Cloud Computing technologies, big data, virtualization, resource management, reliability and security aspects of the considered network architectures. It also works on studies relating to Fixed-Mobile Networks (FMC), mobility management, and enhancements to existing ITU-T Recommendations on mobile communications, including energy-saving aspects. Furthermore, Study Group 13’s responsibility includes studies on emerging network technologies for IMT-2020 networks and future networks, such as Information Centric Networking (ICN)/Content Centric Networking (CCN). Study Group 13 is also responsible for studies relating to standardization of concepts and mechanisms to enable trusted ICT, including frameworks, requirements, capabilities, architectures and implementation scenarios of trusted network infrastructures and trusted cloud solutions in coordination with all study groups concerned. The lead study group roles include:</p> <ul style="list-style-type: none"> - Future networks such as IMT-2020 networks (non-radio related parts); - Mobility management; - Cloud Computing; - Trusted network infrastructures. 																																				
Structure	<table border="0"> <tr> <td>WP1/Q6</td> <td>Quality of service (QoS) aspects including IMT-2020 networks</td> </tr> <tr> <td>WP1/Q20</td> <td>IMT-2020: Network requirements and functional architecture</td> </tr> <tr> <td>WP1/Q21</td> <td>Network softwarization including software-defined networking, network slicing and orchestration</td> </tr> <tr> <td>WP1/Q22</td> <td>Upcoming network technologies for IMT-2020 and Future Networks</td> </tr> <tr> <td>WP1/Q23</td> <td>Fixed-Mobile Convergence including IMT-2020</td> </tr> <tr> <td>WP2/Q7</td> <td>Big data driven networking (bDDN) and Deep packet inspection (DPI)</td> </tr> <tr> <td>WP2/Q17</td> <td>Requirements, ecosystem, and general capabilities for cloud computing and big data</td> </tr> <tr> <td>WP2/Q18</td> <td>Functional architecture for cloud computing and big data</td> </tr> <tr> <td>WP2/Q19</td> <td>End-to-end cloud computing management, cloud security and big data governance</td> </tr> <tr> <td>WP3/Q1</td> <td>Innovative services scenarios, deployment models and migration issues based on Future Networks</td> </tr> <tr> <td>WP3/Q2</td> <td>Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network virtualization (NFV)</td> </tr> <tr> <td>WP3/Q5</td> <td>Applying networks of future and innovation in developing countries</td> </tr> <tr> <td>WP3/Q16</td> <td>Knowledge-centric trustworthy networking and services</td> </tr> </table> <p>Other groups under SG13:</p> <table border="0"> <tr> <td>JCA-IMT2020</td> <td>Joint Coordination Activity on IMT-2020</td> </tr> <tr> <td>JCA-SDN</td> <td>Joint Coordination Activity on Software-Defined Networking</td> </tr> <tr> <td>FG ML5G</td> <td>ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G)</td> </tr> <tr> <td>FG NET2030</td> <td>Focus Group on Technologies for Network 2030</td> </tr> <tr> <td>JRG-CCM</td> <td>Joint Rapporteur Group on Cloud Computing management</td> </tr> </table>	WP1/Q6	Quality of service (QoS) aspects including IMT-2020 networks	WP1/Q20	IMT-2020: Network requirements and functional architecture	WP1/Q21	Network softwarization including software-defined networking, network slicing and orchestration	WP1/Q22	Upcoming network technologies for IMT-2020 and Future Networks	WP1/Q23	Fixed-Mobile Convergence including IMT-2020	WP2/Q7	Big data driven networking (bDDN) and Deep packet inspection (DPI)	WP2/Q17	Requirements, ecosystem, and general capabilities for cloud computing and big data	WP2/Q18	Functional architecture for cloud computing and big data	WP2/Q19	End-to-end cloud computing management, cloud security and big data governance	WP3/Q1	Innovative services scenarios, deployment models and migration issues based on Future Networks	WP3/Q2	Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network virtualization (NFV)	WP3/Q5	Applying networks of future and innovation in developing countries	WP3/Q16	Knowledge-centric trustworthy networking and services	JCA-IMT2020	Joint Coordination Activity on IMT-2020	JCA-SDN	Joint Coordination Activity on Software-Defined Networking	FG ML5G	ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G)	FG NET2030	Focus Group on Technologies for Network 2030	JRG-CCM	Joint Rapporteur Group on Cloud Computing management
WP1/Q6	Quality of service (QoS) aspects including IMT-2020 networks																																				
WP1/Q20	IMT-2020: Network requirements and functional architecture																																				
WP1/Q21	Network softwarization including software-defined networking, network slicing and orchestration																																				
WP1/Q22	Upcoming network technologies for IMT-2020 and Future Networks																																				
WP1/Q23	Fixed-Mobile Convergence including IMT-2020																																				
WP2/Q7	Big data driven networking (bDDN) and Deep packet inspection (DPI)																																				
WP2/Q17	Requirements, ecosystem, and general capabilities for cloud computing and big data																																				
WP2/Q18	Functional architecture for cloud computing and big data																																				
WP2/Q19	End-to-end cloud computing management, cloud security and big data governance																																				
WP3/Q1	Innovative services scenarios, deployment models and migration issues based on Future Networks																																				
WP3/Q2	Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network virtualization (NFV)																																				
WP3/Q5	Applying networks of future and innovation in developing countries																																				
WP3/Q16	Knowledge-centric trustworthy networking and services																																				
JCA-IMT2020	Joint Coordination Activity on IMT-2020																																				
JCA-SDN	Joint Coordination Activity on Software-Defined Networking																																				
FG ML5G	ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G)																																				
FG NET2030	Focus Group on Technologies for Network 2030																																				
JRG-CCM	Joint Rapporteur Group on Cloud Computing management																																				
Webpage	https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx																																				

STANDARDIZATION WORK

Published standards	99	Projects	100
----------------------------	----	-----------------	-----

NATIONAL INVOLVEMENT

Luxembourg’s involvement	ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of ITU-T/SG 13.
---------------------------------	--

COMMENTS

SG 13 publishes the majority of its standards in the Q- and Y- series of ITU-T Recommendations. Its achievements include standards to enable interworking between two dominant technologies in next-generation networks, Ethernet and MPLS (multiprotocol label switching). The group has also undertaken much work in the field of virtual private networks (VPNs), in particular on standards that allow VPNs to work over all kinds of networks – optical, MPLS, IP, etc.

SG 13 has in addition specified functional requirements and architectures for networks supporting content delivery in IPTV, identity management, sensor networks/RFIDs, and open services and platforms for service integration and delivery. Continuing work focuses on cloud computing, ubiquitous networking, distributed service networking, ad-hoc networks, network virtualization, software-defined networking, the Internet of Things(IoT), and energy saving networks – all underscoring future networks, mobile and NGN.

SG 13's standardization work also covers network aspects of the Internet of Things (IoT), additionally ensuring support for IoT across future networks as well as evolving next-generation networks and mobile networks. Cloud computing in support of IoT is an integral part of this work.

The detail of Cloud Computing standards and projects developed by ITU-T/SG 13 can be found in the Appendix (Section 8.2).

4.3 Artificial Intelligence (AI) and Big Data

4.3.1 Artificial Intelligence

Introduced in 1956, the term Artificial Intelligence (AI) referred to a science and engineering of making intelligent machines, based on intelligent computer programs⁶⁸. While various conceptual ideas of AI have been proposed in the literature since then, a straightforward consensus definition of AI is not yet available.

One of the definitions suggested by ISO and IEC introduces AI as an “interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning”⁶⁹. Another definition was provided in 2020, in the first technical report on AI published by ISO/IEC, where AI corresponds to the “capability of an engineered system to acquire, process and apply knowledge and skills”⁷⁰.

AI could be understood as a set of techniques aimed at approximating some aspects of human or animal cognition using machines. It could also be considered as an intelligent agent perceiving the environment and taking actions that maximize its chance of successfully achieving its goals⁷¹. Finally, AI as a discipline is about creating systems that are capable of tackling complex problems in ways similar to human logic and reasoning.

Recently established subcommittee on Artificial Intelligence, ISO/IEC JTC 1/SC 42, aims at defining and providing good practices on the usage of various technologies that support the development of Artificial Intelligence, including Machine Learning, Cloud Computing, Big Data etc. Machine learning is defined by ISO/IEC⁷² as a “process by which a functional unit improves its performance by acquiring new knowledge or skills or by reorganizing existing knowledge or skills”. Currently, Machine Learning is the main technology used to build Artificial Intelligence systems.

Prior to the establishment of SC 42, there existed a working group ISO/IEC JTC 1/WG 9 on Big Data related standardization activities. With the establishment of the SC 42, the work on Big Data was transferred to this new technical subcommittee. Luxembourg was already involved in the work of WG 9 on Big Data and continue to actively participate in the standardization projects related to both Big Data and AI. The basic concepts and common characteristics of Big Data are summarized in Section 4.3.2.

Standards for Artificial Intelligence and Big Data are essential for improving Trust in these technologies, e.g. with respect to Cloud Computing, by enabling interoperability between the various applications and preventing vendor lock-in. Standards can also improve the quality of data analysis, e.g. by avoiding the interpretation of noise or randomness as a truth. Similarly, standards can help building trust in AI and Big Data by providing good practices of using various analytics techniques such as, for example, Machine Learning. Another potential benefit of standardization is the ability to support the integration of multiple data sources. Standards will also play an important role in data quality and data governance by addressing the veracity and value of data. Security and Privacy are of paramount importance for both data quality and protection. Indeed, some data come from social media and medical records and

⁶⁸ John McCarthy, father of AI, Dartmouth, 1956

⁶⁹ ISO/IEC 2382:2015, Information technology -- Vocabulary (def. 2123769) - <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en>

⁷⁰ ISO/IEC TR 24028:2020, Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence - <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24028:ed-1:v1:en:term:3.4>

⁷¹ Poole, David; Mackworth, Alan; Goebel, Randy (1998). Computational Intelligence: A Logical Approach. New York: Oxford University Press. ISBN 0-19-510270-3.

⁷² ISO/IEC TR 24028:2020, Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence - <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24028:ed-1:v1:en:term:3.23>

inherently contain private information. Analysis of such data, particularly in conjunction with its context, must not cause a privacy breach. AI and Big Data systems should be designed with security in mind. If there is no global perspective on security, then fragmented solutions to address security may offer a partial sense of safety rather than full security.

4.3.2 Big Data⁷³

The Big Data can be defined as “technologies and techniques that a company can employ to analyze large-scale, complex data for various applications intended to augment firm performance in various dimensions”⁷⁴.

The definition of Big Data by ISO/IEC⁷⁵ specifies it as follows:

“Extensive datasets - primarily in the data characteristics of volume, variety, velocity, and/or variability - that require a scalable technology for efficient storage, manipulation, management, and analysis.”

Big Data is a topic that has attracted a great deal of attention from industry, governments and academia in recent years. The term Big Data was coined in 1997 to refer to large volumes of scientific data for visualization⁷⁶. Big Data are characterized by a collection of huge data sets (Volume), generated very rapidly (Velocity) and with a great diversity of data types (Variety). Such data is difficult to process by traditional data processing platforms, such as relational databases, and almost impossible to analyze with traditional techniques.

The three Vs (Volume, Velocity and Variety) were introduced in 2001 by Doug Laney from Metagroup. In those days, Laney did not use the term “Big Data”, but he envisioned that accelerated generation of data with incompatible formats and structures as a result of e-commerce pushing traditional data management principles to their limits⁷⁶. IBM, has added a 4th V “Veracity” that relates to the data trustworthiness⁷⁷. Many others have proposed additional Vs, but most of these do not relate to the data itself but to the result of analytics such as expected value. The original 3 Vs, in combination with the 4th V “Veracity” will be used in this standards analysis to refer to the characteristics of Big Data, which are depicted and described in Table 6 and Figure 3 respectively.

Characteristic	Description
Volume	How much data: the amount of data that organizations try to harness to improve decision-making across the enterprise.
Velocity	How fast data is created: the speed of incoming data and how quickly it can be made available for analysis (e.g. payment data from credit cards and location data from mobile phones).

⁷³ Section based on ILNAS, “White Paper Big Data”, 2016 - <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/information-sensibilisation/white-paper-big-data-1-2/wp-bigdata-v1-2.pdf>

⁷⁴ O. Kwon, N. Lee, and B. Shin, “Data quality management, data usage experience and acquisition intention of big data analytics,” *Int. J. Inf. Manage.*, vol. 34, no. 3, pp. 387–394, 2014.

⁷⁵ ISO/IEC 20546:2019, Information technology -- Big data -- Overview and vocabulary - <https://www.iso.org/obp/ui/#iso:std:iso-iec:20546:ed-1:v1:en:term:3.1.2>

⁷⁶ D. Laney, “3D data management: Controlling data volume, velocity and variety,” *META Gr. Res. Note*, vol. 6, p. 70, 2001

⁷⁷ M. Schroeck, R. Shockley, J. Smart, D. Romero-Morales, and P. Tufano, “Analytics: The real-world use of big data: How innovative enterprises extract value from uncertain data,” *IBM Inst. Bus. Value*, 2012.

Characteristic	Description
Variety	The various types of data: the different types of structured and unstructured data that an organization can collect, such as transaction-level data, text and log files and audio or video.
Veracity	How accurate the data is: the trust in the data which might be impaired by the data being uncertain, imprecise or inherently unpredictable (e.g. trustworthiness, origin, and reputation of the data source).

Table 6: The four characteristics of Big Data

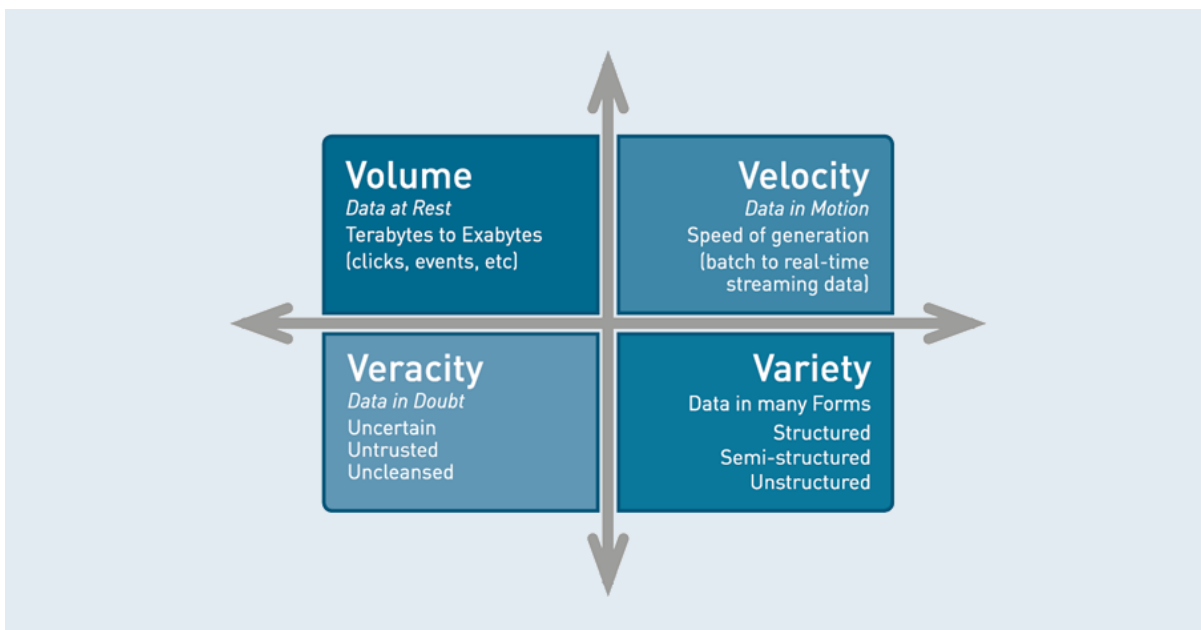


Figure 3: The four Vs of Big Data

Big Data incorporates all kinds of data and from a content perspective one can make the distinction between structured data, semi-structured data and unstructured data⁷⁸:

- **Structured data** – is part of a formal structure of data models associated with e.g. relational databases. It can be generated both by computer software or humans.
- **Semi-structured data** – not part of a formal structure of data models. It contains markers to separate semantic elements and enforce hierarchies of records and fields (example: XML).
- **Unstructured data** – does not belong to a pre-defined data model. Includes data from e-mails, video, social media websites, and text streams. Accounts for more than 80% of all data in organizations.

In practice mixed combinations of these three Big Data types occur which is referred to as **Poly-structured** data⁷⁹.


⁷⁸ CSA, "Defined Categories of Security as a Service - Continuous Monitoring as a Service, Security as a Service Working Group," Cloud Security Alliance, report, 2016.

⁷⁹ J. Girard, Strategic Data-Based Wisdom in the Big Data Era. IGI Global, 2015.

Big Data analytics, or in short Analytics, refers to techniques and technologies that are used to analyze the massive amount of data generated by both humans (e.g. in social media) and things (e.g. sensor networks), in order to acquire information from it. It is applicable to almost all areas of society, including administrative, commercial, and scientific fields, and affects individuals, business, governments, and their relationships. From the acquired information, one can provide new insights, such as “spot business trends, determine quality of research, prevent diseases, link legal citations, combat crime, and determine real-time roadway traffic conditions”.

4.3.3 Artificial Intelligence and Big Data Standardization Committees

This section provides an overview of the AI and Big Data related technical committees currently active in the recognized standardization organizations. In addition, standards and projects of these technical committees, in the AI/Big Data and Digital Trust areas, are listed in the Appendix (Section 8.3).

ISO/IEC JTC 1/SC 42 ARTIFICIAL INTELLIGENCE			
GENERAL INFORMATION			
Creation date	2017	Secretariat	ANSI (United States)
Chairperson	Mr. Wael William Diab	Committee Manager	Ms. Heather Benko
Scope	Standardization in the area of Artificial Intelligence <ul style="list-style-type: none"> - Serve as the focus and proponent for JTC 1's standardization program on Artificial Intelligence; - Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications. 		
Structure	AG 1 AI Management Systems Standard AG 2 AI Systems Engineering AHG 1 Dissemination and outreach AHG 2 Liaison with SC 38 AHG 3 Intelligent systems engineering JWG 1 Joint Working Group ISO/IEC JTC1/SC 42 - ISO/IEC JTC1/SC 40: Governance implications of AI WG 1 Foundational standards WG 2 Big Data WG 3 Trustworthiness WG 4 Use cases and applications WG 5 Computational approaches and computational characteristics of AI systems		
Webpage	https://www.iso.org/committee/6794475.html		
STANDARDIZATION WORK			
Published standards	6	Projects	21
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (31)	Australia, Austria, Belgium, Canada, China, The Democratic Republic of the Congo, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Republic of Korea, Luxembourg , Malta, Netherlands, Norway, Russian Federation, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Uganda, United Arab Emirates, United Kingdom, United States		
O-Members (16)	Argentina, Benin, Cyprus, Hong Kong, Hungary, Indonesia, Lithuania, Mexico, New Zealand, North Macedonia, Philippines, Poland, Portugal, Romania, South Africa, Ukraine		
Luxembourg's involvement (24)	<ul style="list-style-type: none"> - Mrs. Natalia Cassagnes (Chairwoman) - Mr. Johann Amsenga - Mr. Matthias Brust - Mr. Vincent Cady - Mrs. Anna Curridori - Mr. Christophe Delogne 	<ul style="list-style-type: none"> ANEC G.I.E. INCERT GIE University of Luxembourg Tarkett S.A. CSSF Everis Spain SLU 	

- Mrs. Saharnaz Dilmaghani	University of Luxembourg
- Mr. Redouane El Ajjouri	KPMG Luxembourg S.C.
- Mr. Laurent Fisch	Laurent Fisch Luxlegal S.à r.l.
- Mrs. Sylvie Forastier	Linklaters LLP
- Mr. Philippe Germain	PmG SD S.à.r.l.
- Mr. Christophe Keller	Husky S.à.r.l.
- Mrs. Kseniya Khovanova-Rubicondo	EvaLuX S.à.r.l.
- Mr. Andreas Kremer	ITTM
- Mr. Cédric Mauny	Telindus Luxembourg S.A.
- Mr. Benoit Poletti	INCERT GIE
- Mr. Cyrille Rousseau	CORAX IP S.à.r.l.
- Mr. Claude Schanet	ANSSI
- Mr. Mark Scheerlinck	MCS S.à.r.l.
- Mr. Laurent Sliepen	ANSSI
- Mr. Qiang Tang	LIST
- Mrs. Emilia Tantar	Black Swan LUX S.A.
- Mr. Shyam Wagle	ANEC G.I.E.
- Mr. Muhammad Wasim	University of Luxembourg

COMMENTS

ISO/IEC JTC 1/SC 42 “Artificial Intelligence” has been established based on the Resolution 12 of the 32nd Meeting of ISO/IEC JTC 1 in October 2017.

The detail of AI and Big Data standards and projects developed by ISO/IEC JTC 1/SC 42 can be found in the Appendix (Section 8.3).

ISO/IEC JTC 1/SC 32 DATA MANAGEMENT AND INTERCHANGE



GENERAL INFORMATION

Creation date	1997	Secretariat	ANSI (United States)
Chairperson	Mr. Jim Melton	Committee Manager	Mr. Bill Ash
Scope	Standards for data management within and among local and distributed information systems environments. SC32 provides enabling technologies to promote harmonization of data management facilities across sector-specific areas. Specifically, SC32 standards include: <ul style="list-style-type: none"> - Reference models and frameworks for the coordination of existing and emerging standards; - Definition of data domains, data types and data structures, and their associated semantics; - Languages, services and protocols for persistent storage, concurrent access, concurrent update and interchange of data; - Methods, languages, services, and protocols to structure, organize, and register metadata and other information resources associated with sharing and interoperability, including electronic commerce. 		
Structure	WG 1 eBusiness WG 2 MetaData WG 3 Database language WG 6 Data usage		
Webpage	https://www.iso.org/committee/45342.html		

STANDARDIZATION WORK

Published standards	93	Projects	42
----------------------------	----	-----------------	----

INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT

P-Members (19)	Australia, Brazil, Canada, China, Czech Republic, Denmark, Finland, Germany, India, Italy, Japan, Kazakhstan, Republic of Korea, Netherlands, Norway, Russian Federation, Sweden, United Kingdom, United States
-----------------------	---

O-Members (22)	Argentina, Belgium, Bosnia and Herzegovina, Côte d'Ivoire, Egypt, France, Ghana, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Luxembourg, Republic of Moldova, Poland, Portugal, Romania, Serbia, Spain, Switzerland, Turkey, Ukraine
Luxembourg's involvement (1)	- Mrs. Natalia Cassagnes ANEC G.I.E.

COMMENTS

ISO/IEC JTC 1/SC 32 is especially in charge of standardizing the SQL language and developing XML-related standards.

The topics of big data quality and next generation analytics appear frequently both in computing industry and more general news reports. SC 32 follows the development of standardization activities in these domains, namely through the liaison with SC 42. In its turn, the work of SC 32 on metadata for data quality and top-level ontologies is followed by SC 42 since it relates to various types of AI systems.

The detail of AI and Big Data standards and projects developed by ISO/IEC JTC 1/SC 32 can be found in the Appendix (Section 8.3).

ITU-T/SG 16 MULTIMEDIA CODING, SYSTEMS AND APPLICATIONS



GENERAL INFORMATION

Chairperson	Mr. Noah Luo																																				
Scope	<p>Study Group 16 is responsible for studies relating to ubiquitous multimedia applications, multimedia capabilities for services and applications for existing and future networks. This encompasses accessibility; multimedia architectures and applications; human interfaces and services; terminals; protocols; signal processing; media coding and systems (e.g. network signal processing equipment, multipoint conference units, gateways and gatekeepers). Lead Study Group Roles:</p> <ul style="list-style-type: none"> - Multimedia coding, systems and applications; - Ubiquitous multimedia applications; - Telecommunication/ICT accessibility for persons with disabilities; - Human factors; - Multimedia aspects of intelligent transport system (ITS) communications; - E-Health; - Internet Protocol television (IPTV) and digital signage; - Multimedia aspects of e-services. 																																				
Structure	<table border="0"> <tr><td>WP1/Q11</td><td>Multimedia systems, terminals, gateways and data conferencing</td></tr> <tr><td>WP1/Q12</td><td>Visual surveillance systems and services</td></tr> <tr><td>WP1/Q13</td><td>Multimedia application platforms and end systems for IPTV</td></tr> <tr><td>WP1/Q14</td><td>Digital signage systems and services</td></tr> <tr><td>WP1/Q21</td><td>Multimedia framework, applications and services</td></tr> <tr><td>WP2/Q22</td><td>Distributed ledger technologies and e-services</td></tr> <tr><td>WP2/Q23</td><td>Digital culture-related systems and services</td></tr> <tr><td>WP2/Q24</td><td>Human factors related issues for improvement of the quality of life through international telecommunications</td></tr> <tr><td>WP2/Q26</td><td>Accessibility to multimedia systems and services</td></tr> <tr><td>WP2/Q27</td><td>Vehicle gateway platform for telecommunication/ITS services and applications</td></tr> <tr><td>WP2/Q28</td><td>Multimedia framework for e-health applications</td></tr> <tr><td>WP3/Q5</td><td>Artificial intelligence-enabled multimedia applications</td></tr> <tr><td>WP3/Q6</td><td>Visual coding</td></tr> <tr><td>WP3/Q7</td><td>Speech/audio coding, voiceband modems, facsimile terminals and network-based signal processing</td></tr> <tr><td>WP3/Q8</td><td>Immersive live experience systems and services</td></tr> </table> <p>Other groups under SG16:</p> <table border="0"> <tr><td>JCA-MMeS</td><td>Joint Coordination Activity on Multimedia aspects of E-services</td></tr> <tr><td>FG AI4H</td><td>Focus Group on Artificial Intelligence for Health</td></tr> <tr><td>FG AI4AD</td><td>Focus Group on AI for autonomous and assisted driving</td></tr> </table>	WP1/Q11	Multimedia systems, terminals, gateways and data conferencing	WP1/Q12	Visual surveillance systems and services	WP1/Q13	Multimedia application platforms and end systems for IPTV	WP1/Q14	Digital signage systems and services	WP1/Q21	Multimedia framework, applications and services	WP2/Q22	Distributed ledger technologies and e-services	WP2/Q23	Digital culture-related systems and services	WP2/Q24	Human factors related issues for improvement of the quality of life through international telecommunications	WP2/Q26	Accessibility to multimedia systems and services	WP2/Q27	Vehicle gateway platform for telecommunication/ITS services and applications	WP2/Q28	Multimedia framework for e-health applications	WP3/Q5	Artificial intelligence-enabled multimedia applications	WP3/Q6	Visual coding	WP3/Q7	Speech/audio coding, voiceband modems, facsimile terminals and network-based signal processing	WP3/Q8	Immersive live experience systems and services	JCA-MMeS	Joint Coordination Activity on Multimedia aspects of E-services	FG AI4H	Focus Group on Artificial Intelligence for Health	FG AI4AD	Focus Group on AI for autonomous and assisted driving
WP1/Q11	Multimedia systems, terminals, gateways and data conferencing																																				
WP1/Q12	Visual surveillance systems and services																																				
WP1/Q13	Multimedia application platforms and end systems for IPTV																																				
WP1/Q14	Digital signage systems and services																																				
WP1/Q21	Multimedia framework, applications and services																																				
WP2/Q22	Distributed ledger technologies and e-services																																				
WP2/Q23	Digital culture-related systems and services																																				
WP2/Q24	Human factors related issues for improvement of the quality of life through international telecommunications																																				
WP2/Q26	Accessibility to multimedia systems and services																																				
WP2/Q27	Vehicle gateway platform for telecommunication/ITS services and applications																																				
WP2/Q28	Multimedia framework for e-health applications																																				
WP3/Q5	Artificial intelligence-enabled multimedia applications																																				
WP3/Q6	Visual coding																																				
WP3/Q7	Speech/audio coding, voiceband modems, facsimile terminals and network-based signal processing																																				
WP3/Q8	Immersive live experience systems and services																																				
JCA-MMeS	Joint Coordination Activity on Multimedia aspects of E-services																																				
FG AI4H	Focus Group on Artificial Intelligence for Health																																				
FG AI4AD	Focus Group on AI for autonomous and assisted driving																																				

	IRG-AVA IRG-IBB (IBB) JCT-VC JVDS JVET	Intersector Rapporteur Group on Audiovisual Media Accessibility Intersector Rapporteur Group on Integrated Broadcast-Broadband Joint Collaborative Team on Video Coding Joint project team for Vehicle Domain Service (JVDS) Joint Video Experts Team
Webpage	https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/default.aspx	
STANDARDIZATION WORK		
Published standards	222	Projects 180
NATIONAL INVOLVEMENT		
Luxembourg's involvement	Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ITU-T/SG 16.	
COMMENTS		
<p>The objective of this SG 16 is to work on multimedia coding, systems and applications. With big data and artificial intelligence playing more and more important role in the area of multimedia, some of the projects under SG 16 are exploiting the use of the technologies for the domain.</p> <p>On the other hand, analyzing multimedia data and providing valuable applications in different application domains is in scope of SG 16 through the WP3/Q5 "Artificial intelligence-enabled multimedia applications". In this context, the focus group FG AI4H⁸⁰, for health applications, was established under SG 16 in July 2018. The objective of the focus group is to establish a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.</p> <p>The detail of AI and Big Data standards and projects developed by ITU-T/SG 16 can be found in the Appendix (Section 8.3).</p>		

ETSI/ISG SAI SECURING ARTIFICIAL INTELLIGENCE



GENERAL INFORMATION		
Chairperson	Mr. Alex Leadbeater	
Creation date	2019	
Scope	Developing technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources.	
Structure	N/A	
Webpage	https://www.etsi.org/committee/sai	
STANDARDIZATION WORK		
Published standards	0	Projects 6
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT		
Members (44)	44 members organizations	
Luxembourg's involvement	Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ETSI/ISG SAI.	
COMMENTS		
<p>The group has a primary responsibility to develop technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. As a pre-standardization activity, the ISG SAI is intended to frame the security concerns arising from AI and to build the foundation of a longer-term response to the threats to AI in sponsoring the future development of normative technical specifications.</p> <p>In particular the group's work addresses three aspects of AI in the standards domain:</p> <ul style="list-style-type: none"> - Securing AI from attack, e.g. where AI is a component in the system that needs defending. 		

⁸⁰ <https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx>

- Mitigating against AI, e.g. where AI is the 'problem' (or used to improve and enhance other more conventional attack vectors).
- Using AI to enhance security measures against attack from other things, e.g. AI is part of the 'solution' (or used to improve and enhance more conventional countermeasures).

The detail of AI and Big Data standards and projects developed by ETSI/ISG SAI can be found in the Appendix (Section 8.3).

4.4 Blockchain and Distributed Ledger Technologies

A blockchain is a distributed and shared digital ledger that records all transactions that take place in a network. In this context, the ledger is decentralized in the sense that the blockchain database is replicated across many participants/nodes in the network, each of whom collaborate to create, evolve and to keep track of the records in the database. To ensure that ledger transactions are synchronized i.e., only validated transactions are written in the blockchain database and are written in the same order across all replicas, a blockchain system uses consensus mechanisms. The information in a blockchain is recorded as blocks where a new transaction/block is linked/chained to previous blocks in an append-only manner using cryptographic techniques, which ensure that a transaction cannot be modified (i.e., is immutable) once it has been written to the ledger. The chaining of transactions distinguishes blockchain from other distributed ledger technologies (DLT) while being consensus-oriented unites them. Blockchain and distributed ledger solutions are increasingly using smart contracts to support consistent update of information, to enable ledger functions (e.g., querying), and to automate aspects of transactions management (e.g., automatic calculation of account balance, controlling access to information).

ISO has recently defined the terms blockchain and distributed ledger in the first international standard on Blockchain and DLT⁸¹. A blockchain consists in a “distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links. Note: Blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records”, while a distributed ledger is defined as a “ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. Note: a distributed ledger is designed to be tamper resistant, append-only and immutable containing confirmed and validated transactions”.

Blockchain and Distributed Ledger Technologies (DLT)⁸² are foundational to various forms of commerce and their adoption is expected to reduce transaction costs, streamline operational processes and improve profit margins. This potential has resulted in an unparalleled attention from various sectors (e.g., supply chains, healthcare, banking, financial services, industry 4.0), with contributions from industries, academia, start-ups, administrations and standards developing organizations from across the globe.

4.4.1 Characteristics

Characteristic	Description
Public blockchain and private blockchain	<p>Based on the application scenario and parameters such as access control requirements and regulatory compliance goals, a blockchain/DLT system might consider being a:</p> <ul style="list-style-type: none"> - Public blockchain: A blockchain/DLT system in which there is no restriction on reading data and submitting transactions for inclusion into the blockchain. - Private blockchain: A blockchain/DLT system that allows direct access to data and transactions submission only to a predefined list of entities.

⁸¹ ISO 22739:2020, Blockchain and distributed ledger technologies -- Vocabulary - <https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en>

⁸² ILNAS White Paper “Blockchain and Distributed Ledgers” - <https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html>

Characteristic	Description
Permissionless blockchain and permissioned blockchain	<p>Similarly, another classification of blockchain/DLT systems comprises:</p> <ul style="list-style-type: none"> - Permissionless blockchain: A blockchain/DLT system in which there are no restrictions on identities of transaction processors. - Permissioned blockchain: A blockchain/DLT system that allows transaction processing only to a predefined list of subjects with known identities. <p>Typically, blockchain solutions are configured by combining the above two possibilities. For instance, many popular cryptocurrency blockchains are public and permissionless allowing any participant to join as a user and serve as a validating node but also for the data to be publicly transparent.</p>
Secure data registry	<p>When a node creates a new block, it includes in the header of this block a cryptographic reference to the previous block. Data is hence stored in the blockchain in a chronological order in an append-only manner, making the database structure tamper-resistant as well as immutable by design. Furthermore, it suffices that another node verifies the reference to implicitly verify the entire history of the blockchain. This implies that the asset referenced in a transaction is traceable through the blockchain up to the first block, simplifying the task of determining the provenance of information. This aspect of blockchain can be highly useful for industries (e.g., supply chains) in which transparency as well as auditability and traceability are desirable features.</p>
Consensus mechanisms and notion of trust	<p>To maintain the state of the blockchain, typically a consensus mechanism is used which guarantees integrity and consistency, and ensures a common, unambiguous ordering of transactions and blocks. In other words, consensus protocols maintain the sanctity of data recorded on the blockchain and provide the building blocks that allows a blockchain platform to function correctly in normal as well as adversarial conditions.</p> <p>For instance, Proof-of-Work (PoW) accomplishes several tasks:</p> <ul style="list-style-type: none"> - It allows anyone with a processing unit to participate in the process of creating new blocks. - It validates the legitimacy of a transaction. - It allows the network to reach consensus and in the process of doing so, avoids issues such as double spending and Sybil attacks. - It makes blocks tamper-resistant.

Table 7: Key features of Blockchain

4.4.2 Blockchain and Distributed Ledger Technologies Standardization Technical Committee

Considering the disruptive potential of Blockchain and Distributed Ledger Technologies, various standards development organizations have initiated projects in this domain. This section provides an overview of Blockchain and Distributed Ledger Technologies related technical committees currently active in the recognized standardization organizations, namely ISO/TC 307 and CEN/CLC/JTC 19. Moreover, standards for Blockchain and DLT as well as related Digital Trust standards are listed in the Appendix (Section 8.4).

In addition to these technical committees, it has to be noted that ITU-T formed a Focus Group on DLT which concluded its work in August 2019, with the publication of 3 Technical Specifications and 5

Technical Reports⁸³ covering various aspects of DLT (e.g.: terms and definitions, use cases, reference architecture, etc.).

CEN-CENELEC also established a focus group on Blockchain and DLT in 2017, with the aim to identify specific European needs with special attention given to interoperability challenges and to contribute directly to the International technical standardization through ISO/TC 307. The Focus Group notably published a White Paper in 2018, formalizing these specific requirements for the implementation of blockchain and DLT in Europe⁸⁴. This publication was at the origin of the creation of the CEN/CLC/JTC 19 in 2019.

ISO/TC 307 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES			
GENERAL INFORMATION			
Creation date	2016	Secretariat	SA (Australia)
Chairperson	Mr. Craig Dunn	Committee Manager	Ms. Emily Dawson
Scope	Standardization of blockchain technologies and distributed ledger technologies.		
Structure	AG 1 SBP Review Advisory Group AG 2 Liaison Advisory Group AHG 2 Guidance for Auditing DLT Systems CAG 1 Convenors coordination group JWG 4 Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques SG 7 Interoperability of blockchain and distributed ledger technology systems WG 1 Foundations WG 2 Security, privacy and identity WG 3 Smart contracts and their application WG 5 Governance WG 6 Use cases Joint working groups under the responsibility of another committee: ISO/TC 46/SC 11/JWG 1 Joint ISO/TC 46/SC 11 - ISO/TC 307 WG: Blockchain		
Webpage	https://www.iso.org/committee/6266604.html		
STANDARDIZATION WORK			
Published standards	3	Projects	8
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (44)	Australia, Austria, Belgium, Brazil, Cambodia, Canada, China, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Kazakhstan, Republic of Korea, Luxembourg , Malaysia, Malta, Mexico, Netherlands, New Zealand, Nigeria, Norway, Poland, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States		
O-Members (13)	Argentina, Belarus, Colombia, Estonia, Hong Kong, Indonesia, Islamic Republic of Iran, Kenya, Morocco, Philippines, Romania, Slovakia, Uruguay		
Luxembourg's involvement (17)	- Mr. Jean Lancrenon (Chairman) ANEC G.I.E - Mr. Johann Amsenga INCERT GIE - Mr. Jean-Richard Audin Initio Luxembourg S.A.		

⁸³ These reports are available on <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>

⁸⁴ The White Paper "Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies" is available on <ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf>

	- Mr. Monique Bachner	LëtzBlock A.s.b.l.
	- Mr. Benoit Bertholon	COINPLUS S.A.
	- Mr. Guillaume De Vergnies	STAMPIFY S.à.r.l.
	- Mr. Christophe Delogne	Everis Spain SLU
	- Mrs. Caline Djiowa	KPMG Luxembourg S.C.
	- Mr. Sami El Bouamri	Initio Luxembourg S.A.
	- Mrs. Michèle Feltz	ILNAS
	- Mr. Philippe Germain	PmG SD S.à r.l.
	- Mr. Carlo Harpes	itrust consulting S.à.r.l.
	- Mrs. Biba Homsy	LëtzBlock A.s.b.l.
	- Mr. Bernard Legros	ARHS Developments S.A.
	- Mr. Cyrille Rousseau	CORAX IP S.à.r.l.
	- Mr. Laurent Sliepen	ANSSI
	- Mr. Qiang Tang	LIST

COMMENTS

ISO/TC 307 has been set up to meet the growing need for standardization in the area of Blockchain and Distributed Ledger Technologies (DLT) by providing internationally agreed ways of working with it to improve security and privacy and facilitate worldwide use of the technology through better interoperability.

This technical committee is responsible for standardization relating Blockchain and DLT. This includes standards in relation to terminology, reference architecture, security, privacy, identity, smart contracts, governance and interoperability. Recently, a new ad hoc group on auditing Blockchain and DLT systems has also been created.

The detail of Blockchain and DLT standards and projects developed by ISO/TC 307 can be found in the Appendix (Section 8.4).

CEN/CLC/JTC 19 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES



GENERAL INFORMATION			
Creation date	2019	Secretariat	UNI (Italy)
Chairperson	Mr. Andrea Caccia	Secretary	Mrs. Carla Sirocchi
Scope ⁸⁵	<p>To prepare, develop and/or adopt standards for Blockchain and Distributed Ledger technologies covering the following aspects:</p> <ul style="list-style-type: none"> - Organizational frameworks and methodologies, including IT management systems; - Processes and products evaluation schemes; - Blockchain and distributed ledger guidelines; - Smart technology, objects, distributed computing devices, data services. <p>The JTC will focus on European requirements, especially in the legislative and policy context, and will proceed with the identification and possible adoption of standards already available or under development in other SDOs, which could support the EU Digital Single Market and/or EC Directives/Regulations. Special attention will be paid to ISO/TC 307 standards. If required these standards will be augmented by TRs and TSs.</p>		
Structure	N/A		
Webpage	https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2702172&cs=1465AF26367A9ECE85D149F31EF39162E		
STANDARDIZATION WORK			
Published standards	0	Projects	0
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
Members (34)	34 members of CEN/CENELEC		

⁸⁵ The scope of CEN/CLC/JTC 19 is preliminary at the time of writing of this report.

Luxembourg's
involvement
(2)

- Mrs. Michèle Feltz
- Mr. Jean Lancrenon

ILNAS
ANEC G.I.E.

COMMENTS

In order to contribute to ensuring a smooth and safe adoption of new technologies in Europe, CEN and CENELEC established JTC 19 based on the recommendations presented in the CEN-CENELEC White Paper on 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies'⁸⁶. The JTC is responsible for the development and adoption of standards for Blockchain and Distributed Ledger Technologies, covering the following aspects: organizational frameworks and methodologies, processes and products evaluation schemes, distributed ledger guidelines, smart technologies, objects, distributed computing devices and data services.

In particular, CEN/CLC/JTC 19 will proceed with the identification and adoption of international standards already available or under development. The JTC will work in close contact with ISO/TC 307 'Blockchain and distributed ledger technologies'. Furthermore, CEN/CLC/JTC 19 will focus on specific European legislative and policy requirements, in support of the development of the EU Digital Single Market.

The detail of Blockchain and DLT standards and projects developed by CEN/CLC/JTC 19 can be found in the Appendix (Section 8.4).

⁸⁶ <ftp://ftp.cenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf>

4.5 Digital Trust in Smart ICT

Trust in Information and Communication Technology (ICT) systems can be explained, as a computational construct whose value depends on the context and is likely to change over time⁸⁷ whereas trust itself is fragile, distrust is robust. In other words, trust can be lost very quickly by users, in particular, through extensive media coverage of incidents and once the transition point to massive distrust is attained, it is very difficult to restore to the initial state. Thus, building and maintaining trust is essential and requires a constant effort for the ICT service providers.

Apart from the general technical challenges of developing interconnected Smart technologies, such as related to Internet of Things, Cloud Computing and Artificial Intelligence, Digital Trust is steadily becoming an increasingly significant challenge that must be addressed⁸⁸. Trust is essential in ICT and is no longer merely a matter of security alone but is transversal to ICT in almost any aspect of hardware and software ranging from consumer devices and equipment to service providers and data centers. Digital Trust in ICT has to deal not only with purely technical problems, but also with social aspects and constraints that have to be addressed in a technical manner. Beside this, as highlighted in Section 4.4, Blockchain and Distributed Ledger Technologies are expected to support in maintaining Digital Trust between parties keeping transparency in all transactions or interactions, without the need of intermediaries.

As mentioned, Digital Trust is necessary to the broad adoption of any new technology. However, owing to the actual complexity and connectivity of current systems and the data volume involved, this leads to greater vulnerability⁸⁹. This section presents basic components of Digital Trust requirements that are vital for any ICT system, such as privacy, data and information security and interoperability.

4.5.1 Basic Components of Digital Trust

Privacy

With the technological development and advent of the ICT era entailing massive and almost invisible sharing and collection of data, privacy is more than ever a central issue. Although privacy norms greatly differ across cultures, the objective of privacy is a universal and fundamental social requirement⁹⁰. In a study about privacy behaviors regarding information technology, Acquisti *et al.*⁹¹ have characterized privacy based on three key concepts. Privacy is uncertain, meaning that individuals rarely have clear knowledge of what information about them is available to others and how this information can be used and with what consequences. Thus, decision-making on what information to share is often the result of a cost-benefit calculation, which is not always made taking all factors into account. Privacy is context-dependent, meaning that individuals' consent to disclose Personally Identifiable Information is dependent on where (e.g. which platform) they share the information⁹² and if other individuals have already agreed to share the information⁹³. Privacy is malleable, meaning that the acceptable level of

⁸⁷ K. J. Hole, *Anti-fragile ICT Systems*, Simula Spr. Cham: Springer International Publishing, 2016.

⁸⁸ ILNAS "White paper Digital Trust for Smart ICT" - <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/confiance-numerique/etudes-nationales/white-paper-digital-trust-october-2016/white-paper-digital-trust-october-2016.pdf> and ETSI TR 103 306 V1.4.1 (2020-03): "CYBER; Global Cyber Security Ecosystem" - https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.04.01_60/tr_103306v010401p.pdf

⁸⁹ Vulnerability of hyper-connected and complex systems as viewed by the ITU-T Focus Group on Smart Sustainable Cities – Cybersecurity, data protection and cyber resilience in smart sustainable cities.

⁹⁰ D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 Int. Conf. Comput. Sci. Electron. Eng., vol. 1, no. 973, pp. 647–651, 2012.

⁹¹ A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science* (80-.), vol. 347, no. 6221, pp. 509–514, 2015.

⁹² Surprisingly it was found that the more casual the information collecting source was, the more individuals agreed to share secrets, although all collecting sources had the same privacy level.

⁹³ It was also found that individuals trust the collecting source more if it is already well-known.

privacy is often determined by a *construction* instead of a *reflection*. Acquisti *et al.* also showed the influence of default settings in the acceptance of privacy policies in ICT and highlight that the confusion induced by these policies is often deliberate. They state that, if U.S. consumers actually read the privacy policies of the website they visit, the aggregate opportunity cost would be \$781 billion per year.

Data and Information Security

When it comes to Data and Information Systems, security is an abyssal topic and it is out of scope of this standards analysis to deal with the whole stack of existing security systems and techniques. Thus, this section aims at providing a set of the most important aspects in data and information security along with some best practice.

The original triad of Confidentiality, Integrity, and Availability (CIA) in Information Security has long been the basis of numerous studies in ICT. However, the evolution of Information Systems and the complexity of their interrelationships with regard to data might suggest that the CIA model has become outdated. Following this definition in 2002, the OECD's Guidelines for the Security of Information Systems and Networks⁹⁴ proposed nine components of security: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. In 2004, NIST proposed more than 30 principles and best practices for securing Information Systems⁹⁵. Among the many principles proposed, the following should be noted:

- Security Foundation: Treat security as an integral part of overall system design;
- Risk-Based: Protect information while being processed, in transit, and in storage;
- Ease of Use: Base security on open standards for portability and interoperability;
- Increase Resilience: Isolate public access systems from mission critical resources;
- Reduce Vulnerabilities: Do not implement unnecessary security mechanisms;
- Design with Network in Mind: Use unique identities to ensure accountability.

Interoperability

Interoperability between systems is also an important aspect of Digital Trust. Although there are no studies that globally address the interoperability of every Smart technology, several research projects and standards exist for a particular technology and provide different definitions of interoperability⁹⁶. However, in its various definitions, system interoperability is mainly composed of two criteria:

- Compatibility: a system is compatible with other systems if they can communicate and work together to serve a common purpose.
- Interchangeability: a system is interchangeable with other systems if their purpose, functionalities and offered services are the same. Moreover, interchangeability adds the constraint that the system must also allow this transition from one to another. E.g. a Cloud storage provider that prevents (or makes it difficult) to migrate stored data from its Cloud to a competitor cannot claim to be interchangeable and thus is not considered as interoperable.

The rest of the section provides the overview of Digital Trust related standardization activities of various Smart ICT technologies described in Section 4.1 to Section 4.3.

4.5.2 Digital Trust Standardization Related Technical Committees


This section provides an overview of the Digital Trust related technical committees and standards, from the perspective of various components of Smart ICT technologies included in this Standards Analysis,


⁹⁴ OECD, "OECD Guidelines for the Security of Information Systems and Networks," Organ. Econ. Co-operation Dev., 2002

⁹⁵ G. Stoneburner, C. Hayden, and A. Feringa, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A," NIST Spec. Publ. 800-27 Rev A, p. 35, 2004.

⁹⁶ K. Kosanke, "ISO Standards for Interoperability: a Comparison," in Interoperability of Enterprise Software and Applications, D. Konstantas, J.-P. Bourrières, M. Léonard, and N. Boudjlida, Eds. London: Springer London, 2006, pp. 55–64

particularly Internet of Things, Cloud Computing, as well as Artificial Intelligence and Big Data, which are currently active in the recognized standardization organizations. Digital Trust standards related to these Smart ICT technologies are listed in the Appendix (Section 8).

ISO/IEC JTC 1/SC 17 CARDS AND SECURITY DEVICES FOR PERSONAL IDENTIFICATION			
GENERAL INFORMATION			
Creation date	1987	Secretariat	BSI (United Kingdom)
Chairperson	Mr. Peter Waggett	Committee Manager	Ms. Jean Stride
Scope	The current area of work for JTC 1/SC 17 consists of: <ul style="list-style-type: none"> - Identification and related documents; - Cards; - Security devices and tokens; - Interface associated with their use in inter-industry applications and international interchange. 		
Structure	AG 1 Registration Management Group (RMG) AG 2 Virtual ID and related technologies CAG 1 Chairman advisory group WG 1 Physical characteristics and test methods for ID-cards WG 3 Identification cards - Machine readable travel documents WG 4 Generic interfaces and protocols for security devices WG 5 Identification cards - Identification of issuers WG 8 Integrated circuit cards without contacts WG 10 Motor vehicle driver license and related documents WG 11 Application of biometrics to cards and personal identification WG 12 Drone license and drone identity module		
Webpage	https://www.iso.org/committee/45144.html		
STANDARDIZATION WORK			
Published standards	102	Projects	36
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (33)	Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Israel, Italy, Japan, Kazakhstan, Kenya, Republic of Korea, Luxembourg , Malaysia, Netherlands, Norway, Poland, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, United Kingdom, United States		
O-Members (22)	Argentina, Armenia, Belarus, Bosnia and Herzegovina, Croatia, Ghana, Hong Kong, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Lithuania, Republic of Moldova, New Zealand, North Macedonia, Portugal, Serbia, Thailand, Turkey, Ukraine, Viet Nam		
Luxembourg's involvement (2)	- Mr. Benoit Poletti (Chairman)	INCERT GIE	
	- Mr. Abdelkrim Nehari	INCERT GIE	
COMMENTS			
ISO/IEC JTC 1/SC 17 is responsible for the development of standards that are ubiquitous in their use by the sectors that require identification worldwide.			
The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ISO/IEC JTC 1/SC 17 can be found in the Appendix (Section 8).			

ISO/IEC JTC 1/SC 27 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION			
GENERAL INFORMATION			
Creation date	1989	Secretariat	DIN (Germany)
Chairperson	Mr. Andreas Wolf	Committee Manager	Mrs. Krystyna Passia
Scope	<p>The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:</p> <ul style="list-style-type: none"> - Security requirements capture methodology; - Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls and services; - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; - Security aspects of identity management, biometrics and privacy; - Conformance assessment, accreditation and auditing requirements in the area of information security management systems; - Security evaluation criteria and methodology. <p>SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.</p>		
Structure	<p>AG 1 Management Advisory Group AG 2 Trustworthiness AG 3 Concepts and Terminology AG 4 Data security AG 5 Strategy AG 6 Operations CAG Chair's Advisory Group WG 1 Information security management systems WG 2 Cryptography and security mechanisms WG 3 Security evaluation testing and specification WG 4 Security controls and services WG 5 Identity management and privacy technologies</p> <p>Joint working groups under the responsibility of another committee: ISO/TC 307/JWG 4 Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques</p>		
Webpage	https://www.iso.org/committee/45306.html		
STANDARDIZATION WORK			
Published standards	192	Projects	87
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (47)	Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Cyprus, Denmark, Finland, France, Germany, India, Indonesia, Islamic Republic of Iran, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Luxembourg , Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Philippines, Poland, Russian Federation, Rwanda, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay		
O-Members (33)	Algeria, Belarus, Plurinational State of Bolivia, Bosnia and Herzegovina, Bulgaria, Chile, Côte d'Ivoire, Croatia, Czech Republic, El Salvador, Estonia, Eswatini, Ghana, Hong Kong, Hungary, Iceland, Kenya, Lebanon, Lithuania, Morocco, North Macedonia, Pakistan, State of Palestine, Portugal, Romania, Saint Kitts and Nevis, Saudi Arabia, Senegal, Serbia, Sri Lanka, Thailand, Trinidad and Tobago, Turkey		

Luxembourg's involvement (30)	- Mr. Benoit Poletti (Chairman)	INCERT GIE
	- Mr. Carlo Harpes (Vice-Chairman)	itrust consulting S.à r.l.
	- Mr. Johann Amsenga (Convenor WG 4)	INCERT GIE
	- Mr. Olivier Antoine	POST Luxembourg
	- Mr. Matthieu Aubigny	itrust consulting S.à r.l.
	- Mr. Benoit Bertholon	COINPLUS S.A.
	- Mr. Stéphane Cortina	LIST
	- Mrs. Saharnaz Dilmaghani	University of Luxembourg
	- Mrs. Myriam Djerouni	LUXITH G.I.E.
	- Mr. Nicolas Domenjoud	ILNAS
	- Mrs. Michèle Feltz	ILNAS
	- Mr. Ben Fetler	Ministère des Affaires étrangères et européennes
	- Mr. Philippe Germain	PmG SD S.à r.l.
	- Mr. Clement Gort	INCERT GIE
	- Mrs. Carine Grenouillet	INCERT GIE
	- Mrs. Shenglan Hu	POST Telecom PSF S.A.
	- Mr. Jean Lancrenon	ANEC G.I.E.
	- Mr. Chao Liu	University of Luxembourg
	- Mr. Michel Ludwig	ILNAS
	- Mr. Cédric Mauny	Telindus Luxembourg S.A.
	- Mr. Alex Mckinnon	SES S.A.
	- Mr. Abdelkrim Nehari	INCERT GIE
	- Mr. Nicolas Niels	Escent S.A.
	- Mr. Gaëtan Pradel	INCERT GIE
	- Mr. René Saint-Germain	Certi-Trust S.à r.l.
	- Mr. Nader Samir Labib	University of Luxembourg
	- Mr. Claude Schanet	ANSSI
	- Mr. Raphaël Taban	CTIE
- Mr. Qiang Tang	University of Luxembourg	
- Mr. Muhammad Wasim	University of Luxembourg	

COMMENTS

SC 27 is an internationally recognized center of information and IT security standards expertise serving the needs of business sectors as well as governments. Its work covers the development of standards for the protection of information and ICT.

Working Groups

- **WG 1:** the scope of the WG 1 covers all aspects of standardization related to information security management systems: requirements, methods and processes, security controls, sector and application specific use of ISMS, governance, information security economics and accreditation, certification and auditing of ISMS.
- **WG 2:** the scope of the WG 2 covers both cryptographic and non-cryptographic techniques and mechanisms including confidentiality, entity authentication, non-repudiation, key management and data integrity (e.g.: message authentication, hash-functions, digital signatures, etc.).
- **WG 3:** the scope of the WG 3 covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished: security evaluation criteria, methodology for application of the criteria, security functional and assurance specification of IT systems, components and products, testing methodology for determination of security functional and assurance conformance, accreditation schemes, administrative procedures for testing, evaluation and certification.
- **WG 4:** it is developing and maintaining International Standards, Technical Specifications and Technical Reports for information security in the area of Security Controls and Services, to assist organizations in the implementation of the ISO/IEC 27000-series of ISMS International Standards and Technical Reports. Also the Scope of WG 4 includes evaluating and developing International Standards for addressing existing and emerging information security issues and needs and other security aspects that resulted from the proliferation and use of ICT and Internet related technology in organizations (such as multinationals corporations, SMEs, government departments, and non-profit organizations). Since 2018, Luxembourg is managing this WG, Mr. Johann Amsenga being its convenor.

- **WG 5:** it is responsible of the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and privacy.

Standards

The best-known standard developed by SC 27 are ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements and ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls.

It is important to note that the committee works in liaison with many other JTC 1/SCs on the development of standards related to security for specific subsectors. For example, standards concerning the security techniques for IoT and Smart Cities are currently under development under SC 27 in close collaboration with ISO/IEC JTC 1/SC 41:

- ISO/IEC CD 27400, Cybersecurity -- IoT security and privacy -- Guidelines;
- ISO/IEC WD 27402, Cybersecurity -- IoT security and privacy -- Device baseline requirements;
- ISO/IEC WD 27403, Cybersecurity -- IoT security and privacy -- Guidelines for IoT-domotics.

Similarly, SC 27 has published International Standard related to the security for Cloud Computing and regarding security and privacy aspects in cloud SLAs (in liaison with ISO/IEC JTC 1/SC 38):

- ISO/IEC 19086-4:2019, Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Components of security and of protection of PII;
- ISO/IEC 27017:2015, Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018:2019, Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 27036-4:2016, Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services.

On the other hand, standards concerning Big Data security and privacy are currently under development in JTC 1/SC 27, in close collaboration with ISO/IEC JTC 1/SC 42 on Artificial Intelligence:

- ISO/IEC 20547-4, Information technology -- Big data reference architecture -- Part 4: Security and privacy;
- ISO/IEC WD 27045, Information technology -- Big data security and privacy -- Processes;
- ISO/IEC WD 27046, Information technology -- Big data security and privacy -- Implementation guidelines.

The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ISO/IEC JTC 1/SC 27 can be found in the Appendix (Section 8).


ISO/IEC JTC 1/WG 13 TRUSTWORTHINESS



GENERAL INFORMATION

Creation date	2019	Secretariat	DIN (Germany)
Convenor	Mr. Walter Fumy	Secretary	Mr. Andreas Lamm
Scope	<p>Terms of reference:</p> <ul style="list-style-type: none"> - Complete, improve and maintain the inventory including the heat map as a JTC 1 standing document reflecting the landscape of trustworthiness in JTC 1, other ISO and IEC Committees, and other SDOs. - Complete terminology and description of characteristics and determine what type of document should be created. - Develop horizontal deliverables such as frameworks, taxonomy and ontology for ICT trustworthiness for guiding trustworthiness efforts throughout JTC 1 and upon which other deliverables can be developed (beginning with ISO/IEC TS 24462, Ontology for ICT Trustworthiness Assessment). <p>Excluded are domain specific trustworthiness deliverables, such as those within the scope of JTC 1 SCs</p>		

STANDARDIZATION WORK			
Published standards	0	Projects	2
NATIONAL INVOLVEMENT			
Luxembourg's involvement (5)	- Mr. Jean-Philippe Humbert - Mr. Johann Amsenga - Mrs. Natalia Cassagnes - Mr. Nicolas Domenjoud - Mr. Jean Lancrenon	ILNAS INCERT GIE ANEC G.I.E. ILNAS ANEC G.I.E.	
COMMENTS			
<p>ISO/IEC JTC 1/WG 13 is a Working Group under the direct responsibility of ISO/IEC JTC 1. It is responsible for the development of horizontal deliverables for ICT trustworthiness. It notably includes the development and maintenance of an inventory of deliverables related to ICT trustworthiness and of a heat map illustrating the interest of JTC 1 subcommittees in different ICT trustworthiness characteristics. JTC 1/WG 13 is also responsible for the development of standardization deliverables, starting with a Technical Specification providing an ontology for ICT trustworthiness assessment.</p> <p>The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ISO/IEC JTC 1/WG 13 can be found in the Appendix (Section 8).</p>			

ISO/TC 46/SC 11 ARCHIVES/RECORDS MANAGEMENT			
GENERAL INFORMATION			
Creation date	1998	Secretariat	SA (Australia)
Chairperson	Ms. Judith Ellis	Committee Manager	Mr. Saim Riaz
Scope	Standardization of principles for the creation and management of documents, records and archives as evidence of transactions and covering all media including digital multimedia and paper.		
Structure	<p>AG 1 Strategic directions AHG 2 Disposition AHG 3 Structured data environments AHG 4 Records capability maturity JWG 1 Joint ISO/TC 46/SC 11 - ISO/TC 307 WG: Blockchain WG 1 Metadata WG 8 Management systems for records WG 16 Systems design for records WG 17 Records in the cloud WG 18 ISO 13008:2012 Revision WG 19 Risk assessment for records processes and systems</p> <p>Joint working groups under the responsibility of another committee: ISO/TC 42/JWG 26 Joint ISO/TC 42-TC 46/SC 11-TC 171 WG: Imaging system capability qualification for archival recording and approval ISO/TC 171/SC 2/WG 5 Joint TC 171/SC 2 - TC 42 - TC 46/SC 11 - TC 130 WG: Document management applications - Application issues - PDF/A ISO/TC 307/JWG 5 Joint ISO/TC 307 - ISO/TC 46/SC 11 WG: Blockchain</p>		
Webpage	https://www.iso.org/committee/48856.html		
STANDARDIZATION WORK			
Published standards	19	Projects	5
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members (35)	Australia, Belgium, Bulgaria, Canada, China, Colombia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Japan, Kenya, Republic of Korea, Lithuania, Luxembourg , Malaysia, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Serbia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Kingdom, United States		

O-Members (13)	Argentina, Austria, Brazil, Chile, Croatia, Iceland, Islamic Republic of Iran, Poland, Romania, Singapore, Slovakia, Slovenia, Thailand	
Luxembourg's involvement (9)	- Mr. Lucas Colet (Chairman) - Mrs. Sylvie Dessolin - Mrs. Sylvie Forastier - Mr. Jean Lancrenon - Mr. Michel Ludwig - Mr. Henri Montin - Mr. Michel Picard - Mr. Serge Raucq - Mrs. Magalie Soler - Mr. Alain Wahl	SOPRA STERIA PSF Luxembourg S.A. SOPRA STERIA PSF Luxembourg S.A. Linklaters LLP ANEC G.I.E. ILNAS CTIE LIST CTIE <i>Archives nationales de Luxembourg</i> ILNAS

COMMENTS

ISO/TC 46/SC 11 is responsible for the standardization of the best practices in managing archives and records by providing a managerial framework, as well as standards and guidance for the design and application of records practices and processes to ensure authoritative and reliable information and evidence of business activity in organizations.

The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ISO/IEC TC 46/SC 11 can be found in the Appendix (Section 8).

**CEN/CLC/JTC 13
CYBERSECURITY AND DATA PROTECTION**
**GENERAL INFORMATION**

Creation date	2017	Secretariat	DIN (Germany)
Chairperson	Mr. Walter Fumy	Secretary	Mr. Martin Uhlherr
Scope	<p>Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to:</p> <ul style="list-style-type: none"> - Management systems, frameworks, methodologies - Data protection and privacy - Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs) - Competence requirements for cybersecurity and data protection - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices <p>Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1 and other SDOs and international bodies such as ISO, IEC, ITU-T, and industrial fora. Where not being developed by other SDO's, the development of cybersecurity and data protection CEN/CENELEC publications for safeguarding information such as organizational frameworks, management systems, techniques, guidelines, and products and services, including those in support of the EU Digital Single Market.</p>		
Structure	<p>WG 1 Chairman advisory group WG 2 Management systems and controls sets WG 3 Security evaluation and assessment WG 4 Cybersecurity services WG 5 Data Protection, Privacy and Identity Management WG 6 Product security</p>		
Webpage	https://standards.cen.eu/dyn/www/f?p=204:7:0:::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B		

STANDARDIZATION WORK

Published standards	20	Projects	10
----------------------------	----	-----------------	----

INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT

Members (34)	34 members of CEN/CENELEC
-------------------------	---------------------------


Luxembourg's involvement (4)	<ul style="list-style-type: none"> - Mr. Johann Amsenga - Mr. Abdessamad Kahir - Mr. Jean Lancrenon - Mr. René Saint-Germain 	<ul style="list-style-type: none"> INCERT GIE Certi-Trust S.à r.l. ANEC G.I.E. Certi-Trust S.à r.l.
COMMENTS		
<p>The CEN/CLC/JTC 13 was created in 2017 based on the recommendation of the CEN/CLC Cyber Security Focus Group (CSCG), which identified cybersecurity, including data protection and privacy, as an essential need to achieve a Digital Single Market.</p> <p>The aim of the CSCG not being to develop standards, it proposed the creation of this new JTC, with the objective to identify and adopt relevant international standards (particularly from ISO/IEC JTC 1), as well as to develop European Standards where the identical adoption of international standards is not sufficient (e.g.: General Data Protection Regulation).</p> <p>JTC 13 already published height standards directly transposing, at the European level, some international standards developed by ISO/IEC JTC 1/SC 27, such as ISO/IEC 27001.</p> <p>The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by CEN/CLC/JTC 13 can be found in the Appendix (Section 8).</p>		


CEN/TC 224 PERSONAL IDENTIFICATION AND RELATED PERSONAL DEVICES WITH SECURE ELEMENT, SYSTEMS, OPERATIONS AND PRIVACY IN A MULTI SECTORIAL ENVIRONMENT



GENERAL INFORMATION			
Creation date	1989	Secretariat	AFNOR (France)
Chairperson	Mr. Olivier Senot	Secretary	Mrs. Fanny Lannoy
Scope	<p>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. It covers:</p> <ul style="list-style-type: none"> - Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control; - Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces; - Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data; - System components such as accepting devices, servers, cryptographic modules; - CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers. 		
Structure	WG 6 User Interface WG 11 Transport applications WG 17 Protection Profiles in the context of SSCD WG 18 Biometrics WG 19 Breeder Documents		
Webpage	http://standards.cen.eu/dyn/www/f?p=204:7:0:::FSP_LANG_ID,FSP_ORG_ID:25,620&cs=1A98C573151AB3D7A22712120D94364C1#1		
STANDARDIZATION WORK			
Published standards	61	Projects	8

INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT	
Members (34)	34 members of CEN/CENELEC
Luxembourg's involvement (2)	- Mr. Benoit Poletti (Chairman) INCERT GIE - Mrs. Shenglan Hu POST Telecom PSF
COMMENTS	
<p>As a matter of principle, CEN/TC 224 does not duplicate the work of ISO/IEC JTC 1/SC 17 but either transposes some of the related International Standards or uses them as the basis for specific European works. In a number of cases, the ultimate objective of the work of CEN/TC 224 is to contribute to international standardization. CEN/TC 224 is particularly involved in the development of standards under the standardization mandate M/460 concerning Electronic Signatures. In this context, it has published standards on protection profiles for signature creation and verification application (EN 419111 series), application interface for secure elements for electronic identification, authentication and Trusted Services (EN 419212 series) or standards on trustworthy systems supporting server signing (EN 419241 series).</p> <p>The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by CEN/TC 224 can be found in the Appendix (Section 8).</p>	

ETSI/TC CYBER CYBER SECURITY			
GENERAL INFORMATION			
Creation date	2014		
Chairperson	Mr. Alex Leadbeater		
Scope	<p>The activities of ETSI TC CYBER include the following broad areas:</p> <ul style="list-style-type: none"> - Cyber Security - Security of infrastructures, devices, services and protocols - Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators - Security tools and techniques - Provision of security mechanisms to protect privacy - Creation of security specifications and alignment with work done in other TCs. 		
Structure	WG QSC Quantum-Safe Cryptography		
Webpage	https://portal.etsi.org/cyber		
STANDARDIZATION WORK			
Published standards	46	Projects	23
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
Members (170)	170 members organizations		
Luxembourg's involvement (2)	- ILNAS - Luxtrust		
COMMENTS			
<p>ETSI/TC CYBER is responsible for the standardization of cyber security and for providing a center of relevant security expertise. Its WG on quantum safe cryptography is responsible to make assessments and recommendations on the various proposals from industry and academia regarding real-world deployments of quantum-safe cryptography, including practical properties, (such as efficiency, functionality, agility, etc.), security properties, appropriateness of certain quantum-safe cryptographic primitives to various application domains (Internet protocols, wireless systems, resource constrained environments, cloud deployments, big data, etc.).</p> <p>The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ETSI/TC CYBER can be found in the Appendix (Section 8).</p>			

ETSI/TC ESI ELECTRONIC SIGNATURES AND INFRASTRUCTURES			
GENERAL INFORMATION			
Creation date	N/A		
Chairperson	Mr. Riccardo Genghini		
Scope	<p>TC ESI is the lead body within ETSI in relation to Electronic Signatures , related services and trust service Infrastructures, to protect electronic transactions and ensure trust and confidence with business partners, including the preparation of reports and other necessary activities, by:</p> <ul style="list-style-type: none"> - Developing generic standards, guides and reports; - Liaising with other ETSI bodies; - Liaising with bodies external to ETSI; - Establishing a continuing work plan. 		
Structure	N/A		
Webpage	http://portal.etsi.org/esi		
STANDARDIZATION WORK			
Published standards	194	Projects	25
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
Members (71)	71 members organizations		
Luxembourg's involvement (4)	<ul style="list-style-type: none"> - eWitness S.A. - ILNAS - Luxtrust - Nowina Solutions 		
COMMENTS			
<p>The committee addresses some basic needs of secure electronic commerce and of secure electronic document exchange in general by providing specifications for a selected set of technical items that have been found both necessary and sufficient to meet minimum interoperability requirements. Examples of business transactions based on electronic signatures and public key certificates are purchase requisitions, contracts and invoice applications.</p>			
<p>The lack of standards to support the use of electronic signatures and public key certificates has been identified as one of the greatest impediments to electronic commerce. The deployment of vendor-specific new infrastructures is currently in progress. It is recognized by different parties that there is an urgent need for standards to provide the basis for an open electronic commerce environment. Speedy specifications in this area will make it possible to influence early developments.</p>			
<p>TC ESI is notably responsible to maintain standards and specifications published in response to European Commission (EC) Mandate M/460 on Electronic Signature Standardization.</p>			
<p>The detail of standards and projects on Digital Trust related to Smart ICT technologies developed by ETSI/TC ESI can be found in the Appendix (Section 8).</p>			

4.6 Fora and Consortia Related to Digital Trust

The ecosystem of cybersecurity is broad and, in addition to recognized standards development organizations, many fora and consortia are actively working on the development of technical specifications, certification schemes, research or educational programs, with the aim to develop a secure digital ecosystem and to improve Digital Trust in general.

In connection with the “National Cybersecurity Strategy III”, a list of relevant fora and consortia working in the Digital Trust area (and notably in relation with Smart ICT technologies) is provided in this section. This information intends to help national stakeholders to identify, in addition to the standardization technical committees described in Section 4.5.2, organizations that can be relevant to their needs in the Digital Trust area.

In addition to this list, national stakeholders can refer to the ETSI Technical Report 103 306 “CYBER; Global Cyber Security Ecosystem”⁹⁷, which provides the global cybersecurity ecosystem and notably specifies the relevant organizations of the cybersecurity ecosystem at national level.

4.6.1 3GPP - 3rd Generation Partnership Project

	3GPP	Third Generation Partnership Project
Scope	<p>The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standards development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.</p> <p>The project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.</p> <p>The 3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with non-3GPP networks.</p> <p>3GPP specifications and studies are contribution-driven, by member companies, in Working Groups and at the Technical Specification Group level.</p>	
Activities	Standards Development	
Topics	Telecommunications (5G, 4G LTE et 3G)	
Website	https://www.3gpp.org/	

⁹⁷ ETSI TR 103 306 V1.3.1 (2018-08), CYBER; Global Cyber Security Ecosystem (https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.03.01_60/tr_103306v010301p.pdf)

4.6.2 BSI - Bundesamt für Sicherheit in der Informationstechnik

	BSI	Bundesamt für Sicherheit in der Informationstechnik
Scope	The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry.	
Activities	Standards Development, Education, Certification, Research	
Topics	Cybersecurity, Cryptography, Critical Infrastructure Protection, Secure Electronic Identities, Security in Digitalization, Incident Response	
Website	https://www.bsi.bund.de	

4.6.3 CSA - Cloud Security Alliance

	CSA	Cloud Security Alliance
Scope	<p>The Cloud Security Alliance (CSA) is a global organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products.</p> <p>The CSA operates a cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. The CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and organizations that offer qualified professional services based on CSA best practices.</p>	
Activities	Education, Certification, Research	
Topics	Cloud Computing, Artificial Intelligence, Blockchain, Internet of Things	
Website	https://cloudsecurityalliance.org	

4.6.4 EC-Council - International Council of E-Commerce Consultants

	EC-Council	International Council of E-Commerce Consultants
Scope	The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. They are the owner and developer of the Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Certified Security Analyst (ECSA), License Penetration Testing (Practical) programs, among others.	
Activities	Education, Certification, Consultancy	
Topics	Ethical Hacking, Network Defense, Information Security, Threat Intelligence Analyze, Application Security, Security Analyze, Penetration Test	
Website	https://www.eccouncil.org	

4.6.5 EuroCloud

	EuroCloud
Scope	<p>EuroCloud Europe is a pan-European cloud innovation hub, a completely vendor neutral knowledge sharing network between Cloud Computing Customers and Providers, Start-ups and Research centres. It maintains a constant open dialogue with all partners to bring IT and business together. EuroCloud disseminates information about new business models and opportunities especially for SMEs and fosters the development of a European Digital Single Market.</p> <p>EuroCloud delivers orientation, guidance and best practice, as well as providing support services such as networking and knowledge sharing to cloud customers and providers Europe wide.</p> <p>It notably provides the global program StarAudit, which offers a certification scheme to establish trust in cloud services both on the customer and the user side. The purpose of the StarAudit scheme is to provide accountable quality assessment of cloud services through a transparent and reliable certification process.</p>
Activities	Education, Certification
Topics	Cloud Computing
Website	https://eurocloud.org

4.6.6 GIAC - Global Information Assurance Certification

	GIAC	Global Information Assurance Certification
Scope	GIAC (Global Information Assurance Certification) was founded in 1999 to validate the skills of information security professionals. The purpose of GIAC is to provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security.	
Activities	Certification	
Topics	Security Administration, Forensics, Audit, Management, Software Security, Penetration Testing, Digital Forensics, Incident Response, Information Security, Cyber Security	
Website	https://www.giac.org	

4.6.7 IEEE SA - Institute for Electrical and Electronic Engineers Standards Association

	IEEE SA	Institute for Electrical and Electronic Engineers Standards Association
Scope	IEEE Standards Association (IEEE SA) is a leading consensus building organization that nurtures, develops and advances global technologies, through IEEE. It brings together a broad range of individuals and organizations from a wide range of technical and geographic points of origin to facilitate standards development and standards related collaboration. With collaborative thought leaders in more than 160 countries, it promotes innovation, enables the creation and expansion of international markets and helps protect health and public safety. Collectively, its work drives the functionality, capabilities and interoperability of a wide range of products and services that transform the way people live, work, and communicate.	
Activities	Standards Development, Research	

Topics	Aerospace Electronics, Telecommunications, Computer Technology, Consumer Electronics, Electromagnetic Compatibility, Green and Clean Technology, Healthcare IT, Smart Grid, Software and Systems Engineering, Transportation, etc.
Website	https://standards.ieee.org

4.6.8 IETF - Internet Engineering Task Force

	IETF	Internet Engineering Task Force
Scope	<p>The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.</p> <p>The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.</p>	
Activities	Standards Development, Research	
Topics	Networking Technologies (Automated Network Management, IoT, Transport Technologies, Applications and Real-Time, Routing, Security)	
Website	https://www.ietf.org	

4.6.9 GSMA - GSM Association

	GSMA	GSM Association
Scope	<p>The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.</p> <p>GSMA Working Groups provide a forum for consensus building among members concerning the setting of frameworks and standards in respect of operational and technical matters and they provide a focus for harmonising a GSMA view for use outside the organisation.</p>	
Activities	Standards Development	
Topics	Telecommunications, Mobile Internet, Future Networks, IoT	
Website	https://www.gsma.com	

4.6.10 IIC - Industrial Internet Consortium

	IIC	Industrial Internet Consortium
Scope	<p>The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the industrial internet by identifying, assembling, testing and promoting best practices. Members work collaboratively to speed the commercial use of advanced technologies. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations.</p>	
Activities	Standards Development	
Topics	IoT, IIoT, Artificial Intelligence, Blockchain, Cybersecurity, Smart Factory, Smart Cities, Intelligent Transport Systems	
Website	https://www.iiconsortium.org/	

4.6.11 ISACA - Information Systems Audit and Control Association

	ISACA	Information Systems Audit and Control Association
Scope	ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.	
Activities	Education, Certification	
Topics	Risk Management, IT Governance, Cybersecurity, IT audit, IT assurance	
Website	https://www.isaca.org	

4.6.12 (ISC)² - International Information System Security Certification Consortium

	(ISC) ²	International Information System Security Certification Consortium
Scope	(ISC) ² is an international, nonprofit membership association for information security leaders. It provides globally recognized certifications in every aspect of information security (e.g.: CISSP). It is also educating the general public through the support of its Center for Cyber Safety and Education.	
Activities	Education, Certification	
Topics	IT security, Cybersecurity, Application Security, Cloud Computing	
Website	https://www.isc2.org	

4.6.13 ISECOM - Institute for Security and Open Methodologies

	ISECOM	Institute for Security and Open Methodologies
Scope	Back in January 2001, ISECOM (the Institute for Security and Open Methodologies) began with the release of the OSSTMM, the Open Source Security Testing Methodology Manual. It was a move to improve how security was tested and implemented. Many researchers from various fields contributed because they saw the need for an open method, one that was bound towards truth and not commercial gain or political agendas. This is also true for all of the research areas covered by ISECOM projects. And it's not enough to just find the facts, we need to find ways to apply it to the world we live in. So it needs to be a security philosophy and it needs to make sense. And that's what ISECOM does every day for millions of people around the world. From governments to businesses to schools to just regular people, we help to make sense of security.	
Activities	Education, Certification, Research, Consultancy	
Topics	Penetration Testing, Cybersecurity, Physical security, Cyber warfare, Neuro-hacking	
Website	http://www.isecom.org/	

4.6.14 NIST - National Institute of Standards and Technology

	NIST	National Institute of Standards and Technology
Scope	<p>The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories.</p> <p>From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.</p> <p>NIST's cybersecurity and privacy activities strengthen the security of the digital environment. NIST's sustained outreach efforts support the effective application of standards and best practices enabling the adoption of practical cybersecurity and privacy.</p>	
Activities	Standards Development, Research	
Topics	Artificial intelligence, Biometrics, Cloud computing & virtualization, Complex systems, Computational science, Conformance testing, Cyberphysical systems, Cybersecurity, Data & informatics, Health IT, Identity management, IoT, Interoperability testing, Mobile, Networking, Privacy, Software research, Usability & human factors, Visualization research, Voting systems, etc.	
Website	https://www.nist.gov	

4.6.15 OASIS - Organization for the Advancement of Structured Information Standards

	OASIS	Organization for the Advancement of Structured Information Standards
Scope	<p>OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.</p> <p>OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.</p>	
Activities	Standards Development	
Topics	Open source, Cybersecurity, Privacy, Cryptography, Cloud computing, IoT, Augmented Reality, Legal standards, Blockchain, Content management, Localization, Identity management, Business transactions	
Website	https://www.oasis-open.org	

4.6.16 OCF - Open Connectivity Foundation

	OCF	Open Connectivity Foundation
Scope	<p>OCF's Mission is Twofold:</p> <ul style="list-style-type: none"> - Provide specifications, code and a certification program to enable manufacturers to bring OCF Certified products to the market that can interoperate with current IoT devices and legacy systems. 	

	- Make the end user's experience better by seamlessly bridging to other ecosystems within a user's smart home and ensure interoperability with OCF compliant devices.
Activities	Standards Development, Certification
Topics	IoT
Website	https://openconnectivity.org

4.6.17 OMG - Object Management Group

	OMG	Object Management Group
Scope	The mission of the Object Management Group (OMG) is to develop technology standards that provide real-world value for thousands of vertical industries. OMG is dedicated to bringing together its international membership of end-users, vendors, government agencies, universities and research institutions to develop and revise these standards as technologies change throughout the years.	
Activities	Standards Development, Education, Certification	
Topics	IoT, Modeling, Healthcare, Finance, Middleware, Blockchain, Distributed Ledger, Space, Manufacturing, Systems modeling	
Website	https://www.omg.org	

4.6.18 oneM2M

	oneM2M
Scope	The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.
Activities	Standards Development
Topics	IoT, M2M
Website	http://www.onem2m.org

4.6.19 OWASP - The Open Web Application Security Project

	OWASP	The Open Web Application Security Project
Scope	The OWASP Foundation came online on December 1st, 2001 it was established as a not-for-profit charitable organization in the United States on April 21, 2004, to ensure the ongoing availability and support for our work at OWASP. OWASP is an international organization and the OWASP Foundation supports OWASP efforts around the world. OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.	
Activities	Education, Research	

Topics	Open Source, Security, Software, Web, Community, Non-Profit, Code, Frameworks, Information, Cybersecurity, Application Development
Website	https://www.owasp.org

4.6.20 PCI-SSC - PCI Security Standards Council

	PCI-SSC	PCI Security Standards Council
Scope	<p>The PCI Security Standards Council is a global forum for the industry to come together to develop, enhance, disseminate and assist with the understanding of security standards for payment account security.</p> <p>The Council maintains, evolves, and promotes the Payment Card Industry Security Standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.</p>	
Activities	Standards Development, Education	
Topics	Payment Security	
Website	https://www.pcisecuritystandards.org	

4.6.21 SNIA - Storage Networking Industry Association

	SNIA	Storage Networking Industry Association
Scope	<p>The Storage Networking Industry Association (SNIA) is a non-profit organization made up of member companies spanning information technology. A globally recognized and trusted authority, SNIA's mission is to lead the storage industry in developing and promoting vendor-neutral architectures, standards and educational services that facilitate the efficient management, movement and security of information.</p>	
Activities	Standards Development, Education	
Topics	Cloud Storage Technologies, Data Management, Data Security, Next Generation Data Center, Networked Storage, Persistent Memory, Physical Storage, Power Efficiency Measurement, Storage Management	
Website	https://www.snia.org	

4.6.22 TCG - Trusted Computing Group

	TCG	Trusted Computing Group
Scope	<p>Through open standards and specifications, Trusted Computing Group (TCG) enables secure computing. Benefits of TCG technologies include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity. Trusted hardware and applications reduce enterprise total cost of ownership and support regulatory compliance.</p>	
Activities	Standards Development	
Topics	Internet Security, Software Security, Network Security, Hardware Security, Cloud Computing, IoT	
Website	https://trustedcomputinggroup.org	

4.6.23 W3C - World Wide Web Consortium

	W3C	World Wide Web Consortium
Scope	The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor and Director Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.	
Activities	Standards Development,	
Topics	Web standards, Semantic Web, HTML, XML, CSS, RDF, XSL, CSS, Schema, Mobile, SVG, PNG, DOM, SMIL, MathML, Open Web Platform	
Website	https://www.w3.org	

5 PROMISING STANDARDIZATION AREAS

This chapter focuses on recent and promising technologies, which have recently drawn the attention of standardization organizations. In particular, these technologies have been identified as trends to be analyzed and evaluated by the ISO/IEC JTC 1 Advisory Group on Emerging Technology and Innovation. This group advises the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1) on the potential of new technology trends for standards development in order for JTC 1 to provide the standards needed by the market in a timely manner. For each technology included in this chapter, a definition is provided, as well as an overview of current standardization activities launched by ISO/IEC JTC 1.

5.1 Brain Computer Interface

Brain-computer interface (BCI) or brain-machine interface (BMI), corresponds to a human-machine interface providing direct communication between the human brain and an artificial device. BCI is a rapidly developing technology, notably benefiting from the progress of artificial intelligence. There are two types of BCI: invasive BCI, which requires surgery with the implantation of sensors in the body, or non-invasive BCI, consisting in the placement of external sensors.

BCI is highly promising for people with severe motor disabilities since it could allow them to regain mobility by controlling robotic devices directly linked to their brain, for example an exoskeleton. Some applications to help people with neurodegenerative diseases are also explored, as well as the possibility to augment the brain by linking it to an artificial intelligence.

Definitions

IEEE

A brain-machine interface (BMI) is a system that establishes a direct communication channel between the human or animal brain and a computer or an external device. BMIs record or stimulate activity of the central or peripheral nervous system (CNS/PNS) in order to replace, restore, enhance, supplement, or improve natural output/input. Thereby the BMI is able to change the ongoing interactions between the CNS and its external or internal environment.

BMIs typically measure neural activity through sensors placed inside the brain or body (invasive or implanted technologies) or external sensors (non-invasive technologies). This activity is processed in real-time to extract information about the intentions or states of the subject. Processed information is then used to generate an action or stimulus in the external world that is provided as direct or indirect feedback to the user⁹⁸.

ANSI

Brain-computer interfaces (BCI) allow living things to interact with technology in the simplest sense. Think about it: when you move your eyes to read or your fingers to type, you first transmit information from your mind to the parts of the body that you desire to move. Why can't that same idea apply to our input with computer-based machines?⁹⁹

Gartner


Computer-brain interface is a type of user interface, whereby the user voluntarily generates distinct brain patterns that are interpreted by the computer as commands to control an application or device.

⁹⁸ <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/presentations/ieee-neurotech-for-bmi-standards-roadmap.pdf>

⁹⁹ <https://blog.ansi.org/2016/01/brain-computer-interface-bci-technology/#gref>

The best results are achieved by implanting electrodes into the brain to pick up signals. Noninvasive techniques are available commercially that use a cap or helmet to detect the signals through external electrodes¹⁰⁰.

Standardization activities

ISO/IEC JTC 1/AG 16 BRAIN-COMPUTER INTERFACE		
GENERAL INFORMATION		
Creation date	2019	
Convenor	Ms. Yunzhu Liu	
Terms of Reference	<ul style="list-style-type: none"> - Provide a description of key concepts related to Brain-computer Interface, and describe relevant terminology; - Study and document the technological, market and related societal requirements for the future ICT standardization on Brain-computer Interface; - Study and document current technologies that are being deployed in Brain-computer Interface; - Promote the awareness of JTC 1 activities on Brain-computer Interface outside JTC 1; - Assess the current state of standardization activities relevant to Brain-computer Interface within JTC 1, in other relevant ISO and IEC Committees, in other SDOs and in consortia. - Identify and propose how JTC 1 should address the ICT standardization needs of Brain-computer Interface; - Engage with standards setting organizations that are involved in Brain-computer Interface standardization as approved by this Advisory Group on Brain-computer Interface. 	
COMMENTS		
<p>ISO/IEC JTC 1/AG 16 is an advisory group created in 2019 by JTC 1, on the basis of a Technology Trend Report developed by the JTC 1 advisory group on Emerging Technology and Innovation. It is studying BCI in order to assess its potential for the launch of standardization activities and will provide a final report to JTC 1 in November 2020, which will include recommendations on how JTC 1 should address the standardization needs of BCI.</p>		

5.2 Digital Twin

The Digital Twin combines a variety of recent technologies such as the IoT, cyber-physical systems (CPS), 3D modeling, simulation, and artificial intelligence. It is at the heart of the fourth industrial revolution. The digital twin is a virtual clone of a physical system or process. It systematically implies the existence of a digital model and an object it copies. These objects can be a product, a machine, a production line, a process, a supply chain. The Digital Twin evolves over time like its physical twin (the object). It can, for example, improve the management, security and optimization of production lines and factories, digital continuity at the level of the product, from its design to its end of life, monitoring and predictive maintenance. It makes it possible to set up new economic models in the supply chain (as a service model). It allows a gain in product quality by improving process correction. It also increases the traceability of objects or processes by integrating more information on components, suppliers and production. It is a disruptive tool, foreseen for the simulation of complex systems that are difficult to duplicate or transport.

¹⁰⁰ <https://www.gartner.com/en/information-technology/glossary/computer-brain-interface>

Definitions

ISO

A Digital Twin is a digital model of a particular physical element or a process with data connections that enable convergence between the physical and virtual states at an appropriate rate of synchronization¹⁰¹.

IEC

Digital representation of physical individuals as well as of virtual entities in an information framework that interconnects traditionally separated elements and provides an integrated view throughout life cycles (digital twins and digital thread)¹⁰².

Gartner

A digital twin is a digital representation of a real-world entity or system. The implementation of a digital twin is an encapsulated software object or model that mirrors a unique physical object, process, organization, person or other abstraction. Data from multiple digital twins can be aggregated for a composite view across a number of real-world entities, such as a power plant or a city, and their related processes¹⁰³.

Standardization activities

ISO/IEC JTC 1/AG 11 DIGITAL TWIN



GENERAL INFORMATION

Creation date	2019
Convenor	Ms. Sha Wei
Terms of Reference	<ul style="list-style-type: none"> - Provide a description of key concepts and relevant terminology related to Digital Twin; - Identify current technologies and reference models that are being deployed in Digital Twin; - Promote the awareness of JTC 1 activities on Digital Twin outside JTC 1; - Assess the current state of standardization activities relevant to Digital Twin within JTC 1, in other relevant ISO and IEC Committees, in other SDOs and in consortia; - Identify and propose the relevant standardization issues of Digital Twin that needs to be addressed by JTC 1, covering at least foundational areas, ICT standardization needs, etc. - Engage with standards setting organizations that are involved in Digital Twin standardization as approved by the AG on Digital Twin. - Prepare a report and recommendations to JTC 1, which may include proposed New Work Items.

COMMENTS

ISO/IEC JTC 1/AG 11 is an advisory group created in 2019 by JTC 1, on the basis of a Technology Trend Report developed by the JTC 1 advisory group on Emerging Technology and Innovation. It is studying Digital Twin in order to assess its potential for the launch of standardization activities and will provide a final report to JTC 1 in November 2020, which will include recommendations on how JTC 1 should address the standardization needs of Digital Twin. The AG 11 has already proposed two standardization projects on Digital Twin to JTC 1, first one on concepts and terminology, and second one on use cases. Both projects are currently submitted to the vote of JTC 1 members.

¹⁰¹ ISO/TC184/SC4/WG15 ISO CD 23247-1: Digital Twin manufacturing framework - Part 1: Overview and general principles

¹⁰² Draft technical report of IEC/TC 65 ISO/TC 84 JWG 21 on Smart Manufacturing Reference Models.

¹⁰³ <https://www.gartner.com/en/information-technology/glossary/digital-twin>

5.3 Quantum Computing

While traditional computing relies on bits, quantum computing relies on quantum bits, or qubits. Comparatively to bits, which are binary, the qubit is not confined to only 0 and 1, since it is capable of taking these two values at the same time. This is called the principle of superposition of states. But that is not the only peculiarity of qubits. Two qubits can also interact, their states intermixing and becoming interdependent, this is called quantum entanglement. These characteristics have direct consequences on the computing power of a machine since quantum computers can access a multitude of results at once where traditional computers must proceed step by step. Quantum computing promises to revolutionize IT with use cases in all economic sectors, notably through its application to cryptography or Machine Learning.

Definitions

ISO

Quantum computing corresponds to the use of quantum phenomena for computational purposes. Quantum phenomena is the physical effect resulting from the quantum nature of particles, interactions, and secondary effects in quasi-particles in a physical system which disappear in the classical limit (from quantum to classical mechanics)¹⁰⁴.

Gartner

Quantum computing is a type of non-classical computing that operates on the quantum state of subatomic particles. The particles represent information as elements denoted as quantum bits (qubits). A qubit can represent all possible values simultaneously (superposition) until read. Qubits can be linked with other qubits, a property known as entanglement. Quantum algorithms manipulate linked qubits in their undetermined, entangled state, a process that can address problems with vast combinatorial complexity¹⁰⁵.

Standardization activities

ISO/IEC JTC 1/WG 14 QUANTUM COMPUTING



GENERAL INFORMATION

Creation date	2020
Convenor	Ms. Hong Yang
Terms of Reference	<ul style="list-style-type: none"> - Serve as a focus of and proponent for JTC 1's standardization program on Quantum Computing. Identify gaps and opportunities in Quantum Computing standardization. - Develop and maintain a list of existing Quantum Computing standards produced and standards development projects underway in ISO/TCs, IEC/TCs and JTC 1. - Develop deliverables in the area of Quantum Computing. - As a systems integration entity, maintain relationships with other ISO and IEC/TCs and other organizations that are involved in Quantum Computing standardization

COMMENTS

ISO/IEC JTC 1/WG 14 is a working group created in 2020 by JTC 1, based on the recommendations of the JTC 1 advisory group on quantum computing. It is in charge of the development of standards in the quantum computing area, starting with the project ISO/IEC 4879, Quantum computing – Terminology and vocabulary.

¹⁰⁴ ISO/TS 80004-12:2016, Nanotechnologies — Vocabulary — Part 12: Quantum phenomena in nanotechnology

¹⁰⁵ <https://www.gartner.com/en/information-technology/glossary/quantum-computing>

6 OPPORTUNITIES FOR THE NATIONAL MARKET

Technical standardization is important not only to make Smart ICT components interoperable, but also to guarantee the security and safety of the digital world, for example with the support of Digital Trust related standards. The previous chapters have highlighted the basic concepts of Smart ICT technologies, such as the Internet of Things, Cloud Computing, Artificial Intelligence or Blockchain, as well as related standardization developments at European and international levels, which directly contribute to make these technologies secure and trustworthy. The purpose of this Standards Analysis “Smart Secure ICT Luxembourg” is to encourage the participation of national stakeholders in technical standardization. It will directly contribute to support and stimulate the ICT sector in terms of competitiveness, visibility and performance. Many national organizations are now engaged on the path of Smart ICT technical standardization, which offers them unique opportunities to participate in the process and helps in designing the future global Smart Secure ICT landscape. In particular, this chapter provides an overview of ILNAS developments aiming at facilitating the involvement of stakeholders in the technical standardization process, for the benefit of the national economy.

The ICT sector is, at a national level, the most active standardization sector. Luxembourg is a “P-member”¹⁰⁶ of ISO/IEC JTC 1 and represents national interests in its plenary meetings. As mentioned earlier 85 delegates¹⁰⁷ from the country are currently involved in international and European technical standardization committees. Among them, 71 are involved in Smart ICT and Digital Trust related technical committees, such as Internet of Things: 19; Cloud Computing: 11; Artificial Intelligence: 24; Blockchain: 17, Digital Trust: 42. However, considering the rich and vibrant ecosystem of organizations involved in the ICT sector in Luxembourg, ILNAS believes that active technical committees in Smart ICT standardization could still attract more national stakeholders and make them benefit from related opportunities of technical standardization. In this way, ILNAS, with the support of ANEC G.I.E., is following closely Smart ICT related technical committees in order to provide the most relevant information to the national ICT community. Moreover, ANEC G.I.E. standardization project officers are managing, as national chairpersons, the technical committees listed below to facilitate the involvement of national stakeholders in the technical committees and represent the interests of the Grand Duchy of Luxembourg in the international plenary meetings¹⁰⁸.

- ISO/IEC JTC 1 SC 41 - Internet of Things and related Technologies;
- ISO/IEC JTC 1 SC 38 - Cloud Computing and Distributed Platforms;
- ISO/IEC JTC 1 SC 42 - Artificial Intelligence;
- ISO/TC 307 - Blockchain and Distributed Ledger Technologies.

To summarize, ILNAS, with the support of ANEC G.I.E., is performing different activities to inform national stakeholders and support their normative steps. The opportunities presented in this chapter can be considered by national stakeholders as a series of proposals, which lead to go further and to engage in future actions in order to take advantage of standardization. The opportunities listed below are available at the national level, according to the interests of the stakeholders in the Smart ICT sector.

¹⁰⁶ P-members actively participate by voting on the standard at various stages of its development. While O-members can observe the standards that are being developed, offering comments and advice. (<https://www.iso.org/who-develops-standards.html>)

¹⁰⁷ Some experts are participating in more than one technical committee.

¹⁰⁸ More information on: <https://portail-qualite.public.lu/fr/normes-normalisation/secteurs/tic.html>

6.1 Information about Standardization

6.1.1 Smart ICT Workshops and Information Sessions

In order to disseminate ICT standardization knowledge within the related community in Luxembourg (ISO/IEC JTC 1, ETSI, ICT *fora* and *consortia*, etc.), ILNAS organizes, at national level in collaboration with ANEC G.I.E., workshops and information sessions in the framework of ICT prospective and, more specifically in the “Smart Secure ICT” domain.

For instance, breakfasts dedicated to the promotion of Smart Secure ICT standardization were organized in 2019 and 2020 in order to discuss Smart ICT and widespread use of such technologies in a secure way. Beyond the technical aspects, the latest related standardization developments were presented to highlight their importance for the establishment of a trusted digital environment. These breakfasts reviewed various Smart ICT technologies, focusing mainly on Cloud Computing, Internet of Things, Artificial Intelligence, and Blockchain. They were organized to bring together national stakeholders of dedicated Smart ICT subsectors and to provide them with the relevant standardization knowledge and facilitate their engagement in the standards development process. In this manner, ILNAS organizes information sessions dedicated to technical standardization of a specific Smart ICT subsector, on a regular basis¹⁰⁹. For example, a breakfast dedicated to Cloud Computing technical standardization was organized in February 2020, in collaboration with the University of Luxembourg. This event was notably dedicated to further discuss the results of the Technical Reports "Gap Analysis Between Scientific Research and Technical Standardization"¹¹⁰ published in October 2019 and delivering gap analyses between scientific research and technical standardization for three Smart ICT domains (Cloud Computing, Internet of Things and Artificial Intelligence/Big Data).

Moreover, as mentioned in the introduction of this chapter, standardization officers of ANEC G.I.E. are chairing, in support of ILNAS, the National Mirror Committees (NMCs) that gather national experts dedicated to Smart ICT (IoT, Cloud Computing, Artificial Intelligence, and Blockchain). This involvement aims at reinforcing Luxembourg's positioning in these areas and NMC meetings are regularly organized to allow interested national stakeholders to strengthen their commitment to the process of technical standardization (interested people who are not already delegates of technical committees can also participate to be informed and analyze the benefits of taking part in the development of standards). In this context, ANEC G.I.E. participated in eight international plenary meetings of technical committees in 2019. This participation continues during 2020¹¹¹. In this context, it organized NMC meetings to prepare, debrief and exchange on the topics discussed during these plenary meetings with the related national community. In 2020, 10 NMC meetings were organized during the first semester, including NMC meetings open to any interested stakeholder willing to learn more about technical standardization in the Smart ICT domains. For example, a NMC meeting on the IoT was organized in June 2020, gathering people interested in IoT technical standardization and focusing on the National Technical Standardization Report on the IoT¹¹², published by ILNAS in June 2020.

¹⁰⁹ Updates on events organized by ILNAS are regularly published on <https://portail-qualite.public.lu/fr/agenda.html>

¹¹⁰ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/TR-Smart-ICT-Gap-Analysis-SR-TS-ILNAS-UL.pdf>

¹¹¹ Due to the COVID-19 pandemic, most of the Plenary Meetings were organized virtually

¹¹² <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/national-technical-standardization-report-iot-june-2020.pdf>

6.1.2 Awareness Sessions

Another way to obtain relevant standardization knowledge is to contact ILNAS and ANEC G.I.E. in order to program a dedicated awareness session. This kind of meeting aims at providing basic knowledge about standardization as well as information that meets the standards-related interests of the requesting organization. In this way, ILNAS, with the support of ANEC G.I.E. provides a detailed overview of relevant technical committees and standards project under development to allow an organization to take advantage of standardization, for example by registering in the identified technical committees.

To facilitate the organization of such awareness, interested stakeholders can fill a declaration of interest in ICT standardization¹¹³ to be contacted by ILNAS and ANEC G.I.E.

6.1.3 Smart ICT Standards Watch

The objective of the Standards Analysis “Smart Secure ICT Luxembourg” is to facilitate the identification of technical committees in the Smart ICT area that meet organizations’ potential interests. Moreover, ILNAS, with the support of ANEC G.I.E., can execute, on demand, a focused standards watch to answer the needs of a national organization¹¹⁴. This service consists in the analysis of relevant standards (both published and under development) and technical committees related to a specific problematic of a requesting organization. A standards watch report is delivered at the end of the process as a result and some additional steps can be proposed by ILNAS and ANEC G.I.E., like the registration in technical committee(s) to allow the follow-up of the relevant standardization developments by the requesting organization.

6.1.4 Publications and Dissemination

ILNAS, with the support of ANEC G.I.E., publishes and disseminates reports and White Papers at the national level in order to provide valuable information on Smart ICT standardization topics to national stakeholders. In addition to the White Papers described below, ILNAS plans to publish two new National Technical Standardization Reports in 2021: one on Artificial Intelligence and one on Blockchain.

- **National Technical Standardization Report on the Internet of Things**¹¹⁵

ILNAS and ANEC G.I.E. published this National Technical Standardization Report on the Internet of Things in June 2020. It is a follow-up to the White Paper on the IoT published in 2018 with the support of the Ministry of the Economy. The report first revisits the technical landscape of the IoT, with a particular focus on the value of data, and the need for adequate levels of security and privacy. It then gives examples of some national stakeholder IoT use cases, specifically in the areas of satellite-based connectivity supporting IoT and Smart mobility. Finally, it paints an updated picture of the IoT technical standardization landscape, and specifically on the involvement of Luxembourg within it.

- **White Paper Internet of Things and Technical Standardization**¹¹⁶

ILNAS and ANEC G.I.E. published, with the support of the Ministry of the Economy, a White Paper Internet of Things and Technical Standardization in July 2018. The IoT, a network of connected objects capable of collecting and exchanging data, is one of the most promising concepts emerging from the

¹¹³ <https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/normes-normalisation/declarations-interet/declaration-interet-normalisation-tic/declaration-interest-standardization-it.pdf>

¹¹⁴ <https://portail-qualite.public.lu/fr/normes-normalisation/produits-et-services/veille-normative-ciblee.html>

¹¹⁵ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/national-technical-standardization-report-iot-june-2020.pdf>

¹¹⁶ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf>

convergence of ICT technologies. Its adoption is now spreading to all economic sectors, such as industry, energy or logistics, and manifests itself in our daily lives with the development of new services that could deliver significant improvements for both society, economy or the environment. This White Paper aims at providing an overview of its technological implications, market trends, and details the main technical standardization activities in the field, which are critical to the convergence of technologies underlying IoT.

- **White Paper Blockchain and Distributed Ledger Technologies**¹¹⁷

ILNAS and ANEC G.I.E. published, with the support of the Ministry of the Economy, the White Paper Blockchains and Distributed Ledger Technologies in June 2018. Blockchain and Distributed Ledger Technologies (DLT), widely popularized by the rise of crypto currencies, have for some time been gaining interest from many economic sectors, in relation to the potential they could offer in terms of trust, transparency, traceability and immutability. This White Paper was developed as part of Luxembourg's normative strategy, aiming to promote a better understanding of the Blockchain and DLT domain, both in terms of technology and in terms of economic potential, but also through an overview of recently initiated work at the international level for related technical standardization.

- **White Paper Digital Trust for Smart ICT**¹¹⁸

ILNAS and ANEC G.I.E. published, with the support of the Ministry of the Economy, a White Paper Digital Trust for Smart ICT in October 2016 (last update in September 2017) to bring into perspective, through technology, economic view, and need of Digital Trust and technical standardization to aware national market in order to facilitate the widespread adoption of the Smart ICT technologies. It was particularly focused on three Smart ICT technologies, such as the Internet of Things (IoT), Cloud Computing and Big Data. It was aimed at providing national market with relevant knowledge to make easier the establishment of a trusted digital environment and, as a corollary, create value and foster technological development. The appropriation of these concepts will provide a framework to encourage the adoption and the generalization of Smart ICT and their uses.

Moreover, two additional White Papers concerning Smart ICT concepts were published by ILNAS in 2016, with the support of ANEC G.I.E.:

- **White Paper Green Computing**¹¹⁹

This White Paper surveyed, from a holistic perspective, various topics and technologies in the area of sustainability and Information Technology (IT), also known as Green Computing or Green ICT. An investigation is made regarding questions on the environmental impact of current IT usage, energy efficiency of IT products and how IT can contribute to business sustainability. The aim of the document is therefore to present a comprehensive review of the state-of-the-art approaches to help companies in developing sustainable and environmental friendly products and services, which are supported or enabled by IT. In this context, standardization is presented as the cornerstone to guide and support organizations to achieve sustainability. A thorough review is conducted on the most relevant standards related to the topic of Green Computing from different standardization bodies such as ISO, IEC, CENELEC, ETSI, and ITU and *consortia* such as ECMA and IEEE. Finally, the Eco-management and Audit Scheme (EMAS) is surveyed as an environmental management system, which enables organizations to assess, manage, and continuously improve their environmental performance. Because the requirements of ISO 14001 "Environmental management systems" are an integral part of EMAS, organizations that comply with EMAS automatically comply with the requirements of such standard.

¹¹⁷ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-blockchain-june-2018.pdf>

¹¹⁸ <https://portail-qualite.public.lu/dam-assets/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf>

¹¹⁹ <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/information-sensibilisation/white-paper-green-computing/white-paper-green-computing.pdf>

- White Paper Big Data¹²⁰

This document was aimed at surveying current advances in Big Data and Analytics from two complementary points of view: a technical analysis perspective and a business and economic prospective analysis. Therefore, the Standards Analysis is intended for those professionals seeking guidance in one or both domains and can be used in its whole as a compendium where technical and IT governance aspects of Big Data are equally treated. Standards and technical standardization is also presented as an essential tool to improve the interoperability between various applications and prevent vendor lock-in, to provide interfaces between relational and non-relational data stores and to support the large diversity of current data types and structures. Finally, some conclusions on Big Data are presented with an outlook on how to integrate them in the business environment to create value.

6.1.5 Free Consultation of Standards

ILNAS offers the possibility to consult its entire standards' database (including more than 180 000 normative documents from ILNAS, DIN, CEN, CENELEC, ETSI, ISO and IEC) free of charge through reading stations located in six different places in Luxembourg¹²¹:

- ILNAS (Esch-Belval);
- Luxembourg Learning Centre (Esch-Belval);
- Luxembourg Institute of Science and Technology (Belvaux);
- Former library of the University of Luxembourg (Luxembourg-Kirchberg);
- Communal administration of Echternach;
- Security Made in Lëtzebuerg G.I.E. (Luxembourg).

This service allows, for example, interested organizations or individuals to consult a standard before its purchase. The ILNAS e-Shop¹²² offers then the possibility to buy the relevant standards in electronic format at competitive prices.

6.1.6 Smart ICT Standardization Research Results

ILNAS, with the support of ANEC G.I.E., is currently implementing a joint research program with the University of Luxembourg (Interdisciplinary Centre for Security, Reliability and Trust – SnT). An agreement was signed in May 2017¹²³, to reinforce the collaboration of the organizations in the domain of Smart Secure ICT for Business Innovation through Technical Standardization. The research program is intended to analyze and extend standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, Internet of Things and Artificial Intelligence/Big Data. In this frame, three PhD students are conducting research activities in the above-mentioned Smart ICT domains. The team received the “Security Project of the Year” award during the Information Security Day 2019¹²⁴ for the results they already obtained. On the one hand, the results of this research program will support the evolution of the academic program of the Certificate “*Smart ICT for Business Innovation*” (see Section 6.2.2). On the other hand, it will serve as a basis for a future professional Master Program “*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*” (the program will start in February 2021).

¹²⁰ <https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/information-sensibilisation/white-paper-big-data-1-2/wp-bigdata-v1-2.pdf>

¹²¹ <https://portail-qualite.public.lu/fr/normes-normalisation/achat-consultation-normes.html>

¹²² <https://ilnas.services-publics.lu/>

¹²³ <https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2017/ul-ilnas-investissent-smart-ict.html>

¹²⁴ https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team

National stakeholders active in the Smart ICT landscape will have the opportunity to benefit from the results of this research program, for example by participating in the courses offered in the future Master degree (described in the next section). National stakeholders will be also informed through different publications and events related to this research program.

White Paper Data Protection and Privacy in Smart ICT¹²⁵

The White Paper “Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization”, resulting from the collaboration between ILNAS and the University of Luxembourg, was published in October 2018. The objective of this document is to provide a holistic view of privacy and data protection in Smart ICT. To this aim, a review of the state-of-the-art highlighting existing challenges and proposed solutions is presented from two different viewpoints: scientific developments and technical standardization.

Technical Reports "Gap Analysis Between Scientific Research and Technical Standardization"¹²⁶

The White Paper Data Protection and Privacy in Smart ICT was extended in October 2019 with the publication of three Technical Reports delivering gap analyses between scientific research and technical standardization for the three Smart ICT domains studied in the context of the research program.

6.2 Training in Standardization

6.2.1 Training on Smart ICT Standardization

ILNAS, with the support of ANEC G.I.E., develops a training catalogue¹²⁷ annually, which is updated according to market expectations. In addition to general trainings about standards and standardization, technical trainings on Smart ICT standardization and related Digital Trust challenges are proposed:

- Internet of Things and technical standardization;
- Blockchain and technical standardization;
- Cloud Computing and Digital Trust;
- Artificial Intelligence and technical standardization.

These trainings aim at meeting the expectations of national stakeholders in terms of normative knowledge, mainly in the ICT sectors and related Digital Trust challenges. Based on courses proposed in the training catalogue, customized training sessions can also be organized. Any request will be evaluated and a dedicated training program will be proposed to serve specific professional development needs.

6.2.2 Project of Professional “Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions”

ILNAS, supported by ANEC G.I.E., with the University of Luxembourg and the Chamber of Employees (CSL) have developed a Master entitled “*Master in Technopreneurship: mastering smart ICT,*

¹²⁵ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf>

¹²⁶ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/TR-Smart-ICT-Gap-Analysis-SR-TS-ILNAS-UL.pdf>

¹²⁷ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/Training-Catalogue-ILNAS-ANEC-2020.pdf>

*standardisation and digital trust for enabling next generation of ICT solutions*¹²⁸. It is designed for experienced professionals who wish to develop their technological skills in the field of Smart Secure ICT and technopreneurship. It is planned to launch this professional Master in February 2021.

This program focuses on Smart Secure ICT and provides students with the Smart ICT concepts and tools at their disposal to develop their sense of technical innovation (or technopreneurship). Digital Trust is also a central component, and it is not only treated from the point of view of security, but also considering other aspects like reliability, accountability, privacy, transparency, integrity, legitimacy, etc. in order to allow the adoption of Smart ICT technologies and the development of innovative services, products, and business. The Master program tackles various aspects of Smart ICT and their applications, such as the development of Cloud Computing, Internet of Things, Artificial Intelligence or Blockchain and Distributed Ledger Technologies. International experts address these Smart ICT concepts, along with the concepts of information security and Digital Trust, which are essential now more than ever.

This program provides lectures from three points of view:

- Technical: providing the fundamentals of Smart ICT technologies and security techniques and the latest scientific developments;
- Technopreneurship: in order to highlight major opportunities for technical innovation;
- Technical standardization, which plays a key role, as an important source of knowledge and good practices, while defining the future ICT. Concretely, technical standardization remains a main keystone between Smart ICT technologies, the related Digital Trust needs, and the development of business innovation, as it points the way forward.

The Master relies on previous successful projects led by ILNAS in collaboration with the University of Luxembourg, notably the University certificate “*Smart ICT for Business Innovation*”, which is integrated in the Master program.

6.3 Involvement in Standardization

6.3.1 Becoming a National Delegate in Standardization

Benefits of Participation in Smart ICT standardization technical committees

In Luxembourg, registration in technical committees from ISO, IEC, CEN or CENELEC is free of charge¹²⁹. Participating in Smart ICT standardization technical committees offers a broad set of opportunities and benefits, such as:

- Giving your opinion during the standardization process (comments and positions of vote on the draft standards);
- Valuing your know-how and good practices;
- Accessing draft standards;
- Anticipating future evolutions of Smart ICT standardization;
- Collaborating with strategic partners and international experts;
- Enhancing the visibility of your organization at national and international level;
- Identifying development opportunities;
- Making your organization competitive in the market.

¹²⁸ https://www.fr.uni.lu/formations/fstm/master_in_technopreneurship

¹²⁹ <https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html>

Participating in the Training for new delegates in standardization

ILNAS regularly organizes trainings for newcomers in technical standardization¹³⁰, who have registered in a technical committee. They are encouraged to participate in order to better understand the roles and missions of delegates in standardization on one hand, and to become familiar with the tools and services at their disposal for this work on the other.

Support to National Delegates

As the national standards body, ILNAS, with the support of ANEC G.I.E., offers its support to national delegates and coordinates the activities of the different committees at the national level. These duties are of primary importance and well stated in the “Luxembourg’s Policy on ICT technical standardization 2020-2025”, which aims at developing the ICT technical standardization representation at the national level.

Particularly in the ICT sector, ILNAS, with the support of ANEC G.I.E., proposes a dedicated coaching service that is available for any registered national delegate, who requires assistance for the achievement of his standardization work.

Stronger Commitment as a National Delegate (Chairman, Head of Delegation, Editor of European or International Standards)

Registration as a national delegate offers possibilities to assume different levels of involvement, such as:

- Chairman of a national mirror committee: Each national mirror committee has to nominate a chairman who will be in charge of the organization of the national community of delegates registered in the particular committee. Indeed, the chairman has to vote on the draft standards on the basis of the consensual position agreed between the economic entities represented within the national mirror committee;
- Head of delegation: National delegate(s) can be nominated by the national mirror committee to represent its position during the plenary meetings of the corresponding international or European technical committees;
- Editor or co-editor of standards documents: Each standards project is subject to a call for participation. In this frame, a national delegate can choose to actively participate in the project as an editor or co-editor. He will then take the responsibility to ensure the successful conduct of the project until its publication.

Some national delegates from the ICT sector have already been (co-)editors of standards documents such as technical reports (ISO/IEC TR 20000-4, ISO/IEC TR 20000-5 and ISO/IEC TR 27015:2012, ISO/IEC TR 14516-3), international standards (ISO/IEC 27010, ISO/IEC 27034-4, ISO/IEC 33050-4) or other various standards documents (ISO/IEC JTC 1/SC 27/WG 5 Standing Document 2 – Part 1).

6.3.2 Comment Standards under Public Enquiry

ILNAS proposes, through its e-Shop, the opportunity to submit comments on the standards under public enquiry. Every interested national stakeholder can propose changes to the draft standard, regardless of whether such stakeholders are officially registered in the technical committee responsible for the development of this standard.

¹³⁰ <https://portail-qualite.public.lu/fr/formations/normes-normalisation/f03-delegue-normalisation.html>

6.3.3 Propose New Standards Projects

National stakeholders can propose new standardization projects both at international and national levels through ILNAS. The national standards body offers its support to ensure the good implementation of the process and the project's compliance with the related rules and legislation.

This opportunity can allow national stakeholders to take a leading role in the standardization of a specific domain and to benefit from the definition of the future market rules.

6.3.4 Monitor the Standardization Work Performed by the European Multi-Stakeholder Platform on ICT Standardization (MSP)

Since January 2012, ILNAS - Digital trust department, is the Luxembourg's representative within the European Multi-Stakeholder Platform on ICT Standardization. In this frame, ILNAS is the official national contact point dedicated to information exchange between the market and the European multi-stakeholder platform on ICT standardization.

In this context, interested stakeholders can contact the Digital Trust department of ILNAS¹³¹ to join this initiative. It offers the possibility to receive and comment, through ILNAS, documents published by the MSP in different ICT areas.

¹³¹ confiance-numerique@ilnas.etat.lu

HIGHLIGHTS OF OPPORTUNITIES AT THE NATIONAL LEVEL

Luxembourg offers different opportunities to national stakeholders to enable them able to take advantage of technical standardization, summarized as follows:

- To be informed about standardization:
 - o Participate in national Smart ICT workshops;
 - o Benefit from dedicated awareness sessions;
 - o Identify the most relevant Smart ICT technical standardization committees and standards projects from the Smart ICT standards watch;
 - o Consult ILNAS publications on Smart ICT standardization;
 - o Consult freely the national, European and international standards;
 - o Benefit from the ICT standardization research results at national level.

- To be part of the training in technical standardization
 - o Participate in the trainings on Smart ICT standardization;
 - o Participate in the professional “*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*” (beginning of courses in February 2021).

- To be involved in standardization
 - o Become national technical standardization delegate:
 - Participate in Smart ICT technical committees,
 - Register in the training on New delegates in standardization,
 - Benefit from the support offered by the national standards body,
 - Stronger commitment as a national delegate (chairman, head of delegation, editor of European or international standards project),
 - o Submit comments on draft standards under public enquiry;
 - o Propose new standards projects;
 - o Monitor the standardization work performed by the European multi-stakeholder platform on ICT standardization (MSP).

As long as the stakeholders of the sector wish to grab these opportunities, ILNAS, supported by ANEC G.I.E., can facilitate to be on board in the process.

As the national standards body, ILNAS offers national stakeholders the possibility to follow specific standardization activities of technical committees, either at European or international level. It supports those who are interested to participate in standardization activities, namely by providing information and delivering trainings. Therefore, resources from ILNAS and ANEC G.I.E. are specifically dedicated to these aspects and are able to efficiently support and inform for the prospective national delegates¹³².

To reinforce this support, dedicated resources are allocated as specific points of contact for delegates of the Smart ICT sector.

¹³² <https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/normes-normalisation/declarations-interet/declaration-interet-normalisation-tic/declaration-interet-standardization-it.pdf>

7 CONCLUSIONS

The ICT sector is constantly evolving towards smarter technology. Through the development of new and innovative digital products and services, Smart ICT constitutes a major source of economic development and it directly participates in the resolution of current environmental and social concerns. Moreover, Smart ICT technologies, such as the Internet of Things, Cloud Computing, Artificial Intelligence, and Blockchain play a crucial role to support innovation and foster the development of all the other economic sectors where Smart ICT applications and services offer new opportunities. At the same time, Digital Trust remains an essential issue to secure complex systems and give confidence in Smart ICT technologies.

In this context, standards are essential not only to develop ICT, but also to support its interoperability with other sectors. The rapid technological advancements in Smart ICT and their widespread adoption have resulted in a huge demand for careful study and development of relevant technical standards, notably to take into consideration Digital Trust related issues such as data privacy and protection. On the one hand, technical standardization plays an important role not only to give a first-hand insight into the latest developments, thus supporting innovation, but also to contribute to the harmonization of systems and procedures, opening access to external markets, ensuring constant progress, and building trust. On the other hand, standards contribute to promote and share good practices and techniques available through the market. They ensure the quality, security and performance of products, systems, and services. They also facilitate dialogue and exchange between various stakeholders. In this sense, standardization represents an important economic lever to improve business productivity.

ICT is one of the growth sectors identified in the national standardization strategy 2020-2030¹³³, since it supports many innovative or smart developments. Smart ICT is indeed one of the most competitive economic sectors in the Grand Duchy of Luxembourg, which has high-quality communication infrastructures, hosts several world-leading ICT companies as well as many start-ups¹³⁴, and is composed of a market of many companies, associations, administrations, and experts. Luxembourg is also particularly active in creating a secure environment for developing a trusted data-driven economy.

ILNAS, with the support of ANEC G.I.E., is constantly analyzing Smart ICT technical standardization developments and actively supports national stakeholders who want to be involved in this area, according to "Luxembourg's Policy on ICT technical standardization 2020-2025"¹³⁵. The main objectives of this policy are to foster and strengthen the national ICT sector's involvement in standardization work. To achieve this, ILNAS is conducting three intertwined projects:

- a) Promoting ICT technical standardization to the market;
- b) Reinforcing the valorization and the involvement regarding ICT technical standardization
- c) Supporting and strengthening education about standardization and related research activities.

In line with the first project, this Standards Analysis "Smart Secure ICT Luxembourg" constitutes a tool to foster the positioning of Luxembourg in the Smart ICT standardization landscape. It highlights the opportunities offered to the national market to participate in the standardization process especially in Smart ICT related technologies, such as the Internet of Things, Cloud Computing, Artificial Intelligence, Blockchain, and Digital Trust related to these technologies. This Standards Analysis also provides a monitoring of technical committees active in the Digital Trust area, as well as a list of relevant fora and consortia working in the cybersecurity domain, to meet the objectives of the "National Cybersecurity

¹³³ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf>

¹³⁴ <https://www.tradeandinvest.lu/business-sector/ict/>

¹³⁵ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/policy-on-ict-technical-standardization-2020-2025.pdf>

Strategy III”, in terms of technical standardization, and help national stakeholders in building and maintaining secure Smart ICT environments.

Similarly, for the second project, ILNAS, aided by ANEC G.I.E., is offering its support to different industries/organizations through standardization according to the nature of their business at the national level. Smart ICT and/or Digital Trust related technical committees already benefit from a good national representation with 71 national delegates currently registered to participate in one or several of these normative domains (Internet of Things: 19; Cloud Computing: 11; Artificial Intelligence: 24; Blockchain: 17, Digital Trust: 42)¹³⁶. This figure demonstrates the interest of individuals, industries/organizations in technical standardization.

Finally, conforming to the third project, ILNAS, with the support of ANEC G.I.E., has undertaken concrete developments for strengthening education and research activities in the area of technical standardization. It includes the launch of a University certificate dedicated to Smart ICT, focusing on Cloud Computing, the Internet of Things, Big Data, and Digital Trust related to these technologies. This educational program, supported notably by the Ministry of the Economy, ETSI and CEN-CENELEC, was the first step towards the ambitious project of creating a Master program dedicated to Smart Secure ICT. This professional Master “*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*” will start in February 2021. ILNAS and the University of Luxembourg are also implementing a research program¹³⁷ whose objective is to analyze and to extend standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, Internet of Things, and Big Data/Artificial Intelligence. In this context, three PhD students are performing research activities in the above-mentioned Smart ICT domains. As a first result of this collaboration, ILNAS and the University of Luxembourg published a White Paper “Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization”¹³⁸ in October 2018. The work performed by the research team was also rewarded with the “Security Project of the Year” award during the Information Security Day 2019¹³⁹. Moreover, the White Paper Data Protection and Privacy in Smart ICT was extended in October 2019 with the publication of three Technical Reports delivering gap analyses between scientific research and technical standardization for the three Smart ICT domains studied in the context of the research program¹⁴⁰. The research results of this program will facilitate the development of the Master.

In parallel, ILNAS, with the support of ANEC G.I.E., has also published White Papers on Smart ICT and Digital Trust, notably on Blockchain and Distributed Ledger Technology¹⁴¹ and on the Internet of Things¹⁴² in 2018, aiming to create awareness and interest concerning relevant standardization developments within the national market. In addition, the White Paper on the Internet of Things was complemented by a National Technical Standardization Report on the Internet of Things¹⁴³ in June 2020. ILNAS is pursuing this research activity with the development of National Technical Standardization Reports on Artificial Intelligence and Blockchain, which are planned to be published in 2021.

These three projects will allow the national market to make rapid progress and reap the benefits of technical standardization effectively. Proper understanding of the stakes associated with Smart ICT

¹³⁶ Please note that some experts are participating in more than one technical committee

¹³⁷ <https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html>

¹³⁸ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf>

¹³⁹ https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team

¹⁴⁰ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/TR-Smart-ICT-Gap-Analysis-SR-TS-ILNAS-UL.pdf>

¹⁴¹ <https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html>

¹⁴² <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf>

¹⁴³ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/national-technical-standardization-report-iot-june-2020.pdf>

standardization is necessary to adopt the appropriate position across the standardization landscape and benefit from all the related opportunities. Driven by the motto of the national standardization strategy 2020-2030: “Technical standardization – An inclusive tool for performance and excellence to serve the economy”¹⁴⁴, ILNAS, with the support of ANEC G.I.E., stands ready to encourage and assist each initiative in this process.

¹⁴⁴ <https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf>

8 APPENDIX - SMART SECURE ICT STANDARDS AND PROJECTS

This appendix details the Smart Secure ICT related standards - both published and under development of various SDOs. It focuses on four Smart ICT areas (Internet of Things, Cloud Computing, Artificial Intelligence / Big Data and Blockchain & DLT) that are actively followed by ILNAS, with the support of ANEC G.I.E., due to their importance for the national market and for the current developments in education about standardization and research.

The lists of standards and projects included in this Appendix can also be consulted online at: <https://portail-qualite.public.lu/fr/normes-normalisation/secteurs/tic/smart-secure-ict-standards.html>.

8.1 Internet of Things

8.1.1 Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Internet of Things (IoT).

SDO	Reference	Title
ISO/IEC JTC 1	20924:2018	Internet of Things (IoT) - Vocabulary
ISO/IEC JTC 1	21823-1:2019	Internet of Things (IoT) - Interoperability for IoT systems - Part 1: Framework
ISO/IEC JTC 1	21823-2:2020	Internet of Things (IoT) - Interoperability for IoT systems - Part 2: Transport interoperability
ISO/IEC JTC 1	TR 22417:2017	Information technology - Internet of things (IoT) - IoT use cases
ISO/IEC JTC 1	29161:2016	Information technology -- Data structure -- Unique identification for the Internet of Things
ISO/IEC JTC 1	30141:2018	Information technology -- Internet of Things -- Internet of Things Reference Architecture (IoT RA)
ISO/IEC JTC 1	TR 30164:2020	Internet of Things (IoT) - Edge computing
ISO/IEC JTC 1	TR 30166:2020	Internet of Things (IoT) - Industrial IoT
ISO/IEC JTC 1	14543-3-10:2020	Information technology - Home electronic system (HES) architecture - Part 3-10: Wireless short-packet (WSP) protocol optimised for energy harvesting - Architecture and lower layer protocols
ISO/IEC JTC 1	14543-5-12:2019	Information technology – Home electronic system (HES) architecture –Part 5-12: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access test and verification
ISO/IEC JTC 1	14543-5-101:2019	Information technology — Home electronic systems (HES) architecture — Part 5-101: Intelligent grouping and resource sharing remote AV access profile
ISO/IEC JTC 1	14543-5-102:2020	Information technology — Home electronic system (HES) architecture — Part 5-102: Intelligent grouping and resource sharing — Remote universal management profile
ETSI	TR 103 290 V1.1.1 (04/2015)	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
ETSI	TR 103 375 V1.1.1 (10/2016)	SmartM2M; IoT Standards landscape and future evolutions

SDO	Reference	Title
ETSI	TR 103 376 V1.1.1 (10/2016)	SmartM2M; IoT LSP use cases and standards gaps
ETSI	TR 103 467 V1.1.1 (06/2018)	Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem
ETSI	TR 103 527 V1.1.1 (07/2018)	SmartM2M; Virtualized IoT Architectures with Cloud Back-ends
ETSI	TR 103 528 V1.1.1 (08/2018)	SmartM2M; Landscape for open source and standards for cloud native software applicable for a Virtualized IoT service layer
ETSI	TR 103 529 V1.1.1 (08/2018)	SmartM2M; IoT over Cloud back-ends: A Proof of Concept
ETSI	TR 103 536 Ver. 1.1.2 (12/2019)	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms
ETSI	TS 118 101 V2.10.0 (10/2016)	oneM2M; Functional Architecture (oneM2M TS-0001 version 2.10.0 Release 2)
ETSI	TS 118 102 V2.10.2 (03/2020)	oneM2M Requirements (oneM2M TS-0002 version 2.10.2 Release 2A)
ETSI	TS 118 104 V2.7.1 (10/2016)	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 2.7.1 Release 2)
ETSI	TS 118 105 V2.0.2 (03/2020)	oneM2M; Management Enablement (OMA) (oneM2M TS-0005 version 2.0.2 Release 2A)
ETSI	TS 118 106 V2.2.1 (03/2020)	oneM2M; Management Enablement (BBF) (oneM2M TS-0006 version 2.2.1 Release 2A)
ETSI	TS 118 108 V2.6.1 (03/2020)	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 2.6.1 Release 2A)
ETSI	TS 118 109 V2.13.1 (03/2020)	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 2.13.1 Release 2A)
ETSI	TS 118 110 V2.4.1 (09/2016)	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 2.4.1 Release 2)
ETSI	TS 118 111 V2.4.1 (09/2016)	oneM2M; Common Terminology (oneM2M TS-0011 version 2.4.1 Release 2)
ETSI	TS 118 112 V2.2.2 (03/2020)	oneM2M; Base Ontology (oneM2M TS-0012 version 2.2.2 Release 2A)
ETSI	TS 118 113 V2.3.2 (04/2020)	oneM2M; Interoperability Testing (oneM2M TS-0013 version 2.3.2 Release 2A)
ETSI	TS 118 114 V2.0.0 (09/2016)	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 2.0.0 Release 2)
ETSI	TS 118 115 V2.0.0 (09/2016)	oneM2M; Testing Framework (oneM2M TS-0015 version 2.0.0 Release 2)
ETSI	TS 118 120 V2.1.2 (03/2020)	oneM2M; WebSocket Protocol Binding (oneM2M TS-0020 version 2.1.2 Release 2A)
ETSI	TS 118 121 V2.0.1 (03/2020)	oneM2M; oneM2M and AllJoyn® Interworking (oneM2M TS-0021 version 2.0.1 Release 2A)
ETSI	TS 118 122 V2.3.1 (03/2020)	oneM2M Field Device Configuration (oneM2M TS-0022 version 2.3.1 Release 2A)

SDO	Reference	Title
ETSI	TS 118 123 V2.0.2 (03/2020)	oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023 version 2.0.2 Release 2A)
ETSI	TS 118 124 V2.0.2 (03/2020)	oneM2M; OIC Interworking (oneM2M TS-0024 version 2.0.2 Release 2A)
ETSI	TS 118 125 V2.0.0 (03/2020)	Definition of product profiles (oneM2M TS-0025 version 2.0.0 Release 2A)
ETSI	TS 118 126 V3.0.0 (06/2020)	3GPP Interworking (oneM2M TS-0026 version 3.0.0 Release 3)
ETSI	TS 118 132 V2.0.2 (11/2017)	MAF and MEF Interface Specification (oneM2M TS-0032 version 2.0.2 Release 2A)
ETSI	TR 118 501 V1.0.0 (05/2015)	oneM2M Use Case collection
ETSI	TR 118 502 V1.0.0 (04/2015)	Architecture Part 1: Analysis of the architectures proposed for consideration by oneM2M
ETSI	TR 118 503 V1.0.0 (04/2015)	oneM2M Architecture Part 2: Study for the merging of architectures proposed for consideration by oneM2M
ETSI	TR 118 506 V1.0.0 (04/2015)	Study of Management Capability Enablement Technologies for Consideration by oneM2M
ETSI	TR 118 517 V2.0.0 (09/2016)	oneM2M; Home Domain Abstract Information Model (oneM2M TR-0017 version 2.0.0)
ETSI	TR 118 518 V2.5.1 (07/2020)	oneM2M; Industrial Domain Enablement (oneM2M TR-0018 version 2.5.1 Release 2A)
ETSI	TR 118 522 V2.0.0 (09/2016)	oneM2M; Continuation & integration of HGI Smart Home activities (oneM2M TR-0022 version 2.0.0)
ETSI	TR 118 524 V2.0.0 (09/2016)	oneM2M; 3GPP Release 13 Interworking (oneM2M TR-0024 version 2.0.0)
ETSI	TR 118 525 V1.0.0 (03/2016)	oneM2M; Application Developer Guide (oneM2M version 1.0.0 Release 1)
ETSI	GR IP6 008 V1.1.1 (06/2017)	IPv6-based Internet of Things; Deployment of IPv6-based Internet of Things
ITU-T	E.Suppl.11 to ITU-T E series (06/2020)	Criteria for M2M/IoT-related assignments Under Recommendation ITU-T E.164.1 and Recommendation ITU-T E.212 Annex A
ITU-T	Q.3055 (12/2019)	Signalling protocol for Heterogeneous IoT gateways
ITU-T	Q.3745 (04/2020)	Protocol for time constraint IoT-based applications over SDN
ITU-T	Q.3913 (08/2014)	Set of parameters for monitoring internet of things devices
ITU-T	Q.3952 (01/2018)	The architecture and facilities of Model network for IoT testing
ITU-T	Q.4060 (10/2018)	The structure of the testing of heterogeneous Internet of Things gateways in a laboratory environment
ITU-T	X.676 (11/2018)	Object identifier-based resolution framework for IoT grouped services
ITU-T	X.sup31 (09/2017)	Supplement 31 to ITU-T X-series Recommendations - ITU-T X.660 Guidelines for using object identifiers for the Internet of things
ITU-T	Y.4000 / Y.2060 (06/2012)	Overview of Internet of Things

SDO	Reference	Title
ITU-T	Y.4003 (06/2018)	Overview of Smart Manufacturing in the context of Industrial Internet of Things
ITU-T	Y.4050 / Y.2069 (07/2012)	Terms and definitions for Internet of Things
ITU-T	Y.4100 / Y.2066 (06/2014)	Common requirements of Internet of Things
ITU-T	Y.4101/Y.2067 (10/2017)	Common requirements and capabilities of a gateway for Internet of Things applications
ITU-T	Y.4102 / Y.2074 (01/2015)	Requirements for Internet of Things devices and operation of Internet of Things applications during disaster
ITU-T	Y.4103 / F.748.0 (10/2014)	Common requirements for Internet of Things (IoT) applications
ITU-T	Y.4111 / Y.2076 (02/2016)	Semantics based requirements and framework of the Internet of Things
ITU-T	Y.4112 / Y.2077 (02/2016)	Requirements of the Plug and Play capability of the Internet of Things
ITU-T	Y.4113 (09/2016)	Requirements of the network for the Internet of Things
ITU-T	Y.4114 (07/2017)	Specific requirements and capabilities of the IoT for Big Data
ITU-T	Y.4115 (04/2017)	Reference architecture for IoT device capability exposure
ITU-T	Y.4117 (10/2017)	Requirements and capabilities of Internet of Things for support of wearable devices and related services
ITU-T	Y.4118 (06/2018)	Internet of Things requirements and technical capabilities for support of accounting and charging
ITU-T	Y.4119 (03/2018)	Requirements and capability framework for IoT-based automotive emergency response system
ITU-T	Y.4120 (06/2018)	Requirements of Internet of things applications for smart retail stores
ITU-T	Y.4121 (06/2018)	Requirements of an Internet of Things enabled network for support of applications for global processes of the Earth
ITU-T	Y.4203 (02/2019)	Requirements of things description in the Internet of Things
ITU-T	Y.4204 (02/2019)	Accessibility requirements for the Internet of things applications and services
ITU-T	Y.4205 (02/2019)	Requirements and reference model of IoT-related crowdsourced systems
ITU-T	Y.4208 (01/2020)	IoT requirements for support of edge computing
ITU-T	Y.4210 (08/2020)	Requirements and use cases for universal communication module of mobile IoT devices
ITU-T	Y.4401 / Y.2068 (03/2015)	Functional framework and capabilities of the Internet of Things
ITU-T	Y.4416 (06/2018)	Architecture of the Internet of Things based on NGNe
ITU-T	Y.4417 (06/2018)	Framework of self-organization network in the IoT environments
ITU-T	Y.4418 (06/2018)	Functional architecture of gateway for Internet of things applications
ITU-T	Y.4455 (10/2017)	Reference architecture for Internet of things network service capability exposure
ITU-T	Y.4457 (06/2018)	Architectural framework for transportation safety services

SDO	Reference	Title
ITU-T	Y.4459 (01/2020)	Digital entity architecture framework for IoT interoperability
ITU-T	Y.4460 (06/2019)	Architectural reference models of devices for IoT applications
ITU-T	Y.4462 (01/2020)	Requirements and functional architecture of open IoT identity correlation service
ITU-T	Y.4463 (01/2020)	Framework of delegation service for IoT devices
ITU-T	Y.4464 (01/2020)	Framework of blockchain of things as decentralized service platform
ITU-T	Y.4465 (01/2020)	Framework of IoT Services based on Visible Light Communications
ITU-T	Y.4469 (08/2020)	Reference architecture of spare computational capability exposure of IoT devices for smart home
ITU-T	Y.4473 (08/2020)	SensorThings API - Sensing
ITU-T	Y.4474 (08/2020)	Functional architecture for IoT services based on Visible Light Communications
ITU-T	Y.4475 (08/2020)	Lightweight intelligent software framework for IoT devices
ITU-T	Y.4552 / Y.2078 (02/2016)	Application support models of the Internet of Things
ITU-T	Y.4555 (02/2019)	Service Functionalities of Self-quantification over Internet of things
ITU-T	Y.4560 (08/2020)	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities
ITU-T	Y.4561 (08/2020)	Blockchain-based Data Management for supporting Internet of things and smart cities and communities
ITU-T	Y.4702 (03/2016)	Common requirements and capabilities of device management in the Internet of Things
ITU-T	Y.Sup.53 to Y.4000 series (12/2018)	IoT use cases
ITU-T	Y.Sup.54 to ITU-T Y.4000-series (04/2019)	Framework for home environment profiles and levels of IoT systems
ITU-T	Y.Suppl.58 (12/2019)	Internet of Things and smart cities and communities standards roadmap
ITU-T	Y.Suppl.61 to ITU-T Y.4400 series (07/2020)	Features of application programming interface (APIs) for IoT data in smart cities and communities
ITU-T	Y.Suppl.62 to ITU-T Y.4000 series (07/2020)	Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
ITU-T	Y.Suppl.63 to ITU-T Y.4000 series	Unlocking Internet of things with artificial intelligence

8.1.2 Digital Trust related Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Digital Trust for Internet of Things (IoT).

SDO	Reference	Title
ETSI	SR 003 680 (03/2020)	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach
ETSI	TS 103 458 V1.1.1 (06/2018)	Application of Attribute Based Encryption for PII and personal data protection on IoT devices, WLAN, Cloud and mobile services – High-level requirements
ETSI	TR 103 533 V1.1.1 (08/2019)	SmartM2M; Security; Standards Landscape and best practices
ETSI	TR 103 534-1 V1.1.1 (08/2019)	SmartM2M; Teaching material; Part 1: Security
ETSI	TR 103 534-2 Ver. 1.1.1 (10/2019)	SmartM2M; Teaching material; Part 2: Privacy
ETSI	TS 103 645 V2.1.2 (2020-06)	CYBER; Cyber Security for Consumer Internet of Things
ETSI	EN 303 645 V2.1.1 (06/2020)	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
ETSI	TS 118 103 V2.12.1 (04/2019)	oneM2M; Security solutions (oneM2M TS-0003 version 2.12.1 Release 2A)
ETSI	TR 118 508 V1.0.0 (07/2014)	Analysis of Security Solutions for the oneM2M System
ETSI	TR 118 512 V2.0.0 (09/2016)	oneM2M; End-to-End Security and Group Authentication (oneM2M TR-0012 version 2.0.0)
ETSI	TR 118 516 V2.0.0 (09/2016)	oneM2M; Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies (oneM2M TR-0016 version 2.0.0)
ITU-T	X.1361 (09/2018)	Security framework for the Internet of things based on the gateway model
ITU-T	X.1362 (03/2017)	Simple encryption procedure for Internet of Things (IoT) environments
ITU-T	X.1363 (05/2020)	Technical framework of personally identifiable information (PII) handling system in Internet of things (IoT) environment
ITU-T	X.1364 (03/2020)	Security requirements and framework for narrow band Internet of things
ITU-T	X.1365 (03/2020)	Security methodology for use of identity-based cryptography in support of Internet of Things (IoT) services over telecommunication networks
ITU-T	Y.4806 (11/2017)	Security capabilities supporting safety of the Internet of Things
ITU-T	Y.4807 (01/2020)	Agility by design for Telecommunications/ICT Systems Security used in the Internet of Things
ITU-T	Y.4808 (08/2020)	Digital entity architecture framework to combat counterfeiting in IoT

8.1.3 Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Internet of Things (IoT).

SDO	Reference	Title
ISO/IEC JTC 1	20924 (ed. 2)	Internet of Things (IoT) - Vocabulary
ISO/IEC JTC 1	21823-3	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 3: Semantic interoperability
ISO/IEC JTC 1	21823-4	Internet of Things (IoT) - Interoperability for Internet of Things Systems –Part 4: Syntactic interoperability
ISO/IEC JTC 1	30141 (ed. 2)	Internet of Things (IoT) - Reference architecture
ISO/IEC JTC 1	30161	Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services
ISO/IEC JTC 1	30162	Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems
ISO/IEC JTC 1	30163	Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring
ISO/IEC JTC 1	30165	Internet of Things (IoT) -- Real-time IoT framework
ISO/IEC JTC 1	TR 30167	Internet of Things (IoT) - Underwater Communication Technologies for IoT
ISO/IEC JTC 1	30169	Internet of things (IoT) - IoT applications for electronic label system (ELS)
ISO/IEC JTC 1	TR JTC1-SC41-2	Internet of Things (IoT) - Guidance on the application of the IoT Reference Architecture to Wearables and Implantables based IoT Systems
ISO/IEC JTC 1	JTC1-SC41-3	Internet of Things (IoT) – Socialized IoT system resembling human social interaction dynamics
ISO/IEC JTC 1	TR JTC1-SC41-4	Internet of Things (IoT) - Integration of IoT and DLT/Blockchain: Use Cases
CEN	EN 17230	Information technology – RFID in rail
ETSI	TS 103 757	SmartM2M; Asynchronous Contact Tracing System; Fighting pandemic disease with Internet of Things
ETSI	TS 118 101	oneM2M; Functional Architecture (oneM2M TS-0001 version 3.9.0 Release 3)
ETSI	TS 118 102	oneM2M Requirements (oneM2M TS-0002 version 3.1.0 Release 3)
ETSI	TS 118 104	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 3.9.0 Release 3)
ETSI	TS 118 105	oneM2M; Management Enablement (OMA) (oneM2M TS-0005 version 3.4.0 Release 3)
ETSI	TS 118 106	oneM2M; Management Enablement (BBF) (oneM2M TS-0006 version 3.6.0 Release 3)
ETSI	TS 118 108	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 3.2.0 Release 3)
ETSI	TS 118 109	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 3.1.0 Release 3)
ETSI	TS 118 110	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 3.0.0 Release 3)

SDO	Reference	Title
ETSI	TS 118 111	oneM2M; Common Terminology (oneM2M TS-0011 version 3.0.0 Release 3)
ETSI	TS 118 112	oneM2M; Base Ontology (oneM2M TS-0012 version 3.7.1 Release 3)
ETSI	TS 118 114	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 3.1.0 Release 3)
ETSI	TS 118 115	oneM2M; Testing Framework (oneM2M TS-0015 version 2.0.0 Release 2A)
ETSI	TS 118 117	oneM2M Implementation Conformance Statements (oneM2M TS-0017 version 2.1.1 Release 2)
ETSI	TS 118 118	oneM2M Test Suite Structure and Test Purposes (oneM2M TS-0018 version 2.13.1 Release 2)
ETSI	TS 118 119	oneM2M Abstract Test Suite and Implementation eXtra Information for Test (oneM2M TS-0019 version 2.3.0 Release 2)
ETSI	TS 118 123	oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023 version 3.7.1 Release 3)
ETSI	TS 118 124	oneM2M; OIC Interworking (oneM2M TS-0024 version 3.2.0 Release 3)
ETSI	TS 118 130	oneM2M Ontology based Interworking (oneM2M TS-0030 v3.0.1 Release 3)
ETSI	TS 118 131	oneM2M Feature Catalogue (oneM2M TS-0031v2.2.0 Release 2A)
ETSI	TS 118 134	oneM2M; Semantics Support (oneM2M TS-0034 version 0.5.0 Release 3)
ETSI	TS 118 135	oneM2M; OSGi Interworking (oneM2M TS-0035 version 0.2.0 Release 3)
ETSI	TR 118 501	oneM2M; Use Case collection (oneM2M TR-0001 version 2.4.1 Release 2A)
ETSI	TR 118 503	oneM2M Roles and Focus Areas
ETSI	TR 118 507	oneM2M; Study on Abstraction and Semantics Enablement (oneM2M TR-0007 Version 2.11.1 Release 2A)
ETSI	TR 118 513	oneM2M Home Domain Enablement
ETSI	TR 118 514	oneM2M; oneM2M and AllJoyn Interworking (oneM2M TR-0014)
ETSI	TR 118 520	oneM2M Study of service transactions and re-usable service layer context
ETSI	TR 118 521	oneM2M Study of the action triggering in M2M
ETSI	TR 118 523	oneM2M and OIC Interworking
ETSI	TR 118 526	oneM2M: Vehicular Domain Enablement (oneM2M TR-0026 version 0.10.0)
ETSI	TR 118 530	oneM2M Service Layer Forwarding (oneM2M TR-0030 v03.0)
ETSI	TR 118 531	oneM2M LWM2M DM & Interworking Enhancements (oneM2M TR-0031 v0.5.0)
ETSI	TR 118 533	oneM2M Study on Enhanced Semantic Enablement (oneM2M TR-0033 study on Enhanced Semantic Enablement Release 3)

SDO	Reference	Title
ETSI	TR 118 534	oneM2M; Developer Guide: CoAP binding and long polling for temperature monitoring (oneM2M TR-0034 v2.0.0 release 2A)
ETSI	TR 118 535	oneM2M; Developer guide: device management (oneM2M TR-0035 v2.0.0 release 2A)
ETSI	TR 118 538	oneM2M; Developer guide: Implementing security example (oneM2M TR-0038 v2.0.0 release 2A)
ETSI	TR 118 539	oneM2M; Developer guide; Interworking Proxy using SDT (oneM2M TR-0039 version 2.0.0 release 2A)
ETSI	TR 118 541	oneM2M Decentralized Authentication (oneM2M TR-0041 version 0.4.0 Release 4)
ETSI	TR 118 545	oneM2M; Developer Guide: Implementing Semantics (oneM2M TR-0045 version 2.0.0)
ETSI	TR 118 551	oneM2M API guide (oneM2M TR-0051 version 0.6.0 Release 2A)
ETSI	TR 118 556	oneM2M; Summary of Differences between Release 2A & Release 3 (oneM2M TR-0056 version 1.0.0)
ETSI	GS MEC 033	Multi-access Edge Computing (MEC); IoT API
ITU-T	D.IoT/M2M Roaming	Roaming aspects of IoT and M2M including any related development and tariff principles
ITU-T	D.IoTpolicy	Guidelines on Tariff and regulatory aspects of Internet of Things (IoT)
ITU-T	E.IoT-NNAI	Internet of Things Naming Numbering Addressing and Identifiers
ITU-T	G.IoT	System architecture, PHY layer and DLL layer for IoT Smart Home over PLC
ITU-T	Q.4062	Framework for IoT Testing
ITU-T	Q.4063	The framework of testing of identification systems used in IoT
ITU-T	Q.GDC-IoT-test	Testing requirements and procedures for Internet of Things based green data centres
ITU-T	TR_IoTM2M_roaming	Roaming aspects of IoT and M2M including any related development and tariff principles
ITU-T	Y.4472	Open data application programming interface (APIs) for IoT data in smart cities and communities
ITU-T	Y.4908	Performance evaluation frameworks of e-health systems in the IoT
ITU-T	Y.AM-SC-reqts	IoT technical requirements and framework for monitoring physical city assets
ITU-T	Y.BC-SON	Framework of blockchain-based self-organization networking in IoT environments
ITU-T	Y.blockchain-terms	Vocabulary for blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
ITU-T	Y.cii	Requirements and reference model of IoT related data from city infrastructure
ITU-T	Y.cnce-IoT-arch	Functional architecture of cellular-radio network capability exposure for smart hospital based on Internet of things
ITU-T	Y.CS-framework	Service requirements and capability framework of IoT-related crowdsourced systems

SDO	Reference	Title
ITU-T	Y.data-MP	Framework for data middle-platform in IoT and smart sustainable cities
ITU-T	Y.dec-IoT-arch	Decentralized IoT communication architecture based on information centric networking and blockchain
ITU-T	Y.DFR-SM	Data format requirements and protocols for remote data collection in smart metering systems
ITU-T	Y.DPM-framework	Data processing and management framework for IoT and smart cities and communities
ITU-T	Y.DPM-interop	Requirements and functional model to support data interoperability in IoT environments
ITU-T	Y.DPM-qm	Requirements and functional model to support data quality management in IoT
ITU-T	Y.FW.IC.MDSC	Framework of identification and connectivity of moving devices in smart city
ITU-T	Y.IoT-AOS-prot	Protocols of supporting autonomic operations in the Internet of things
ITU-T	Y.IoT-AR	Framework for AR and VR based control in IoT
ITU-T	Y.IoT-Ath-SC	Framework of IoT-devices authentication in smart city
ITU-T	Y.IoT-AV-Reqts	Requirements and capability framework of IoT infrastructure to support network-assisted autonomous vehicles
ITU-T	Y.IoT-BPM-reqts	Specific requirements of the Internet of things for business process management
ITU-T	Y.IoT-CEIHMon-Reqts	Requirements of IoT-based civil engineering infrastructure health monitoring system
ITU-T	Y.IoT-CSIADE-fw	Reference framework of converged service for identification and authentication for IoT devices in decentralized environment
ITU-T	Y.IoT-EC-GW	Capabilities and framework of edge computing-enabled gateway in the IoT
ITU-T	Y.IoT-SQAF	Sensing quality assessment framework of IoT systems
ITU-T	Y.IoT-UAS-Reqts	Use cases, requirements and capabilities of unmanned aircraft systems for Internet of things
ITU-T	Y.RA-FML	Requirements and reference architecture of IoT and smart city & community service based on federated machine learning
ITU-T	Y.SCC-Reqts	Common requirements and capabilities of smart cities and communities from IoT and ICT perspectives
ITU-T	Y.Sup.SmartAgri-usecases	Use cases of IoT based smart agriculture
ITU-T	Y.Sup.Web-DM	Web based data model for IoT and smart city
ITU-T	Y.Sup-IoT-Eco-Plan	Framework for Internet of things ecosystem master plan
ITU-T	Y.TM.DM-API	IoT Device Management API REST Specification
ITU-T	Y.TM.SM-API	IoT Service Management API REST Specification
ITU-T	YSTR.Feas-DID-IoT	Feasibility of Decentralised Identifiers (DIDs) in IoT
ITU-T	YSTR-IADIoT	Intelligent Anomaly Detection System for IoT

8.1.4 Digital Trust related Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Digital Trust for Internet of Things (IoT).

SDO	Reference	Title
ISO/IEC JTC 1	15045-3-1	Information technology — Home Electronic System (HES) gateway — Part 3-1: Introduction to privacy, security, and safety
ISO/IEC JTC 1	15045-3-2	Information technology — Home Electronic System — HES Gateway Privacy Framework
ISO/IEC JTC 1	27400	Cybersecurity -- IoT security and privacy -- Guidelines
ISO/IEC JTC 1	27402	Cybersecurity -- IoT security and privacy -- Device baseline requirements
ISO/IEC JTC 1	27403	Cybersecurity -- IoT security and privacy -- Guidelines for IoT-domotics
ISO/IEC JTC 1	30147	Information technology -- Internet of things -- Methodology for trustworthiness of IoT system/service
ISO/IEC JTC 1	30149	Internet of Things (IoT) -- Trustworthiness framework
ISO/IEC JTC 1	TS 30168	Internet of Things (IoT) - Generic Trust Anchor Application Programming Interface for Industrial IoT Devices
ISO/IEC JTC 1	JTC1-SC41-172	Internet of Things (IoT) - Trustworthiness Principles
ETSI	TS 103 486	CYBER; Identity Management and Discovery for IoT
ETSI	TS 103 646	MTS; Test Specification for foundational Security IoT-Profile
ETSI	TS 103 701	CYBER; Cybersecurity assessment for consumer IoT products
ETSI	TS 118 103	oneM2M; Security solutions (oneM2M TS-0003 version 3.10.0 Release 3)
ETSI	TS 118 116	oneM2M; Secure Environment Abstraction (oneM2M TS-0016 version 3.0.0 Release 3)
ETSI	TS 118 129	oneM2M; Security Abstract Test Suite & Implementation eXtra Information for Test
ETSI	TR 118 508	oneM2M; Security (oneM2M TR-0008 version 2.0.0 Release 2A)
ETSI	TR 118 519	oneM2M Dynamic Authorization for IoT (oneM2M TR-0019 version 2.0.0 Release 2)
ETSI	TR 118 538	oneM2M; Developer guide: Implementing security example (oneM2M TR-0038 v2.0.0 release 2A)
ETSI	DTR/CYBER-0057	CYBER; Guide to Cyber Security for Consumer Internet of Things
ITU-T	X.1366	Aggregate message authentication scheme for IoT environment (X. amas-iot)
ITU-T	X.1367	Standard format for Internet of things error logs for security incident operations
ITU-T	X.iotsec-4	Security requirements for IoT devices and gateway
ITU-T	X.sc-iot	Security controls for Internet of Things (IoT) systems
ITU-T	X.secup-iot	Secure software update for IoT devices
ITU-T	X.ssp-iot	Security requirements and framework for IoT service platform
ITU-T	Y.Data.Sec.IoT-Dev	Requirements of data security for the heterogeneous IoT devices
ITU-T	Y.IoT-IoD-PT	Identity of IoT devices based on secure procedures to enhance trust of IoT systems

SDO	Reference	Title
ITU-T	Y.IoT-Smartcity-Risk	Reference framework of cybersecurity risk management of IoT ecosystems on smart cities

8.2 Cloud Computing

8.2.1 Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Cloud Computing.

SDO	Reference	Title
ISO/IEC JTC 1 / ITU-T	17788:2014 / Y.3500 (08/2014)	Information technology -- Cloud computing -- Overview and vocabulary
ISO/IEC JTC 1 / ITU-T	17789:2014 / Y.3502 (08/2014)	Information technology -- Cloud computing -- Reference architecture
ISO/IEC JTC 1	17826:2016	Information technology -- Cloud Data Management Interface (CDMI)
ISO/IEC JTC 1	19086-1:2016	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts
ISO/IEC JTC 1	19086-2:2018	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model
ISO/IEC JTC 1	19086-3:2017	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements
ISO/IEC JTC 1	19831:2015	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol -- An Interface for Managing Cloud Infrastructure
ISO/IEC JTC 1	19941:2017	Information technology -- Cloud computing -- Interoperability and portability
ISO/IEC JTC 1	19944:2017	Information technology -- Cloud computing -- Cloud services and devices: Data flow, data categories and data use
ISO/IEC JTC 1	TR 20000-9:2015	Information technology -- Service management -- Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
ISO	TR 22428-1	Managing records in cloud computing environments — Part 1: Issues and concerns
ISO/IEC JTC 1	22624:2020	Information technology — Cloud computing — Taxonomy based data handling for cloud services
ISO/IEC JTC 1	TR 22678:2019	Information technology -- Cloud computing – Guidance for policy development
ISO/IEC JTC 1	TS 23167:2020	Information technology — Cloud computing — Common technologies and techniques
ISO/IEC JTC 1	TR 23187:2020	Information technology — Cloud computing — Interacting with cloud service partners (CSNs)
ISO/IEC JTC 1	TR 23188:2020	Information technology — Cloud computing — Edge computing landscape

SDO	Reference	Title
ISO/IEC JTC 1	TR 23613:2020	Information technology — Cloud computing — Cloud service metering elements and billing modes
ISO/IEC JTC 1	TR 23951:2020	Information technology — Cloud computing — Guidance for using the cloud SLA metric model
ETSI	SR 003 381 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Identification of Cloud user needs
ETSI	SR 003 382 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Cloud Computing Standards and Open Source; Optimizing the relationship between standards and Open Source in Cloud Computing
ETSI	SR 003 392 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards
ETSI	TR 102 997 V1.1.1 (04/2010)	CLOUD; Initial analysis of standardization requirements for Cloud services
ETSI	TS 103 125 V1.1.1 (11/2012)	CLOUD; SLAs for Cloud services
ETSI	TR 103 126 V1.1.1 (11/2012)	CLOUD; Cloud private-sector user recommendations
ETSI	TS 103 142 V1.1.1 (04/2013)	CLOUD; Test Descriptions for Cloud Interoperability
ETSI	GS/NFV-EVE011 V3.1.1 (10/2018)	Network Functions Virtualisation (NFV) Release 3; Software Architecture; Specification of the Classification of Cloud Native VNF implementations
ETSI	GR/NFV-IFA029 V3.3.1 (11/2019)	Network Functions Virtualisation (NFV); Software Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"
ITU-T	F.743.2 (07/2016)	Requirements for cloud storage in visual surveillance
ITU-T	F.743.8 (05/2019)	Requirements for cloud computing platform supporting a visual surveillance system
ITU-T	FG Cloud TR Part 1 (02/2012)	Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements
ITU-T	FG Cloud TR Part 2 (02/2012)	Technical Report: Part 2: Functional requirements and reference architecture
ITU-T	FG Cloud TR Part 3 (02/2012)	Technical Report: Part 3: Requirements and framework architecture of cloud infrastructure
ITU-T	FG Cloud TR Part 4 (02/2012)	Technical Report: Part 4: Cloud Resource Management Gap Analysis
ITU-T	FG Cloud TR Part 6 (02/2012)	Technical Report: Part 6: Overview of SDOs involved in cloud computing
ITU-T	FG Cloud TR Part 7 (02/2012)	Technical Report: Part 7: Cloud computing benefits from telecommunication and ICT perspectives
ITU-T	H.626.2 (12/2017)	Architectural requirements for cloud storage in video surveillance
ITU-T	M.3071 (01/2018)	Cloud-based network management functional architecture
ITU-T	M.3371 (10/2016)	Requirements for service management in cloud-aware telecommunication management system

SDO	Reference	Title
ITU-T	M.3372 (08/2018)	Requirements for resource management in cloud-aware telecommunication management systems
ITU-T	Q Suppl. 65 (07/2014)	Draft Q Supplement 65 to Q.39xx-series Recommendations (Q.Supp-CCI) Cloud computing interoperability activities
ITU-T	Q.3914 (01/2018)	Set of parameters of cloud computing for monitoring
ITU-T	Q.4040 (02/2016)	The framework and overview of cloud computing interoperability testing
ITU-T	Q.4041.1 (01/2018)	Cloud computing infrastructure capabilities interoperability testing - part 1: Interoperability testing between CSC and CSP
ITU-T	Q.4042.1 (12/2018)	Cloud interoperability testing about web application - part 1: Interoperability testing between CSC and CSP
ITU-T	Supplement 49 to ITU-T Y.3500-series (11/2018)	Cloud Computing standardization roadmap
ITU-T	Y.3500-series Supplement 46 (11/2017)	Scenarios of Implementing Cloud Computing in networks of developing countries
ITU-T	Y.3501 (06/2016)	Cloud computing framework and high-level requirements (edition 2 under development)
ITU-T	Y.3503 (05/2014)	Requirements for desktop as a service
ITU-T	Y.3504 (06/2016)	Functional architecture for Desktop as a Service
ITU-T	Y.3505 (05/2018)	Cloud computing – Overview and functional requirements for data storage federation
ITU-T	Y.3506 (05/2018)	Cloud Computing Requirements for Cloud Service Brokerage
ITU-T	Y.3507 (12/2018)	Cloud computing-Functional requirements of physical machine
ITU-T	Y.3508 (08/2019)	Cloud computing - Overview and high-level requirements of distributed cloud
ITU-T	Y.3509 (12/2019)	Cloud computing - Functional architecture for data storage federation
ITU-T	Y.3510 (02/2016)	Cloud computing infrastructure requirements (edition 2 under development)
ITU-T	Y.3511 (03/2014)	Framework of inter-cloud computing
ITU-T	Y.3512 (08/2014)	Cloud computing - Functional requirements of Network as a Service
ITU-T	Y.3513 (08/2014)	Cloud computing - Functional requirements of Infrastructure as a Service
ITU-T	Y.3515 (07/2017)	Cloud computing - Functional architecture of Network as a Service
ITU-T	Y.3516 (09/2017)	Cloud computing - Functional architecture of inter-cloud computing
ITU-T	Y.3518 (12/2018)	Cloud computing - functional requirements of inter-cloud data management
ITU-T	Y.3519 (12/2018)	Cloud computing - Functional architecture of Big Data as a Service
ITU-T	Y.3520 (09/2015)	Cloud computing framework for end to end resource management (edition 2 under development)
ITU-T	Y.3521/M.3070 (03/2016)	Overview of end-to-end cloud computing management
ITU-T	Y.3522 (09/2016)	End-to-end cloud service lifecycle management requirements

SDO	Reference	Title
ITU-T	Y.3523 (08/2019)	Metadata framework for NaaS service lifecycle management
ITU-T	Y.3524 (12/2019)	Cloud computing maturity requirements and framework
ITU-T	Y.3600 (11/2015)	Big data – Cloud computing based requirements and capabilities

8.2.2 Digital Trust related Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Digital Trust for Cloud Computing.

SDO	Reference	Title
ISO/IEC JTC 1 / ITU-T	27017:2015 / X.1631 (07/2015)	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC JTC 1	27018:2019	Information technology -- Security techniques – Guidance for the assessment of information security controls
ISO/IEC JTC 1	27036-4:2016	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ISO/IEC JTC 1	21878:2018	Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers
ISO/IEC JTC 1	19086-4:2019	Information technology -- Cloud computing – agreement (SLA) framework – Part 4: Components of security and protection of PII
ISO/IEC JTC 1	TR 23186:2018	Information technology -- Cloud computing -- Framework of trust for processing of multi-sourced data
ETSI	SR 003 391 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing
ETSI	TR 103 304 V1.1.1 (07/2016)	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ETSI	TS 103 458 v1.1.1 (06/2018)	Application of Attribute Based Encryption for PII and personal data protection on IoT devices, WLAN, Cloud and mobile services – High-level requirements
ETSI	TS 103 532 V1.1.1 (03/2018)	Attribute Based Encryption for Attribute Based Access Control
ITU-T	FG Cloud TR Part 5 (02/2012)	Technical Report: Part 5: Cloud security
ITU-T	X.1601 (10/2015)	Security framework for cloud computing (edition 2 under development)
ITU-T	X.1602 (03/2016)	Security requirements for software as a service application environments
ITU-T	X.1603 (03/2018)	Data security requirements for the monitoring service of cloud computing
ITU-T	X.1604 (03/2020)	Security requirements of network as a service (NaaS) in cloud computing
ITU-T	X.1605 (03/2020)	Security requirements of public infrastructure as a service (IaaS) in cloud computing
ITU-T	X.1641 (09/2016)	Guidelines for cloud service customer data security
ITU-T	X.1642 (03/2016)	Guidelines of operational security for cloud computing

SDO	Reference	Title
ITU-T	Y.3514 (05/2017)	Cloud computing - Trusted inter-cloud computing framework and requirements
ITU-T	Y.3517 (12/2018)	Cloud Computing - Overview of Inter-Cloud Trust Management

8.2.3 Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Cloud Computing.

SDO	Reference	Title
ISO/IEC JTC 1	5140	Information technology — Cloud computing — Concepts for multi-cloud and other interoperation of multiple cloud services
ISO/IEC JTC 1	19944-1	Cloud computing — Cloud services and devices: data flow, data categories and data use — Part 1: Fundamentals
ISO/IEC JTC 1	19944-2	Cloud computing and distributed platforms — Cloud services and devices: data flow, data categories and data use — Part 2: Guidance on application and extensibility
ISO/IEC JTC 1	22123-1	Information technology — Cloud computing — Part 1: Terminology
ISO/IEC JTC 1	22123-2	Information technology — Cloud computing — Part 2: Concepts
ISO/IEC JTC 1	23751	Information Technologies -- Cloud Computing and distributed platforms – Data sharing agreement (DSA) framework
ITU-T	H.CCVS	Architecture for cloud computing in visual surveillance
ITU-T	J.cloud-vr	E2E Network Requirements of Cloud-VR Services
ITU-T	Y.3505 (Rev)	Cloud computing - Overview and functional requirements for data storage federation
ITU-T	Y.3525	Cloud computing - Requirements for cloud service development and operation management
ITU-T	Y.3530	Cloud computing - Functional requirements for blockchain as a service
ITU-T	Y.3531	Cloud computing - Functional requirements for machine learning as a service
ITU-T	Y.cccm-reqts	Cloud Computing - Requirements for Containers
ITU-T	Y.cccnp-reqts	Cloud computing - Functional requirements of cloud native PaaS
ITU-T	Y.CCDCFA	Cloud computing - Distributed cloud functional architecture
ITU-T	Y.ccdm-reqts	Cloud computing - Framework and functional requirements of cloud data mobility management
ITU-T	Y.ccecm	Cloud Computing - Requirements of edge cloud management
ITU-T	Y.ccfrcm	Cloud Computing - Framework and requirements of container management in inter-cloud
ITU-T	Y.ccvnf-dm	Cloud computing - Data model framework for NaaS OSS virtualized network function
ITU-T	Y.csb-arch	Cloud Computing -Functional architecture for cloud service brokerage
ITU-T	Y.e2efapm	Cloud Computing - End-to-end fault and performance management framework of virtual network services in inter-cloud

SDO	Reference	Title
ITU-T	Y.ecloud-reqts	Cloud computing - Functional requirements of edge cloud
ITU-T	Y.mc-reqts	Cloud Computing -Functional requirements of cloud service partner for multi-cloud
ITU-T	Y.RaaS-reqts	Cloud Computing - Functional requirements for Robotics as a Service

8.2.4 Digital Trust related Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Digital Trust for Cloud Computing.

SDO	Reference	Title
ISO/IEC JTC 1	TR 3445	Information technology -- Cloud computing -- Audit of cloud services
ISO	TR 21332	Health informatics -- Cloud computing considerations for health information systems security and privacy
ISO	TR 22428-1	Managing records in cloud computing environments -- Part 1: Issues and concerns
ITU-T	X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment
ITU-T	X.nssa-cc	Requirements of network security situational awareness platform for cloud computing
ITU-T	X.sgcc	Security guidelines for container in cloud computing environment
ITU-T	Y.ccrm	Cloud computing - Framework of risk management
ITU-T	X.sgcd	Security guidelines for distributed cloud
ITU-T	X.sr-cphr	Security requirements of cloud-based platform under low latency and high reliability application scenarios

8.3 Artificial Intelligence and Big Data

8.3.1 Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Artificial Intelligence and Big Data.

SDO	Reference	Title
ISO/IEC JTC 1	9075-1:2016	Information technology -- Database languages -- SQL -- Part 1: Framework (SQL/Framework)
ISO/IEC JTC 1	9075-9:2016	Information technology -- Database languages -- SQL -- Part 9: Management of External Data (SQL/MED)
ISO/IEC JTC 1	9075-15:2019	Information technology -- Database languages -- SQL -- Part 15: Multi-dimensional arrays (SQL/MDA)
ISO/IEC JTC 1	11179-1:2015	Information technology -- Metadata registries (MDR) -- Part 1: Framework

SDO	Reference	Title
ISO/IEC JTC 1	TR 11179-2:2019	Information technology -- Metadata registries (MDR) -- Part 2: Classification
ISO/IEC JTC 1	11179-3:2013	Information technology -- Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes
ISO/IEC JTC 1	11179-4:2004	Information technology -- Metadata registries (MDR) -- Part 4: Formulation of data definitions
ISO/IEC JTC 1	11179-5:2015	Information technology -- Metadata registries (MDR) -- Part 5: Naming principles
ISO/IEC JTC 1	11179-6:2015	Information technology -- Metadata registries (MDR) -- Part 6: Registration
ISO/IEC JTC 1	13249-3:2016	Information technology — Database languages — SQL multimedia and application packages — Part 3: Spatial
ISO/IEC JTC 1	13249-6:2006	Information technology — Database languages — SQL multimedia and application packages — Part 6: Data mining
ISO/IEC JTC 1	TR 19075-8:2019	Information technology database languages -- SQL technical reports -- Part 8: Multi-dimensional arrays (SQL/MDA)
ISO/IEC JTC 1	19503:2005	Information technology -- XML Metadata Interchange (XMI)
ISO/IEC JTC 1	19763-1:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 1: Framework
ISO/IEC JTC 1	19763-3:2010	Information technology -- Metamodel framework for interoperability (MFI) -- Part 3: Metamodel for ontology registration
ISO/IEC JTC 1	19763-5:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 5: Metamodel for process model registration
ISO/IEC JTC 1	19763-6:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 6: Registry Summary
ISO/IEC JTC 1	19763-7:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 7: Metamodel for service model registration
ISO/IEC JTC 1	20546:2019	Information technology -- Big Data -- Overview and Vocabulary
ISO/IEC JTC 1	TR 20547-1	Information technology -- Big data reference architecture -- Part 1: Framework and application process
ISO/IEC JTC 1	TR 20547-2:2018	Information technology – Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
ISO/IEC JTC 1	20547-3:2020	Information technology — Big data reference architecture — Part 3: Reference architecture
ISO/IEC JTC 1	TR 20547-5:2018	Information technology -- Big data reference architecture – Part 5: Standards roadmap
ISO/IEC JTC 1	20944-1:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 1: Framework, common vocabulary, and common provisions for conformance
ISO/IEC JTC 1	20944-2:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 2: Coding bindings
ISO/IEC JTC 1	20944-3:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 3: API bindings
ISO/IEC JTC 1	20944-4:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 4: Protocol bindings

SDO	Reference	Title
ISO/IEC JTC 1	24707:2018	Information technology -- Common Logic (CL) -- A framework for a family of logic-based languages
ETSI	GS ENI 001 V1.1.1 (04/2018)	Experiential Networked Intelligence (ENI); ENI use cases
ETSI	GS ENI 002 V2.1.1 (09/2019)	Experiential Networked Intelligence (ENI); ENI requirements
ETSI	GS ENI 003 V1.1.1 (06/2018)	Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis
ETSI	GS ENI 004 V2.1.1 (10/2019)	Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI
ETSI	GS ENI 005 V1.1.1 (09/2019)	Experiential Networked Intelligence (ENI); System Architecture
ETSI	GS ENI 006 Ver. 2.1.1 (05/2020)	Experiential Networked Intelligence (ENI); Proof of Concepts Framework
ETSI	GR ENI 007 Ver. 1.1.1 (11/2019)	Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks
ETSI	TS 129 520 – V16.4.0 (08/2020)	5G; 5G System; Network Data Analytics Services
ETSI	GR ZSM 005 V1.1.1 (05/2020)	Zero-touch network and Service Management (ZSM); Means of Automation
ITU-T	E.475 (01/2020)	Guidelines for Intelligent Network Analytics and Diagnostics
ITU-T	F.743.7 (05/2019)	Requirements for big data enhanced visual surveillance services
ITU-T	F.743.20 (08/2020)	Assessment framework for big data infrastructure
ITU-T	L.1305 (11/2019)	Data centre infrastructure management system based on big data and artificial intelligence technology
ITU-T	Y.3519 (12/2018)	Cloud computing - Functional architecture of Big Data as a Service
ITU-T	Y.3600 (11/2015)	Big data - Cloud computing based requirements and capabilities
ITU-T	Y.3601 (05/2018)	Big data - framework and requirements for data exchange
ITU-T	Y.3602 (12/2018)	Big data - Functional requirements for data provenance
ITU-T	Y.3603 (12/2019)	Big data - Requirements and conceptual model of metadata for data catalogue
ITU-T	Y.3604 (02/2020)	Big data - Overview and requirements for data preservation
ITU-T	Y.3600-series Supplement 40 (07/2016)	Big Data Standardization Roadmap
ITU-T	Supplement 65 to ITU-T Y.3600-series (07/2020)	Big Data Adoption in Developing Countries
ITU-T	Y.3650 (01/2018)	Framework of big data driven networking
ITU-T	Y.3651 (12/2018)	Big-data-driven networking - mobile network traffic management and planning

SDO	Reference	Title
ITU-T	Y.3652 (06/2020)	Big data driven networking – requirements
ITU-T	Supplement 50 to ITU-T Y.3650-series (11/2018)	Use case and application scenario of big data driven networking
ITU-T	Y.4114 (07/2017)	Specific requirements and capabilities of the IoT for Big Data
ITU-T	Y.4470 (08/2020)	Reference architecture of artificial intelligence service exposure for smart sustainable cities
ITU-T	Y.Suppl.63 to ITU-T Y.4000 series (07/2020)	Unlocking Internet of things with artificial intelligence

8.3.2 Digital Trust related Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Digital Trust for Artificial Intelligence and Big Data.

SDO	Reference	Title
ISO/IEC JTC 1	15944-5:2008	Information technology -- Business operational view -- Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints
ISO/IEC JTC 1	15944-7:2009	Information technology -- Business operational view -- Part 7: eBusiness vocabulary
ISO/IEC JTC 1	15944-8:2012	Information technology -- Business operational view -- Part 8: Identification of privacy protection requirements as external constraints on business transactions
ISO/IEC JTC 1	15944-9:2015	Information technology -- Business operational view -- Part 9: Business transaction traceability framework for commitment exchange
ISO/IEC JTC 1	15944-12:2020	Information technology -- Business operational view -- Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)
ISO/IEC JTC 1	20889:2018	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC JTC 1	TR 24028:2020	Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
ITU-T	X.1147 (11/2018)	Security requirements and framework for big data analytics in mobile internet services

8.3.3 Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Artificial Intelligence and Big Data.

SDO	Reference	Title
ISO/IEC JTC 1	TS 4213	Information technology — Artificial Intelligence — Assessment of machine learning classification performance
ISO/IEC JTC 1	5059	Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality Model for AI-based systems
ISO/IEC JTC 1	5207	Information technology — Data usage — Terminology and use cases
ISO/IEC JTC 1	5212	Information technology — Data usage — Guidance for data usage
ISO/IEC JTC 1	5259-1	Data quality for analytics and ML — Part 1: Overview, terminology, and examples
ISO/IEC JTC 1	5259-3	Data quality for analytics and ML — Part 3: Data Quality Management Requirements and Guidelines
ISO/IEC JTC 1	5259-4	Data quality for analytics and ML — Part 4: Data quality process framework
ISO/IEC JTC 1	5338	Information technology — Artificial intelligence — AI system life cycle processes
ISO/IEC JTC 1	5339	Information Technology — Artificial Intelligence — Guidelines for AI applications
ISO/IEC JTC 1	5392	Information technology — Artificial intelligence — Reference architecture of knowledge engineering
ISO/IEC JTC 1	15944-1	Information technology -- Business operational view -- Part 1: Operational aspects of open-edi for implementation
ISO/IEC JTC 1	15944-10	Information technology -- Business operational view -- Part 10: IT-enabled coded domains as semantic components in business transactions
ISO/IEC JTC 1	TR 15944-14	Information technology -- Business operational view -- Part 14: Open-edi, model and cloud computing architecture
ISO/IEC JTC 1	22989	Artificial Intelligence -- Concepts and Terminology
ISO/IEC JTC 1	23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
ISO/IEC JTC 1	TR 24027	Information technology -- Artificial Intelligence (AI) -- Bias in AI systems and AI aided decision making
ISO/IEC JTC 1	TR 24030	Information technology -- Artificial Intelligence (AI) -- Use cases
ISO/IEC JTC 1	TR 24372	Information technology -- Artificial intelligence (AI) -- Overview of computational approaches for AI systems
ISO/IEC JTC 1	24668	Information technology — Artificial intelligence — Process management framework for Big data analytics
ISO/IEC JTC 1	38507	Information technology -- Governance of IT -- Governance implications of the use of artificial intelligence by organizations
ISO/IEC JTC 1	21838-1	Information technology -- Top-level ontologies -- Part 1: Requirements
ISO/IEC JTC 1	21838-2	Information technology -- Top-level ontologies -- Part 2: Basic Formal Ontology (BFO)

SDO	Reference	Title
ISO/IEC JTC 1	21838-3	Information technology -- Top-level ontologies -- Part 3: Descriptive ontology for linguistic and cognitive engineering (DOLCE)
ISO/IEC JTC 1	21838-4	Information technology -- Top-level ontologies -- Part 4: TUpper
ISO/IEC JTC 1	42001	Information Technology -- Artificial intelligence -- Management system
ISO/IEC JTC 1	39075	Information Technology — Database Languages — GQL
ETSI	GS ENI 005	Experiential Networked Intelligence (ENI); System Architecture
ETSI	GR ENI 008	Experiential Networked Intelligence (ENI); Intent Aware Network Autonomicity
ETSI	GR ENI 009	Experiential Networked Intelligence (ENI); Definition of data processing mechanisms
ETSI	GR ENI 010	Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks
ETSI	GR ENI 011	Experiential Networked Intelligence (ENI); Mapping between ENI architecture and operational systems
ETSI	GR ENI 022	ENI Reactive In-situ Flow Information Telemetry
ETSI	TR 103 821	Autonomic network engineering for the self-managing Future Internet (AFI); Artificial Intelligence (AI) in Test Systems and Testing AI models
ITU-T	F.AI-MLTF	Technical framework for shared machine learning system
ITU-T	F.AI-MKGDS	Requirements for the construction of multimedia knowledge graph database structure based on artificial intelligence
ITU-T	F.AI-SF	Requirements for smart factory based on artificial intelligence
ITU-T	F.SCAI	Requirements for smart class based on artificial intelligence
ITU-T	F.Supp-OCAIB	Overview of convergence of artificial intelligence and blockchain
ITU-T	F.VS-AIMC	Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence
ITU-T	H.AI-SaMD-Req	Requirements for artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD)
ITU-T	H.CUAV-AIF	Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence
ITU-T	H.VSBD	Architecture for big data application in visual surveillance system
ITU-T	HSTP.Med-AI-CCTA	Technical Paper: Guidelines on development and application of artificial intelligence in coronary computed tomography angiography
ITU-T	Study_bigdata	Technical Paper on economic and policy aspects of Big Data in international telecommunication services and networks
ITU-T	Suppl on Y. Sup.airs	Artificial Intelligence Standard Roadmap
ITU-T	Suppl.40 to ITU-T Y-3600 series	Supplement on Big data Standardization roadmap
ITU-T	Y. bDDN-MCMec	Management and control mechanisms of big data driven networking

SDO	Reference	Title
ITU-T	Y.2245	Service model of the Agriculture Information based Convergence Service
ITU-T	Y.3605	Big data - Reference architecture
ITU-T	Y.4470	Reference architecture of artificial intelligence service exposure for smart sustainable cities
ITU-T	Y.Arch-INRA	Functional architecture of intelligent awareness for network requirements
ITU-T	Y.bDDN-FunArch	Functional architecture of big data driven networking
ITU-T	Y.bDDN-MLMec	Mechanisms of machine learning for big data driven networking
ITU-T	Y.bDDN-NSMec	Mechanism of network service provisioning in bDDN
ITU-T	Y.bdi-reqts	Big Data - Overview and functional requirements for data integration
ITU-T	Y.bDPI-Mec	Mechanism of deep packet inspection applied in network big data context
ITU-T	Y.Mec-INSA	Mechanism of intelligent network status awareness
ITU-T	Y.MecTA-ML	Mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning
ITU-T	Y.ML-IMT2020-NA-RAFR	Architecture framework of AI-based network automation for resource adaptation and failure recovery in future networks including IMT-2020

8.3.4 Digital Trust related Under Development Standards (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Digital Trust for Artificial Intelligence and Big Data.

SDO	Reference	Title
ISO/IEC JTC 1	TR 5469	Artificial intelligence — Functional safety and AI systems
ISO/IEC JTC 1	15944-8	Information technology -- Business operational view -- Part 8: Identification of privacy protection requirements as external constraints on business transactions
ISO/IEC JTC 1	15944-9	Information technology -- Business operational view -- Part 9: Business transaction traceability framework for commitment exchange
ISO/IEC JTC 1	15944-17	Information technology -- Business operational view -- Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in EDI and collaboration space context
ISO/IEC JTC 1	20547-4	Information technology -- Big data reference architecture -- Part 4: Security and privacy
ISO/IEC JTC 1	23894	Information technology -- Artificial Intelligence (AI) -- Risk management
ISO/IEC JTC 1	TR 24029-1	Artificial Intelligence (AI) -- Assessment of the robustness of neural networks -- Part 1: Overview
ISO/IEC JTC 1	TR 24029-2	Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods

ISO/IEC JTC 1	TR 24368	Information technology -- Artificial intelligence -- Overview of ethical and societal concerns
ISO/IEC JTC 1	27045	Information technology -- Big data security and privacy -- Processes
ISO/IEC JTC 1	27046	Information technology -- Big data security and privacy -- Implementation guidelines
ETSI	DGR/SAI-001	AI Threat Ontology
ETSI	DGR/SAI-002	Data Supply Chain Report
ETSI	DGS/SAI-003	Security Testing of AI
ETSI	DGR/SAI-004	Securing AI (SAI) Problem Statement
ETSI	DGR/SAI-005	SAI Mitigation Strategy report
ETSI	DGR/SAI-006	Hardware in SAI
CEN-CLC/JTC 13	prEN 17529	Data protection and privacy by design and by default
ITU-T	D.princip_bigdata	policy framework and principles for data protection in the context of big data relating to international telecommunication services
ITU-T	TR.sgfdm	Technical Report: Security guidelines for FHE-based data collaboration in machine learning
ITU-T	TR.cs-ML	Technical Report: Countering spam based on machine learning
ITU-T	X.1750	Guidelines on security of big data as a service for Big Data Service Providers
ITU-T	X.1751	Security guidelines on big data lifecycle management for telecommunication operators
ITU-T	X.icd-schemas	Security data schemas for integrated cyber defence solutions
ITU-T	X.mdcv	Security-related misbehaviour detection mechanism using big data for connected vehicles
ITU-T	X.sgBDIP	Security guidelines for big data infrastructure and platform
ITU-T	X.tf-mpc	Technical framework and application for secure multi-party computation

8.4 Blockchain and Distributed Ledger Technologies

8.4.1 Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Blockchain and Distributed Ledger Technologies.

SDO	Reference	Title
ISO	22739:2020	Blockchain and distributed ledger technologies -- Vocabulary
ISO	TR 23455:2019	Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
ETSI	GS PDL 005 V1.1.1 (2020-03)	Permissioned Distributed Ledger (PDL); Proof of Concepts Framework

SDO	Reference	Title
ETSI	GR PDL 001 V1.1.1 (2020-03)	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies
ITU-T	F.751.0 (08/2020)	Requirements for distributed ledger systems
ITU-T	F.751.1 (08/2020)	Assessment criteria for distributed ledger technology (DLT) platforms
ITU-T	F.751.2 (08/2020)	Reference framework for distributed ledger technologies
ITU-T	Y.2342 (12/2019)	Scenarios and Capability Requirements of Blockchain in Next Generation Network Evolution
ITU-T	Y.4464 (01/2020)	Framework of blockchain of things as decentralized service platform
ITU-T	Y.Suppl.62 to ITU-T Y.4000 series (07/2020)	Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects

8.4.2 Digital Trust related Published Standards

This section lists (non-exhaustive list) the standards already published by the recognized SDO related to Digital Trust for Blockchain and Distributed Ledger Technologies.

SDO	Reference	Title
ISO	TR 23244:2020	Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations
ITU-T	X.1401 (11/2019)	Security threats of distributed ledger technology
ITU-T	X.1402 (07/2020)	Security framework for distributed ledger technology

8.4.3 Standards Under Development (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Blockchain and Distributed Ledger Technologies.

SDO	Reference	Title
ISO	TR 3242	Blockchain and distributed ledger technologies -- Use cases
ISO	23257	Blockchain and distributed ledger technologies -- Reference architecture
ISO	TS 23258	Blockchain and distributed ledger technologies -- Taxonomy and Ontology
ISO	TS 23259	Blockchain and distributed ledger technologies -- Legally binding smart contracts
ETSI	GR PDL 002	PDL Applicability and compliance to data processing requirements
ETSI	GR PDL 003	PDL Application Scenarios
ETSI	GR PDL 004	PDL; Smart Contracts Permissioned Distributed Ledgers; System Architecture and Functional Specification

SDO	Reference	Title
ETSI	GR PDL 006	Inter-Ledger Interoperability
ETSI	MI/PDL-007	Research Landscape
ITU-T	F.BVSSI	Scenarios and requirements for blockchain in visual surveillance system interworking
ITU-T	F.DLIM-AHFS	Requirements of the distributed ledger incentive model for agricultural human factor services
ITU-T	F.DLS-SHFS	Requirements of distributed ledger systems (DLS) for secure human factor services
ITU-T	F.DLT.HC	Requirements of distributed ledger technologies (DLT) for human-care services
ITU-T	F.DLT.PHR	Service models of distributed ledger technologies (DLT) for personal health records (PHRs)
ITU-T	F.DLT-FIN	Financial distributed ledger technology application guideline
ITU-T	F.HFS-BC	Requirements and framework for blockchain-based human factor service models
ITU-T	F.Supp-OCAIB	Overview of convergence of artificial intelligence and blockchain
ITU-T	H.DLT-INV	General framework of DLT-based invoices
ITU-T	H.DLT-TFR	Technical framework for DLT regulation
ITU-T	L.Energy_Crypto_currency	Energy consumption of crypto currency
ITU-T	M.immbs	Information model for management of blockchain system
ITU-T	M.rmbs	Requirements for management of blockchain system
ITU-T	Q.BaaS-iop-reqts	Interoperability testing requirements of blockchain as a service
ITU-T	X.dlt-td	Terms and definitions for distributed ledger technology
ITU-T	Y.3530	Cloud computing - Functional requirements for blockchain as a service
ITU-T	Y.4560	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities
ITU-T	Y.4561	Blockchain-based Data Management for supporting Internet of things and smart cities and communities
ITU-T	Y.4907	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities
ITU-T	Y.BC-SON	Framework of blockchain-based self-organization networking in IoT environments
ITU-T	Y.blockchain-terms	Vocabulary for blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
ITU-T	Y.dec-IoT-arch	Decentralized IoT communication architecture based on information centric networking and blockchain
ITU-T	Y.IoT-rf-dlt	OID-based Resolution framework for transaction of distributed ledger assigned to IoT resources
ITU-T	Y.NRS-DLT-reqts	Scenarios and requirements of network resource sharing based on distributed ledger technology
ITU-T	Y.SCid-fr	Requirements and converged framework of self-controlled identity based on blockchain

8.4.4 Digital Trust related Under Development Standards (Under Study)

This section lists (non-exhaustive list) the standards under development in the recognized SDO related to Digital Trust for Blockchain and Distributed Ledger Technologies.

SDO	Reference	Title
ISO	TR 23245	Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities
ISO	TR 23249	Blockchain and distributed ledger technologies -- Overview of existing DLT systems for identity management
ISO	TR 23576	Blockchain and distributed ledger technologies -- Security management of digital asset custodians
ISO	TS 23635	Blockchain and distributed ledger technologies -- Guidelines for governance
ITU-T	H.DLT-DE	Digital evidence services based on distributed ledger technologies
ITU-T	H.DLT-GTI	DLT governance and Technical interoperability Framework
ITU-T	HSTP.DLT-Risk	DLT-based application development risks and their mitigations
ITU-T	X.1403	Security guidelines for using DLT for decentralized identity management
ITU-T	X.BaaS-sec	Guideline on DLT as a service (BaaS) security
ITU-T	X.das-mgt	Security threats and requirements for data access and sharing management system based on distributed ledger technology
ITU-T	X.sa-dlt	Security assurance for distributed ledger technology
ITU-T	X.sc-dlt	Security controls for distributed ledger technology
ITU-T	X.srip-dlt	Security requirements for intellectual property management based on distributed ledger technology
ITU-T	X.ss-dlt	Security services based on distributed ledger technology
ITU-T	X.stov	Security threats to online voting using distributed ledger technology
ITU-T	X.str-dlt	Security threats and requirements for digital payment services based on distributed ledger technology
ITU-T	X.tf-spd-dlt	Technical framework for secure software programme distribution mechanism based on distributed ledger technology

AUTHORS AND CONTACTS

ILNAS

Southlane Tower I – 1, Avenue du Swing
L-4367 Belvaux

Email: info@ilnas.etat.lu

Phone: (+352) 24 77 43 00

<https://portail-qualite.public.lu/fr.html>


 The logo for ILNAS features the letters 'ILNAS' in a serif font. The 'I' and 'L' are blue, while the 'N' is yellow. The 'A', 'S', and 'S' are blue.

Institut luxembourgeois de la normalisation,
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS is an administration under the supervision of the Minister of the Economy in Luxembourg. It was created on the basis of the law of May 20, 2008 (which has been repealed by the law of July 4, 2014, regarding the reorganization of ILNAS and the law of February 17, 2017 modifying the law of July 4, 2014 regarding the reorganization of ILNAS) and started its activities on June 1, 2008. For reasons of complementarity, effectiveness and transparency as well as for purposes of administrative simplification, ILNAS is in charge of several administrative and technical legal missions that were previously the responsibility of different public structures. These assignments have been strengthened and new tasks have since been assigned to ILNAS corresponding to a network of skills for competitiveness and consumer protection.

ANEC G.I.E.

Southlane Tower I – 1, Avenue du Swing
L-4367 Belvaux

Email: anec@ilnas.etat.lu

Phone: (+352) 24 77 43 70

<https://portail-qualite.public.lu/fr.html>



ANEC

AGENCE POUR LA NORMALISATION ET
L'ÉCONOMIE DE LA CONNAISSANCE

The Interest Economic Grouping “*Agence pour la Normalisation et l’Economie de la Connaissance*” (ANEC G.I.E.) was created in October 2010 by ILNAS, “*Chambre de Commerce*”, “*Chambre des Métiers*” and STATEC. It is actually divided into 3 departments: Standardization, Metrology and Budget and Administration. The role of the standardization department of ANEC G.I.E. is to implement the national standardization strategy established by ILNAS in order to support the development of standardization activities at national level and to promote the benefits of participating in the standardization process.





ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation
et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : info@ilnas.etat.lu

www.portail-qualite.lu