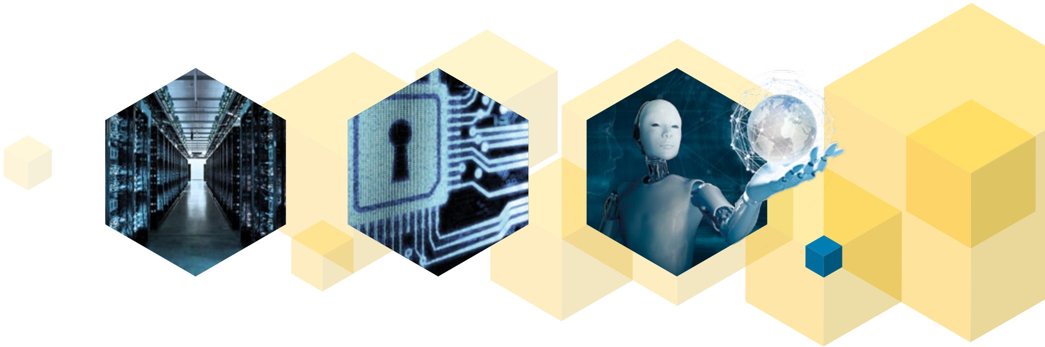
ILNAS

STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 1.0 · November 2018



ANEC

STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 1.0 · November 2018

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

FOREWORD

Technical standardization and standards play an important role in the support of economy development. They can provide, for example, a guide of the best practices for services and product development, governance, guarantee quality and assessment, safety, etc. Nowadays, almost every professional sector relies on standards to perform its daily activities and provide services in an efficient manner. Standards remain under a voluntary application scheme, but often they are a real added value in order to comply with legislation. Those standards are considered as a source of benefits in each sector of the economy and it is particularly true in the Information and Communication Technology (ICT) sector, which supports all the other economic developments.

Indeed, the ICT sector has gained more and more importance in the society as a whole in the last decades. The rapid evolution of the technologies and their usages in our daily lives are drawing a new paradigm in which ICT has an increasing role. The ability of all the "things" to be connected, to communicate between each other and to collect information is deeply changing the world we know and we are probably only at the beginning of this transformation where ICT become Smart. In this context, technical standardization plays a key role, for example to connect all the 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 this state of fact and an ambitious development strategy is led by the government since several years, not only to be part of this transformation, but also to take a major role in the future of the digital landscape. To support this development, the "*Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services"* (ILNAS) has drawn up the "Luxembourg Standardization Strategy 2014-2020"[1], signed by the Minister of the Economy, in which the ICT sector is one of the cornerstones.

In addition to the legal missions carried out by ILNAS in the ICT domain, the Institute also benefits from the support of the Economic Interest Grouping "*Agence pour la Normalisation et l'Économie de la Connaissance*" (ANEC G.I.E.) to strengthen the national ICT sector involvement in standardization work, in accordance with the "Luxembourg's policy on ICT technical standardization 2015-2020"[2].

In this frame, with the support of ANEC G.I.E., ILNAS has launched several activities dedicated to reinforce the ICT-related standardization landscape at the national level in terms of education and involvement of stakeholders. Some concrete examples are the creation of a University certificate "*Smart ICT for Business Innovation*" in collaboration with the University of Luxembourg or the current development of a research program[3] on Digital Trust for Smart ICT with the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg. This research program focuses on three important pillars in the Smart ICT landscape - Cloud Computing, Internet of Things and Big Data - notably considering Digital Trust aspects related to these technologies. The main objective of this collaboration is to facilitate the development of a Master degree "*Smart Secure ICT for Business Innovation*" at the horizon 2020. A first result of this program was the publication of a White Paper "Data Protection and Privacy in Smart ICT"[4] in October 2018.

Another axe of the policy on ICT technical standardization consists in strengthening the normative culture about ICT technical standardization at national level. In this frame, White Papers on different Smart ICT topics have been drawn-up along recent years, such as on "Internet of Things"[5], "Blockchain and Distributed Ledger Technologies"[6] or "Digital Trust for Smart ICT"[7]. In parallel, this Standards Analysis "Smart Secure ICT Luxembourg" is regularly published, generally twice a year, in order to provide to the national market an overview of the recent Smart ICT developments from a technical standardization perspective. The first Standards Analysis on the ICT sector was published in 2012, and, to follow the national market interests, the document has evolved over recent years to focus now on the Smart Secure ICT domain.

This Standards Analysis "Smart Secure ICT Luxembourg" is thus intended to serve as a practical tool to discover latest standardization developments in Smart ICT related technologies, such as Internet of Things, Cloud Computing, Artificial Intelligence, Blockchain as well as Digital Trust related standards for those technologies. Therefore, the present document will allow national stakeholders to identify relevant standardization technical committees in the Smart Secure ICT area, with the final 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] ILNAS, "Luxembourg Standardization Strategy 2014-2020", 2014

[2] ILNAS, "Luxembourg's policy on ICT technical standardization 2015-2020", 2015

[3] https://smartict.gforge.uni.lu/

[4] ILNAS & University of Luxembourg, White Paper "Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization", 2018

[5] ILNAS, White Paper "Internet of Things (IoT) - Technology, Economic View and Technical Standardization", 2018

[6] ILNAS, White Paper "Blockchain and Distributed Ledgers - Technology, Economic Impact and Technical Standardization", 2018

[7] ILNAS, White Paper "Digital Trust for Smart ICT" (3rd edition), 2017

EXECUTIVE SUMMARY

This Standards Analysis “Smart Secure ICT Luxembourg” is conceived as a practical guide to all the national stakeholders regarding standardization activities in the field of selected Smart ICT domains, such as Internet of Things, Cloud Computing, Artificial Intelligence as well as Blockchain together with Digital Trust related standards developments to these technologies. This document is intended to help the national market to identify issues and interests in technical standardization and to encourage their participation in Smart ICT technical committees to benefit from the related knowledge to build secure Smart ICT environment in their business. Different opportunities, presented in this Standards Analysis, are available for national stakeholders with the objective to make them able to take advantage of standards and standardization.

In this context, this Standards Analysis is designed to develop an information and exchange network for Smart ICT standardization knowledge in the Grand Duchy of Luxembourg. Currently ILNAS has registered 95[8] experts as national delegates in the ICT sector. Among them, 74 are directly involved in Smart ICT and Digital Trust related technical committees[9], such as in Internet of Things: 16; Cloud Computing: 16; Artificial Intelligence: 17; Blockchain: 16, Digital Trust: 44.

ILNAS, with the support of ANEC G.I.E., encourages national experts to develop their normative culture in Smart ICT areas and to take advantage of technical standardization for their business. In that sense, and in accordance with the national ICT technical standardization policy, the implementation plan for ICT technical standardization, annually set-up by ILNAS, focuses on strengthening Smart ICT technical standardization since 2017, with the aim to support the related economic development. ILNAS priorities notably consists in the management of the national Smart ICT technical committees, as well as in making national organizations aware of the relevant standardization activities in their area of work. The objective of ILNAS is to foster the 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 of the Smart ICT standardization development at international and European level to support national stakeholders. Firstly, it introduces basic components of Smart ICT technologies as well as Digital Trust requirement for Smart ICT and secondly it presents standardization activities performed at 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.

[8] National register of standardization delegates – October 2018

[9] Please note that some experts are participating in more than one technical committee

TABLE OF CONTENTS

INTRODUCTION

The Information and Communication Technology (ICT) sector is a keystone of the worldwide 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. 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.

ILNAS works on the development of this key sector for the economy. 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 committees[10]. 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*", in 2015-2016, was its first step to work closely with academia aiming to provide standards-based knowledge on recent emerging Smart ICT technologies to ICT professionals at national level. The course, offered for two semesters, was completed successfully with great interest of participations from multiple industries of different sectors and the second promotion of the University certificate is currently underway since February 2018.

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, Internet of Things and Big Data. In this frame, 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" in October 2018[11]. One objective of this program is to rely on the research results to develop new academic programs on ICT technical standardization, including a planned Master Program "*Smart Secure ICT for Business Innovation*" expected at the horizon 2020.

In relation with above-mentioned developments, this Standards Analysis "Smart Secure ICT Luxembourg" concentrates on standards development of recognized Standards Development Organizations (SDOs) towards the Smart ICT landscape, such as 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 secure and trustworthy Smart ICT environment through technical standardization. For this purpose, this analysis provides a brief overview of the technical background of above-mentioned Smart ICT technologies as well as details on the technical committees active in these domains. The document also provides an introduction of common Digital Trust issues for Smart ICT technologies together with related technical standards developments. Moreover, a list of relevant standards in all these areas is provided with the purpose of helping national stakeholders in building and maintaining secure Smart ICT environments.

Apart from this, the Standards Analysis "Smart Secure ICT Luxembourg" also introduces a section dedicated to introduce two topics currently receiving a particular attention from the economic market:

[10] Note: In this report, the term "standardization technical committee" is generic and covers "technical committees", "subcommittees", "working groups", etc.

[11] ILNAS & University of Luxembourg, White Paper "Data Protection and Privacy in Smart ICT - Scientific Research And Technical Standardization", 2018

fifth generation mobile communication (5G) and Intelligent Transport Systems (ITS). On the one hand, communication infrastructure is a key element to provide services to the end users for such Smart ICT technologies. Indeed, telecommunications services, as part of the communication infrastructure, are considered as backbone network of Smart ICT technologies. 5G mobile communication is expected to transform societies to support new services and new business models as Telecommunication services[12]. On the other hand, ITS will deeply change the field of road transport, including infrastructure, vehicles and users, in traffic management and mobility management, as well as interfaces with other modes of transport. ITS are nowadays center of attention of governments and private sectors around the globe, for example to achieve efficient management of current public transport network for passengers and enterprises.

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 national level (i.e., in research and education).

This Standards Analysis is organized as follows. The importance of standardization along with its objectives and introduction of standardization landscape in national, European and international level have been included in Chapter 1. Chapter 2 proposes a definition of Smart ICT, provides an economical overview of ICT and introduces main interactions between the Smart ICT technologies included in this analysis. Chapter 3 further details each of these Smart ICT technologies 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. 5G and Intelligent Transport Systems (ITS) are included at the end of this chapter to aware national stakeholder about the standardization developments in these areas. Chapter 4 presents opportunities related to standardization for national stakeholders. It also introduces how ILNAS is supporting national economy through technical standardization. Chapter 5 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 for each Smart ICT technology, as well as related Digital Trust standards.

[12] https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2018/documents/DiscussionPaper_Setting%20the%20scene%20for%205G_GSR18.pdf

1. 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)[13] 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 process[14].

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 technologies[15]. 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 Initiative[16], "they enable the dissemination of knowledge, the interoperability between new products and services for a platform for further innovation". It is more relevant in the current context that 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.

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

[13] WTO, "Second triennial review of the operation and implementation of the agreement on technical barriers to trade – Annex," 2000. Available: http://docsonline.wto.org/imrd/directdoc.asp?DDFDocuments/t/G/TBT/9.doc

[14] Based on: Regulation (EU) N°1025/2012 of the Parliament and of the Council

[15] CEN-CENELEC, "Standards and your business," 2013.
Available: https://www.cencenelec.eu/news/publications/Publications/Standards-and-your-business_2013-09.pdf

[16] European Commission, "Europe 2020 Flagship Initiative, Innovation Union, COM(2010) 546," 2010.
Available: https://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf

- 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 economical tool offering the possibility to pursue various objectives, such as:

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

1.2. Standardization Landscape

In Europe, the three recognized European Standardization Organizations (ESO), as stated in the Regulation (EU) No 1025/2012[17], 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).

The standardization frame allows cooperation between standards 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.

[17] Regulation (EU) N°1025/2012 of the Parliament and of the Council

Table 1 presents the main figures of the European and international standards bodies.

Table 1: Figures of European and International Standardization Organizations[18]

European and International Standardization Bodies		Date of Creation	Number of Members	Number of Published Standards
ISO	International Organization for Standardization	1946	162	21991
IEC	International Electrotechnical Commission	1906	86	7537
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector	1865	266[19]	5440
CEN	European Committee for Standardization	1961	34	16845
CENELEC	European Committee for Electrotechnical Standardization	1973	34	7328
ETSI	European Telecommunications Standards Institute	1988	872[19] (67 countries)	18220

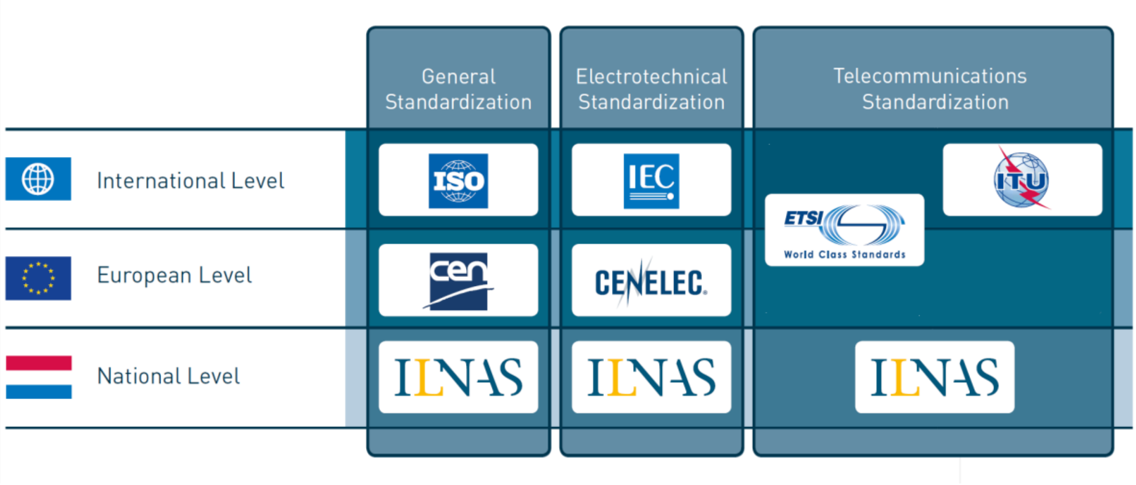
At national levels, one or several national standards bodies protect the interests of the country within the European and international standardization organizations. In Luxembourg, ILNAS – the only official national standards body – is member of the European and international standardization organizations 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 the standardization work on the different fields (Figure 1).

[18] Source: Websites of organizations - October 2018

[19] 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

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 Agreement[20], 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 Agreement[21] 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 72% of those ratified by CENELEC, are respectively identical to ISO or IEC standards[22]. In that respect, the European and international organizations do not duplicate work.

Similarly, ITU-T and ETSI have agreed on a Memorandum of Understanding (MoU) lastly renewed in 2016[23] (the first MoU was signed in 2000) that paves the way for European regional standards, developed by ETSI, to be recognized internationally.

[20] Agreement on technical co-operation between ISO and CEN (Vienna Agreement)

[21] IEC-CENELEC Agreement on Common planning of new work and parallel voting (Frankfurt Agreement)

[22] CEN-CENELEC Quarterly Statistical Pack – 2018 Q2

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

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 the area of work is overlapping the two organizations.

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 organizations[24]. 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 22,000 standards published and more than 4,700 standards under development[25]. 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. ISO/IEC JTC 1 has taken a leading role in Smart ICT standardization since a couple of years with the creation of working groups and technical committees 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 the CEN-CENELEC are detailed in an annual common Work Program, which was published in December 2017 for the year 2018[26]. They are active in several ICT-related areas covering both the Digital & Information Society and the Smart Technologies: Biometrics, Electronic invoicing, eSkills and eLearning, Privacy Management, e-Procurement, e-Signatures, Intelligent Transport Systems, Smart Grids, Smart Metering, Internet of Things, Smart Homes and Smart Cities.

❖ ETSI - European Telecommunications Standards Institute

ETSI produces globally applicable standards for ICT including fixed, mobile, radio, converged, broadcast and internet technologies. 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 Internet of Things (ETSI/TC SmartM2M), Digital Trust (e.g.: ETSI/TC ESI and ETSI/TC CYBER) or Intelligent Transport Systems (e.g.: ETSI/TC ITS).

[24] http://www.worldstandardscooperation.org/

[25] https://www.iso.org/iso-in-figures.html

[26] https://www.cencenelec.eu/News/Publications/Publications/WorkProgramme-2018_UK_acces.pdf

- **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 represents defining elements in the global infrastructure of ICT. It is currently composed of 11 Study Groups working on different aspects of ICT.

2. SMART ICT LANDSCAPE

2.1. Smart ICT Definition and Economical Overview

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

Dynamism in the 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 as Smart ICT technologies. For example, Cloud Computing, 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 a (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 the Smart ICT, which could eliminate the need for some intermediaries in the interactions or transactions. For the sake of high-level understanding of Smart ICT, a definition is proposed here:

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 crowdsourcing[27].

Worldwide revenues for IT services crossed the $1 trillion mark in 2017[28]. In the same time, companies' investment in IT keeps growing. Gartner estimates that global IT spending will be increased by 4.5% than 2017 for this year, reaching $3.7 trillion[29]. According to the 2017 EU Industrial R&D Investment Scoreboard, Research & Development global investment into R&D in 2017 increased by 5.8% over the previous year, with a total of €741.6 billion invested by companies analyzed in the study. This growth was mainly driven by ICT services (+11.7%) and ICT producers (+6.8%)[30]. Moreover, the coming trends show that the sector is still innovating with the development of technologies such as Artificial Intelligence, Intelligent Apps & Analytics, Intelligent Things, Digital Twins, Edge Computing, Conversational Platforms, Immersive Experience (augmented reality, virtual reality, mixed reality), Blockchain, etc.[31]

[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").

[28] https://www.idc.com/getdoc.jsp?containerId=prUS43814918

[29] https://www.gartner.com/en/newsroom/press-releases/2018-01-16-gartner-says-global-it-spending-to-reach-37-trillion-in-2018

[30] The 2017 EU Industrial R&D Investment Scoreboard

[31] https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/

At the European level, the ICT sector has been directly responsible for 5% of GVA[32] (Gross Value Added), with a market value of EUR 666 billion in 2016[33], but it contributes far more to the overall productivity growth. This is not only due to the high levels of dynamism and innovation inherent in this 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 2017, with 87% (Luxembourg: 97%) of households having a broadband connection[34], 81% (Luxembourg: 96%) of individuals using the Internet on a regular basis[35] of which 73% (Luxembourg: 86%) used a mobile device to connect to the Internet away from home or work[36].

The European Commission also promotes research and innovation in the ICT sector, through innovative Public-Private Partnerships and through the Horizon 2020 research funding programs that encompasses 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 budget (EUR 1.7 billion) for 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*"[37].

Finally, at the national level, ICT is considered as a key economic sector. Within the National Government Program[38], having a developed ICT sector is a cornerstone, especially to support other economic sectors: eco-technologies (e.g. Smart Grid, IT management), logistics (e.g. e-commerce), biotechnologies (e.g. Archiving, Data Management), industrial and financial sector (e.g. Cloud Computing).

This program was reinforced in autumn 2014, with the launch of the "Digital Lëtzebuerg" initiative[39], aiming at strengthening and consolidating the position of Luxembourg in terms of ICT, for the benefits of the economy and society as a whole. In this frame, several strategic areas were defined:

- Development of the telecommunications infrastructure;
- Support to start-ups for innovation and access to funding;
- Innovation in services dedicated to the financial sector (Fintech);
- Digital skills;
- Electronic administration;
- Promotion of Luxembourg's assets abroad.

Through the national policy pursued in the 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 ICT capabilities of Luxembourg. For example:

[32] 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)

[33] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_a64&lang=en

[34] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en

[35] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=tin00091&lang=en

[36] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=tin00083&lang=en

[37] http://europa.eu/rapid/press-release_MEMO-17-4123_en.htm

[38] https://gouvernement.lu/dam-assets/fr/actualites/articles/2013/11-novembre/29-signature/Programme-gouvernemental.pdf

[39] https://gouvernement.lu/en/dossiers/2014/digital-letzebuerg.html

- The "Digital (4) Education" strategy[40], presented in May 2015 with the objective to reinforce digital skills in the educative system and answer the growing demand for skilled ICT professionals;
- The strategic study on the “Third Industrial Revolution”[41], 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[42], lastly updated in May 2018 and which intends to provide an environment conducive to digital development, while ensuring maximum security for all stakeholders.

The ICT sector is already a competitive sector in Luxembourg, which ranks 5th out of the 28 EU Member States in the “European Commission Digital Economy and Society Index” (DESI) 2018[43]. The country is particularly running ahead in terms of connectivity (ranks 2nd), human capital (ranks 5th) and use of the Internet (ranks 4th). The ICT sector represents 2 238 companies in 2015 and 4.4% of the total employment at the first semester 2018[44]. Moreover, the ICT sector contributes to 7% of GDP in Luxembourg[45].

2.2. Smart ICT Components and their Interactions

Although many terminologies come in mind while talking about Smart ICT, but the technologies, such as Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI) and Blockchain are considered as some of the most important components of Smart ICT in this Standards Analysis.

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

- Internet of Things collects enormous amount of data or information of various environments. Communication networks including telecommunications help to exchange collected data to the specific destinations.
- Big Data stores, analyzes and provides mechanisms for operating and understanding the large amount of data produced.
- Cloud Computing supports these environments by providing the processing power and infrastructure to allow the capture, storage, analysis of the data.
- Artificial Intelligence, corresponding to a set of techniques aimed at approximating some aspects of human or animal cognition without human intervention, allow, for example, the automatization of processes in relation with the analysis of data. Data based learning is the highly applied approximation approach in AI.
- Blockchain tracks the records of smart devices to make interactions more transparent and trustful.
- To utilize maximum efficiency of the Smart ICT technology, building and maintaining a 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.

[40] http://portal.education.lu/digital4education/

[41] http://www.troisiemerevolutionindustrielle.lu/etude-strategique/

[42] http://luxembourg.public.lu/en/actualites/2018/05/14-cybersecurity/index.html

[43] https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg

[44] Source: STATEC

[45] https://smc.gouvernement.lu/fr/service/communications-electroniques/statistiques.html

In this context, Chapter 3 provides a technological introduction of above-mentioned Smart ICT technologies including Digital Trust. 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 Smart Secure ICT environment.

3. 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 it, this chapter introduces basic concepts of Smart ICT technologies, such as Internet of Things (IoT), Cloud Computing, Artificial Intelligence and Blockchain as well as 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.

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 international and European level is intended to help them in building secure and trustworthy environment in Smart ICT technologies through the technical standardization. In particular, this Standards Analysis focuses on ISO/IEC, CEN, CENELEC, ETSI and ITU-T standardization developments.

3.1. Internet of Things (IoT)

Internet of Things (IoT) refers to an emerging paradigm consisting of a continuum of uniquely addressable things communicating with each other to form worldwide dynamic networks[46]. This network of uniquely identifiable connected devices such as objects, devices, sensors and everyday items with computing services is called IoT[47]. It describes a world where anything can be connected and can interact in an intelligent fashion. Table 2 provides definitions of IoT provided by different standard development organizations (SDOs).

Table 2: IoT definitions

SDO	IoT Definition
ISO/IEC[48]	"It is an infrastructure of **interconnected objects**, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react."
ITU-T[49]	"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." *Note 1* – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

[46] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1-31, 2014

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

[48] ISO/IEC 20924 Information technology - Internet of Things (IoT) - Definitions and vocabulary, https://www.iso.org/obp/ui/#iso:std:iso:19731:ed-1:v1:en:term:3.21

[49] ITU-T Y.2060 "https://www.itu.int/ITU-T," June 2012. [Online].
Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=en

SDO	IoT Definition
	Note 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications. “**Things**: With regard to the Internet of things, these are an object of the physical world (physical devices) or the information world (virtual things), which are capable of being identified and integrated into communication networks.”
IEEE[50]	“The Internet of Things (IoT) is a framework in which all **things** have a representation and a presence in the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represents the baseline communication that enables the interactions between Things and applications in the Cloud.”

3.1.1. Characteristics

The IoT is a complex system with a number of characteristics that can be defined from the perspectives of IoT components/devices used, services provided, usability, and security. Given the evolving character of IoT, it is too early to determine its complete features. However, some of the general and key characteristics are highlighted in Table 3.

Table 3: IoT Basic Characteristics

Characteristic	Description
Smart data collection and smart handling	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.
Interconnectivity	The IoT is able to interconnect anything (physical or virtual things) with the help of global information and communication infrastructure. Communication infrastructure [51] refers to the 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.
Things-related services	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 the technologies in physical world and information world are required.

[50] http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps
[51] 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 the 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 the management of the generated data and its interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

3.1.2. IoT Standardization Technical Committees

Many organizations are actively involved in the standardization that is evolving around the Internet of Things and its standardization has proven to be difficult. It is widely acknowledged that many standardization challenges need to be addressed for further spread of IoT. Issues include, but are not limited to, security, privacy, interfaces, data structures, and architecture. Because IoT covers everything from the 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 fragmented[52]. The urgent need for standardization and necessary improvements in interoperability are critical success factors for accelerated adoption of IoT systems[53]. 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. Moreover, standards for IoT and Digital Trust related to IoT are listed in the Appendix (Section 6.1).

[52] OECD, "OECD Digital Economy Outlook 2015," OECD Publishing, Paris, report, 2015

[53] McKinsey, "The Internet of Things: mapping the value beyond the hype." McKinsey Global Institute, 2015.

3.1.2.1. ISO/IEC JTC 1/SC 41

General information			
Committee	**ISO/IEC JTC 1/SC 41**	**Title**	**Internet of Things and related technologies**

Creation date	2017	**MEMBERS**	**Participating Countries (25):**
			Republic of Korea, Australia, Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, **Luxembourg**, Malaysia, Netherlands, Norway, Russian Federation, Singapore, Sweden, Switzerland, United Kingdom, United States
			
			Observing Countries (9):
			Argentina, Belarus, Iceland, Iran, Kenya, Mexico, Pakistan, Saudi Arabia, Slovakia

Secretariat	KATS (Republic of Korea)		
Secretary	Ms. Jooran Lee		
Chairperson	Dr. François Coallier		
Organizations in liaison	AIM, AIOTI, GS1, IIC, INCOSE, ITU-T, OCF, OGC		
Web site	http://www.iec.ch/dyn/www/f?p=103:29:2698958918431::::FSP_ORG_ID,FSP_LANG_ID:20486,25#3		
Scope	Standardization in the area of Internet of Things and related technologies. 1. 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. 2. Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications.		

Structure	JTC 1/SC 41/AG 6	JTC 1/SC 41 Advisory Group
	JTC 1/SC 41/WG 3	IoT Architecture
	JTC 1/SC 41/WG 4	IoT Interoperability
	JTC 1/SC 41/WG 5	IoT Applications
	JTC 1/SC 41/SG 7	Study group on Wearables
	JTC 1/SC 41/SG 14	Ad hoc group on Business Plan
	JTC 1/SC 41/SG 15	Communication and outreach
	JTC 1/SC 41/SG 16	Study Group on Reference Architecture and Vocabulary Harmonization
	JTC 1/SC 41/SG 17	Study Group on Societal and human factors in IoT based services
	JTC 1/SC 41/SG 18	Study Group on Integration of IoT and Blockchain
	JTC 1/SC 41/SG 19	Study Group on Realizing Context Specific Solution / System Architecture based on IoT RA

Standardization work	
Published standards	18
Standards under development	16

Involvement of Luxembourg

16 delegates

- Mr. Shyam Wagle (Chairman)	ANEC G.I.E.
- Mr. Anouar Adlani	vyzVoice S.A.
- Mr. Johann Amsenga	INCERT GIE
- Mr. Raphael Bleuse	University of Luxembourg
- Mr. Matthias Brust	University of Luxembourg

-	Mr. Arunas Buknys	FANUC Europe Corporation
-	Mr. Vincent Cady	Tarkett S.A.
-	Mr. Cyril Cassagnes	Proximus Luxembourg
-	Mr. Sankalp Ghatpande	University of Luxembourg
-	Mr. Abdallah Ibrahim	University of Luxembourg
-	Mr. Jean Lancrenon	itrust consulting S.à r.l.
-	Ms. Maria Rita Palattella	Luxembourg Institute of Science and Technology
-	Mr. Benoit Poletti	INCERT GIE
-	Mr. Nader Samir Labib	University of Luxembourg
-	Mr. Ridha Soua	University of Luxembourg
-	Mr. Robert Spicer	vyzVoice S.A.

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 through study groups on various topics like wearables, trustworthiness, industrial IoT and real-time IoT. Its current work programs notably include:

- PWI TR JTC1-SC41-1 Internet of things (IoT) -- Edge Computing;
- PNW JTC1-SC41-45, Internet of Things (IoT) -- Trustworthiness framework;
- PNW JTC1-SC41-51, Internet of Things (IoT) -- Application framework for industrial facility demand response energy management;
- PNW JTC1-SC41-52, Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services;
- PNW JTC1-SC41-58, Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems;
- PNW JTC1-SC41-59, Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services;
- ISO/IEC 20924, Internet of Things (IoT) -- Vocabulary;
- ISO/IEC 21823-1, Internet of Things (IoT) -- Interoperability for IoT Systems -- Part 1: Framework;
- ISO/IEC 21823-2, Internet of Things (IoT) -- Interoperability for IoT Systems -- Part 2: Transport interoperability;
- ISO/IEC 21823-3, Internet of Things (IoT) -- Interoperability for IoT Systems -- Part 3: Semantic interoperability;
- ISO/IEC 30142, Internet of Things (IoT) -- Underwater Acoustic Sensor Network (UWASN) -- Network management system overview and requirements;
- ISO/IEC 30143, Internet of Things (IoT) -- Underwater Acoustic Sensor Network (UWASN) -- Application Profiles;
- ISO/IEC 30144, Internet of Things (IoT) -- Wireless sensor network system supporting electrical power substation;
- ISO/IEC 30147, Internet of Things (IoT) -- Methodology for implementing and maintaining trustworthiness of IoT systems and services;
- ISO/IEC TR 30148, Internet of Things (IoT) -- Technical requirements and application of sensor network for wireless gas meters.

3.1.2.2. ISO/IEC JTC 1/SC 31

General information			
Committee	**ISO/IEC JTC 1/SC 31**	**Title**	**Automatic identification and data capture techniques**

Creation date	1996	**MEMBERS**	**Participating Countries (25):**
			United States, Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Japan, Kazakhstan, Republic of Korea, Mauritania, Netherlands, Peru, Romania, Russian Federation, Slovakia, South Africa, Sweden, Switzerland, United Kingdom
			
			Observing Countries (23):
			Argentina, Bosnia and Herzegovina, Colombia, Czech Republic, Ghana, Hong Kong, Hungary, Indonesia, Islamic Republic of Iran, Italy, Kenya, **Luxembourg**, Malaysia, New Zealand, Pakistan, Philippines, Serbia, Singapore, Slovenia, Spain, Thailand, Turkmenistan, Ukraine

Secretariat	ANSI (United States)		
Secretary	Mr. Eddy Merrill		
Chairperson	Mr. Henri Barthel		
Organizations in liaison	AIM Global, Ecma International, ETSI, GS1, IATA, IEEE, ITU, OGC, UPU, NATO		
Web site	https://www.iso.org/committee/45332.html		
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	JTC 1/SC 31/WG 1 JTC 1/SC 31/WG 2 JTC 1/SC 31/WG 4 JTC 1/SC 31/WG 8	Data carrier Data and structure Radio communications Application of AIDC standards	

Standardization work	
Published standards	125
Standards under development	24

Involvement of Luxembourg

1 delegate

- Mr. Shyam Wagle ANEC G.I.E.

Comments[54]

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.

AIDC is an industry term that describes the identification and/or direct collection of data into a microprocessor-controlled device, such as a computer system or a programmable logic controller (PLC),

[54] Source: ISO/IEC JTC 1/SC 25 Business plan October 2017 to September 2018

without the use of a keyboard. AIDC technologies provide a reliable means not only to identify but also to track items. It is possible to encode a wide range of information, beginning with a basic item or the identification of a person, to comprehensive details about the item or person, e.g. item description, size, weight, color, etc.

ISO/IEC JTC 1/SC 31, Automatic identification and data capture techniques, is responsible for more than 100 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.

The current work program of ISO/IEC JTC 1/SC 31 includes for example:

- The revision of the multipart standard ISO/IEC 15961 regarding “Information technology -- Radio frequency identification (RFID) for item management: Data protocol”;
- The development of the multipart standard ISO/IEC 19823 entitled “Information technology -- Conformance test methods for security service crypto suites”;
- The development of the multipart standard ISO/IEC 29167 concerning security services in the area of “Information technology -- Automatic identification and data capture techniques”.

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.

3.1.2.3. ISO/IEC JTC 1/SC 25

General information			
Committee	**ISO/IEC JTC 1/SC 25**	Title	**Interconnection of information technology equipment**

Creation date	1990	MEMBERS	**Participating Countries (28):**
			Germany, Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, India, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Lebanon, Mexico, Netherlands, Norway, Poland, Russian Federation, Singapore, Spain, Sweden, Switzerland, United Kingdom, United States
			
			Observing Countries (17):
			Argentina, Bosnia and Herzegovina, Croatia, Cuba, Ghana, Greece, Hungary, Iceland, Indonesia, Kenya, Malaysia, New Zealand, Pakistan, Philippines, Romania, Serbia, Turkey, Ukraine

Secretariat	DIN (Germany)		
Secretary	Mr. Jürgen Tretter		
Chairperson	Mr. Rainer Schmidt		
Organizations in liaison	EC, ECMA, ITU, UNCTAD, UNECE		
Web site	http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:3399		
Scope	Standardization of microprocessor systems and of interfaces, protocols, architectures and associated interconnecting media for information technology equipment and networks, generally for commercial and residential environments, to support embedded and distributed computing environments, storage systems, other input/output components, home and building electronic systems including customer premises smart grid applications for electricity, gas, water and heat.		
Structure	JTC 1/SC 25/WG 1 JTC 1/SC 25/WG 3 JTC 1/SC 25/WG 4	Home electronic systems Customer Premises Cabling Interconnection of Computer Systems and Attached Equipment	
Standardization work			
Published standards	212		
Standards under development	15		
Involvement of Luxembourg			
NO (no registered delegate)			
Comments			
Homes are increasingly equipped with home systems conforming to the 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 is 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.			

[55] Source: ISO/IEC JTC 1/SC 25 Business plan September 2018 to September 2019

WG 1 is responsible for the Home Electronic System (HES) series of standards. It develops standards for the interconnection of electrical and electronic equipment and products for homes and small buildings. The primary markets for WG 1 standards are developers, manufacturers, and installers of these products and related services. Homes are made intelligent with interconnected sensors, actuators, user interfaces, and controllers, which may be embedded in smart consumer appliances. Such networks use a variety of media: IT cabling, wireless and power line communication. Home networks using structured cabling specified by subcommittee 25 are now routinely offered for many new and renovated homes. Wireless and power line carrier technologies are facilitating the introduction of networks into existing homes.

This committee has already developed more than 200 standards. Some examples of recently developed series of standards for home electronic system are: universal interfaces class 1 (part 1), simple interfaces type 1 etc. considering national interest and current market trends in this domain, particularly in Internet of Things (IoT). Some of the standards under development are dedicated to further extend standardization works in home electronic system from different perspectives, such as wireless short-packet (WSP) protocol optimized for energy harvesting - architecture and lower layer protocols, application model -- Part 3-3: model of distributed energy management agent (EMA) for demand response energy management, and intelligent grouping and resource sharing -- remote universal management profile.

The current work programs of ISO/IEC JTC 1/SC 25 include, for example:

- ISO/IEC 14543-3-10, Information technology - Home electronic system (HES) architecture - Part 3-10: Wireless short-packet (WSP) protocol optimized for energy harvesting - Architecture and lower layer protocols;
- ISO/IEC 14543-5-12, Intelligent grouping and resource sharing - Part 12: Remote access test and verification;
- ISO/IEC 14543-5-101, Information technology -- Home electronic systems (HES) architecture -- Part 5-101:Intelligent grouping and resource sharing remote AV access profile;
- ISO/IEC 14543-5-102, Information technology -- Home electronic system (HES) architecture -- Part 5-102: Intelligent grouping and resource sharing -- Remote universal management profile.

3.1.2.4. CEN/TC 225

General information			
Committee	CEN/TC 225	Title	AIDC Technologies
Creation date	1989	MEMBERS	34 members of CEN/CENELEC
Secretariat	TSE (Turkey)		
Secretary	Ms. Aysegül Ibrisim		
Chairperson	Mr. Claude Tételin		
Organizations in liaison	ECISS, EDIFICE, EDMA (Brussels), EFPIA, EHIBCC, EUCOMED, EuroCommerce, GS1, ODETTE, UPU		
Web site	http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6206&cs=1E12277AECC001196A7556B8DBCDF0A1C		
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	CEN/TC 225/WG 1 CEN/TC 225/WG 3 CEN/TC 225/WG 4 CEN/TC 225/WG 5 CEN/TC 225/WG 6	Optical Readable Media Security and data structure Automatic ID applications RFID, RTLS and on board sensors Internet of Things - Identification, Data Capture and Edge Technologies	
Standardization work			
Published standards	26		
Standards under development	3		
Involvement of Luxembourg			
NO (no registered delegate)			
Comments			

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:

- 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.

The Working Group 6 of CEN/TC 225 is the focal point for IoT issues within CEN. It advises CEN/TC 225 on IoT issues in order to ensure a consistent and proactive approach to the IoT by all its WGs and assists

CEN/TC 225 to act as an agent of change within CEN by facilitating IoT knowledge transfer between CEN and CENELEC TCs.

The current work program of CEN/TC 225 includes the development of three standards concerning:

- EN 17071, Information technology - Automatic identification and data capture techniques - Electronic identification plate (under publication);
- prEN 17099, Information technology - Fish and fish products - requirements for labelling of distribution units and pallets in the trade of seafood products;
- prEN 17230, Information technology – RFID in rail.

3.1.2.5. ETSI/TC SmartM2M

General information			
Committee	**ETSI/TC SmartM2M**	**Title**	**Smart Machine-to-Machine Communication**
Creation date	N/A	**MEMBERS**	N/A
Chairperson	Mr. Enrico Scarrone		
Organizations in liaison	ATIS, BIF, Broadband Forum, CCC, CCSA, CEN, CENELEC, CEPT COM-ITU, Continua Health Alliance, ECSO, ESMIG, Eurosmart, FIEEC, GCF, GISFI, GSMA, IEEE, IPSO Alliance, ISOC/IETF, ITU, NIST, OASIS, OMA, TAICS, TIA, TSDSI, TTA, TTC, ULE Alliance		
Web site	http://portal.etsi.org/portal/server.pt/community/SmartM2M		
Scope	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 oneM2M, and the conversion of the oneM2M specifications into European Standards. The activities of TC Smart M2M include the following: - 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 M2M.		
Structure	/		
Standardization work			
Published standards	52		
Standards under development	25		
Involvement of Luxembourg			
2 companies - Skylane Optics - FBConsulting S.A.R.L. Note: ILNAS, with the support of ANEC G.I.E. is also monitoring the developments of the ETSI/TC SmartM2M.			
Comments			
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.

3.1.2.6. ITU-T/SG 20

General information			
Committee	**ITU-T/SG 20**	**Title**	**Internet of Things, smart cities and communities**
Creation date	N/A	**MEMBERS**	N/A
Chairperson	Mr. Nasser Al Marzouqi		
Organizations in liaison	3GPP, AIOTI, CCSA, CITS, ETSI, IoT Forum, IoT Lab, IPv6 Forum, ISO/IEC JTC 1, OCF, OneM2M, SCV, UNE		
Web site	https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx		
Scope	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: - Lead study group on Internet of things (IoT) and its applications; - Lead study group on smart cities and communities, including its e services and smart services; - Lead study group for Internet of things identification.		
Structure	WP1/Q1 End to end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C WP1/Q2 Requirements, capabilities, and use cases across verticals WP1/Q3 Architectures, management, protocols and Quality of Service WP1/Q4 e/Smart services, applications and supporting platforms WP2/Q5 Research and emerging technologies, terminology and definitions WP2/Q6 Security, privacy, trust and identification for IoT and SC&C WP2/Q7 Evaluation and assessment of Smart Sustainable Cities and Communities **Other groups under SG 20**: JCA-IoT and SC&C Joint Coordination Activity on Internet of Things and Smart Cities and Communities FG-DPM Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities		
Standardization work			
Published standards	96 (Recommendations)		
Standards under development	75		
Involvement of Luxembourg			
Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ITU-T/SG 20.			
Comments			
The objective of this 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 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.

3.2. Cloud Computing

Cloud Computing technology is considered as an IT paradigm that 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.

Table 4: Definitions of Cloud Computing

SDO / Organization	Definition
ITU-T Y.3500 and ISO/IEC 17788[56]	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[57]	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

3.2.1. Characteristics

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

Considering its rapid implementation across multiple sectors, long list of Cloud Computing characteristics can be listed. 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.

Table 5: Characteristics of Cloud Computing[58]

Characteristic	Explanation
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms as well as other traditional or Cloud-based software services.
Rapid Elasticity	Capabilities can be rapidly and elastically provisioned to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

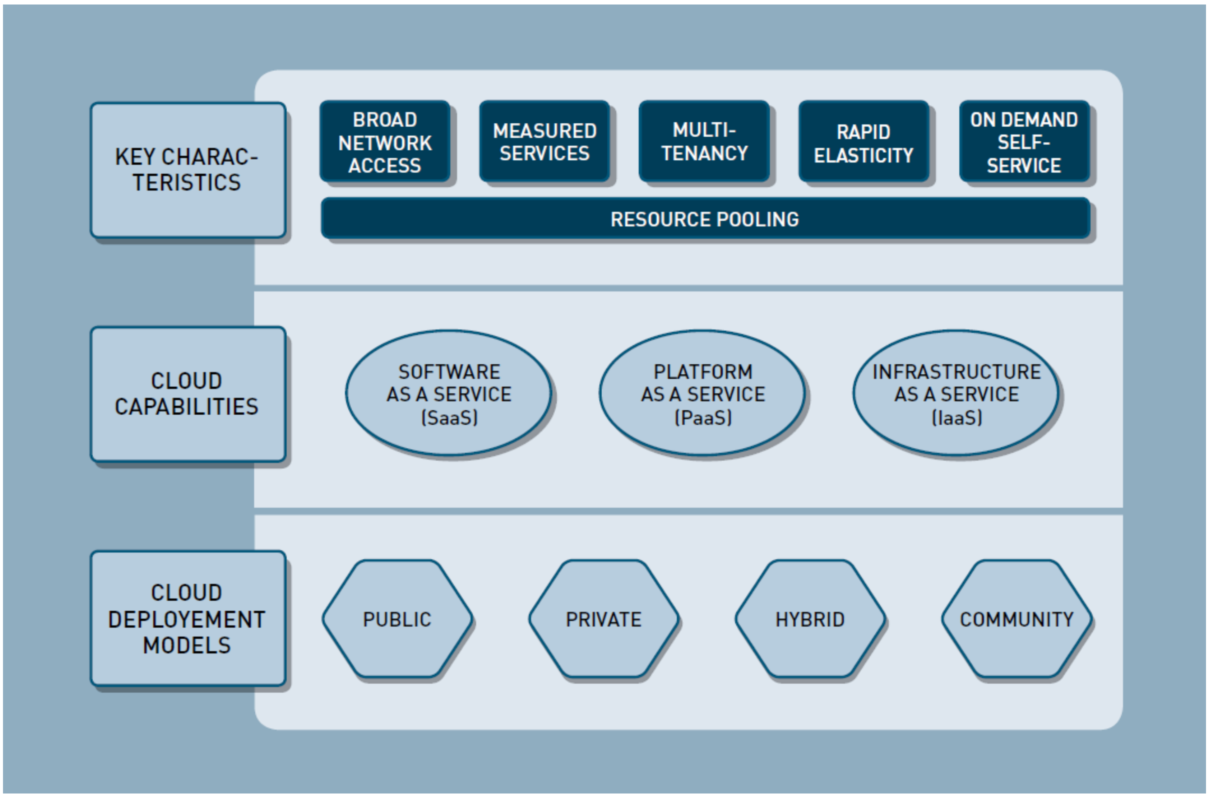
[56] See Rec. ITU-T Y.3500 | ISO/IEC 17788

[57] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[58] CSA, “Security Guidance for critical areas of focus in cloud computing V3.0,” Cloud Security Alliance, report, 2011

Characteristic	Explanation
Measured Service	Cloud systems automatically control and optimize resource usage by leveraging a metering of e.g. storage, processing, bandwidth, or active user accounts. It provides transparency for both the provider and consumer of the service by means of monitoring, controlling and reporting.
On Demand Service	A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically without requiring human interaction with a service provider.
Multi Tenancy	With the capabilities of multi-tenancy of a Cloud resource, 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.
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Figure 2: Visual Model of ISO/IEC Cloud Computing Definition[59]



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

3.2.2. Cloud Computing Standardization Technical Committees

The standards landscape for Cloud Computing is extensive, since many standards developing organizations are active in the Cloud Computing subsector and many standards and specifications have been developed. As specified by the European Commission in its European Cloud Computing Strategy[60], it is necessary to cut “through the jungle of standards” in order to identify existing solutions, market needs and, finally, to increase Cloud Computing adoption. This section provides an overview of the Cloud Computing related technical committees and standards currently active in the recognized standardization organizations. Moreover, standards for Cloud Computing and Digital Trust related to Cloud Computing are listed in the Appendix (Section 6.2).

3.2.2.1. ISO/IEC JTC 1/SC 38

General information			
Committee	**ISO/IEC JTC 1/SC 38**	**Title**	**Cloud Computing and Distributed Platforms**

Creation date	2009	**MEMBERS**	**Participating Countries (31):**
			United States, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, **Luxembourg**, Netherlands, Pakistan, Panama, Poland, Russian Federation, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, United Kingdom
			Observing Countries (13):
			Argentina, Bosnia and Herzegovina, Czech Republic, Hong Kong, Hungary, Kenya, Mexico, Norway, Portugal, Serbia, Turkey, Uruguay, Zambia

Secretariat	ANSI (USA)		
Secretary	Mrs. Lisa Rajchel		
Chairperson	Dr. Donald Deutsch		
Organizations in liaison	Cloud Security Alliance, CSCC, Ecma International, IEEE, INLAC, ITU, OASIS, OGF, SNIA, The Open Group, EC, EuroCloud, TM Forum		
Web site	https://www.iso.org/committee/601355.html		
Scope	Standardization in the area of Cloud Computing and Distributed Platforms including: - 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.		
Structure	JTC 1/SC 38/AG 1 Communications committee JTC 1/SC 38/WG 3 Cloud Computing Fundamentals (CCF) JTC 1/SC 38/WG 5 Data in cloud computing and related technologies		
Standardization work			
Published standards	13		
Standards under development	9		

[60] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0529&from=EN

Involvement of Luxembourg

16 delegates

- Mr. Johnatan Pecero (Chairman)	ANEC G.I.E.
- Mr. Raphaël Bleuse	University of Luxembourg
- Mr. Matthias Brust	University of Luxembourg
- Mr. Cyril Cassagnes	Proximus Luxembourg
- Mrs. Myriam Djerouni	LUXITH G.I.E.
- 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
- Mrs. Digambal Nayagum	AS AVOCATS
- Mr. Joost Pisters	LuxCloud S.A.
- Mr. Jean Rapp	Actimage S.A.
- Mr. Jean-Michel Remiche	POST Telecom S.A.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology
- Mr. Shyam Wagle	ANEC G.I.E.

Comments

ISO/IEC JTC 1/SC 38, Cloud Computing and Distributed Platforms, 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.

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. By initiating standardization activities only after first identifying Cloud Computing standardization requirements, 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.

The current SC 38 work program includes:

- ISO/IEC FDIS 19086-2, Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric model;
- ISO/IEC CD 22123, Information Technology -- Cloud Computing -- Concepts and terminology;
- ISO/IEC CD 22624, Information technology -- Cloud Computing -- Taxonomy based data handling for cloud services;
- ISO/IEC PRF TR 22678, Information Technologies -- Cloud Computing -- Guidance for Policy Development;
- ISO/IEC AWI TS 23167, Information Technology -- Cloud Computing -- Common Technologies and Techniques;
- ISO/IEC PDTR 23186, Information technology -- Cloud computing -- Framework of trust for processing of multi-sourced data;
- ISO/IEC NP TR 23187, Information technology -- Cloud computing -- Interacting with cloud service partners (CSNs);
- ISO/IEC NP TR 23188, Information technology -- Cloud computing -- Edge computing landscape.
- ISO/IEC NP TR 23613, Information technology -- Cloud service metering and billing elements.

Moreover, 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 27018:2014 (under review), which respectively define 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. Currently, ISO/IEC JTC 1/SC 27 is developing the fourth part of ISO/IEC 19086, concerning the security and privacy aspects of the SLA framework and technology.

3.2.2.2. ITU-T/SG 13

General information			
Committee	**ITU-T/SG 13**	**Title**	**Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures**
Creation date	N/A	**MEMBERS**	N/A
Chairperson	Mr. Leo Lehmann		
Organizations in liaison	3GPP, ATIS, BBF, ETSI, Home Networks, ICT and Climate Change, IETF, ISO/IEC JTC 1, TM Forum		
Web site	https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx		
Scope	Study Group 13 has led ITU's standardization work on next-generation networks and now caters to the evolution of NGNs, while focusing on future networks and network aspects of mobile telecommunications. Today, SG13 focuses on future networks (FNs) – networks of the future beyond NGN – expected to enjoy early realization sometime around 2020 in prototyping or phased deployments. Cloud computing is an important part of SG13 work and the group develops standards that detail requirements and functional architectures of the cloud computing ecosystem, covering inter- and intra-cloud computing and technologies supporting XaaS (X as a Service). This work includes infrastructure and networking aspects of cloud computing models, as well as deployment considerations and requirements for interoperability and data portability. Given that cloud computing relies on the interplay of a variety of telecom and IT infrastructure resources, SG13 develops standards enabling consistent end-to-end, multi-cloud management and monitoring of services exposed by and across different service providers' domains and technologies. The lead study group roles include: - Lead study group on future networks such as IMT-2020 networks (non-radio related parts) - Lead study group on mobility management - Lead study group on cloud computing - Lead study group on trusted network infrastructures		
Structure	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 function virtualization (NFV) WP3/Q5 Applying networks of future and innovation in developing countries WP3/Q16 Knowledge-centric trustworthy networking and services **Other groups under SG13**: JCA-IMT2020 Joint Coordination Activity on IMT-2020		

	JCA-SDN	Joint Coordination Activity on Software-Defined Networking
Standardization work		
Published standards	468	
Standards under development	78	
Involvement of Luxembourg		
Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of ITU-T/SG 13.		
Comments		
SG13 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. SG13 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.		

3.3. Artificial Intelligence (AI) and Big Data

3.3.1. Artificial Intelligence

Introduced in 1956, the term Artificial Intelligence (AI) referred to a science and engineering of making intelligent machines, especially intelligent computer programs[61]. However a straightforward consensus definition of AI is not yet available, various conceptual ideas of AI have been proposed in the literature. One of the definitions suggested by ISO and IEC introduces AI as a "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"[62] Another definition that emerged in the ITU-T community says that[63]: "AI refers to the ability of a computer or a computer-enabled robotic system to process information and produce outcomes in a manner similar to the thought process of humans in learning, decision making and solving problems". 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 for perceiving environment and taking actions that maximize its chance of successfully achieving targeted goals[64]. In summary, the goal of AI systems is to develop systems capable of tackling complex problems in ways similar to human logic and reasoning.

Recently created sub-committee 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[65] as a "process using algorithms rather than procedural coding that enables learning from existing data in order to predict future outcomes". 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 sub-committee. 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 3.3.2.

Standards for Artificial Intelligence and Big Data technologies are essential for improving Trust in this technology, e.g. with respect to Cloud Computing, by enabling interoperability between the various applications and preventing vendor lock-in. Standards can also help to prevent over fitting in data analysis. This occurs when analysis designers tweak a model repeatedly to fit the data and begin to interpret noise or randomness as 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. Security and Privacy are of paramount importance for both data quality and for protection. Some of the large volume of data come from social media and medical records and inherently contain private information. Analysis of such data, particularly in conjunction with its context, must protect privacy. AI and Big Data systems should be designed with security in mind. If there is no global

[61] John McCarthy, father of AI, Dartmouth, 1956

[62] ISO/IEC 2382:2015(en), 2123769

[63] During ITU-T SG 3: Workshop on Policies in relation to impact of Artificial Intelligence on ICT services, Available on https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Documents/Shailendra%20Hajela_Presentation.pdf

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

[65] ISO/IEC 38505-1:2017, Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data

perspective on security, then fragmented solutions to address security may offer a partial sense of safety rather than full security. Standards will play an important role in data quality and data governance by addressing the veracity and value of data. Section 3.3.3 provides an overview of the AI and Big Data related technical committees currently active in the recognized standardization organizations. Moreover, standards for Artificial Intelligence and Big Data, as well as Digital Trust standards related to these areas, are listed in the Appendix (Section 6.3).

3.3.2. Big Data[66]

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"[67].

The definition of Big Data by ISO/IEC[68] [69] specifies it as follows:

"Data set(s) with characteristics (e.g. volume, velocity, variety, variability, veracity, etc.) that for a particular problem domain at a given point in time cannot be efficiently processed using current/existing/established/traditional technologies and techniques in order to extract value."

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 visualization[70]. 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 would push traditional data management principles to their limits[70]. Many others have added other Vs, but most of these do not relate to the data itself but to the result of analytics such as previewed value. IBM, has added a 4th V "Veracity" that specifically relates to the data itself[71]. This additional V in combination with the original 3Vs will be used in this report to refer to the characteristics of Big Data, which are depicted and described in Table 6 and Figure 3 respectively.

Table 6: The four characteristics of Big Data

Characteristic	Description
Volume	How much data: the amount of data that organizations try to harness to improve decision-making across the enterprise.

[66] Section based on ILNAS, "White Paper Big Data", 2016

[67] 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.

[68] ISO/IEC 38505-1:2017, Information technology -- Governance of IT -- Governance of data -- Part 1: Application of ISO/IEC 38500 to the governance of data

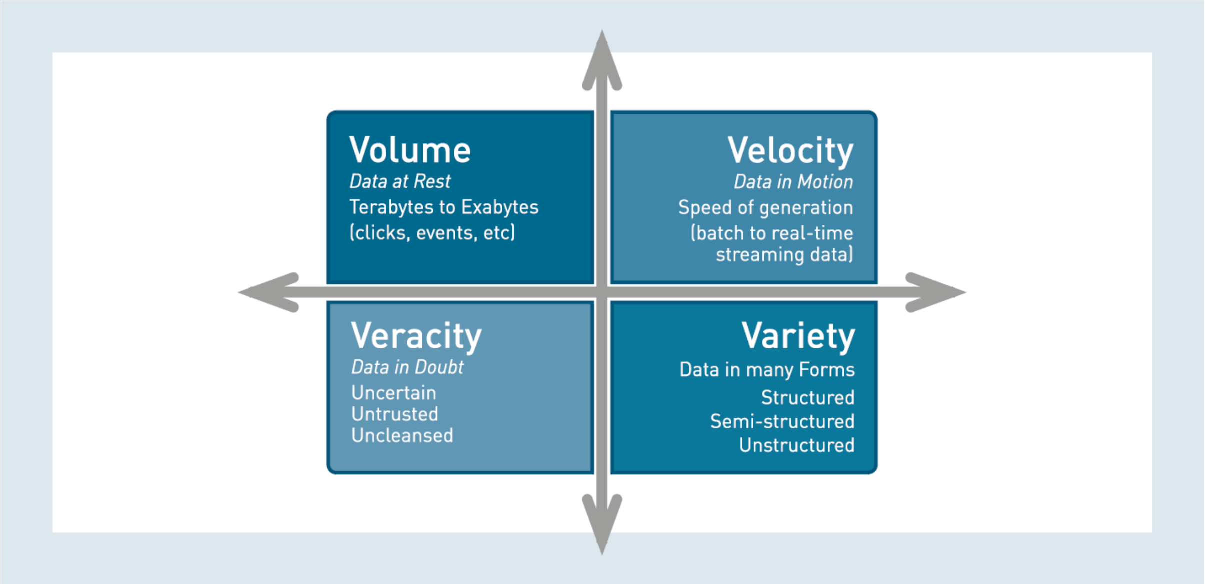
[69] ISO/IEC 20546:Information technology -- Big data -- Definition and vocabulary

[70] D. Laney, "3D data management: Controlling data volume, velocity and variety," META Gr. Res. Note, vol. 6, p. 70, 2001

[71] 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
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).
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).

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 data[72]:

- **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.

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

In practice mixed combinations of these three Big Data types occur which is referred to as **Poly-structured** data[73].

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”.

3.3.3. Artificial Intelligence and Big Data Standardization Committees

3.3.3.1. ISO/IEC JTC 1/SC 42

General information			
Committee	**ISO/IEC JTC 1/SC 42**	**Title**	**Artificial Intelligence**

Creation date	2017	**MEMBERS**	**Participating Countries (22):**
			United States, Australia, Austria, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Republic of Korea, **Luxembourg**, Portugal, Russian Federation, Spain, Sweden, Switzerland, United Kingdom
			
			Observing Countries (8):
			Belgium, Hungary, Mexico, Netherlands, New Zealand, Norway, Philippines, Poland

Secretariat	ANSI (USA)		
Secretary	Ms. Heather Benko		
Chairperson	Mr. Wael William Diab		
Organizations in liaison	IEEE, OGC		
Web site	https://www.iso.org/committee/6794475.html		
Scope	Standardization in the area of Artificial Intelligence Specifically, SC 42 standards include: 1. Serve as the focus and proponent for JTC 1's standardization program on Artificial Intelligence; 2. Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications.		
Structure	JTC 1/SC 42/WG 1 JTC 1/SC 42/SG 1 JTC 1/SC 42/SG 2 JTC 1/SC 42/SG 3	Foundational standards Computational approaches and characteristics of artificial intelligence systems Trustworthiness Use cases and applications	
Standardization work			
Published standards	2		
Standards under development	5		

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

Involvement of Luxembourg

15 delegates

- Mrs. Natalia Cassagnes (Chairwoman)	ANEC G.I.E.
- Mr. Johann Amsenga	INCERT GIE
- Mr. Matthias Brust	University of Luxembourg
- Mr. Vicent Cady	Tarkett S.A.
- Mr. Cyril Cassagnes	Proximus Luxembourg
- Mr. Christophe Delogne	Everis Spain SLU
- Mrs. Saharnaz Dilmaghani	University of Luxembourg
- Mr. Laurent Fisch	Laurent Fisch Luxlegal S.à r.l.
- Mrs. Aida Horaniet	Docler Holding
- Mr. Emmanuel Kieffer	University of Luxembourg
- Mr. Andreas Kremer	ITTM
- Mr. Johnatan Pecero	ANEC G.I.E.
- Mr. Benoit Poletti	INCERT GIE
- Mrs. Emilia Tantar	PwC
- Mr. Shyam Wagle	ANEC G.I.E.

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.

There are currently 4 approved working items under the responsibility of JTC 1/SC 42:

- ISO/IEC AWI TR 20547-1, Information technology -- Big data reference architecture -- Part 1: Framework and application process;
- ISO/IEC DIS 20547-3, Information technology -- Big data reference architecture -- Part 3: Reference architecture;
- ISO/IEC AWI 22989, Artificial Intelligence Concepts and Terminology;
- ISO/IEC AWI 23053, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

The committee also counts 2 published standards, resulted from the work of former ISO/IEC JTC 1/WG 9 Big Data:

- ISO/IEC TR 20547-2, Information technology -- Big data reference architecture -- Part 2: Use cases and derived requirements;
- ISO/IEC TR 20547-5, Information technology -- Big data reference architecture -- Part 5: Standards roadmap.

3.3.3.2. ISO/IEC JTC 1/SC 32

General information			
Committee	**ISO/IEC JTC 1/SC 32**	**Title**	**Data management and interchange**

Creation date	1997	**MEMBERS**	**Participating Countries (14):**
			United States, Canada, China, Côte d'Ivoire, Czech Republic, , Finland, Germany, India, Italy, Japan, Kazakhstan, Republic of Korea, Russian Federation, United Kingdom
			Observing Countries (23):
			Argentina, Austria, Belgium, Bosnia and Herzegovina, Egypt, France, Ghana, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, **Luxembourg**, Republic of Moldova, Netherlands, Poland, Portugal, Romania, Serbia, Spain, Switzerland, Turkey, Ukraine

Secretariat	ANSI (USA)		
Secretary	Ms. Michaela Miller		
Chairperson	Mr. Jim Melton		
Organizations in liaison	Infoterm, UNECE, LDBC		
Web site	https://www.iso.org/committee/45342.html		
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: - 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	JTC 1/SC 32/AHG 1 JTC 1/SC 32/WG 1 JTC 1/SC 32/WG 2 JTC 1/SC 32/WG 3 JTC 1/SC 32/WG 4	Ad Hoc Group of WG 2 and WG 4 eBusiness MetaData Database language SQL/Multimedia and application packages	

Standardization work	
Published standards	78
Standards under development	43

Involvement of Luxembourg

3 delegates

- Mrs. Natalia Cassagnes	ANEC G.I.E.
- Mr. Christophe Delogne	Everis Spain SLU
- Mr. Johnatan Pecero	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.

Examples of standards developed by ISO/IEC JTC 1/SC 32 are:

- ISO/IEC 9075-1:2016, Information technology -- Database languages -- SQL -- Part 1: Framework (SQL/Framework);
- ISO/IEC 11179-1:2015, Information technology -- Metadata registries (MDR) -- Part 1: Framework;
- ISO/IEC 19503:2005, Information technology -- XML Metadata Interchange (XMI);
- ISO/IEC 19763-1:2015, Information technology -- Metamodel framework for interoperability (MFI) -- Part 1: Framework.

Current work program of JTC 1/SC 32 includes for example:

- The development of a new part in the ISO/IEC 9075 series of standards concerning the integration of multi-dimensional arrays in the SQL database language (ISO/IEC FDIS 9075-15);
- The development of ISO/IEC 21838 series that will recommend the characteristics of a top-level ontology, which will provide guidance to various parties who are currently developing or who will develop a top-level ontology. For those seeking to select and use an existing top-level ontology, it will provide at least one from which to choose. It will also facilitate the merging of top-level ontologies, since they will already possess the recommended characteristics;
- The creation of new series of standards on metadata (ISO/IEC 19583 series), notably for data provenance metadata, which will support Big Data;
- The development of standards in support of electronic data interchange (EDI) for businesses, including privacy protection requirements, model for transborder data flows, etc. (ISO/IEC 15944 series).

The topics of next generation analytics and big data appear frequently both in computing industry and more general news reports. SC 32 initiated a study group in these areas and delivered a preliminary report to JTC 1 that identified existing SC 32 standards that support these technologies and opportunities for enhancing work in these areas.

3.4. Blockchain and Distributed Ledger Technologies

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., are immutable) once it has been written to the ledger. The chaining of transactions distinguishes blockchain from other distributed ledger technologies 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).

Blockchain and DLT 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.

3.4.1. Characteristics

Table 7: Key features of Blockchain

Characteristic	Description
Public blockchain and private blockchain	Based on the application scenario and parameters such as access control requirements and regulatory compliance goals, a blockchain/DLT system might consider being a: - Public blockchain: The 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.
Permissionless blockchain and permissioned blockchain	Similarly, another classification of blockchain/DLT systems comprises: - Permissionless blockchain: The 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. Typically, blockchain solutions are configured by combining the above two possibilities. For instance, bitcoin blockchain is public and permissionless since it is not only open for any participant to join as users and serve as nodes but also for the data to be publicly transparent.

Characteristic	Description
Secure data registry	When a node creates a new block, it includes in the header of this block a 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, if another node verifies the referenced hash to be the same as it recognizes, it implicitly verifies that both nodes agree on 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.
Consensus mechanisms and notion of trust	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. For instance, Proof-of-Work (PoW) accomplishes several tasks: - 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 introduces new cryptocurrency (e.g., bitcoin) into the system at a steady rate and rewards miners using an arguably fair distribution mechanism. - It makes blocks tamper-resistant.

3.4.2. Blockchain and Distributed Ledger Technologies Standardization Technical Committees

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 the Blockchain and Distributed Ledger Technologies related technical committees currently active in the recognized standardization organizations.

3.4.2.1. ISO/TC 307

General information			
Committee	**ISO/TC 307**	**Title**	**Blockchain and distributed ledger technologies**
Creation date	2016	**MEMBERS**	**Participating Countries (39):** Australia, Austria, Belgium, Brazil, Cambodia, Canada, China, Croatia, Cyprus, Denmark, Finland, France, Germany, Hungary, India, Ireland, Italy, Jamaica, Japan, Kazakhstan, Republic of Korea, **Luxembourg**, Malaysia, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden,
Secretariat	SA (Australia)		
Secretary	Ms. Emily Dawson		
Chairperson	Mr. Craig Dunn		
Organizations in liaison	EC, FIG, IEEE, ITU, SWIFT, UNECE		

			Switzerland, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States **Observing Countries (13):** Argentina, Belarus, Czech Republic, Hong Kong, Indonesia, Islamic Republic of Iran, Israel, Kenya, Mexico, Morocco, Philippines, Slovakia, Uruguay
Web site	https://www.iso.org/committee/6266604.html		
Scope	Standardization of blockchain technologies and distributed ledger technologies.		
Structure	ISO/TC 307/CAG 1	Convenors coordination group	
	ISO/TC 307/WG 1	Foundations	
	ISO/TC 307/WG 2	Security, privacy and identity	
	ISO/TC 307/WG 3	Smart contracts and their application	
	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	
	ISO/TC 307/WG 5	Governance	
	ISO/TC 307/SG 2	Use cases	
	ISO/TC 307/SG 6	Governance of blockchain and distributed ledger technology systems	
	ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems	
Standardization work			
Published standards	0		
Standards under development	11		

Involvement of Luxembourg

16 delegates

- Mr. Johnatan Pecero (Acting Chairman)	ANEC G.I.E
- Mr. Johann Amsenga	INCERT GIE
- Mr. Monique Bachner	LetzBlock A.s.b.l.
- Mr. Benoit Bertholon	COINPLUS S.A.
- Mr. Cyril Cassagnes	Proximus Luxembourg
- Mr. Elias Chbeir	ELIAS S.à.r.l.-S.
- Mr. Christophe Delogne	Everis Spain SLU
- Mr. Sami El Bouamri	Initio Luxembourg S.A.
- Mrs. Michèle Feltz	ILNAS
- Mr. Antoine Gaury	Etix Everywhere S.A.
- Mr. Philippe Germain	PmG SD S.à r.l.
- Mr. Jean Lancrenon	itrust consulting S.à r.l.
- Mrs. Marie-Charlotte Renaux	Initio Luxembourg S.A.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology (LIST)
- Mr. Sebastien Varrette	University of Luxembourg
- Mr. Povilas Zinys	LuxTrust

Comments

Standards and/or projects under the direct responsibility of ISO/TC 307:

- ISO/CD 22739, Blockchain and distributed ledger technologies -- Terminology;

- ISO/AWI 23257, Blockchain and distributed ledger technologies -- Reference architecture;
- ISO/AWI TS 23258, Blockchain and distributed ledger technologies -- Taxonomy and Ontology;
- ISO/AWI TS 23259, Blockchain and distributed ledger technologies -- Legally binding smart contracts;

The following projects are currently under balloting process and will be added to the program of work if they are approved:

- ISO/NP TR 23244, Blockchain and distributed ledger technologies -- Overview of privacy and personally identifiable information (PII) protection;
- ISO/NP TR 23245, Blockchain and distributed ledger technologies -- Overview of privacy and personally identifiable information (PII) protection;
- ISO/NP 23246, Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies;
- ISO/NP TR 23455, Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems;
- ISO/NP TR 23576, Blockchain and distributed ledger technologies -- Security of digital asset custodians;
- ISO/NP TR 23578, Blockchain and distributed ledger technologies -- Discovery issues related to interoperability.

3.4.2.2. ITU-T FG DLT

General information			
Committee	**ITU-T/FG DLT**	**Title**	**Focus Group on Application of Distributed Ledger Technology**
Creation date	2017	**MEMBERS**	N/A
Chairperson	Mr. David Watrin		
Organizations in liaison	ISO, GSMA, SWIFT		
Web site	https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx		
Scope	The ITU-T FG DLT will analyze applications and services based on DLT that can be standardized by ITU-T study groups, identify best practices and guidance which could support the implementation of such applications and services on a global scale and identify a way forward that ITU-T SGs need to study in order to meet the urgent market needs. It will develop a security standardization roadmap for interoperable services based on DLT taking into consideration the activities currently undertaken by the various relevant groups, standards developing organizations (SDOs) and forums and a regulatory toolkit which may be used by national policymakers and regulatory authorities from ITU Member States.		
Structure	/		
Standardization work			
Published standards	/		
Standards under development	/		
Involvement of Luxembourg			
Note: ILNAS, with the support of ANEC G.I.E., is monitoring the standardization developments of the ITU-T/FG DLT.			
Comments			
In May 2017, ITU-T created a Focus Group called the "Application of Distributed Ledger Technology" (FG DLT) with the objective of developing a standardization roadmap for interoperable DLT-based services, taking into consideration the activities underway in ITU, other standards developing organizations, forums and groups. Several projects are already under development in different ITU-T SGs. The Telecommunication Standardization Advisory Group (TSAG) advises ITU-T SGs on developments required by the market and cooperates with other parties involved in blockchain and DLT standardization in order to avoid duplication of work (e.g., with ISO/TC 307).			

3.5. 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 time[74] 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 addressed[75]. 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 3.4, 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 vulnerability[76]. 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.

3.5.1. Basic Components of Digital Trust

3.5.1.1. 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 requirement[77]. In a study about privacy behaviors regarding information technology, Acquisti *et al.*[78] *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 information[79] and if other individuals have already agreed to share the information[80]. Privacy is **malleable**, meaning that the acceptable level of 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

[74] K. J. Hole, Anti-fragile ICT Systems, Simula Spr. Cham: Springer International Publishing, 2016.

[75] ILNAS "White paper Digital Trust for Smart ICT", 2016 and ETSI TR 103 306 V1.2.1 (2017-03): "CYBER; Global Cyber Security Ecosystem".

[76] 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.

[77] 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.

[78] 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.

[79] 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.

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

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.

3.5.1.2. 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 Networks[81] 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 Systems[82]. 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.

3.5.1.3. 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 interoperability[83] [12]. 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 3.1 to Section 3.3.

[81] OECD, “OECD Guidelines for the Security of Information Systems and Networks,” Organ. Econ. Co-operation Dev., 2002

[82] 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.

[83] 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

3.5.2. Digital Trust Standardization 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, particularly Internet of Things, Cloud Computing, as well as Artificial Intelligence and Big Data, which are currently active in the recognized standardization organizations.

3.5.2.1. ISO/IEC JTC 1/SC 17

General information			
Committee	**ISO/IEC JTC 1/SC 17**	**Title**	**Cards and personal identification**

Creation date	1987	**MEMBERS**	**Participating Countries (32):**
			United Kingdom, Armenia, Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Israel, Italy, Japan, Kenya, Republic of Korea, **Luxembourg**, Malaysia, Netherlands, Poland, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, United States
			Observing Countries (21):
			Argentina, Bosnia and Herzegovina, Croatia, Ghana, Hong Kong, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Kazakhstan, Lithuania, Republic of Moldova, New Zealand, Norway, Portugal, Serbia, Thailand, Turkey, Ukraine, Viet Nam

Secretariat	BSI (United Kingdom)		
Secretary	Ms. Jean Stride		
Chairperson	Dr. Peter Waggett		
Organizations in liaison	AMEX, CCETT, Ecma International, IATA, ICAO, ICMA, ILO, MasterCard, SBS, VISA, EUDCA, JAVA CARD FORUM, NFC Forum, UNECE, EUDCA		
Web site	https://www.iso.org/committee/45144.html		
Scope	The current area of work for JTC 1/SC 17 consists of: - Identification and related documents; - Cards; - Security devices and tokens; - Interface associated with their use in inter-industry applications and international interchange.		
Structure	JTC 1/SC 17/CAG 1 Chairman advisory group JTC 1/SC 17/SG 1 Mobile identification JTC 1/SC 17/SWG 1 Registration Management Group (RMG) JTC 1/SC 17/WG 1 Physical characteristics and test methods for ID-cards JTC 1/SC 17/WG 3 Identification cards - Machine readable travel documents JTC 1/SC 17/WG 4 Integrated circuit card with contacts JTC 1/SC 17/WG 5 Identification cards - Identification of issuers JTC 1/SC 17/WG 8 Integrated circuit cards without contacts JTC 1/SC 17/WG 10 Motor vehicle driver license and related documents JTC 1/SC 17/WG 11 Application of biometrics to cards and personal identification JTC 1/SC 17/WG 12 Drone license and drone identity module		
Standardization work			
Published standards	114		

Standards under development	24

Involvement of Luxembourg

4 delegates

- Mr. Valentin Lacave	Telindus S.A.
- Mr. Abdelkrim Nehari	INCERT GIE
- Mr. Enrico Ozzano	BIL S.A.
- Mr. Benoit Poletti	INCERT GIE

Comments

ISO/IEC JTC 1/SC 17 is responsible for the development of a large portfolio of card standards in support of interoperability and data interchange.

At a minimum, the standards define the physical dimensions of the card and the geometry of the terminals which read those cards (e.g. the slot in an ATM). Then, depending on the reading technology, the standards define how the card "couples" with the card terminal and thereby communicates with the underlying application (e.g. motorized mag strip readers in ATMs, magnetic stripe swipe readers in Point-of-Sale terminals, slot readers in hotel card key locks).

At their most basic level, standards maintain interoperability between cards and the card readers that read them. For a closed system or national implementation, interoperability is important so that components, such as the cards or the chips on smart cards sourced on the open market from various manufacturers, will interoperate, with a high degree of confidence, with card readers sourced from different manufacturers.

Two of the most sophisticated technologies involve microprocessors embedded in the card, also known as "smart cards". These are "cards with contacts" and "contactless cards". Cards with contacts are usually inserted manually into a "dip reader" whereas contactless cards use radio frequency coupling to enable "touch and go" for rapid transit ticket gates and "wave and pay" to make low value purchases in retail outlets such as fast food restaurants. Electronic passports (ePassports) and citizen identification cards are further examples where contactless standards have been adopted.

JTC 1/SC 17 has recently revised ISO/IEC 7812-1, Identification cards -- Identification of issuers -- Part 1: Numbering system, to answer the need to expand the Issuer Identification Numbering scheme (IINs) from its present 6-digit IIN to an 8-digit IIN going forward.

Current work programs of JTC 1/SC 17 include, for example:

- The revision of ISO/IEC 7810:2003 regarding the physical characteristics of identification cards;
- The revision of ISO/IEC 18013 series of standards concerning ISO-compliant driving licence.

3.5.2.2. ISO/IEC JTC 1/SC 27

General information			
Committee	ISO/IEC JTC 1/SC 27	Title	IT Security techniques

Creation date	1989	MEMBERS	**Participating Countries (51):**
			Germany, Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, Costa Rica, Côte d'Ivoire, Denmark, Finland, France, India, Indonesia, Islamic Republic of Iran, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, Republic of Korea, Lebanon, **Luxembourg**, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Panama, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay
			Observing Countries (26):
			Belarus, Bosnia and Herzegovina, Bulgaria, Cyprus, Czech Republic, El Salvador, Estonia, Eswatini, Ghana, Hong Kong, Hungary, Iceland, Lithuania, Morocco, Norway, Pakistan, State of Palestine, Rwanda, Saudi Arabia, Senegal, Serbia, Slovenia, Sri Lanka, Thailand, The Former Yugoslav Republic of Macedonia, Turkey

Secretariat	DIN (Germany)		
Secretary	Ms. Krystyna Passia		
Chairperson	Dr. Andreas Wolf		
Organizations in liaison	(ISC)2, CalConnect, CCETT, CSA, ECBS, Ecma International, ENISA, EPC, ETSI, Global Platform Inc., IEEE, ISACA, ISSEA, ITU, MasterCard, SBS, ABC4Trust, Article 29 Data Protection Working Party, CCBD, CREDENTIAL, CSCC, Cyber Security, EUDCA, EuroCloud, FIRST, IFAA, INLAC, Interpol, ISA – Automation, ISCI, ISF, Kantara Initiative, OASIS-PMRM, OECD, OIDF, Opengroup – United Kingdom, PICOS, PQCRYPTO, PRIPARE, PRISMACLOUD, SAFEcrypto, TAS3, TCG, TNForum, TREsPASS, WITDOM		
Web site	https://www.iso.org/committee/45306.html		
Scope	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: - 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; - Security evaluation criteria and methodology. 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.		
Structure	JTC 1/SC 27/AG 1 JTC 1/SC 27/SG 1	Management Advisory Group Data Security	

	JTC 1/SC 27/SWG-T	Transversal Items
	JTC 1/SC 27/WG 1	Information security management systems
	JTC 1/SC 27/WG 2	Cryptography and security mechanisms
	JTC 1/SC 27/WG 3	Security evaluation testing and specification
	JTC 1/SC 27/WG 4	Security controls and services
	JTC 1/SC 27/WG 5	Identity management and privacy technologies

Standardization work

Published standards	183
Standards under development	67

Involvement of Luxembourg

32 delegates

-	Mr. Benoit Poletti (Chairman)	INCERT GIE
-	Mr. Cédric Mauny (Vice-Chairman)	Telindus Luxembourg S.A.
-	Mr. Carlo Harpes (Vice-Chairman)	itrust consulting S.à r.l.
-	Mr. Johann Amsenga (Convenor WG 4)	INCERT GIE
-	Mr. Matthieu Aubigny	itrust consulting S.à r.l.
-	Mr. François Barret	KPMG Luxembourg S.C.
-	Mr. Stanley Beeks	INCERT GIE
-	Mr. Benoit Bertholon	COINPLUS S.A.
-	Mr. Raphaël Bleuse	University of Luxembourg
-	Mr. Hervé Cholez	LIST
-	Mr. Stéphane Cortina	LIST
-	Mrs. Saharnaz Dilmaghani	University of Luxembourg
-	Mrs. Myriam Djerouni	LUXITH G.I.E.
-	Mr. Nicolas Domenjoud	ILNAS
-	Mrs. Cécile Doussine	INCERT GIE
-	Mrs. Michèle Feltz	ILNAS
-	Mr. Ben Fetler	CTIE
-	Mr. Philippe Germain	PmG SD S.à r.l.
-	Mr. Clement Gorlt	INCERT GIE
-	Mrs. Shenglan Hu	POST Telecom PSF S.A.
-	Mrs. Céline Kerger	INCERT GIE
-	Mr. Jean Lancrenon	itrust consulting S.à r.l.
-	Mr. Tom Leclerc	Telindus Luxembourg S.A.
-	Mr. Michel Ludwig	ILNAS
-	Mr. Nicolas Mayer	LIST
-	Mr. Olivier Montee	Cours@home Luxembourg S.à.r.l.
-	Mr. Enrico Ozzano	BIL S.A.
-	Mr. Gaëtan Pradel	INCERT GIE
-	Mr. René Saint-Germain	ALTIRIAN S.A.
-	Mr. Nader Samir Labib	University of Luxembourg
-	Mr. Raphaël Taban	CTIE
-	Mr. Qiang Tang	LIST

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. Organizations setting up an ISMS certified compliant with ISO/IEC 27001 are increasingly numerous[84].

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 and ISO/IEC JTC 1/WG 11:

- ISO/IEC AWI 27030, Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT);
- ISO/IEC AWI TS 27570, Information Technology -- Security Techniques -- Privacy guidelines for Smart Cities.

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

- ISO/IEC 27018:2014, Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- 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 27036-4:2016, Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services;
- ISO/IEC DIS 19086-4, Information technology -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Components of security and of protection of PII.

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

- ISO/IEC CD 20547-4, Information technology -- Big data reference architecture -- Part 4: Security and privacy.

[84] Source: ISO survey 2017

3.5.2.3. ISO/TC 46/SC 11

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td><b>Committee</b></td><td><b>ISO/TC 46/SC 11</b></td><td><b>Title</b></td><td><b>Archives/records management</b></td></tr>
<tr><td><b>Creation date</b></td><td>1998</td><td rowspan="5"><b>MEMBERS</b></td><td rowspan="5"><b>Participating Countries (33):</b>
Australia, Belgium, Bulgaria, Canada, China, Colombia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Japan, Kenya, Republic of Korea, Lithuania, Malaysia, Netherlands, New Zealand, Norway, Portugal, Russian Federation, South Africa, Spain, Sweden, Switzerland, Ukraine, United Kingdom, United States

<b>Observing Countries (16):</b>
Argentina, Austria, Brazil, Chile, Cuba, Iceland, Islamic Republic of Iran, <b>Luxembourg</b>, Poland, Romania, Serbia, Singapore, Slovakia, Slovenia, Sri Lanka, Thailand</td></tr>
<tr><td><b>Secretariat</b></td><td>SA (Australia)</td></tr>
<tr><td><b>Secretary</b></td><td>Ms. Clare Hobern</td></tr>
<tr><td><b>Chairperson</b></td><td>Ms. Judith Ellis</td></tr>
<tr><td><b>Organizations in liaison</b></td><td>ICA, InterPARES, IRMT, ITU</td></tr>
<tr><td><b>Web site</b></td><td colspan="3">https://www.iso.org/committee/48856.html</td></tr>
<tr><td><b>Scope</b></td><td colspan="3">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.</td></tr>
<tr><td><b>Structure</b></td><td colspan="3">TC 46/SC 11/AHG Strategic Directions
TC 46/SC 11/AHG 5 Risk management
TC 46/SC 11/WG 1 Metadata
TC 46/SC 11/WG 8 Management of systems for records
TC 46/SC 11/WG 14 Records requirements in enterprise Architecture
TC 46/SC 11/WG 15 Appraisal for Managing Records
TC 46/SC 11/WG 16 Systems design for records
TC 46/SC 11/WG 17 Records in the cloud
TC 46/SC 11/WG 18 ISO 13008:2012 Revision</td></tr>
<tr><th colspan="4">Standardization work</th></tr>
<tr><td><b>Published standards</b></td><td colspan="3">17</td></tr>
<tr><td><b>Standards under development</b></td><td colspan="3">7</td></tr>
<tr><th colspan="4">Involvement of Luxembourg</th></tr>
<tr><td colspan="4"><b>8 delegates</b>

- Mr. Lucas Colet (Chairman) Altirian S.A.
- Mrs. Sylvie Dessolin SOPRA STERIA PSF Luxembourg S.A.
- Mrs. Sylvie Forastier Linklaters LLP
- Mr. Michel Ludwig ILNAS
- Mr. Henri Montin <i>Centre des Technologies de l’Information de l’Etat</i> (CTIE)
- Mr. Michel Picard Luxembourg Institute of Science and Technology (LIST)
- Mr. Serge Raucq CTIE
- Mr. Alain Wahl ILNAS</td></tr>
</table>

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.

ISO/TC 46/SC 11 is currently developing seven standards, including:

- ISO 16175 series defining the principles and functional requirements for records in electronic office environments;
- ISO/DTR 22428, Information and documentation -- Records management in the cloud: Issues and concerns.

3.5.2.4. CEN/CLC/JTC 8

General information			
Committee	**CEN/CLC/JTC 8**	Title	**Privacy management in products and services**
Creation date	2014	MEMBERS	34 members of CEN/CENELEC
Secretariat	DIN (Germany)		
Secretary	Mr. Martin Uhlherr		
Chairperson	Mr. Alessandro Guarino		
Organizations in liaison	N/A		
Web site	https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2273903&cs=1BB28F0625D0C6BA121FBC4A04EC8ED55		
Scope	The scope of the JTC 8 is to cover privacy and personal data protection in products and services.		
Structure	JTC 8/WG 1 Privacy management in products and services JTC 8/WG 2 Video surveillance and access control		
Standardization work			
Published standards	0		
Standards under development	1		

Involvement of Luxembourg

2 delegates

-	Mrs. Natalia Cassagnes	ANEC G.I.E.
-	Mrs. Andra Giurgiu	University of Luxembourg

Comments

In 2014, CEN and CENELEC created a new Joint Working Group (JWG) whose main task is to provide the response to the new EC standardization request on 'Privacy management in the design and development and in the production and service provision processes of security technologies'[85]. The request aims at the implementation of Privacy-by-design principles for security technologies and/or services lifecycle. The new standardization deliverables are intended to define and share best practices balancing security, transparency and privacy concerns for security technologies, manufacturers and service providers in Europe.

In 2017, the JWG was transformed in a new joint technical committee CEN/CLC/JTC 8 that met for the first time in July. The TC has now started working on the development of a new European Standard setting out requirements on privacy by design principles in the design and implementation of security technologies and services.

[85] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548

3.5.2.5. CEN/CLC/JTC 13

General information			
Committee	**CEN/CLC/JTC 13**	**Title**	**Cybersecurity and Data Protection**
Creation date	2017	**MEMBERS**	34 members of CEN/CENELEC
Secretariat	DIN (Germany)		
Secretary	Mr. Martin Uhlherr		
Chairperson	Mr. Walter Fumy		
Organizations in liaison	N/A		
Web site	https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B		
Scope	Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to: - 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 Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1and 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.		
Structure	JTC 13/WG 1 Chairman advisory group JTC 13/WG 2 Cybersecurity Management Systems JTC 13/WG 3 Security evaluation and assessment JTC 13/WG 4 Cybersecurity services JTC 13/WG 5 Data Protection, Privacy and Identity Management JTC 13/WG 6 Product security		
Standardization work			
Published standards	8		
Standards under development	1		
Involvement of Luxembourg			
NO (no registered delegate)			

Comments

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.

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).

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. The committee is currently working on the adoption of the last version (2018) of ISO/IEC 27000, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.

3.5.2.6. CEN/TC 224

General information			
Committee	**CEN/TC 224**	**Title**	**Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment**
Creation date	1989	**MEMBERS**	34 members of CEN/CENELEC
Secretariat	AFNOR (France)		
Secretary	Ms. Fanny Lannoy		
Chairperson	Mr. Franck Leroy		
Organizations in liaison	ANEC, FRONTEX, GlobalPlatform, UIC		
Web site	http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_LANG_ID,FSP_ORG_ID:25,6205&cs=1A98C573151AB3D7A22712120D94364C1#1		
Scope	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: - 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	CEN/TC 224/WG 6 User Interface CEN/TC 224/WG 11 Transport applications CEN/TC 224/WG 15 European citizen card CEN/TC 224/WG 16 Application Interface for smart cards used as Secure Signature Creation Devices CEN/TC 224/WG 17 Protection Profiles in the context of SSCD CEN/TC 224/WG 18 Biometrics CEN/TC 224/WG 19 Breeder Documents		

Standardization work	
Published standards	61
Standards under development	8

Involvement of Luxembourg	
3 delegates	
- Mr. Benoit Poletti (Chairman)	INCERT GIE
- Mrs. Shenglan Hu	POST Telecom PSF
- Mr. Enrico Ozzano	BIL S.A.

Comments

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.

The current objectives of CEN/TC 224 are to elaborate or maintain standards on:

- General card characteristics and technologies;
- Man machine interface;
- Inter-sector electronic purse;
- Telecommunications integrated circuit cards and terminals;
- Surface transport applications;
- Identification, Authentication and Signature (IAS) services based on smart secure devices;
- Biometrics for the need of European travel or governmental documents;
- Health sector cards.

Additional objectives of CEN/TC 224 are to consider the requirements for further standardization in the following areas:

- Additional devices under the control of the card (new displays, new embedded input/output devices on-board the card including electronic display, capacitive or resistive keypad, button, biosensor, power supply device, etc.) leading to new use relevant cases
- Privacy Impact Assessment (PIA): requirement for an evaluation model of privacy-by-design card-based products and/or services
- Privacy by design and convergence platform: starting the design with privacy requirements at the project outset and capitalizing on a common platform ground fulfilling a minimum requirement set for privacy supporting a diversity of applications on top of it.

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 recently published standards on protection profiles for signature creation and verification application (EN 419111 series) or on an application interface for secure elements for electronic identification, authentication and Trusted Services (EN 419212 series). It is also currently developing standards on trustworthy systems supporting server signing (EN 419241 series).

3.5.2.7. ETSI/TC CYBER

General information			
Committee	ETSI/TC CYBER	Title	Cyber Security
Creation date	2014	MEMBERS	135 member organizations of ETSI
Chairperson	Mr. Alex Leadbeater		
Organizations in liaison	BIF, CEN, CENELEC, CIS, ECSO, ENISA, Eurosmart, GISFI, GSMA, ISO/IEC JTC 1, TAICS, TCG, TTA		
Web site	https://portal.etsi.org/cyber		
Scope	The activities of ETSI TC CYBER include the following broad areas: - 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 to ensure security - Creation of security specifications and alignment with work done in other TCs.		
Structure	WG-QSC Quantum-Safe Cryptography		
Standardization work			
Published standards	34		
Standards under development	20		

Involvement of Luxembourg

Note: ILNAS is monitoring the developments of the ETSI/TC CYBER.

Comments

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.).

The work program of TC CYBER include the following projects:

- DTS/CYBER-0024, CYBER; Critical Infrastructure Metrics for Identification of CI;
- DTS/CYBER-0027-4, CYBER; Middlebox Security Protocol; Part 4: Profile for network based IPsec traffic;
- DMI/CYBER-0030; ETSI mcTLS protocol demonstration;
- DTS/CYBER-0040, CYBER; Critical Security Controls for MSP middlebox defence;
- DTS/CYBER-0044, CYBER; External encodings for the Advanced Encryption Standard;
- DMI/CYBER-QSC-0010, CYBER QSC Extended Roadmap; CYBER QSC Extended Roadmap Related Material;
- ETSI TS 102 165-2, CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures;
- ETSI TR 103 331, CYBER; Structured threat information sharing;

- ETSI TR 103 370, CYBER; Practical introductory guide to privacy;
- ETSI TS 103 485, CYBER; Mechanisms for privacy assurance and verification;
- ETSI TS 103 486, CYBER; Identity management and naming schema protection mechanisms;
- ETSI TS 103 523-1, CYBER; Middlebox Security Protocol; Part 1: Capability Requirements;
- ETSI TS 103 523-2, CYBER; Middlebox Security Protocol; Part 2: Transport layer MSP, Profile for fine grained access control;
- ETSI TS 103 532, CYBER; Attribute Based Encryption for Attribute Based Access Control;
- ETSI TR 103 616, CYBER; Quantum Safe Signatures;
- ETSI TR 103 618, CYBER; Quantum-Safe Identity-Based Encryption;
- ETSI TR 103 619, CYBER; Migration strategies and recommendations to Quantum-Safe schemes;
- ETSI TR 103 643, CYBER; Report on techniques for assurance of digital material used in legal proceedings;
- ETSI TR 103 644, CYBER; Guidelines for increasing smart meter security;
- ETSI TS 103 645, CYBER; Cyber Security for Consumer Internet of Things.

3.5.2.8. ETSI/TC ESI

General information			
Committee	**ETSI/TC ESI**	**Title**	**Electronic Signatures and Infrastructures**
Creation date	/	**MEMBERS**	70 member organizations of ETSI
Chairperson	Mr. Riccardo Genghini		
Organizations in liaison	CAB Forum, CEN, CENELEC, CEPT COM-ITU, EA, ECSO, ENISA, Eurosmart, ISO, ISO/IEC JTC 1, ISOC/IETF, ITU, OASIS, OpenPEPPOL, PRETA, SAFE-BioPharma, TTA, UNECE, UPU		
Web site	http://portal.etsi.org/esi		
Scope	TC ESI is the lead body within ETSI in relation to Electronic Signatures and Infrastructures, including the preparation of reports and other necessary activities, by: - Developing generic standards, guides and reports relating to electronic signatures and related trust infrastructures to protect electronic transactions and ensure trust and confidence with business partners; - Liaising with other ETSI bodies in relation to electronic signatures and related trust infrastructures; - Liaising with bodies external to ETSI in relation to electronic signatures and related trust infrastructures; - Establishing a continuing work plan in relation to electronic signatures and related trust infrastructures.		
Structure	/		
Standardization work			
Published standards	158		
Standards under development	39		

Involvement of Luxembourg

3 companies

- eWitness S.A.
- Luxtrust
- POST Luxembourg

Note: ILNAS, with the support of ANEC G.I.E. is monitoring the standardization developments of the ETSI/TC ESI.

Comments

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.

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.

TC ESI maintains standards and specifications published in response to European Commission (EC) Mandate M/460 on Electronic Signature Standardization. During 2017, the committee started maintenance of deliverables published in response to mandate M/460. The European Standard (EN) providing statements for qualified certificates was re-published. The EN on general security and policy requirements for trust service providers (TSP) as well as the two ENs on security and policy requirements for trust service providers issuing (qualified) certificates have been reviewed to consider feedback from implementations and auditors, latest specifications from the CA/Browser Forum and also cover additional features requested by the eIDAS Regulation.

3.6. Introduction on 5G and Intelligent Transport Systems (ITS) Technical Standardization

This section focuses on two topics currently receiving a particular attention from the economic market: fifth generation mobile communication (5G) and Intelligent Transport Systems (ITS). They could significantly and deeply transform our economy and society due to the high impact they will have on our lifestyles, in relation with current Smart ICT developments. A standards watch on these topics has been performed in order to provide insights on existing developments as well as to encourage involvement of interested stakeholders at the national level.

3.6.1. Fifth-generation wireless (5G)

Fifth-generation wireless, 5G, is the latest iteration of previous cellular technologies, such as of 3G and 4G. It is designed to greatly increase the speed and responsiveness of the wireless networks. With 5G, up to 20 Gbps data speed exceeding wireline networks speeds, as well as 1 millisecond or lower latency are expected over wireless broadband networks, which is sufficient for the real-time feedback. 5G is also considered as a backbone network for Internet of Things (IoT) implementation. A self-driving car, for example, would require an extremely fast, low latency connection so a vehicle could navigate in a real-time. In this context, self-driving car could take full advantage of 5G technology. The primary beneficiaries of 5G will be consumers, but 5G presents a huge opportunity for the digitization of economies and modernization of all industry sectors.

Several industry sectors are being engaged in the process of building 5G, and are actively shaping the technology to meet their needs through participation in the standardization process. The basic performance criteria for 5G systems have been set in IMT-2020 recommendation of ITU. A Focus Group of ITU-T, presented below, is currently working to prepare next developments of wireless networks technical standardization.

3.6.1.1. ITU- T FG NET-2030

General information			
Committee	**ITU-T/FG NET-2030**	**Title**	**Focus Group Technologies for Network 2030 (FG NET-2030)**
Creation date	2018	**MEMBERS**	N/A
Chairperson	Dr. Richard Li		
Organizations in liaison	N/A		
Web site	https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx		
Scope	The objectives of the focus group include: - To study, review and survey existing technologies, platforms, and standards for identifying the gaps and challenges towards Network 2030, which are not supported by the existing and near future networks like 5G/IMT-2020; - To formulate all aspects of Network 2030, including vision, requirements, architecture, novel use cases, evaluation methodology, and so forth; - To provide guidelines for standardization roadmap; - To establish liaisons and relationships with other SDOs.		

Structure	Sub-Group 1 Use Cases & Requirements Sub-Group 2 Network Services & Technology Sub-Group 3 Architecture & Infrastructure
Standardization work	
Published standards	-
Standards under development	-
Involvement of Luxembourg	
/	
Comments	
The ITU-T Focus Group Technologies for Network 2030 (FG NET-2030) was established by Study Group 13 at its Geneva meeting in July 2018. This group intends to study the capabilities of networks for the year 2030 and beyond, when it is expected to support novel forward-looking scenarios, such as holographic type communications, extremely fast response in critical situations and high-precision communication demands of emerging market verticals. The study aims to answer specific questions on what kinds of network architecture and the enabling mechanisms are suitable for such novel scenarios. This study is collectively called ‘Network 2030’. It will be further realized by the exploration of new communication mechanisms from a broad perspective and is not restricted by existing notions of network paradigms or to any particular existing technologies. Network 2030 may be built upon a new or refined network architecture to carry information in a manner that may evolve from, or is quite different from today’s networks. Regardless, Network 2030 based systems shall ensure they remain fully backward compatible, supporting both existing and new applications. The FG NET-2030, as a platform to study and advance international networking technologies, will investigate the future network architecture, requirements, use cases, and capabilities of the networks for the year 2030 and beyond.	

3.6.2. Intelligent Transport Systems (ITS)

Intelligent transport systems (ITS) include telematics and all types of communication in vehicles, between vehicles (e.g. car-to-car), and between vehicles and fixed locations (e.g. car-to-infrastructure). Digitization of public transport in general and Intelligent Transportation Systems (ITS) in particular are expected to take a leap forwards by the European Commission (EC) as part of the Digital Single Market Strategy[86]. The ITS solutions are aimed to achieve efficient management of transport network for passengers and enterprises. The next generation of ITS solutions, cooperative-ITS (C-ITS), allows effective data exchange through wireless technologies, which enables the vehicles to be connected with each other, with the road users and road infrastructure, and in turn to communicate and negotiate mutual and/or conflicting goals. The C-ITS is primarily driven by applications for active traffic efficiency and road safety to help drivers to be aware of other vehicles, road conditions and real time information of traffic conditions for speed management and navigation[87]. ITS standards are essential to achieve

[86] https://ec.europa.eu/commission/priorities/digital-single-market/

[87] A. Festag, “Cooperative Intelligent Transport Systems Standards in Europe,” AUTOMOTIVE NETWORKING AND APPLICATIONS, IEEE Communications Magazine, pp. 166-172, December 2014.

interoperability among different communication devices of multiple vendors for vehicles and road infrastructure.

Next sections provide an overview of the ITS related technical committees currently active in the recognized standardization organizations.

3.6.2.1. ISO/TC 204

General information			
Committee	**ISO/TC 204**	**Title**	**Intelligent transport systems**

Creation date	1992	**MEMBERS**	**Participating Countries (29):**
			United States, Australia, Belarus, Belgium, Canada, China, Cyprus, Czech Republic, Ethiopia, France, Germany, Hungary, India, Islamic Republic of Iran, Ireland, Italy, Japan, Republic of Korea, Malaysia, Netherlands, New Zealand, Norway, South Africa, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, United Kingdom
			Observing Countries (28):
			Algeria, Bulgaria, Chile, Colombia, The Democratic Republic of the Congo, Croatia, Cuba, Denmark, Egypt, Finland, Greece, Hong Kong, Indonesia, Israel, Mexico, Mongolia, Montenegro, Pakistan, Philippines, Poland, Portugal, Romania, Russian Federation, Serbia, Singapore, Slovakia, Thailand, Turkey

Secretariat	ANSI (United States)		
Secretary	Mr. Adrian Guan		
Chairperson	Mr. Dick Schnacke		
Organizations in liaison	APEC, ETSI, ICAO, IEEE, ISOC, ITU, OGC, TISA, UNECE, NFC Forum, SAE		
Web site	https://www.iso.org/committee/54706.html		
Scope	The current area of work for TC 204 consists of: - Standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveler information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field. Excluded: - In-vehicle transport information and control systems (ISO/TC 22).		
Structure	TC 204/WG 1 Architecture TC 204/WG 3 ITS database technology TC 204/WG 4 Automatic vehicle and equipment identification TC 204/WG 5 Fee and toll collection TC 204/WG 7 General fleet management and commercial/freight TC 204/WG 8 Public transport/emergency TC 204/WG 9 Integrated transport information, management and control TC 204/WG 10 Traveller information systems TC 204/WG 14 Vehicle/roadway warning and control systems TC 204/WG 16 Communications TC 204/WG 17 Nomadic Devices in ITS Systems TC 204/WG 18 Cooperative systems		
Standardization work			
Published standards	Number of published ISO standards under the direct responsibility of TC 204 (number includes updates): 256		

Standards under development	84

Involvement of Luxembourg

NO (no registered delegate)

Comments

ISO/TC 204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work program in this field including the schedule for standards development, taking into account the work of existing international standardization bodies.

3.6.2.2. CEN/TC 278

General information			
Committee	**CEN/TC 278**	**Title**	**Intelligent transport systems**
Creation date	1991	**MEMBERS**	34 members of CEN/CENELEC
Secretariat	NEN (Netherlands)		
Secretary	Mr. Maarten Peelen		
Chairperson	Mr. Hans Nobbe		
Organizations in liaison	ETSI, ISO		
Web site	http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_LANG_ID,FSP_ORG_ID:25,6205&cs=1A98C573151AB3D7A22712120D94364C1#1		
Scope	Standardization in the field of telematics to be applied to road traffic and transport, including those elements that need technical harmonization for intermodal operation in the case of other means of transport. It shall notably support: - Vehicle, container, swap body and goods wagon identification; - Communication between vehicles and road infrastructure; - Communication between vehicles; - Vehicle man machine interfacing as far as telematics is concerned; - Traffic and parking management; - User fee collection; - Public transport management; - User information.		
Structure	CEN/TC 278/WG 1	Electronic fee collection and access control (EFC)	
	CEN/TC 278/WG 3	Public transport (PT)	
	CEN/TC 278/WG 4	Traffic and traveller information (TTI)	
	CEN/TC 278/WG 5	Traffic control (TC)	
	CEN/TC 278/WG 7	ITS spatial data	
	CEN/TC 278/WG 8	Road traffic data (RTD)	
	CEN/TC 278/WG 10	Man-machine interfaces (MMI)	
	CEN/TC 278/WG 13	Architecture and terminology	
	CEN/TC 278/WG 14	After theft systems for the recovery of stolen vehicles	
	CEN/TC 278/WG 15	eSafety	
	CEN/TC 278/WG 16	Cooperative ITS	
	CEN/TC 278/WG 17	Urban ITS	
Standardization work			
Published standards	158		
Standards under development	68		
Involvement of Luxembourg			
1 delegate			
- Mr. Harold Linke	HITEC Luxembourg S.A..		

Comments

CEN/TC 278's vision statement for ITS standardization in Europe in the first quarter of the twenty-first century is: “To provide a family of Standards and related specifications, interoperable on a pan-European basis, that will enable services to be provided to travelers (be they drivers, pedestrians or users of public transport); to provide services to transport and highway managers and operators; to commercial fleet managers and commercial service providers, utilizing information technology to maximize efficiency, safety and the quality of service provided. To ensure that by co-operating in international standardization, International Standards provide the best solutions for European stakeholders.”

A new Standardization Request on ITS in urban areas was accepted in 2017 and several projects are in progress in 2018: location-referencing harmonization; mixed vendor environments; traffic management system status, fault and quality standards; emissions management in urban areas; traffic management data models and infrastructure.

The European Commission has laid down the legal framework to accelerate the deployment of ITS across Europe (Directive 2010/40/EU) and has requested that the ESOs develop and adopt European Standards in support of this framework (M/453), to ensure interoperability across countries. These standards developed by CEN/TC 278 cover a variety of aspects including cooperative systems, travel and traffic information, route guidance and navigation, public transport, emergency vehicles and electronic fee collection (M/338).

3.6.2.3. ETSI TC/ITS

General information

Committee	**ETSI/TC ITS**	**Title**	**Automotive Intelligent Transport**
Creation date	/	**MEMBERS**	135 member organizations of ETSI
Chairperson	Mr. Andersen Niels Peter Skov		
Organizations in liaison	APT, ARIB, CCC, CCSA, CEN, CENELEC, CEPT, CEPT COM-ITU, ECC, ENISA, ERA, ERTICO, GCF, IEEE, IPv6 Forum, ISO, ISOC/IETF, ITU, OST-R, SAE Int., TISA, TTA, TTC, UNECE		
Web site	https://portal.etsi.org/ITS		
Scope	The ETSI TC ITS is responsible for the development and maintenance of standards, specifications and other deliverables to support the development and implementation of ITS service provision across the network, for transport networks, vehicles and transport users, including interface aspects and multiple modes of transport and interoperability between systems, but not including ITS application standards, radio matters, and EMC. The scope of this committee includes communication media, and associated physical layer, transport layer, network layer, security, lawful intercept and the provision of generic web services.		
Structure	TC ITS/WG1 Application Requirements and Services TC ITS/WG2 Architecture and Cross Layer TC ITS/WG3 Transport and Network TC ITS/WG4 Media and Medium Related TC ITS/WG5 Security		

Standardization work

Published standards	249
Standards under development	51

Involvement of Luxembourg

1 company

- FBConsulting S.A.R.L.

Comments

The following important topics related to automotive ITS are currently being addressed:

- Dedicated Short-Range Communications (DSRC): It provides communications between the vehicle and the roadside in specific locations (for example toll plazas). Applications such as Electronic Fee Collection (EFC) will operate over DSRC;
- Cooperative-ITS (C-ITS) and its evolution to support full autonomous driving including wireless short range communications (ITS-G5) dedicated to automotive ITS and Road Transport and Traffic Telematics (RTTT). C-ITS provides connectivity between road participants and infrastructure;
- Automotive ITS Security: This includes trust and privacy management and certificate formats;
- Automotive radar.

Examples of the latest published ETSI standards and technical reports on ITS are:

- TS 102 894-2, Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary;
- TS 103 301, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services;
- TS 101 539-2, Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification;
- TS 102 941, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management;
- TR 103 415, Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management;
- TS 102 940, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.

The standardization scope of ETSI covers all types of transport, including rail, water, and air transport. CEN also covers tolling systems as well as road infrastructure in addition to the ETSI’s activities. The standardization efforts are driven by the European Car-2-Car Communication Consortium (C2C-CC). ETSI’s Center for Testing and Interoperability, ETSI CTI, provides hands-on support and assistance to the ETSI’s technical committees, the 3GPP and the oneM2M Partnership Project on the application of testing and validation techniques in standards making.

4. 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. Previous chapters have highlighted the basic concepts of Smart ICT technologies, such as 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. As mentioned in the introduction, 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 ICT landscape. In particular, this chapter focuses on the initiations of ILNAS, with the support of ANEC G.I.E., to involve national stakeholders in the technical standardization process.

The ICT sector is, at national level, the most active standardization sector. Luxembourg recently registered as "P-member"[88] of ISO/IEC JTC 1. Currently, 74 delegates[89] from Luxembourg are involved in international and European technical committees in the ICT sector. Among them, several experts are involved in Smart ICT and Digital Trust related technical committees, such as in Internet of Things: 16; Cloud Computing: 16; Artificial Intelligence: 17; Blockchain: 16, Digital Trust: 43. 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 benefitted from related opportunities of technical standardization. In this way, ILNAS, with the support of ANEC G.I.E., is following closely the Smart ICT related technical committees, listed below, in order to provide the most relevant information to the national ICT community and to facilitate their involvement in the technical committees.

- 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;
- Technical committees related to Digital Trust (e.g.: ISO/IEC JTC 1/SC 27).

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 could be seen 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.

4.1. Information about Standardization

4.1.1. Smart ICT Workshops

In order to disseminate the ICT standardization knowledge with 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 in the framework of ICT prospective and, more specifically in the domain of "Smart Secure ICT".

[88] 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)
[89] Some experts are participating in more than one technical committee.

For instance, a series of breakfasts dedicated to the promotion of Smart ICT standardization and Digital Trust were organized last year. Indeed, in relation with the publication of the White Papers "Digital Trust for Smart ICT", four workshops (breakfast meetings) were organized in 2016 and 2017 in order to discuss the role of Digital Trust in Smart ICT and widespread use of such technologies. Beyond the technical aspects, latest related standardization developments were presented to highlight their importance for the establishment of a trusted digital environment. This series of breakfasts reviewed various Smart ICT technologies, focusing mainly on the Cloud Computing, Internet of Things, and Big Data, the three topics developed in this White Paper, through the prisms of Digital Trust and standardization. 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 basis[90]. Recently in 2018, ILNAS, with the support of ANEC G.I.E., published two White Papers dedicated to Blockchain[91] and to Internet of Things[92], in order to make national stakeholder aware about related technology, economic perspectives and developments of technical standardization in such technologies. Several breakfast meetings were organized to present the Blockchain White Paper. Similarly, the IoT White Paper was released during the ILNAS-ETSI joint event with great participation of national stakeholders interested in this domain.

Moreover, ILNAS aims at managing and reinforcing the National Mirror Committees (NMC) dedicated to Smart ICT (e.g.: ISO/IEC JTC 1/SC 41 for IoT and related technologies, ISO/IEC JTC 1/SC 38 for Cloud Computing, ISO/IEC JTC 1/SC 42 for Artificial Intelligence, ISO/TC 307 for Blockchain and Distributed Ledger Technologies, etc.). These NMC are gathering national experts participating in these technical committees. In this frame, NMC meetings are regularly organized, which allow interested national stakeholders to strengthen their commitment into the process of technical standardization (interested people who are not already delegates of technical committees can also participate).

For example, ANEC G.I.E. participated in five international plenary meetings of technical committees in 2017 and six in 2018[93]. In this frame, it organized NMC meetings to prepare, debrief and exchange on the topics dealt during these plenary meetings with related national community.

4.1.2. Awareness Sessions

Another way to get the 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 the basic knowledge about standardization as well as the 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 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 standardization[94] to be contacted by ILNAS and ANEC G.I.E.

[90] Updates on events organized by ILNAS are regularly published on https://portail-qualite.public.lu/fr/agenda.html

[91] White Paper Blockchain and Distributed Ledgers https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html

[92] White Paper Internet of Things https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-iot.html

[93] More international plenary meetings are also planned to attend in 2018

[94] https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/normes-normalisation/declarations-interet/declaration-interet-normalisation-tic/declaration-interest-standardization-it.pdf

4.1.3. Smart ICT Standards Watch

As mentioned earlier, 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 organization. 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.

4.1.4. Publications and Disseminations

ILNAS, with the support of ANEC G.I.E., publishes and disseminates reports and White Papers at national level in order to provide valuable information on Smart ICT standardization topics to national stakeholders.

- **White Paper Internet of Things**[95]

ILNAS and ANEC G.I.E. published, with the support of the Ministry of the Economy, a White Paper Internet of Things 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 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**[96]

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 Blockchains 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 technical standardization in relation.

- **White Paper Digital Trust for Smart ICT** [97]

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

[95] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf

[96] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-blockchain-june-2018.pdf

[97] https://portail-qualite.public.lu/dam-assets/publications/confiance-numerique/white-paper-digital-trust-september-2017.pdf

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**[98]

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.

- **White Paper Big Data**[99]

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.

4.1.5. Free Consultation of the Standards

ILNAS offer the free consultation of its entire standards’ database (including more than 170 000 normative documents from ILNAS, DIN, CEN, CENELEC, ETSI, ISO and IEC) through lecture stations located in six different places in Luxembourg[100]:

- University of Luxembourg (Luxembourg Belval);
- House of Entrepreneurship (Luxembourg Kirchberg);
- National library of Luxembourg (Luxembourg);
- ILNAS (Esch-Belval);
- LIST (House of Innovation – Esch-Belval);

[98] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/information-sensibilisation/white-paper-green-computing/white-paper-green-computing.pdf

[99] 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

[100] https://portail-qualite.public.lu/fr/normes-normalisation/achat-consultation-normes.html

- LIST (Belvaux).

This service allows, for example, interested organizations or individuals to peruse a standard before its purchase. The ILNAS e-Shop[101] offers then the possibility to buy the relevant standards in electronic format at competitive prices.

4.1.6. 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 2017, 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 Big Data. In this frame, three PhD students are performing research activities in the above-mentioned Smart ICT domains. 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 4.2.2). On the other hand, it will serve as a basis for a future Master Program "*Smart Secure ICT for Business Innovation*" (expected in 2020).

National stakeholders active in the Smart ICT landscape will have the opportunity to be benefited from the results of this research program, for example by participating in the courses offered in the University certificate, or 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 ICT[102]

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" 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

4.2. Training in Standardization

4.2.1. Trainings on Smart ICT Standardization

ILNAS, with the support of ANEC G.I.E., develops a training catalogue[103] annually, which is updated according to market expectations. In 2018, in particular, on demand technical trainings on Smart ICT standardization and related digital trust challenges have been proposed:

- Digital trust in Smart ICT;
- Internet of Things and technical standardization;
- Blockchain and technical standardization;
- Cloud Computing and digital trust;
- Big Data and digital trust.

[101] https://ilnas.services-publics.lu/

[102] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf

[103] https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2018/catalogue-formation-normalisation-2018.pdf

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. In this context, trainings on Big Data and Digital Trust was already organized in May 2018. Trainings related to Blockchain[104] and IoT[105] White Papers were also organized in September and October respectively. Similarly, training on Cloud Computing and Digital Trust will be organized in November 2018. Other related trainings as listed above could be also organized at any time based on customer demand.

4.2.2. University certificate "Smart ICT for Business Innovation"

ILNAS and ANEC G.I.E., in collaboration with the University of Luxembourg, have developed the University certificate "*Smart ICT for Business Innovation*" program, which represents an innovative way to better understand Smart ICT standardization and develop new related skills. The second edition of this program is running since February 2018. This program allows students to take a broad view of the cutting-edge Smart ICT concepts and tools at their disposal in order to develop their sense of innovation. Overall, the University certificate focuses on important aspects of Smart ICT and their applications, such as the development of Smart Cities, Big Data, Internet of Things and Cloud Computing. The program also proposes an overview of some challenges to fully exploit the potential of Smart ICT:

- Digital Trust: Technologies must offer security, privacy and trust guarantees to ensure their adoption and proper implementation;
- Governance of IT: Economic actors must take ownership and support these technologies to benefit from their advantages;
- Green ICT: The massive digitalization of our society has important repercussions on our environment and our quality of life. It has become necessary to take into account the environmental impact of the Smart ICT but also to take advantage of the solutions provided by Smart ICT.

All of these technologies and challenges are now being considered by international and European standardization organizations. Technical standardization is therefore at the core of the curriculum as it is a key source of knowledge in continuous evolution. Technical standardization committees could indeed be considered as only platforms gathering all interest groups of manufacturers, researchers, business innovators and other stakeholders, making them the beating heart of Smart ICT progress.

4.3. Involvement in Standardization

4.3.1. Become National Delegate in Standardization

4.3.1.1. Benefits of Participation in Smart ICT standardization technical committees

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;

[104] https://portail-qualite.public.lu/fr/formations/normes-normalisation/2018/blockchain-training.html

[105] https://portail-qualite.public.lu/fr/formations/normes-normalisation/2018/iot-training.html

- Valuing your organization at national and international level;
- Identifying development opportunities;
- Making your organization competitive in the market.

4.3.1.2. Participation in the Training -New delegates in standardization

Newcomers in technical standardization, who have registered in a technical committee, are encouraged to participate in the dedicated training offered by ILNAS. It allows them, from one side, to better understand the roles and missions of delegates in standardization, and from the other side, to become familiar with the tools and services at their disposal for this work.

4.3.1.3. 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 2015-2020", 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.

4.3.1.4. 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).

4.3.2. 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 could propose changes in the draft standard, regardless of whether such stakeholders are officially registered in the technical committee responsible for the development of this standard.

4.3.3. 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 specific domain and to benefit from the definition of the future market rules.

4.3.4. 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 an official national contact point dedicated to exchange information between the market and the European multi-stakeholder platform on ICT standardization.

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

Highlights of Opportunities at the National Level

Luxembourg offers different opportunities to national stakeholders in order to make them able to take advantage of technical standardization, which are summarized as follows:

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

- To be part of the training in technical standardization
  - Participate in the trainings on Smart ICT standardization;
  - Register in the University certificate "*Smart ICT for Business Innovation*".

- To be involved in standardization
  - 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),
  - Submit comments on draft standards under public enquiry;
  - Propose new standards projects;
  - 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 delegates[106].

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

[106] https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/normes-normalisation/declarations-interet/declaration-interet-normalisation-tic/declaration-interest-standardization-it.pdf

5. CONCLUSIONS

The ICT sector is constantly evolving towards smarter technological products and services. 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 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. In the same time, Digital Trust become 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 latest developments, thus supporting innovation, but also to contribute in 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.

As described in the national standardization strategy 2014-2020[107], ICT is a horizontal sector supporting many innovative or smart developments. Smart ICT is indeed one of the most competitive economic sectors in the Grand Duchy of Luxembourg, having communication infrastructures of high quality, hosting several world-leading ICT companies as well as many start-ups[108] and with a market composed 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 the "Luxembourg's Policy on ICT technical standardization 2015-2020"[109]. The main objectives of this policy are to foster and strengthen the national ICT sector's involvement in the standardization work. To achieve this, ILNAS is conducting three intertwined projects:

a) Developing market interest and involvement,
b) Promoting and reinforcing market participation, and
c) Supporting and strengthening the 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 Internet of Things, Cloud Computing, Artificial Intelligence, Blockchain and Digital Trust related to these technologies. Apart from this Standards Analysis, this year,

[107] ILNAS, "Luxembourg Standardization Strategy 2014-2020", 2014

[108] https://www.tradeandinvest.lu/business-sector/ict/

[109] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf

with the support of ANEC G.I.E., ILNAS published two White Papers - Blockchain and Distributed Ledger Technology[110] and Internet of Things[111] - aiming at creating awareness and interest concerning relevant standardization developments within the national market.

Similarly, for the second project, ILNAS, with the support of ANEC G.I.E., is offering its support to different industries/organizations through standardization according to their nature of business at the national level. Smart ICT and/or Digital Trust related technical committees already beneficiate from a good national representation with 74 national delegates currently registered to participate in one or several of these normative domains (Internet of Things: 16; Cloud Computing: 16; Artificial Intelligence: 17; Blockchain: 16, Digital Trust: 43)[112]. This figure demonstrates the interest of individuals, industries/organizations towards the 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[113], focusing on the Cloud Computing, 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 the CEN-CENELEC, was the first step towards the ambitious project of creating a Master program dedicated to Smart Secure ICT. ILNAS and the University of Luxembourg are also implementing a research program[114] whose objective is to analyze and to extend the standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, Internet of Things and Big Data. In this frame, 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"[115] in October 2018. The research results of this program will also facilitate the development of the Master Program "*Smart Secure ICT for Business Innovation*" expected at the horizon 2020.

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 to Smart ICT 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 2014-2020: "Technical standardization as a service"[116], ILNAS, with the support of ANEC G.I.E., stands ready to encourage and assist each initiative in this process.

[110] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html

[111] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf

[112] Please note that some experts are participating in more than one technical committee

[113] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/projets-phares-dans-l_education-a-la-normalisation.html

[114] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html

[115] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf

[116] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf

6. 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 three Smart ICT areas (Internet of Things, Cloud Computing, Artificial Intelligence / Big Data) 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.

6.1. Internet of Things

6.1.1. 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	ISO/IEC TR 22417:2017	Information technology - Internet of things (IoT) - IoT use cases
ISO/IEC JTC 1	ISO/IEC 29161:2016	Information technology -- Data structure -- Unique identification for the Internet of Things
ISO/IEC JTC 1	ISO/IEC 30141:2018	Information technology -- Internet of Things -- Internet of Things Reference Architecture (IoT RA)
ETSI	ETSI TR 103 290 (04/2015)	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
ETSI	ETSI TR 103 375 (10/2016)	SmartM2M; IoT Standards landscape and future evolutions
ETSI	ETSI TR 103 376 (10/2016)	SmartM2M; IoT LSP use cases and standards gaps
ETSI	ETSI TS 118 101 V2.10.0 (10/2016)	oneM2M; Functional Architecture (oneM2M TS-0001 version 2.10.0 Release 2)
ETSI	ETSI TS 118 102 V2.7.1 (09/2016)	oneM2M Requirements (oneM2M TS-0002 version 2.7.1 Release 2)
ETSI	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	ETSI TS 118 105 V2.0.0 (09/2016)	oneM2M; Management Enablement (OMA) (oneM2M TS-0005 version 2.0.0 Release 2)
ETSI	ETSI TS 118 106 V2.0.1 (09/2016)	oneM2M; Management Enablement (BBF) (oneM2M TS-0006 version 2.0.1 Release 2)
ETSI	ETSI TS 118 109 V2.6.1 (09/2016)	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 2.6.1 Release 2)
ETSI	ETSI TS 118 110 V2.4.1 (09/2016)	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 2.4.1 Release 2)
ETSI	ETSI TS 118 111 V2.4.1 (09/2016)	oneM2M; Common Terminology (oneM2M TS-0011 version 2.4.1 Release 2)
ETSI	ETSI TS 118 112 V2.0.0 (09/2016)	oneM2M; Base Ontology (oneM2M TS-0012 version 2.0.0 Release 2)
ETSI	ETSI TS 118 114 V2.0.0 (09/2016)	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 2.0.0 Release 2)
ETSI	ETSI TS 118 115 V2.0.0 (09/2016)	oneM2M; Testing Framework (oneM2M TS-0015 version 2.0.0 Release 2)
ETSI	ETSI TS 118 120 V2.0.0 (09/2016)	oneM2M; WebSocket Protocol Binding (oneM2M TS-0020 version 2.0.0 Release 2)

SDO	Reference	Title
ETSI	ETSI TS 118 121 V2.0.0 (09/2016)	oneM2M; oneM2M and AllJoyn® Interworking (oneM2M TS-0021 version 2.0.0 Release 2)
ETSI	ETSI TS 118 122 V2.0.0 (05/2017)	oneM2M Field Device Configuration (oneM2M TS-0022 version 2.0.0 Release 2)
ETSI	ETSI TS 118 123 V2.0.0 (09/2016)	oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023 version 2.0.0 Release 2)
ETSI	ETSI TS 118 124 V2.0.0 (09/2016)	oneM2M; OIC Interworking (oneM2M TS-0024 version 2.0.0 Release 2)
ETSI	ETSI TS 118 132 V2.0.2 (11/2017)	MAF and MEF Interface Specification (oneM2M TS-0032 version 2.0.2 Release 2A)
ETSI	ETSI TR 118 517 V2.0.0 (09/2016)	oneM2M; Home Domain Abstract Information Model (oneM2M TR-0017 version 2.0.0)
ETSI	ETSI TR 118 518 V2.0.0 (09/2016)	oneM2M; Industrial Domain Enablement (oneM2M TR-0018 version 2.0.0 Release 2)
ETSI	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	ETSI TR 118 524 V2.0.0 (09/2016)	oneM2M; 3GPP Release 13 Interworking (oneM2M TR-0024 version 2.0.0)
ITU-T	ITU-T X.1362 (03/2017)	Simple encryption procedure for Internet of Things (IoT) environments
ITU-T	ITU-T Q.3913 (08/2014)	Set of parameters for monitoring internet of things devices
ITU-T	ITU-T Y.4000 / Y.2060 (06/2012)	Overview of Internet of Things
ITU-T	ITU-T Y.4050 / Y.2069 (07/2012)	Terms and definitions for Internet of Things
ITU-T	ITU-T Y.4100 / Y.2066 (06/2014)	Common requirements of Internet of Things
ITU-T	ITU-T Y.4101/ Y.2067 (06/2014)	Common requirements and capabilities of a gateway for Internet of Things applications
ITU-T	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	ITU-T Y.4103 / F.748.0 (10/2014)	Common requirements for Internet of Things (IoT) applications
ITU-T	ITU-T Y.4111 / Y.2076 (02/2016)	Semantics based requirements and framework of the Internet of Things
ITU-T	ITU-T Y.4112 / Y.2077 (02/2016)	Requirements of the Plug and Play capability of the Internet of Things
ITU-T	ITU-T Y.4113 (09/2016)	Requirements of the network for the Internet of Things
ITU-T	ITU-T Y.4115 (04/2017)	Reference architecture for IoT device capability exposure
ITU-T	ITU-T Y.4401 / Y.2068 (03/2015)	Functional framework and capabilities of the Internet of Things
ITU-T	ITU-T Y.4455 (10/2017)	Reference architecture for Internet of things network service capability exposure
ITU-T	ITU-T Y.4552 / Y.2078 (02/2016)	Application support models of the Internet of Things
ITU-T	ITU-T Y.4702 (03/2016)	Common requirements and capabilities of device management in the Internet of Things

6.1.2. 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	ETSI TS 118 103 V2.4.1 (09/2016)	oneM2M; Security solutions (oneM2M TS-0003 version 2.4.1 Release 2)
ETSI	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	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)
ETSI	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

6.1.3. 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	ISO/IEC DIS 20924	Information technology -- Internet of Things -- Definition and Vocabulary
ISO/IEC JTC 1	ISO/IEC CD 21823-1	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 1: Framework
ISO/IEC JTC 1	ISO/IEC WD 21823-2	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 2: Transport interoperability
ISO/IEC JTC 1	ISO/IEC WD 21823-3	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 3: Semantic interoperability
ISO/IEC JTC 1	ISO/IEC NP 30160	Internet of Things (IoT) -- Application framework for industrial facility demand response energy management
ISO/IEC JTC 1	ISO/IEC NP 30161	Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services
ISO/IEC JTC 1	ISO/IEC 30162	Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems
ISO/IEC JTC 1	PWI TR JTC1-SC41-1 ED1	Internet of things (IoT) -- Edge Computing
ISO/IEC JTC 1	PNW JTC1-SC41-59	Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services
ISO/IEC JTC 1	PNW JTC1-SC41-67	Internet of Things (IoT) -- Real-time IoT framework
ETSI	ETSI GR IP6 008	IPv6-based Internet of Things; Deployment of IPv6-based Internet of Things
ETSI	ETSI TR 103 467	Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem
ETSI	ETSI SR 003 438	USER; User centric approach in IoT

SDO	Reference	Title
ETSI	ETSI PWI BOARDM2M IOT 1501 v1	SmartM2M; oneM2M platform for AIOTI (Alliance for Internet of Things Innovation), a common interworking framework for information sharing
ETSI	ETSI TS 118 034	oneM2M; Semantics Support (oneM2M TS-0034 version 0.5.0 Release3)
ETSI	ETSI TS 118 101	oneM2M; Functional Architecture (oneM2M TS-0001 version 2.14.0 Release 2A)
ETSI	ETSI TS 118 102	oneM2M Requirements (oneM2M TS-0002 version 2.7.1 Release 2A)
ETSI	ETSI TS 118 104	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 2.12.0 Release 2A)
ETSI	ETSI TS 118 105	oneM2M; Management Enablement (OMA) (oneM2M TS-0005 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 106	oneM2M; Management Enablement (BBF) (oneM2M TS-0006 version 2.0.1 Release 2A)
ETSI	ETSI TS 118 107	oneM2M; Service Components (oneM2M TS-0007 version 2.0.1 Release 2A)
ETSI	ETSI TS 118 108	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 2.3.0 Release 2A)
ETSI	ETSI TS 118 109	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 2.9.0 Release 2A)
ETSI	ETSI TS 118 110	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 2.6.0 Release 2A)
ETSI	ETSI TS 118 111	oneM2M; Common Terminology (oneM2M TS-0011 version 2.7.0 Release 2A)
ETSI	ETSI TS 118 112	oneM2M; Base Ontology (oneM2M TS-0012 version 3.5.0 Release 3)
ETSI	ETSI TS 118 114	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 115	oneM2M; Testing Framework (oneM2M TS-0015 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 117	oneM2M Implementation Conformance Statements
ETSI	ETSI TS 118 118	oneM2M Test Suite Structure and Test Purposes
ETSI	ETSI TS 118 119	oneM2M Abstract Test Suite and Implementation eXtra Information for Test
ETSI	ETSI TS 118 120	oneM2M; WebSocket Protocol Binding (oneM2M TS-0020 version 2.1.0 Release 2A)
ETSI	ETSI TS 118 121	oneM2M; oneM2M and AllJoyn® Interworking (oneM2M TS-0021 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 122	oneM2M Field Device Configuration (oneM2M TS-0022 version 2.1.0 Release 2A)
ETSI	ETSI TS 118 123	oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 124	oneM2M; OIC Interworking (oneM2M TS-0024 version 2.0.0 Release 2A)
ETSI	ETSI TS 118 130	oneM2M Ontology based Interworking
ETSI	ETSI TR 118 501	oneM2M; Use Case collection (oneM2M TR-0001)
ETSI	ETSI TR 118 503	oneM2M Roles and Focus Areas
ETSI	ETSI TR 118 507	oneM2M; Study on Abstraction and Semantics Enablement (oneM2M TR-0007 Release 2)
ETSI	ETSI TR 118 513	oneM2M Home Domain Enablement

SDO	Reference	Title
ETSI	ETSI TR 118 514	oneM2M; oneM2M and AllJoyn Interworking (oneM2M TR-0014)
ETSI	ETSI TR 118 518	oneM2M; Industrial Domain Enablement (oneM2M TR-0018 version 2.5.0 Release 2A)
ETSI	ETSI TR 118 520	oneM2M Study of service transactions and re-usable service layer context
ETSI	ETSI TR 118 521	oneM2M Study of the action triggering in M2M
ETSI	ETSI TR 118 523	oneM2M and OIC Interworking
ETSI	ETSI TR 118 526	Vehicular Domain Enablement
ETSI	ETSI TR 118 533	oneM2M Study on Enhanced Semantic Enablement (oneM2M TR-0033 study on Enhanced Semantic Enablement Release 3)
ETSI	ETSI TR 118 534	oneM2M; Developer Guide: CoAP binding and long polling for temperature monitoring (oneM2M TR-0034 v2.0.0 release 2A)
ETSI	ETSI TR 118 535	oneM2M; Developer guide: device management (oneM2M TR-0035 v2.0.0 release 2A)
ETSI	ETSI TR 118 538	oneM2M; Developer guide: Implementing security example (oneM2M TR-0038 v2.0.0 release 2A)
ETSI	ETSI TR 118 539	oneM2M; Developer guide; Interworking Proxy using SDT (oneM2M TR-0039 version 2.0.0 release 2A)
ETSI	ETSI TR 118 545	oneM2M; Developer Guide: Implementing Semantics (oneM2M TR-0045 version 2.0.0)
ITU-T	ITU-T Draft D.IoTRoaming	Roaming for the Internet of Things (IoT)
ITU-T	ITU-T Draft E.IoT-NNAI	NNAI for Internet of Things
ITU-T	ITU-T Draft Q.Het_IoT_Gateway_Test	The structure of the testing of heterogeneous Internet of Things gateways in a laboratory environment
ITU-T	ITU-T Draft TR.AI4SC	Artificial Intelligence and Internet of Things
ITU-T	ITU-T Draft X.iotsec-2	Security framework for Internet of things
ITU-T	ITU-T Draft X.oiddev	Object identifier assignments for the Internet of things
ITU-T	ITU-T Draft X.oid-iot	ITU-T X.660 - Supplement on Guidelines for using object identifiers for the Internet of things
ITU-T	ITU-T Draft Supp.-Y.IoT Scenarios for Developing Countries	Scenarios of Implementing Internet of Things in networks of developing countries
ITU-T	ITU-T Draft Y.2067	Common requirements and capabilities of a gateway for Internet of Things applications
ITU-T	ITU-T Draft Y.Accessibility-IoT	Accessibility requirements for the Internet of things applications and services
ITU-T	ITU-T Draft Y.IoT-AC-reqts	Requirements for accounting and charging capabilities of the Internet of Things
ITU-T	ITU-T Draft Y.IoT-ITS-framework	Framework of Cooperative Intelligent Transport Systems based on the Internet of Things
ITU-T	ITU-T Draft Y.IoT-NCM-reqts	Requirements and capabilities of network connectivity management in the Internet of Things
ITU-T	ITU-T Draft Y.IoT-things-description-reqts	Requirements of things description in the Internet of Things
ITU-T	ITU-T Draft Y.IoT-WDS-Reqts	Requirements and capabilities of Internet of Things for support of wearable devices and related services
ITU-T	ITU-T Draft Y.SmartMan-IIoT-overview	Overview of Smart Manufacturing in the context of Industrial Internet of Things
ITU-T	ITU-T Draft Supp-Y.IPv6-IoT	IPv6 Potential for the Internet of Things and Smart Cities

SDO	Reference	Title
ITU-T	ITU-T Draft Y.IPv6RefModel	Reference Model of IPv6 Subnet Addressing Plan for Internet of Things Deployment
ITU-T	ITU-T Draft Y.IPv6-suite	Reference Model of Protocol Suite for IPV6 interoperable Internet of Things Deployments
ITU-T	ITU-T Draft Y.NGNe-IoT-arch	Architecture of the Internet of Things based on NGNe
ITU-T	ITU-T Draft Y.IoT-SQ-fns	Service Functionalities of Self-quantification over Internet of things
ITU-T	ITU-T Draft Y.IoT-sec-safety	Security capabilities supporting safety of the Internet of Things
ITU-T	ITU-T Draft X.nb-iot	Security Requirements and Framework for Narrow Band Internet of Things
ITU-T	ITU-T X.iotsec-3	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment
ITU-T	ITU-T Draft Supp-Y.IoT-Use-Cases	IoT Use Cases
ITU-T	ITU-T Draft Y.IoT-son	Framework of self-organization network in the IoT environments

6.1.4. 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	ISO/IEC 30147	Internet of Things (IoT) -- Methodology for implementing and maintaining trustworthiness of IoT systems and services
ISO/IEC JTC 1	ISO/IEC 30149	Internet of Things (IoT) -- Trustworthiness framework
ETSI	ETSI TS 118 103	oneM2M; Security solutions (oneM2M TS-0003 version 2.9.0 Release 2A)
ETSI	ETSI TS 118 116	oneM2M Secure Environment Abstraction
ETSI	ETSI TS 118 129	oneM2M; Security Abstract Test Suite & Implementation eXtra Information for Test
ETSI	ETSI TR 118 508	oneM2M; Analysis of Security Solutions for the oneM2M System (oneM2M TR-0018 version 2.0.0 Release 2)
ETSI	ETSI TR 118 519	oneM2M Dynamic Authorization for IoT (oneM2M TR-0019 version 2.0.0 Release 2)
ETSI	ETSI TR 118 538	oneM2M; Developer guide: Implementing security example (oneM2M TR-0038 v2.0.0 release 2A)
ITU-T	ITU-T Draft X.nb-iot	Security Requirements and Framework for Narrow Band Internet of Things
ITU-T	ITU-T X.iotsec-3	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment
ITU-T	ITU-T X.iotsec-2	Security framework for IoT
ITU-T	ITU-T X.secup-iot	Secure software update procedure for IoT devices
ITU-T	ITU-T X.nb-iot	Security requirements and frameworks for Narrow Band IoT

6.2. Cloud Computing

6.2.1. 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	ISO/IEC 17788:2014 / ITU-T Y.3500 (08/2014)	Information technology -- Cloud computing -- Overview and vocabulary
ISO/IEC JTC 1 / ITU-T	ISO/IEC 17789:2014 / ITU-T Y.3502 (08/2014)	Information technology -- Cloud computing -- Reference architecture
ISO/IEC JTC 1	ISO/IEC 17826:2016	Information technology -- Cloud Data Management Interface (CDMI)
ISO/IEC JTC 1	ISO/IEC 19086-1:2016	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts
ISO/IEC JTC 1	ISO/IEC 19086-3:2017	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements
ISO/IEC JTC 1	ISO/IEC 19831:2015	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol -- An Interface for Managing Cloud Infrastructure
ISO/IEC JTC 1	ISO/IEC 19941:2017	Information technology -- Cloud computing -- Interoperability and portability
ISO/IEC JTC 1	ISO/IEC 19944:2017	Information technology -- Cloud computing -- Cloud services and devices: Data flow, data categories and data use
ISO/IEC JTC 1	ISO/IEC TR 20000-9:2015	Information technology -- Service management -- Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
ETSI	ETSI TR 102 997 V1.1.1 (04/2010)	CLOUD; Initial analysis of standardization requirements for Cloud services
ETSI	ETSI TS 103 125 V1.1.1 (11/2012)	CLOUD; SLAs for Cloud services
ETSI	ETSI TR 103 126 V1.1.1 (11/2012)	CLOUD; Cloud private-sector user recommendations
ETSI	ETSI TS 103 142 V1.1.1 (04/2013)	CLOUD; Test Descriptions for Cloud Interoperability
ETSI	ETSI SR 003 381 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Identification of Cloud user needs
ETSI	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	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
ITU-T	ITU-T F.743.2 (07/2016)	Requirements for cloud storage in visual surveillance
ITU-T	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	ITU-T FG Cloud TR Part 2 (02/2012)	Technical Report: Part 2: Functional requirements and reference architecture

SDO	Reference	Title
ITU-T	ITU-T FG Cloud TR Part 3 (02/2012)	Technical Report: Part 3: Requirements and framework architecture of cloud infrastructure
ITU-T	ITU-T FG Cloud TR Part 4 (02/2012)	Technical Report: Part 4: Cloud Resource Management Gap Analysis
ITU-T	ITU-T FG Cloud TR Part 5 (02/2012)	Technical Report: Part 5: Cloud security
ITU-T	ITU-T FG Cloud TR Part 6 (02/2012)	Technical Report: Part 6: Overview of SDOs involved in cloud computing
ITU-T	ITU-T FG Cloud TR Part 7 (02/2012)	Technical Report: Part 7: Cloud computing benefits from telecommunication and ICT perspectives
ITU-T	ITU-T M.3371 (10/2016)	Requirements for service management in cloud-aware telecommunication management system
ITU-T	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	ITU-T Q.4040 (02/2016)	The framework and overview of cloud computing interoperability testing
ITU-T	ITU-T Y.3501 (06/2016)	Cloud computing framework and high-level requirements (edition 2 under development)
ITU-T	ITU-T Y.3503 (05/2014)	Requirements for desktop as a service
ITU-T	ITU-T Y.3504 (06/2016)	Functional architecture for Desktop as a Service
ITU-T	ITU-T Y.3510 (02/2016)	Cloud computing infrastructure requirements (edition 2 under development)
ITU-T	ITU-T Y.3511 (03/2014)	Framework of inter-cloud computing
ITU-T	ITU-T Y.3512 (08/2014)	Cloud computing - Functional requirements of Network as a Service
ITU-T	ITU-T Y.3513 (08/2014)	Cloud computing - Functional requirements of Infrastructure as a Service
ITU-T	ITU-T Y.3515 (ex Y.CCNaaS-arch) (07/2017)	Cloud computing - Functional architecture of Network as a Service
ITU-T	ITU-T Y.3516 (ex Y.CCIC-arch) (09/2017)	Cloud computing - Functional architecture of inter-cloud computing
ITU-T	ITU-T Y.3520 (09/2015)	Cloud computing framework for end to end resource management (edition 2 under development)
ITU-T	ITU-T Y.3521/M.3070 (03/2016)	Overview of end-to-end cloud computing management
ITU-T	ITU-T Y.3522 (09/2016)	End-to-end cloud service lifecycle management requirements
ITU-T	ITU-T Y.3600 (11/2015)	Big data – Cloud computing based requirements and capabilities

6.2.2. 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	ISO/IEC 27017:2015 / ITU-T X.1631 (07/2015)	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

SDO	Reference	Title
ISO/IEC JTC 1	ISO/IEC 27018:2014	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC JTC 1	ISO/IEC 27036-4:2016	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ETSI	ETSI TR 103 304 V1.1.1 (07/2016)	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ETSI	ETSI SR 003 391 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing
ETSI	ETSI TS 103 532 V1.1.1 (03/2018)	Attribute Based Encryption for Attribute Based Access Control
ETSI	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
ITU-T	ITU-T X.1601 (10/2015)	Security framework for cloud computing (edition 2 under development)
ITU-T	ITU-T X.1602 (03/2016)	Security requirements for software as a service application environments
ITU-T	ITU-T X.1641 (09/2016)	Guidelines for cloud service customer data security
ITU-T	ITU-T X.1642 (03/2016)	Guidelines of operational security for cloud computing
ITU-T	Y.3514 (ex Y.CCTIC) (05/2017)	Cloud computing - Trusted inter-cloud computing framework and requirements

6.2.3. 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	ISO/IEC NP TR 15944-14	Information technology -- Business operational view -- Part 14: Open-edi, model and cloud computing architecture
ISO/IEC JTC 1	ISO/IEC FDIS 19086-2	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model
ISO/IEC JTC 1	ISO/IEC CD 22123	Information technology -- Cloud computing -- Concepts and terminology
ISO/IEC JTC 1	ISO/IEC CD 22624	Information technology -- Cloud Computing -- Taxonomy based data handling for cloud services
ISO/IEC JTC 1	ISO/IEC PRF TR 22678	Information Technologies -- Cloud Computing -- Guidance for Policy Development
ISO/IEC JTC 1	ISO/IEC AWI TS 23167	Information Technology -- Cloud Computing -- Common Technologies and Techniques
ISO/IEC JTC 1	ISO/IEC NP TR 23187	Information technology -- Cloud computing -- Interacting with cloud service partners (CSNs)
ISO/IEC JTC 1	ISO/IEC NP TR 23188	Information technology -- Cloud computing -- Edge computing landscape
ISO/IEC JTC 1	ISO/IEC NP TR 23613	Information technology -- Cloud service metering and billing elements

SDO	Reference	Title
ETSI	ETSI GS/NFV-EVE011	Network Functions Virtualisation (NFV) Release 3; Software Architecture; Specification of the Classification of Cloud Native VNF implementations
ETSI	ETSI GR/NFV-IFA029	Network Functions Virtualisation (NFV); Software Architecture; Report on the Enhancements of the NFV architecture towards “Cloud-native” and "PaaS"
ETSI	ETSI GR IP6 007	IPv6-based Cloud Computing; IPv6-based Deployment of Cloud Computing
ITU-T	ITU-T Draft Y.csb-reqts	Cloud Computing Requirements for Cloud Service Brokerage
ITU-T	ITU-T Draft Y.CCICTM	Cloud Computing - Overview of Inter-Cloud Trust Management
ITU-T	ITU-T Draft H.248.CLOUD	Gateway control protocol: Cloudification of packet gateways
ITU-T	ITU-T Draft H.CSVS-Arch	Architectural requirements for cloud storage in video surveillance
ITU-T	ITU-T Draft H.VSCC	Architecture for cloud computing in visual surveillance
ITU-T	ITU-T Draft M.cbnmsa	Cloud-based network management system architecture
ITU-T	ITU-T Draft Q.CCP	Set of parameters of cloud computing for monitoring
ITU-T	ITU-T Draft Q.wa-iop	Cloud Interoperability testing about Web Application
ITU-T	ITU-T Draft Supp-Y.Cloud Computing Scenarios for Developing Countries	Scenarios of Implementing Cloud Computing in networks of developing countries
ITU-T	ITU-T Draft Y.BDaaS-arch	Cloud computing - Functional architecture of Big Data as a Service
ITU-T	ITU-T Draft Y.cccm-reqts	Cloud Computing - Requirements for Containers and Micro-services
ITU-T	ITU-T Draft Y.ccdc-reqts	Distributed cloud overview and high-level requirements
ITU-T	ITU-T Draft Y.CCICDM-Req	Cloud Computing - Requirements for Inter-Cloud Data Management
ITU-T	ITU-T Draft Y.ccpm-reqts	Cloud computing-Functional requirements of physical machine
ITU-T	ITU-T Draft Y.cslm-metadata	Metadata framework for cloud service lifecycle management
ITU-T	ITU-T Draft Y.sup.ccsr	Supplement on Cloud Computing Standardization Roadmap

6.2.4. 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	ISO/IEC FDIS 19086-4	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy
ISO/IEC JTC 1	ISO/IEC PRF TR 23186	Information technology -- Cloud computing -- Framework of trust for processing of multi-sourced data
ISO/IEC JTC 1	ISO/IEC FDIS 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ETSI	ETSI TS 103 458	CYBER; Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services
ITU-T	ITU-T Draft X.dsms	Data security requirements for the monitoring service of cloud computing

SDO	Reference	Title
ITU-T	ITU-T Draft X.SRIaaS	Security requirements of public infrastructure as a service (IaaS) in cloud computing
ITU-T	ITU-T Draft X.SRNaaS	Security requirements of Network as a Service (NaaS) in cloud computing

6.3. Artificial Intelligence and Big Data

6.3.1. 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	ISO/IEC 11179-1:2015	Information technology -- Metadata registries (MDR) -- Part 1: Framework
ISO/IEC JTC 1	ISO/IEC 11179-2:2005	Information technology -- Metadata registries (MDR) -- Part 2: Classification
ISO/IEC JTC 1	ISO/IEC 11179-3:2013	Information technology -- Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes
ISO/IEC JTC 1	ISO/IEC 11179-4:2004	Information technology -- Metadata registries (MDR) -- Part 4: Formulation of data definitions
ISO/IEC JTC 1	ISO/IEC 11179-5:2015	Information technology -- Metadata registries (MDR) -- Part 5: Naming principles
ISO/IEC JTC 1	ISO/IEC 11179-6:2015	Information technology -- Metadata registries (MDR) -- Part 6: Registration
ISO/IEC JTC 1	ISO/IEC 19763-1:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 1: Framework
ISO/IEC JTC 1	ISO/IEC 19763-3:2010	Information technology -- Metamodel framework for interoperability (MFI) -- Part 3: Metamodel for ontology registration
ISO/IEC JTC 1	ISO/IEC 19763-5:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 5: Metamodel for process model registration
ISO/IEC JTC 1	ISO/IEC 19763-6:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 6: Registry Summary
ISO/IEC JTC 1	ISO/IEC 19763-7:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 7: Metamodel for service model registration
ISO/IEC JTC 1	ISO/IEC 19763-8:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 8: Metamodel for role and goal model registration
ISO/IEC JTC 1	ISO/IEC TR 19763-9:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 9: On demand model selection
ISO/IEC JTC 1	ISO/IEC 19763-10:2014	Information technology -- Metamodel framework for interoperability (MFI) -- Part 10: Core model and basic mapping
ISO/IEC JTC 1	ISO/IEC 19763-12:2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 12: Metamodel for information model registration

SDO	Reference	Title
ISO/IEC JTC 1	ISO/IEC TS 19763-13:2016	Information technology -- Metamodel framework for interoperability (MFI) -- Part 13: Metamodel for form design registration
ISO/IEC JTC 1	ISO/IEC TR 20547-2:2018	Information technology – Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
ISO/IEC JTC 1	ISO/IEC TR 20547-5:2018	Information technology -- Big data reference architecture -- Part 5: Standards roadmap
ISO/IEC JTC 1	ISO/IEC 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	ISO/IEC 20944-2:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 2: Coding bindings
ISO/IEC JTC 1	ISO/IEC 20944-3:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 3: API bindings
ISO/IEC JTC 1	ISO/IEC 20944-4:2013	Information technology -- Metadata Registries Interoperability and Bindings (MDR-IB) -- Part 4: Protocol bindings
ISO/IEC JTC 1	ISO/IEC 24707:2018	Information technology -- Common Logic (CL) -- A framework for a family of logic-based languages
ITU-T	ITU-T Y.3600 (11/2015)	Big data - Cloud computing based requirements and capabilities
ITU-T	ITU-T Y.3600-series Supplement 40 (07/2016)	Big Data Standardization Roadmap
ITU-T	Y.4114 (ex Y.IoT-BigData-reqts) (07/2017)	Specific requirements and capabilities of the IoT for Big Data

6.3.2. 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	ISO/IEC 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	ISO/IEC 15944-7:2009	Information technology -- Business operational view -- Part 7: eBusiness vocabulary
ISO/IEC JTC 1	ISO/IEC 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	ISO/IEC 15944-9:2015	Information technology -- Business operational view -- Part 9: Business transaction traceability framework for commitment exchange

6.3.3. 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	ISO/IEC FDIS 20546	Information technology -- Big Data -- Overview and Vocabulary
ISO/IEC JTC 1	ISO/IEC AWI TR 20547-1	Information technology -- Big data reference architecture -- Part 1: Framework and application process
ISO/IEC JTC 1	ISO/IEC DIS 20547-3	Information technology -- Big data reference architecture -- Part 3: Reference architecture
ISO/IEC JTC 1	ISO/IEC WD 22989	Artificial Intelligence -- Concepts and Terminology
ISO/IEC JTC 1	ISO/IEC WD 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
ISO/IEC JTC 1	ISO/IEC CD 21838-1	Information technology -- Top-level ontologies -- Part 1: Requirements
ISO/IEC JTC 1	ISO/IEC CD 21838-2	Information technology -- Top-level ontologies -- Part 2: Basic Formal Ontology (BFO)
ISO/IEC JTC 1	ISO/IEC NP TR 29075-1	Information technology -- Data management and interchange -- Design notes for new database language technologies -- Part 1: SQL support for streaming data
ISO/IEC JTC 1	ISO/IEC DIS 15944-1	Information technology -- Business operational view -- Part 1: Operational aspects of open-edi for implementation
ISO/IEC JTC 1	ISO/IEC DIS 15944-10	Information technology -- Business operational view -- Part 10: IT-enabled coded domains as semantic components in business transactions
ISO/IEC JTC 1	ISO/IEC DIS 15944-12	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	ISO/IEC DIS 15944-13	Information technology -- Business operational view -- Part 13: Open-edi, jurisdictional domains and transborder data flows (TBDF) including privacy protection
ISO/IEC JTC 1	ISO/IEC DIS 15944-14	Information technology -- Business operational view -- Part 14: Open-edi, model and cloud computing architecture
ISO/IEC JTC 1	ISO/IEC DIS 15944-15	Information technology -- Business operational view -- Part 15: Application of open-edi business transaction ontology in distributed business transaction repositories and open value networks
ITU-T	ITU-T Draft Y.BigDataEX-arch	Big data - Functional architecture of big data exchange
ITU-T	ITU-T Draft Study_bigdata	Technical Paper on economic and policy aspects of Big Data in international telecommunication services and networks
ITU-T	ITU-T Draft F.VSBD	Requirements for big data application in visual surveillance system
ITU-T	ITU-T Draft Y. bDDN-MNTMP	Big data driven mobile network traffic management and planning
ITU-T	ITU-T Draft Y.BDaaS-arch	Cloud computing - Functional architecture of Big Data as a Service

SDO	Reference	Title
ITU-T	ITU-T Draft Y.bDDN-fr	Framework of big data driven networking based on Deep Packet Inspection
ITU-T	ITU-T Draft Y.bDDN-req	Requirement of big data-driven networking
ITU-T	ITU-T Draft Y.BDDP-reqts	Big data - Overview and requirements for data preservation
ITU-T	ITU-T Draft Y.bdi-reqts	Big Data - Overview and functional requirements for data integration
ITU-T	ITU-T Draft Y.bdm-sch	Big data - Metadata framework and conceptual model
ITU-T	ITU-T Draft Y.bDPI-Mec	Mechanism of deep packet inspection applied in network big data context
ITU-T	ITU-T Draft Y.bdp-reqts	Big data - Requirements for data provenance
ITU-T	ITU-T Draft Y.BigDataEX-reqts	Big data exchange framework and requirements
ITU-T	ITU-T Draft Y.Sup-bDDN-usecase	Supplement for use cases and application scenarios of big data driven networking

6.3.4. 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	ISO/IEC DIS 15944-5	Information technology -- Business operational view -- Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints
ISO/IEC JTC 1	ISO/IEC DIS 15944-7	Information technology -- Business operational view -- Part 7: e-Business vocabulary
ISO/IEC JTC 1	ISO/IEC DIS 15944-8	Information technology -- Business operational view -- Part 8: Identification of privacy protection requirements as external constraints on business transactions
ISO/IEC JTC 1	ISO/IEC DIS 15944-9	Information technology -- Business operational view -- Part 9: Business transaction traceability framework for commitment exchange
ISO/IEC JTC 1	ISO/IEC AWI 20547-4	Information technology -- Big data reference architecture -- Part 4: Security and privacy
ISO/IEC JTC 1	ISO/IEC FDIS 20889	Privacy enhancing data de-identification terminology and classification of techniques
ITU-T	ITU-T Draft X.GSBDaaS	Guidelines on security of Big Data as a Service
ITU-T	ITU-T Draft X.srfb	Security Requirements and Framework for Big Data Analytics in mobile Internet services

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

ILNAS
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 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 2 departments: Standardization, and Metrology. 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.

November 2018 · Smart Secure ICT · Version 1.0 · © ILNAS/ANEC

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