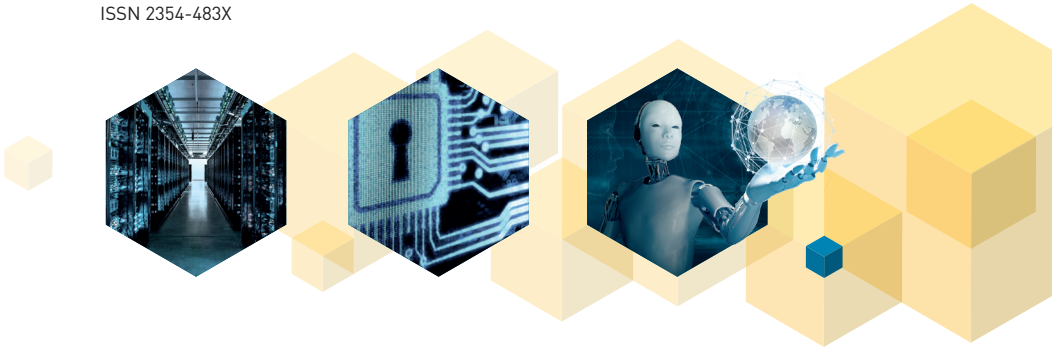
STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 2.0 · October 2019
ISSN 2354-483X



ANEC

STANDARDS ANALYSIS

SMART SECURE ICT

LUXEMBOURG

Version 2.0 · October 2019

ISSN 2354-483X

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

Indeed, the ICT sector has gained more and more importance in society as a whole in the 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 "things" to be connected, to communicate between each other and to collect information is deeply changing the world we know it 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 has been led by the government for several years, not only to be part of this transformation, but also to take a major role in the future of the digital landscape by setting a secure and trusted data-driven economy. 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 "Luxembourg's policy on ICT technical standardization 2015-2020"[2].

In this context, 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 achievements were the creation of a University certificate "*Smart ICT for Business Innovation*" in collaboration with the University of Luxembourg, and the research program[3] on Digital Trust for Smart ICT launched in 2017 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/Artificial Intelligence - notably considering Digital Trust aspects related to these technologies. A first result of this program was the publication of a White Paper "Data Protection and Privacy in Smart ICT"[4] in October 2018. These collaborations are contributing to the development of a professional Master degree "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*", forecast to be launched in September 2020 (including the program of the University certificate "Smart ICT for Business Innovation").

Another component of the policy on ICT technical standardization consists in strengthening the normative culture about ICT technical standardization at the national level. In this framework, White Papers have been drawn-up in recent years, such as on "Internet of Things" [5] , "Blockchain and Distributed Ledger Technologies"[6] or "Digital Trust for Smart ICT"[7]. In parallel, the Standards Analysis "Smart Secure ICT Luxembourg" is regularly updated in order to provide to the national market an overview of the recent Smart Secure ICT developments from a technical standardization perspective. The document has evolved over recent years to focus now on the Smart Secure ICT domain, following the national market's interests.

This Standards Analysis "Smart Secure ICT Luxembourg" is intended to serve as a practical tool to discover the latest standardization developments in Smart ICT related technologies, such as Internet of Things, Cloud Computing, Artificial Intelligence, and Blockchain, as well as Digital Trust related standards for those technologies. It is also directly answering the objectives fixed by the "National Cybersecurity Strategy III" [8] in terms of standardization needs for digital infrastructure protection. Therefore, the present document will allow national stakeholders to identify relevant standardization technical committees and Fora & Consortia 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"

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

[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"

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

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

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

[8] Luxembourg's National Cybersecurity Strategy III

EXECUTIVE SUMMARY

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

In this context, this Standards Analysis is designed to develop an information and exchange network for Smart Secure ICT standardization knowledge in the Grand Duchy of Luxembourg. Currently, 91[9] experts are registered through ILNAS as national delegates in the ICT sector. Among them, 74 are directly involved in Smart ICT and Digital Trust related technical committees[10], such as in Internet of Things: 18; Cloud Computing: 15; Artificial Intelligence: 23; Blockchain: 22, Digital Trust: 38.

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 consist 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 on the Smart ICT standardization development at international and European levels to support national stakeholders. Firstly, it introduces basic components of Smart ICT technologies as well as Digital Trust requirements for Smart ICT, and secondly, it presents related standardization activities performed at 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. This new edition also aims at helping the national market in the identification of relevant cybersecurity standardization activities, to support the implementation of the "National Cybersecurity Strategy III" through a monitoring of standardization technical committees and Fora and Consortia working in the Digital Trust area.

[9] National register of standardization delegates – September 2019

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

TABLE OF CONTENTS

INTRODUCTION 1

1. TECHNICAL STANDARDIZATION AND STANDARDS 3

1.1. Standardization Objectives and Principles 3

1.2. Standardization Landscape 4

2. SMART SECURE ICT LANDSCAPE 9

2.1. Introduction, Definition and Interactions between Smart ICT Components 9

2.2. Economic Overview 10

2.3. Smart Secure ICT in Luxembourg 11

3. SMART SECURE ICT STANDARDS WATCH 13

3.1. Internet of Things (IoT) 13

3.2. Cloud Computing 28

3.3. Artificial Intelligence (AI) and Big Data 34

3.4. Blockchain and Distributed Ledger Technologies 44

3.5. Digital Trust in Smart ICT 48

3.6. Fora and Consortia in the Digital Trust Area 66

4. OPPORTUNITIES FOR THE NATIONAL MARKET 75

4.1. Information about Standardization 75

4.2. Training in Standardization 80

4.3. Involvement in Standardization 81

5. CONCLUSIONS 85

6. APPENDIX - SMART SECURE ICT STANDARDS AND PROJECTS 87

6.1. Internet of Things 87

6.2. Cloud Computing 94

6.3. Artificial Intelligence and Big Data 98

AUTHORS AND CONTACTS 105

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[11]. To enhance these activities also at the academic level, ILNAS is notably working with the University of Luxembourg to develop standards-related education and research. The University certificate "*Smart ICT for Business Innovation*", organized in 2015-2016 and in 2018-2019, was its first step to working 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 implemented successfully, and was of great interest to participants from multiple industries of different sectors.

In line with the University certificate, ILNAS and the University of Luxembourg are also implementing a research program whose objective is to analyze and extend standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, Internet of Things and Artificial Intelligence/Big Data. In this context, three PhD students are performing research activities in the above-mentioned Smart ICT domains. Some of the first results of this collaboration are the publication of a White Paper "Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization" in October 2018[12], as well as the awarding of the research team with the "Security Project of the Year" during the Information Security Day 2019[13]. One objective of this program is to rely on the research results to develop new academic courses on ICT technical standardization, notably through the planned professional Master Program "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*" expected to be launched in September 2020.

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

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

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

[13] https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team

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. Objectives of technical standardization and introduction of its landscape in national, European and international levels have been included in Chapter 1. Chapter 2 proposes a definition of Smart ICT, provides an economic overview of ICT and introduces the main interactions between the Smart ICT domains included in this analysis. Chapter 3 further details each of these Smart ICT domains by providing some basic concepts and presenting relevant technical committees. Requirements of Digital Trust for Smart ICT are also detailed in this chapter, together with related technical committees and Fora and Consortia. Chapter 4 presents opportunities related to standardization for national stakeholders. It also introduces the way ILNAS is supporting the 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 domain, as well as related Digital Trust standards.

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)[14] 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[15].

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[16]. 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[17], "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.

[14] 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

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

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

[17] 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 economic 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[18], 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.

[18] 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[19]

European and International Standardization Bodies		Date of Creation	Number of Members	Number of Published Standards
ISO	International Organization for Standardization	1946	164	22 771
IEC	International Electrotechnical Commission	1906	86	6 755
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector	1865	269[20]	5 512
CEN	European Committee for Standardization	1961	34	16 979
CENELEC	European Committee for Electrotechnical Standardization	1973	34	7 352
ETSI	European Telecommunications Standards Institute	1988	913[20] (65 countries)	46 765

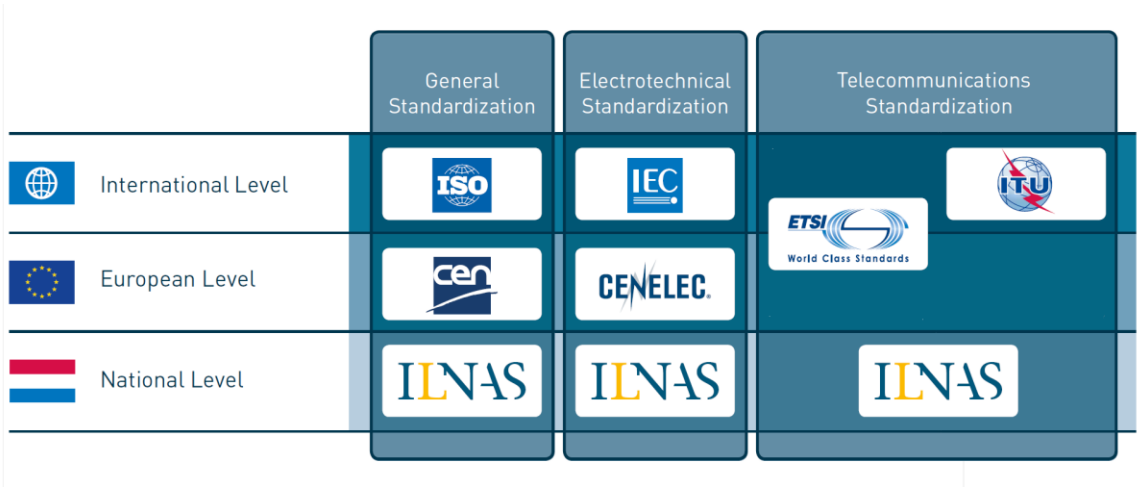
At national levels, one or several national standards bodies protect the interests of the country within the European and international standardization organizations. In Luxembourg, ILNAS – the only official national standards body – is member of the European and international standardization organizations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

[19] Source: Websites of organizations - September 2019

[20] 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[21], 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[22] 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, 32% of all European standards ratified by CEN, as well as 73% of those ratified by CENELEC, are respectively identical to ISO or IEC standards[23]. 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) in 2000, lastly renewed in 2016[24], that paves the way for European regional standards, developed by ETSI, to be recognized internationally.

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

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

[23] CEN CENELEC in figures – 2019 Q2

[24] 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 (e.g.: ISO/IEC JTC 1 for the Information Technology domain).

ISO, IEC and ITU have also established the World Standards Cooperation (WSC) in 2001, a high-level collaboration system intending to strengthen and advance the voluntary consensus-based international standards system and to resolve issues related to the technical cooperation between the three organizations[25]. 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 22,700 standards published and more than 4,700 standards under development[26]. 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. It 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 CEN and CENELEC are detailed in an annual common Work Program, which was published in December 2018 for the year 2019[27]. They are active in several ICT-related areas covering both the Digital Society and the Smart Technologies: e-Signatures, Intelligent Transport Systems, Smart Grids, Smart Metering, Internet of Things, Smart Homes, Smart Cities, Advanced Manufacturing, Artificial Intelligence, Blockchain and Distributed Ledger Technologies, Cybersecurity and Data Protection, etc.

❖ 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 the Smart Secure ICT area – e.g.: Internet of Things (ETSI/TC SmartM2M) or Digital Trust (e.g.: ETSI/TC ESI and ETSI/TC CYBER).

[25] http://www.worldstandardscooperation.org/
[26] https://www.iso.org/iso-in-figures.html (accessed 09.2019)
[27] https://www.cencenelec.eu/News/Publications/Publications/CEN-CENELEC_WP_2019.pdf (accessed 09.2019)

❖ 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 SECURE ICT LANDSCAPE

2.1. Introduction, Definition and Interactions between Smart ICT Components

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 affected 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[28]".

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

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

- 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 collected data.
- Cloud Computing supports these environments by providing the processing power and infrastructure used by Big data and analytics tools to produce/extract value from data collected, for example by an IoT system.
- 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 (Big) data. Data based learning is the highly applied approximation approach in AI. AI is now offered as a service through the Cloud.

[28] 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").

- Blockchain tracks the records of smart devices (for example used by IoT systems) to make interactions more transparent and trustful.
- To utilize maximum efficiency of the Smart ICT technology, building and maintaining Digital Trust among stakeholders is extremely important. Different components of Digital Trust are important for Smart ICT technology adoption, such as privacy, data and information security and interoperability. Standards, in that context, are produced as a tool offering a set of good practices allowing for creating, maintaining and strengthening Digital Trust (e.g., by setting appropriate information management systems, making possible interoperability among Smart ICT, guidelines for protecting data, etc.).

A technological introduction of above-mentioned Smart ICT technologies including Digital Trust is provided in Chapter 3. 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, creating digital trust.

2.2. Economic Overview

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

Worldwide revenues for IT services crossed the $1 trillion mark in 2018[29]. In the same time, companies' investment in IT keeps growing. Gartner estimates that global IT spending will be increased by 0.6% for this year as compared to 2018, reaching $3.74 trillion[30]. According to the 2018 EU Industrial R&D Investment Scoreboard, Research & Development global investment into R&D in 2018 increased by 8.3% over the previous year, with a total of €736.4 billion invested by companies analyzed in the study (accounting for approximately 90% of the world's business-funded R&D). This growth was mainly driven by the sectors of ICT services (+13%) and ICT producers (+11%)[31]. Moreover, the coming trends show that the sector is still innovating with the development of Smart ICT technologies such as Autonomous things, Augmented analytics, Artificial Intelligence, Digital twins, Edge computing, Immersive technologies, Blockchain, Smart spaces, Quantum computing, etc.[32]

The development of Smart ICT technologies, which are increasingly interconnected, represents great opportunities for the economy, but also implies new threats. Nowadays, cyber defense appears as one of the main challenges for companies and countries considering the cost of cybercrime for the global economy. The Center for Strategic and International Studies (CSIS) estimates[33] that the global cost of cybercrime may be as much as $600 billion a year, meaning nearly one percent of the global GDP. In the same time, worldwide investments in Information Security are forecast to reach $124 billion in 2019, representing an increase of 8.7% compared to 2018.

[29] https://www.idc.com/getdoc.jsp?containerId=prUS45011519

[30] https://www.gartner.com/en/newsroom/press-releases/2019-10-07-gartner-says-global-it-spending-to-grow-06-in-2019 (accessed 09.2019)

[31] The 2018 EU Industrial R&D Investment Scoreboard (accessed 09.2019)

[32] https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/ (accessed 09.2019)

[33] https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf (accessed 09.2019)

At the European level, the ICT sector has been directly responsible for 5% of GVA[34] (Gross Value Added), with a market value of €688 billion in 2017[35], but it contributes far more to the overall productivity growth. This is not only due to the high levels of dynamism and innovation inherent to the sector, but also due to the enabler role this sector plays, in changing how other sectors do business. At the same time, the social impact of ICT has become significant. This is supported by European statistics of 2018, with 89% (Luxembourg: 97%) of households having a broadband connection[36], 83% (Luxembourg: 96%) of individuals using the Internet on a regular basis [37] of which 77% (Luxembourg: 91%) used a mobile device to connect to the Internet away from home or work[38].

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*"[39].

2.3. Smart Secure ICT in Luxembourg

ICT is considered a key economic sector in the Grand Duchy of Luxembourg. Within the Coalition Agreement of the Government[40], the follow-up of Smart ICT development constitutes an important aspect since they represent great opportunities for the Economy. At the same time, it is important to mitigate threats related to their generalization. The Government works to make the country one of the leaders of the ICT sector and has adopted strategies in order to accelerate developments in different areas, such as 5G, Artificial Intelligence or High Performance Computing (HPC)[41], while taking into account cybersecurity related challenges. In this context, the "National Cybersecurity Strategy III"[42], last updated in May 2018, provides the way forward in order to ensure maximum security for all stakeholders.

This program ensures continuity in the ICT sector's growth in the country. Indeed, since the last decade, multiple actions have been initiated to foster the positioning of Luxembourg in the ICT landscape. One was the launch of "Digital Lëtzebuerg"[43] in 2014, which is responsible to execute the digitalization strategy of the Government. Through the national policy pursued in recent years, Luxembourg aims to accompany the transition to a digital economy and society. Indeed, several initiatives have been launched to consolidate and expand the country's ICT capabilities. For example:

---

[34] 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)

[35] Source: Eurostat - National accounts aggregates by industry (accessed 09.2019)

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

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

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

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

[40] https://gouvernement.lu/dam-assets/documents/actualites/2018/12-decembre/Accord-de-coalition-2018-2023.pdf

[41] https://gouvernement.lu/dam-assets/fr/publications/accord-coalition/2018-2023/Declaration-sur-le-programme-gouvernemental-2018-2023-version-FR.pdf

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

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

- The strategic study on the “Third Industrial Revolution”[44], presented in November 2016, which proposes concrete actions and tools, including a range of strategic measures and projects, to prepare the country, its society and its economy to begin the process of the "Third Industrial Revolution".
- The “National Cybersecurity Strategy III”[45], lastly updated in May 2018 and which intends to provide an environment conducive to digital development, while ensuring maximum security for all stakeholders. This strategy is notably highlighting the importance of monitoring standards development in order to take into account internationally recognized practices in the cybersecurity area.
- The “5G strategy for Luxembourg”[46], published in November 2018, which fixes the objective of the country to develop the infrastructure supporting 5G deployment.
- The document “Artificial Intelligence: a Strategic Vision for Luxembourg”[47], published in May 2019, which defines three main ambitions for the country: to be among the most advanced digital societies in the world, especially in the EU; to become a data-driven and sustainable economy; to support human-centric AI development.
- The “Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg”[48], published in May 2019. It provides an approach to accelerate the Digitalization-enabled transformation of Luxembourg’s industry across key strategic sectors, boosting productivity across the entire Luxembourg economy.

All these developments have allowed Luxembourg to establish a competitive ICT sector in Luxembourg. The country ranks 6th out of the 28 EU Member States in the “European Commission Digital Economy and Society Index” (DESI) 2019[49]. The country is particularly strong in terms of connectivity (ranks 2nd), human capital (ranks 3rd) and use of the Internet (ranks 6th). The ICT sector represents 2 304 companies in 2016 and 4.4% of the total employment at the first semester 2019[50].

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

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

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

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

[48] https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-economie/The-Data-driven-Innovation-Strategy.pdf

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

[50] Source: STATEC

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, along with a list of Fora and consortia active in the Digital Trust area.

In addition, lists of standards both published and under development for the selected Smart ICT technologies and related Digital Trust are provided in the Appendix. This overview of standards and projects at 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[51]. This network of uniquely identifiable connected devices such as objects, devices, sensors and everyday items with computing services is called IoT[52]. 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[53]	"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[54]	"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.

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

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

[53] 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

[54] 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[55]	"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[56]

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 [57] 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.

[55] http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps

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

[57] http://www.blackwellreference.com

Characteristic	Description
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.
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[58]. The urgent need for standardization and necessary improvements in interoperability are critical success factors for accelerated adoption of IoT systems[59]. 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).

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

[59] 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, Belarus, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Israel, Italy, Japan, **Luxembourg**, Malaysia, Netherlands, Norway, Russian Federation, Singapore, Sweden, Switzerland, United Kingdom, United States **Observing Countries (13):** Argentina, Iceland, Iran, Ireland, Kenya, Mexico, Pakistan, Republic of the Philippines, Poland, Portugal, Romania, Saudi Arabia, Slovakia
Secretariat	KATS (Republic of Korea)		
Committee Manager	Ms. Jooran Lee		
Chairperson	Dr. François Coallier		
Organizations in liaison	AIM, AIOTI, GS1, IIC, INCOSE, ITU-T, OCF, OGC		
Web site	https://www.iec.ch/dyn/www/f?p=103:29:3410818666523		
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/WG 3 — IoT Architecture JTC 1/SC 41/WG 4 — IoT Interoperability JTC 1/SC 41/WG 5 — IoT Applications JTC 1/SC 41/JWG 17 — System interface between industrial facilities and the smart grid Managed by TC 65 JTC 1/SC 41/AG 6 — JTC 1/SC 41 Advisory Group JTC 1/SC 41/AG 20 — Sectorial Liaison Group (SLG 1) on Industrial IoT (IIoT) JTC 1/SC 41/AG 21 — Sectorial Liaison Group (SLG 2) on Utilities IoT JTC 1/SC 41/AG 22 — Liaison Coordination Group (LCG) on IoT Trustworthiness JTC 1/SC 41/AHG 14 — Ad hoc group on Business Plan JTC 1/SC 41/AHG 15 — Communication and outreach JTC 1/SC 41/AHG 17 — Study Group on Societal and human factors in IoT based services JTC 1/SC 41/AHG 18 — Study Group on Integration of IoT and Blockchain JTC 1/SC 41/AHG 23 — Ad hoc group on IoT Personnel positioning management system (PPMS) JTC 1/SC 41/AHG 24 — Ad hoc group on IoT use cases		
Standardization work			
Published standards	20		
Standards under development	17		
Involvement of Luxembourg			
18 delegates - Mr. Shyam Wagle (Chairman) — ANEC G.I.E.			

- Mr. Anouar Adlani	vyzVoice S.A.
- Mr. Johann Amsenga	INCERT GIE
- Mr. Philippe Bovy	KPMG Luxembourg S.C.
- Mr. Matthias Brust	University of Luxembourg
- Mr. Arunas Buknys	FANUC Europe S.A
- Mr. Vincent Cady	Tarkett S.A.
- Mr. Cyril Cassagnes	University of Luxembourg
- Mr. Sankalp Ghatpande	University of Luxembourg
- Mr. Abdallah Ibrahim	University of Luxembourg
- Mr. Jean Lancrenon	ANEC G.I.E.
- Ms. Maria Rita Palattella	Luxembourg Institute of Science and Technology
- Mr. Benoit Poletti	INCERT GIE
- Mr. Cyrille Rousseau	CORAX IP S.à.r.l
- Mr. Nader Samir Labib	University of Luxembourg
- Mr. Ridha Soua	University of Luxembourg
- Mr. Robert Spicer	vyzVoice S.A.
- Mr. Muhammad Wasim	University of Luxembourg

Comments

ISO/IEC JTC 1/SC 41 “Internet of Things and related technologies” has been established according to the Resolution 12 of the 31st Meeting of ISO/IEC JTC 1 in November 2016. It is currently developing standards to build IoT foundations and exploring new areas of work through study groups on various topics like Integration of IoT and Blockchain or IoT Personnel positioning management system (PPMS). Its current work programs notably include:

- PWI TR JTC1-SC41-1, Internet of Things (IoT) - Underwater Communication Technologies for IoT;
- PWI TR JTC1-SC41-2, Internet of Things (IoT) - Guidance on the application of the IoT Reference Architecture to Wearables and Implantables based IoT Systems;
- ISO/IEC 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 21823-4, Internet of Things (IoT) -- Interoperability for IoT Systems -- Part 4: Syntactic 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) -- Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 systems engineering processes;
- ISO/IEC TR 30148, Internet of Things (IoT) -- Technical requirements and application of sensor network for wireless gas meters;
- ISO/IEC 30149, Internet of Things (IoT) -- Trustworthiness framework;
- ISO/IEC 30160[60], Internet of Things (IoT) -- Application framework for industrial facility demand response energy management;
- ISO/IEC 30161, Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services;
- ISO/IEC 30162, Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems;
- ISO/IEC 30163, Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services;
- ISO/IEC 30164, Internet of things (IoT) -- Edge Computing;
- ISO/IEC 30165, Internet of Things (IoT) -- Real-time IoT framework;
- ISO/IEC TR 30166, Internet of Things (IoT) -- Industrial IoT.

[60] This work item is developed by the JTC 1/SC 41/JWG 17 between JTC 1/SC 41 Internet of Things and related technologies and IEC/TC 65 Industrial-process measurement, control and automation. In order to avoid duplication of IEC TC 65 project IEC TS 62872, the IEC TS 62872 becomes Part 1 of a multipart project and the ISO/IEC 30160 becomes Part 2 of a multipart project that is IEC 62872-2.

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 (26):** United States, Austria, Belgium, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Japan, Kazakhstan, Republic of Korea, **Luxembourg**, Mauritania, Netherlands, Peru, Romania, Russian Federation, Slovakia, South Africa, Sweden, Switzerland, United Kingdom **Observing Countries (22):** Argentina, Bosnia and Herzegovina, Colombia, Czech Republic, Ghana, Hong Kong, Hungary, Indonesia, Islamic Republic of Iran, Italy, Kenya, , Malaysia, New Zealand, Pakistan, Philippines, Serbia, Singapore, Slovenia, Spain, Thailand, Turkmenistan, Ukraine
Secretariat	ANSI (United States)		
Committee Manager	Mr. Eddy Merrill		
Chairperson	Mr. Henri Barthel		
Organizations in liaison	AIM Global, Ecma International, ETSI, GS1, IATA, IEEE, ITU, NATO, OGC, UPU		
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 Data carrier JTC 1/SC 31/WG 2 Data and structure JTC 1/SC 31/WG 4 Radio communications JTC 1/SC 31/WG 8 Application of AIDC standards		
Standardization work			
Published standards	123		
Standards under development	24		
Involvement of Luxembourg			
4 delegates - Mr. Benoit Poletti (Chairman) INCERT G.I.E. - Mr. Clément Gorlt INCERT G.I.E. - Mr. Abdelkrim Nehari INCERT G.I.E. - Mr. Shyam Wagle ANEC G.I.E.			
Comments			
Technologies such as bar coding and radiofrequency identification (RFID) provide quick, accurate and cost-effective ways to identify, track, acquire and manage data and information about items, personnel, transactions and resources. These are known as the automatic identification and data capture (AIDC) technologies. The focus is on efficient implementations of the standards. Governmental bodies in a growing number of countries mandate AIDC technologies, for example in the pharmaceutical and medical device sectors or			

in the areas of fighting against illicit trade in the tobacco industry. There are however still requirements for new technology standards, specifically new barcodes and additional crypto standards to secure information stored in RFID tags.

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

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

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 revision of a series of standards on supply chain applications of RFID.

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 (29):** 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 (18):** Argentina, Bosnia and Herzegovina, Croatia, Cuba, Ghana, Greece, Hungary, Iceland, Indonesia, Kenya, Malaysia, New Zealand, Pakistan, Philippines, Romania, Serbia, Turkey, Ukraine
Secretariat	DIN (Germany)		
Committee Manager	Mr. Marco Peter		
Chairperson	Mr. Rainer Schmidt		
Organizations in liaison	EC, ECMA, ITU, UNCTAD, UNECE		
Web site	https://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 Home electronic systems JTC 1/SC 25/WG 3 Customer Premises Cabling JTC 1/SC 25/WG 4 Interconnection of Computer Systems and Attached Equipment JTC 1/SC 25/PT 40G Channels in support of 40Gbit/s JTC 1/SC 25/PT TT Project Team Taxonomy and Terminology JTC 1/SC 25/AHG 1 Bonding adhoc JTC 1/SC 25/JPT 1 Joint modelling task group linked to SC 46C, SC 48B		
Standardization work			
Published standards	220		
Standards under development	21		
Involvement of Luxembourg			
NO (no registered delegate)			
Comments[61]			
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			

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

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.

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 14543-5-102, Information technology -- Home electronic system (HES) architecture -- Part 5-102: Intelligent grouping and resource sharing -- Remote universal management profile;
- ISO/IEC 15045-3-1, Information technology -- Home Electronic System (HES) gateway -- Part 3-1: Introduction to privacy, security, and safety;
- ISO/IEC 15045-3-2, Information technology -- Home Electronic System -- HES Gateway Privacy Framework;
- ISO/IEC 24383, Information technology -- Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment.

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	GS1, MedTech Europe, VISA EUROPE		
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	27		
Standards under development	2		
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 the two following standards:

- EN 17099, Information technology -- Fish and fish products -- Requirements for labelling of distribution units and pallets in the trade of seafood products (under publication);
- FprEN 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** 	112 member organizations of ETSI
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	55		
Standards under development	28		
Involvement of Luxembourg			
2 organizations - 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, ISO/TMBG/SAG, ITU-R, JCA on multimedia aspects of e-services JCA-AHF, JCA-IMT2020 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 **<u>Other groups under SG 20</u>**: JCA-IoT and SC&C Joint Coordination Activity on Internet of Things and Smart Cities and Communities		
Standardization work			
Published standards	60[62]		
Standards under development	77[62]		
Involvement of Luxembourg			
Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ITU-T/SG 20.			

[62] For the study period 2017-2020 (accessed 09.2019)

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 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[63]	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[64]	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[63]

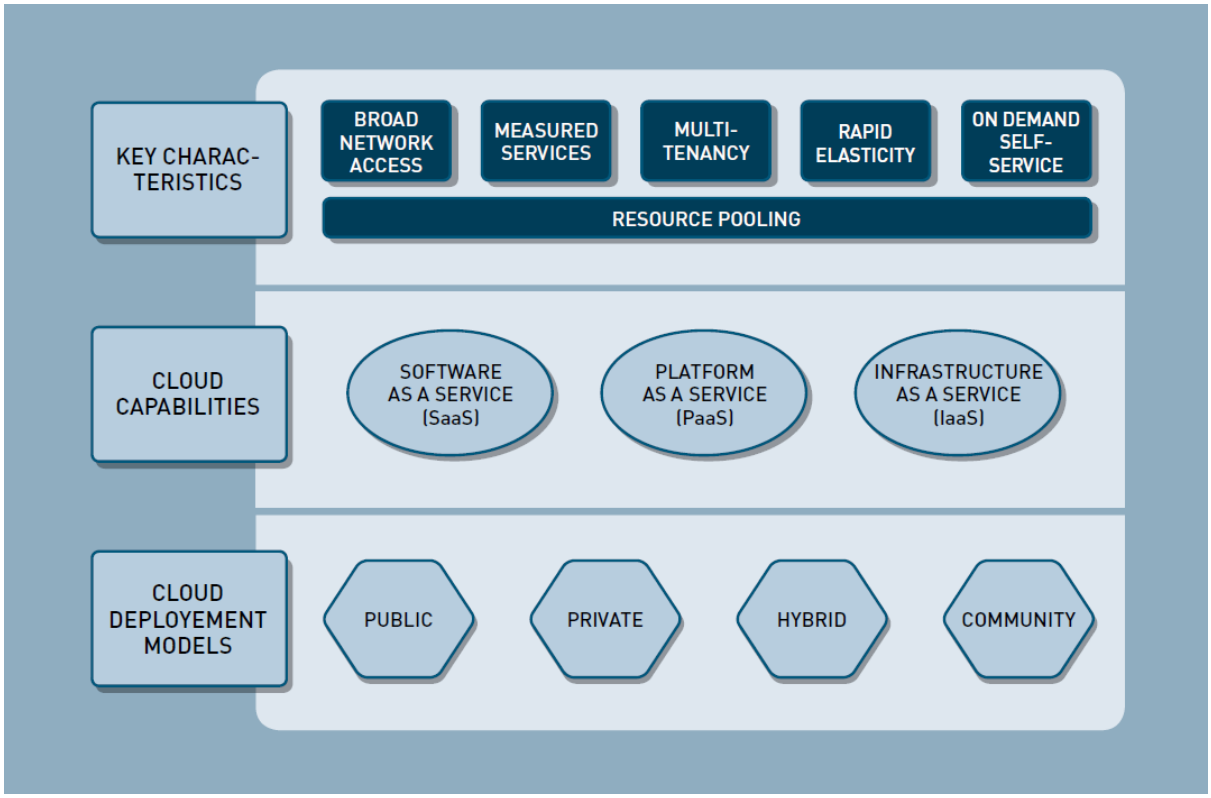
Characteristic	Explanation
Broad Network Access	The physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms.
Measured Service	The metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed. The customer may only pay for the resources that they use.

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

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

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

Figure 2: Visual Model of ISO/IEC Cloud Computing Definition[65]



[65] 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. 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

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td>Committee</td><td>ISO/IEC JTC 1/SC 38</td><td>Title</td><td>Cloud Computing and Distributed Platforms</td></tr>
<tr><td>Creation date</td><td>2009</td><td rowspan="5">MEMBERS
  </td><td rowspan="5">Participating Countries (29):
United States, Australia, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Republic of Korea, Luxembourg, Netherlands, Panama, Poland, Russian Federation, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, United Kingdom

Observing Countries (17:
Argentina, Austria, Bosnia and Herzegovina, Czech Republic, Hong Kong, Hungary, Kenya, Mexico, Norway, Pakistan, Portugal, Serbia, Trinidad and Tobago ,Turkey, Ukraine, Uruguay, Zambia</td></tr>
<tr><td>Secretariat</td><td>ANSI (USA)</td></tr>
<tr><td>Committee Manager</td><td>Mr. Bill Ash</td></tr>
<tr><td>Chairperson</td><td>Mr. Steve Holbrook</td></tr>
<tr><td>Organizations in liaison</td><td>Cloud Security Alliance, , Ecma International, IEEE, INLAC, ITU, OASIS, OGF, SNIA, EC, EuroCloud, TM Forum</td></tr>
<tr><td>Web site</td><td colspan="3">https://www.iso.org/committee/601355.html</td></tr>
<tr><td>Scope</td><td colspan="3">Standardization in the areas 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.</td></tr>
<tr><td>Structure</td><td colspan="3">JTC 1/SC 38/AG 1 Communications committee
JTC 1/SC 38/AG 2 JTC 1/SC 38 Officers group
JTC 1/SC 38/CG 1 Liaison coordination group for JTC 1/SC 27
JTC 1/SC 38/CG 2 Liaison coordination group for JTC 1/SC 41
JTC 1/SC 38/CG 3 Liaison coordination group for JTC 1/SC 42
JTC 1/SC 38/WG 3 Cloud Computing Fundamentals (CCF)
JTC 1/SC 38/WG 5 Data in cloud computing and related technologies</td></tr>
<tr><th colspan="4">Standardization work</th></tr>
<tr><td>Published standards</td><td colspan="3">15</td></tr>
<tr><td>Standards under development</td><td colspan="3">9</td></tr>
</table>

Involvement of Luxembourg

15 delegates

- Mr. Johnatan Pecero (Chairman)	ANEC G.I.E.
- Mr. Matthias Brust	University of Luxembourg
- Mr. Cyril Cassagnes	University of Luxembourg
- Mr. Boonyarit Changaival	University of Luxembourg
- Mrs. Myriam Djerouni	LUXITH G.I.E.
- Mr. Michael Feddema	KPMG Luxembourg S.C.
- Mr. Laurent Fisch	Laurent Fisch Luxlegal S.à r.l.
- Mrs. Shenglan Hu	POST Telecom PSF S.A.
- Mr. Abdallah Ibrahim	University of Luxembourg
- Mr. Andreas Kremer	ITTM
- Mr. Chao Liu	University of Luxembourg
- Mr. Jean-Michel Remiche	POST Telecom S.A.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology
- Mr. Shyam Wagle	ANEC G.I.E.
- Mr. Muhammad Wasim	University of Luxembourg

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 CD 22123, Information Technology -- Cloud Computing -- Concepts and terminology;
- ISO/IEC DIS 22624, Information technology -- Cloud Computing -- Taxonomy based data handling for cloud services;
- ISO/IEC PDTS 23167, Information Technology -- Cloud Computing -- Common Technologies and Techniques;
- ISO/IEC NP TR 23187, Information technology -- Cloud computing -- Interacting with cloud service partners (CSNs);
- ISO/IEC PDTR 23188, Information technology -- Cloud computing -- Edge computing landscape.
- ISO/IEC PDTR 23613, Information technology -- Cloud service metering and billing elements;
- ISO/IEC AWI 23751, Information technology -- Cloud computing and distributed platforms -- Data sharing agreement (DSA) framework;
- ISO/IEC NP TR 23951, Information technology -- Cloud computing -- Best practices for cloud SLA metrics.

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 27018:2019 (lastly updated in 2019), 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. ISO/IEC JTC 1/SC 27 also developed the fourth part of ISO/IEC 19086-4:2019, concerning the security and privacy aspects of the SLA framework and technology.

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 (SG 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. SG 13 focuses on future networks (FNs) – networks of the future beyond NGN – expected to enjoy early realization sometime around 2020 in prototyping or phased deployments. Moreover, SG is responsible for studies related to the requirements, architectures, capabilities and mechanisms of future networks including studies relating to service awareness, data awareness, environmental awareness and socio-economic awareness of future networks. Cloud Computing is an important part of SG 13 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, SG 13 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
	FG ML5G	ITU-T Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G)
	FG NET2030	Focus Group on Technologies for Network 2030
	JRG-CCM	Joint Rapporteur Group on Cloud Computing management

Standardization work	
Published standards	76[66]
Standards under development	83[66]

Involvement of Luxembourg

Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of ITU-T/SG 13.

Comments

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

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

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

[66] For the study period 2017-2020 (accessed 09.2019)

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[67]. 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 an "interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning"[68]. Another definition that emerged in the ITU-T community says that[69]: "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[70]. 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[71] 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

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

[68] ISO/IEC 2382:2015, Information technology -- Vocabulary (def. 2123769)

[69] 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

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

[71] 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

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 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[72]

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"[73].

The definition of Big Data by ISO/IEC[74] specifies it as follows:

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

Big Data is a topic that has attracted a great deal of attention from industry, governments and academia in recent years. The term Big Data was coined in 1997 to refer to large volumes of scientific data for visualization[75]. 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[75]. 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[76]. This additional V in combination with the original 3Vs will be used in this standards analysis to refer to the characteristics of Big Data, which are depicted and described in Table 6 and Figure 3 respectively.

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.

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

[73] 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.

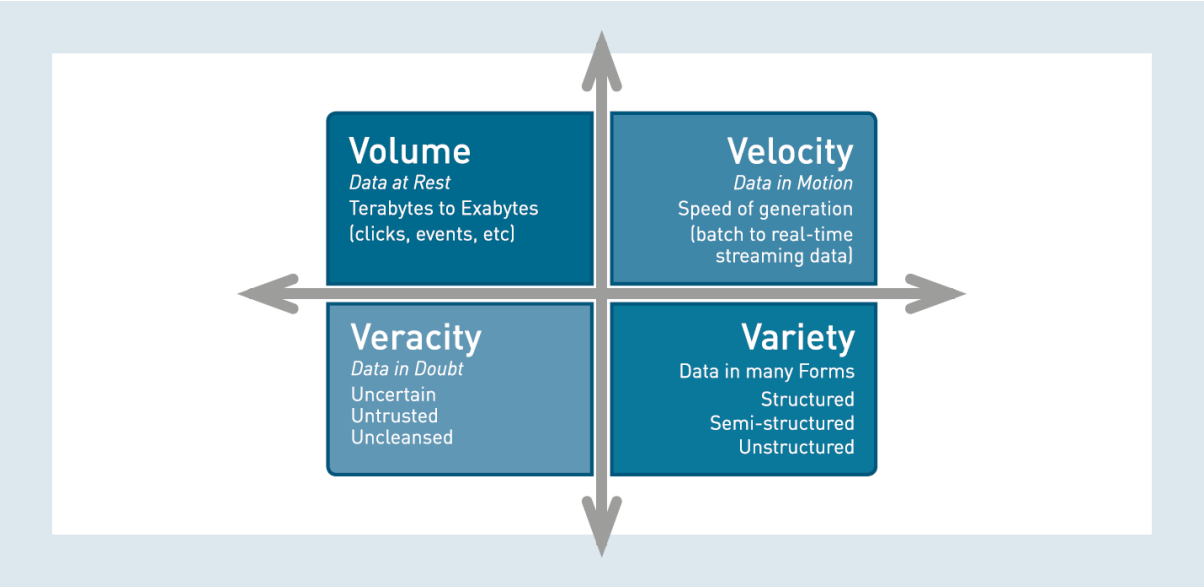
[74] ISO/IEC 20546:2019, Information technology -- Big data -- Overview and vocabulary

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

[76] 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[77]:

- **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.

[77] 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[78].

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

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td>Committee</td><td>ISO/IEC JTC 1/SC 42</td><td>Title</td><td>Artificial Intelligence</td></tr>
<tr><td>Creation date</td><td>2017</td><td rowspan="5">MEMBERS
  </td><td rowspan="5">Participating Countries (29):
United States, Australia, Austria, Belgium, Benin, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Republic of Korea, Luxembourg, Malta, Netherlands, Norway, Russian Federation, Singapore, Spain, Sweden, Switzerland, Uganda, United Kingdom

Observing Countries (12):
Argentina, Cyprus, Hungary, Lithuania, Mexico, New Zealand, Philippines, Poland, Portugal, Romania, South Africa, Ukraine</td></tr>
<tr><td>Secretariat</td><td>ANSI (USA)</td></tr>
<tr><td>Committee Manager</td><td>Ms. Heather Benko</td></tr>
<tr><td>Chairperson</td><td>Mr. Wael William Diab</td></tr>
<tr><td>Organizations in liaison</td><td>BDVA, Consumers International, IEEE, OGC</td></tr>
<tr><td>Web site</td><td colspan="3">https://www.iso.org/committee/6794475.html</td></tr>
<tr><td>Scope</td><td colspan="3">Standardization in the area of Artificial Intelligence Specifically:
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.</td></tr>
<tr><td>Structure</td><td colspan="3">JTC 1/SC 42/AHG 1 Dissemination and outreach
JTC 1/SC 42/AHG 2 Liaison with SC 38
JTC 1/SC 42/AHG 3 Intelligent systems engineering
JTC 1/SC 42/JWG 1 Joint Working Group ISO/IEC JTC1/SC 42 - ISO/IEC JTC1/SC 40: Governance implications of AI
JTC 1/SC 42/WG 1 Foundational standards
JTC 1/SC 42/WG 2 Big Data
JTC 1/SC 42/WG 3 Trustworthiness
JTC 1/SC 42/WG 4 Use cases and applications
JTC 1/SC 42/WG 5 Computational approaches and computational characteristics of AI systems</td></tr>
</table>

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

Standardization work	
Published standards	3
Standards under development	13

Involvement of Luxembourg

23 delegates

- Mrs. Natalia Cassagnes (Chairwoman)	ANEC G.I.E.
- Mr. Johann Amsenga	INCERT GIE
- Mr. Matthias Brust	University of Luxembourg
- Mr. Vincent Cady	Tarkett S.A.
- Mr. Cyril Cassagnes	University of Luxembourg
- Mr. Boonyarit Changaival	University of Luxembourg
- Mrs. Anna Curridori	CSSF
- Mr. Christophe Delogne	Everis Spain SLU
- Mrs. Saharnaz Dilmaghani	University of Luxembourg
- Mr. Redouane El Ajjouri	KPMG Luxembourg S.C.
- Mr. Laurent Fisch	Laurent Fisch Luxlegal S.à r.l.
- Mr. Philippe Germain	PmG SD S.àr.l.
- Mrs. Andra Giurgiu	University of Luxembourg
- Mr. David Hagen	CSSF
- Mr. Andreas Kremer	ITTM
- Mr. Johnatan Pecero	ANEC G.I.E.
- Mr. Benoit Poletti	INCERT GIE
- Mr. Cyril Rousseau	CORAX IP S.à.r.l.
- Mr. Mark Scheerlinck	MCS S.à.r.l.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology
- Mrs. Emilia Tantar	INCERT GIE
- Mr. Shyam Wagle	ANEC G.I.E.
- Mr. Muhammad Wasim	University of Luxembourg

Comments

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

There are currently 13 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 WD 22989, Artificial Intelligence -- Concepts and Terminology;
- ISO/IEC WD 23053, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML);
- ISO/IEC AWI 23894, Information Technology -- Artificial Intelligence -- Risk Management;
- ISO/IEC NP TR 24027, Information technology -- Artificial Intelligence (AI) -- Bias in AI systems and AI aided decision making;
- ISO/IEC PDTR 24028, Information technology -- Artificial Intelligence (AI) -- Overview of trustworthiness in Artificial Intelligence;
- ISO/IEC NP TR 24029-1, Artificial Intelligence (AI) -- Assessment of the robustness of neural networks - Part 1: Overview;
- ISO/IEC NP TR 24030, Information technology -- Artificial Intelligence (AI) -- Use cases;
- ISO/IEC AWI TR 24368, Information technology -- Artificial Intelligence (AI) -- Overview of ethical and societal concerns;
- ISO/IEC AWI TR 24372, Information technology -- Artificial Intelligence (AI) -- Overview of computational approaches for AI systems;

- ISO/IEC AWI 24668, Information technology -- Artificial intelligence --Process management framework for Big data analytics;
- ISO/IEC AWI 38507, Information technology -- Governance of IT -- Governance implications of the use of AI by organizations.

The committee also counts 3 published standards, resulted from the work of former ISO/IEC JTC 1/WG 9 Big Data:

- ISO/IEC 20547-2:2018, Information technology -- Big data reference architecture -- Part 2: Use cases and derived requirements;
- ISO/IEC 20547-5:2018, Information technology -- Big data reference architecture -- Part 5: Standards roadmap;
- ISO/IEC 20546:2019, Information technology -- Big data -- Overview and vocabulary.

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 (16):** United States, Canada, China, Czech Republic, Denmark, Finland, Germany, India, Italy, Japan, Kazakhstan, Republic of Korea, Netherlands, Russian Federation, Sweden, United Kingdom **Observing Countries (24):** Argentina, Austria, Belgium, Bosnia and Herzegovina, Côte d'Ivoire, Egypt, France, Ghana, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, **Luxembourg**, Republic of Moldova, Poland, Portugal, Romania, Serbia, Spain, Switzerland, Turkey, Ukraine
Secretariat	ANSI (USA)		
Committee Manager	Mr. Bill Ash		
Chairperson	Mr. Jim Melton		
Organizations in liaison	Infoterm, UNECE, IEEE, 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/WG 1 eBusiness JTC 1/SC 32/WG 2 MetaData JTC 1/SC 32/WG 3 Database language		
Standardization work			
Published standards	86		
Standards under development	40		
Involvement of Luxembourg			
2 delegates - Mrs. Natalia Cassagnes ANEC G.I.E. - 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;
- ISO/IEC 19075-8:2019, Information technology database languages -- SQL technical reports -- Part 8: Multi-dimensional arrays (SQL/MDA);
- ISO/IEC 15944-8:2012, Information technology -- Business operational view -- Part 8: Identification of privacy protection requirements as external constraints on business transactions (under revision);
- ISO/IEC 15944-9:2015, Information technology -- Business operational view -- Part 9: Business transaction traceability framework for commitment exchange (under revision).

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

- The revision of different parts in the ISO/IEC 9075 series of standards concerning the SQL database language;
- 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 big data quality and next generation analytics appear frequently both in computing industry and more general news reports. SC 32 follows the development of standardization activities in these domains, namely through the liaison with SC 42. In its turn, the work of SC 32 on metadata for data quality and top-level ontologies is followed by SC 42 since it relates to various types of AI systems.

3.3.3.3. ITU-T/SG 16

General information			
Committee	**ITU-T/SG 16**	**Title**	**Multimedia coding, systems and applications**
Creation date	N/A	**MEMBERS** 	N/A
Chairperson	Mr. Noah Luo		
Organizations in liaison	CITS, GSMA, IEC/TC 100, W3C, APT, CENELEC TC108X, DAISY, ETSI, IETF, ISO/TC 215, ISO/IEC JTC 1		
Web site	https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/default.aspx		
Scope	Study Group 16 is responsible for studies relating to ubiquitous multimedia applications, multimedia capabilities for services and applications for existing and future networks. This encompasses accessibility; multimedia architectures and applications; human interfaces and services; terminals; protocols; signal processing; media coding and systems (e.g. network signal processing equipment, multipoint conference units, gateways and gatekeepers). Lead Study Group Roles: - multimedia coding, systems and applications; - ubiquitous multimedia applications; - telecommunication/ICT accessibility for persons with disabilities; - human factors; - multimedia aspects of intelligent transport system (ITS) communications; - Internet Protocol television (IPTV) and digital signage; - multimedia aspects of e-services.		
Structure	WP1/Q11 Multimedia systems, terminals, gateways and data conferencing WP1/Q12 Visual surveillance systems and services WP1/Q13 Multimedia application platforms and end systems for IPTV WP1/Q14 Digital signage systems and services WP1/Q21 Multimedia framework, applications and services WP2/Q22 Distributed ledger technologies and e-services WP2/Q24 Human factors related issues for improvement of the quality of life through international telecommunications WP2/Q26 Accessibility to multimedia systems and services WP2/Q27 Vehicle gateway platform for telecommunication/ITS services and applications WP2/Q28 Multimedia framework for e-health applications WP3/Q5 Artificial intelligence-enabled multimedia applications WP3/Q6 Visual coding WP3/Q7 Speech/audio coding, voiceband modems, facsimile terminals and network-based signal processing WP3/Q8 Immersive live experience systems and services **Other groups under SG16**: JCA-MMeS Joint Coordination Activity on Multimedia aspects of E-services FG AI4H ITU-T Focus Group on Artificial Intelligence for Health IRG-AVA ITU Intersector Rapporteur Group on Audiovisual Media Accessibility IRG-IBB ITU Intersector Rapporteur Group on Integrated Broadcast-Broadband (IBB)		

Standardization work	
Published standards	156[79]
Standards under development	127[79]

Involvement of Luxembourg

Note: ILNAS, with the support of ANEC G.I.E is monitoring the standardization developments of the ITU-T/SG 16.

Comments

The objective of this SG 16 is to work on multimedia coding, systems and applications. With big data and artificial intelligence playing more and more important role in the area of multimedia, some of the projects under SG 16 are exploiting the use of the technologies for the domain:

- ITU-T F.743.7 (05/2019), Requirements for big data application in visual surveillance system (published);
- ITU-T F.AFBDI, Assessment framework for big data infrastructure (ongoing);
- ITU-T H.VSBD, Architecture for Big Data Application in Visual Surveillance System (ongoing);
- ITU-T H.CUAV-AIF, Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence (ongoing);
- ITU-T F.VS-AIMC, Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence (ongoing).

On the other hand, analyzing multimedia data and providing valuable applications in different application domains is in scope of SG 16 through the WP3/Q5 “Artificial intelligence-enabled multimedia applications”. In this context, the focus group FG AI4H[80], for health applications, was established under SG 16 in July 2018. The objective of the focus group is to establish a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.

[79] For the study period 2017-2020 (accessed 09.2019)

[80] https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx (accessed 09.2019)

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 Distributed Ledger Technologies (DLT) [81] 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.

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

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 ISO/TC 307, the Blockchain and Distributed Ledger Technologies related technical committee currently active in the recognized standardization organizations.

In addition to this technical committee, it has to be noted that ITU-T formed a Focus Group on DLT which concluded its work in August 2019, with the publication of 3 Technical Specifications and 5 Technical Reports[82] covering various aspects of DLT (e.g.: terms and definitions, use cases, reference architecture, etc.).

CEN-CENELEC also established a focus group on Blockchain and DLT in 2017, with the aim to identify specific European needs with special attention given to interoperability challenges and to contribute directly to the International technical standardization through ISO/TC 307. The Focus Group notably

[82] These reports are available on https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx (accessed 09.2019)

published a White Paper in 2018, formalizing these specific requirements for the implementation of blockchain and DLT in Europe[83].

3.4.2.1. ISO/TC 307

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td>Committee</td><td>ISO/TC 307</td><td>Title</td><td>Blockchain and distributed ledger technologies</td></tr>
<tr><td>Creation date</td><td>2016</td><td rowspan="5">MEMBERS
  </td><td rowspan="5">Participating Countries (43):
Australia, Austria, Belgium, Brazil, Cambodia, Canada, China, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Kazakhstan, Republic of Korea, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States

Observing Countries (12):
Argentina, Belarus, Estonia, Hong Kong, Indonesia, Islamic Republic of Iran, Kenya, Morocco, Philippines, Romania, Slovakia, Uruguay</td></tr>
<tr><td>Secretariat</td><td>SA (Australia)</td></tr>
<tr><td>Committee Manager</td><td>Ms. Emily Dawson</td></tr>
<tr><td>Chairperson</td><td>Mr. Craig Dunn</td></tr>
<tr><td>Organizations in liaison</td><td>EC, EEA Inc., FIG, IEEE, ITU, OECD, SBS, SWIFT, UNECE</td></tr>
<tr><td>Web site</td><td colspan="3">https://www.iso.org/committee/6266604.html</td></tr>
<tr><td>Scope</td><td colspan="3">Standardization of blockchain technologies and distributed ledger technologies.</td></tr>
<tr><td>Structure</td><td colspan="3">TC 307/AG 1 SBP Review Advisory Group
TC 307/AHG 1 Liaison Review Ad Hoc Group
TC 307/CAG 1 Convenors coordination group
TC 307/JWG 4 Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
TC 307/SG 7 Interoperability of blockchain and distributed ledger technology systems
TC 307/WG 1 Foundations
TC 307/WG 2 Security, privacy and identity
TC 307/WG 3 Smart contracts and their application
TC 307/WG 5 Governance
TC 307/WG 6 Use cases</td></tr>
<tr><th colspan="4">Standardization work</th></tr>
<tr><td>Published standards</td><td colspan="3">0</td></tr>
<tr><td>Standards under development</td><td colspan="3">11</td></tr>
</table>

[83] The White Paper "Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies" is available on ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf (accessed 09.2019)

Involvement of Luxembourg

21 delegates

- Mr. Jean Lancrenon (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. Jeff Braun	LetzBlock A.s.b.l.
- Mr. Cyril Cassagnes	University of Luxembourg
- Mr. Guillaume De Vergnies	STAMPIFY S.à.r.l.
- Mr. Christophe Delogne	Everis Spain SLU
- Mrs. Caline Djiowa	KPMG Luxembourg S.C.
- Mr. Sami El Bouamri	Initio Luxembourg S.A.
- Mrs. Michèle Feltz	ILNAS
- Mr. Antoine Gaury	Etix Everywhere S.A.
- Mr. Philippe Germain	PmG SD S.à r.l.
- Mrs. Biba Homsy	LetzBlock A.s.b.l.
- Mr. Ravi Jhawar	PwC
- Mr. Bernard Legros	ARHS Developments S.A.
- Mr. Johnatan Pecero	ANEC G.I.E.
- Mr. Cyrille Rousseau	CORAX IP S.à.r.l.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology (LIST)
- Mr. Sebastien Varrette	University of Luxembourg
- Mr. Povilas Zinys	LuxTrust S.A.

Comments

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

This technical committee is responsible for standardization relating blockchain and DLT. This includes standards in relation to terminology, reference architecture, security, privacy, identity, smart contracts, governance and interoperability.

Following projects are under the direct responsibility of ISO/TC 307:

- ISO/DIS 22739, Blockchain and distributed ledger technologies -- Terminology;
- ISO/DTR 23244, Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations;
- ISO/DTR 23245, Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities;
- ISO/NP TR 23246, Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies;
- ISO/CD 23257, Blockchain and distributed ledger technologies -- Reference architecture;
- ISO/WD TS 23258, Blockchain and distributed ledger technologies -- Taxonomy and Ontology;
- ISO/PRF TS 23259, Blockchain and distributed ledger technologies -- Legally binding smart contracts;
- ISO/DTR 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 management of digital asset custodians;
- ISO/NP TR 23578, Blockchain and distributed ledger technologies -- Discovery issues related to interoperability;
- ISO/NP TS 23635, Blockchain and distributed ledger technologies -- Guidelines for governance.

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[84] 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[85]. 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[86]. 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[87]. In a study about privacy behaviors regarding information technology, Acquisti *et al.*[88] *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[89] and if other individuals have already agreed to share the information[90]. 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

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

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

[86] 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.

[87] 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.

[88] 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.

[89] 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.

[90] 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[91] 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[92]. 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[93]. 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.

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

[92] 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.

[93] 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 Related Technical Committees

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

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td>Committee</td><td>ISO/IEC JTC 1/SC 17</td><td>Title</td><td>Cards and security devices for personal identification</td></tr>
<tr><td>Creation date</td><td>1987</td><td rowspan="5">MEMBERS
  </td><td rowspan="5">Participating Countries (31):
United Kingdom, 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 (24):
Argentina, Armenia, Belarus, Bosnia and Herzegovina, Croatia, Ghana, Hong Kong, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Kazakhstan, Lithuania, Republic of Moldova, New Zealand, North Macedonia, Norway, Portugal, Serbia, Thailand, Turkey, Ukraine, Viet Nam</td></tr>
<tr><td>Secretariat</td><td>BSI (United Kingdom)</td></tr>
<tr><td>Committee Manager</td><td>Ms. Jean Stride</td></tr>
<tr><td>Chairperson</td><td>Dr. Peter Waggett</td></tr>
<tr><td>Organizations in liaison</td><td>AMEX, Ecma International, Global Platform, IATA, ICAO, ICMA, MasterCard Int., SBS, VISA, ETSI, EUDCA, JAVA CARD FORUM, NFC Forum, UNECE, , Wi-Fi Alliance</td></tr>
<tr><td>Web site</td><td colspan="3">https://www.iso.org/committee/45144.html</td></tr>
<tr><td>Scope</td><td colspan="3">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.</td></tr>
<tr><td>Structure</td><td colspan="3">JTC 1/SC 17/CAG 1 Chairman advisory group
JTC 1/SC 17/SG 2 Virtual ID and related technologies
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 Generic interfaces and protocols for security devices
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</td></tr>
</table>

Standardization work	
Published standards	110
Standards under development	37

Involvement of Luxembourg

2 delegates

- Mr. Benoit Poletti (Chairman) INCERT GIE
- Mr. Abdelkrim Nehari INCERT GIE

Comments

ISO/IEC JTC 1/SC 17 is responsible for the development of standards that are ubiquitous in their use by the sectors that require identification worldwide.

Current work program of JTC 1/SC 17 includes, 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;
- The development of the ISO/IEC 22460 multi-part standard on ISO license and drone identity module for drone (Ultra light vehicle or unmanned aircraft system).

JTC 1/SC 17 has also planned on the revision of the ISO/IEC 7501 series of standards transposing ICAO document on Machine Readable Travel Documents.

3.5.2.2. ISO/IEC JTC 1/SC 27

<table>
<tr><th colspan="4">General information</th></tr>
<tr><td>Committee</td><td>ISO/IEC JTC 1/SC 27</td><td>Title</td><td>Information Security, cybersecurity and privacy protection</td></tr>
<tr><td>Creation date</td><td>1989</td><td rowspan="5">MEMBERS
  </td><td rowspan="5">Participating Countries (48):
Germany, Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Cyprus, Denmark, Finland, France, India, Indonesia, Islamic Republic of Iran, Ireland, Israel, Italy, Japan, Republic of Korea, Lebanon, Luxembourg, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Poland, Romania, Russian Federation, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay

Observing Countries (30):
Belarus, Bosnia and Herzegovina, Bulgaria, Chile, Côte d’Ivoire, Czech Republic, El Salvador, Estonia, Eswatini, Ghana, Hong Kong, Hungary, Iceland, Kazakhstan, Kenya, Lithuania, Morocco, North Macedonia, Pakistan, State of Palestine, Philippines, Portugal, Rwanda, Saudi Arabia, Senegal, Serbia, Slovenia, Thailand, Trinidad and Tobago, Turkey</td></tr>
<tr><td>Secretariat</td><td>DIN (Germany)</td></tr>
<tr><td>Committee Manager</td><td>Ms. Krystyna Passia</td></tr>
<tr><td>Chairperson</td><td>Dr. Andreas Wolf</td></tr>
<tr><td>Organizations in liaison</td><td>(ISC)2, CalConnect, CCETT, CSA, ECBS, Ecma International, ENISA, EPC, ETSI, Global Platform, IEEE, ISACA, ISSEA, ITU, MasterCard Int., SBS, ABC4Trust, Article 29 Data Protection Working Party, CCDB, CCUF, CREDENTIAL, CSCC, Cyber Security, EUDCA, EuroCloud, FIDO Alliance, FIRST, IFAA, INLAC, Interpol, ISA – Automation, ISCI, ISF, Kantara Initiative, OASIS-PMRM, OECD, OIDF, Opengroup – United Kingdom, PICOS, PQCRYPTO, PRIPARE, PRISMACLOUD, SAFECode, SAFEcrypto, TAS3, TCG, TMForum, TREsPASS, WITDOM</td></tr>
<tr><td>Web site</td><td colspan="3">https://www.iso.org/committee/45306.html</td></tr>
<tr><td>Scope</td><td colspan="3">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.</td></tr>
</table>

Structure	JTC 1/SC 27/AG 1	Management Advisory Group
	JTC 1/SC 27/SG 1	Data Security
	JTC 1/SC 27/SG 2	Trustworthiness
	JTC 1/SC 27/SG 3	Concepts and Terminology
	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	184
Standards under development	80

Involvement of Luxembourg

27 delegates

- Mr. Benoit Poletti (Chairman)	INCERT GIE
- Mr. Carlo Harpes (Vice-Chairman)	itrust consulting S.à r.l.
- Mr. Johann Amsenga (Convenor WG 4)	INCERT GIE
- Mr. Matthieu Aubigny	itrust consulting S.à r.l.
- Mr. Benoit Bertholon	COINPLUS S.A.
- 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. Michèle Feltz	ILNAS
- Mr. Ben Fetler	CTIE
- Mr. Philippe Germain	PmG SD S.à r.l.
- Mr. Clement Gorlt	INCERT GIE
- Mrs. Carine Grenouillet	INCERT GIE
- Mrs. Shenglan Hu	POST Telecom PSF S.A.
- Mr. Ravi Jhawar	PwC
- Mr. Jean Lancrenon	ANEC G.I.E.
- Mr. Chao Liu	University of Luxembourg
- Mr. Michel Ludwig	ILNAS
- Mr. Alex Mckinnon	SES S.A.
- Mr. Gaëtan Pradel	INCERT GIE
- Mr. René Saint-Germain	Certi-Trust S.àr.l.
- Mr. Nader Samir Labib	University of Luxembourg
- Mr. Raphaël Taban	CTIE
- Mr. Qiang Tang	University of Luxembourg
- Mr. Muhammad Wasim	University of Luxembourg

Comments

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

Working Groups

- **WG 1**: the scope of the WG 1 covers all aspects of standardization related to information security management systems: requirements, methods and processes, security controls, sector and application specific use of ISMS, governance, information security economics and accreditation, certification and auditing of ISMS.

- **WG 2**: the scope of the WG 2 covers both cryptographic and non-cryptographic techniques and mechanisms including confidentiality, entity authentication, non-repudiation, key management and data integrity (e.g.: message authentication, hash-functions, digital signatures, etc.).
- **WG 3**: the scope of the WG 3 covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished: security evaluation criteria, methodology for application of the criteria, security functional and assurance specification of IT systems, components and products, testing methodology for determination of security functional and assurance conformance, accreditation schemes, administrative procedures for testing, evaluation and certification.
- **WG 4**: it is developing and maintaining International Standards, Technical Specifications and Technical Reports for information security in the area of Security Controls and Services, to assist organizations in the implementation of the ISO/IEC 27000-series of ISMS International Standards and Technical Reports. Also the Scope of WG 4 includes evaluating and developing International Standards for addressing existing and emerging information security issues and needs and other security aspects that resulted from the proliferation and use of ICT and Internet related technology in organizations (such as multinationals corporations, SMEs, government departments, and non-profit organizations). Since 2018, Luxembourg is managing this WG, Mr. Johann Amsenga being its convenor.
- **WG 5**: it is responsible of the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and privacy.

Standards

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

It is important to note that the committee works in liaison with many other JTC 1/SCs on the development of standards related to security for specific subsectors. For example, standards concerning the security techniques for IoT and Smart Cities are currently under development under SC 27 in close collaboration with ISO/IEC JTC 1/SC 41 and ISO/IEC JTC 1/WG 11:

- ISO/IEC WD 27030, Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT);
- ISO/IEC PDTS 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 regarding security and privacy aspects in cloud SLAs (in liaison with ISO/IEC JTC 1/SC 38):

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

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

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

3.5.2.3. ISO/TC 46/SC 11

General information			
Committee	**ISO/TC 46/SC 11**	**Title**	**Archives/records management**
Creation date	1998	**MEMBERS** 	**Participating Countries (35):** Australia, Belgium, Brazil, 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, Sri Lanka, Sweden, Switzerland, Ukraine, United Kingdom, United States **Observing Countries (15):** Argentina, Austria, Chile, Croatia, Cuba, Iceland, Islamic Republic of Iran, **Luxembourg**, Poland, Romania, Serbia, Singapore, Slovakia, Slovenia, Thailand
Secretariat	SA (Australia)		
Committee Manager	Mr. Saim Riaz		
Chairperson	Ms. Judith Ellis		
Organizations in liaison	ICA, InterPARES, IRMT, ITU		
Web site	https://www.iso.org/committee/48856.html		
Scope	Standardization of principles for the creation and management of documents, records and archives as evidence of transactions and covering all media including digital multimedia and paper.		
Structure	TC 46/SC 11/AG 1 Strategic directions TC 46/SC 11/AHG Strategic Directions TC 46/SC 11/AHG 2 Disposition TC 46/SC 11/AHG 3 Structured data environments TC 46/SC 11/AHG 4 Records capability maturity TC 46/SC 11/JWG 1 Joint ISO/TC 46/SC 11 - ISO/TC 307 WG: Blockchain TC 46/SC 11/WG 1 Metadata TC 46/SC 11/WG 8 Management systems for 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		
Standardization work			
Published standards	19		
Standards under development	6		
Involvement of Luxembourg			
8 delegates - Mr. Lucas Colet (Chairman) SOPRA STERIA PSF Luxembourg S.A. - Mrs. Sylvie Dessolin SOPRA STERIA PSF Luxembourg S.A. - Mrs. Sylvie Forastier Linklaters LLP - Mr. Michel Ludwig ILNAS - Mr. Henri Montin CTIE - Mr. Michel Picard Luxembourg Institute of Science and Technology (LIST) - Mr. Serge Raucq CTIE - Mr. Alain Wahl ILNAS			

Comments
ISO/TC 46/SC 11 is responsible for the standardization of the best practices in managing archives and records by providing a managerial framework, as well as standards and guidance for the design and application of records practices and processes to ensure authoritative and reliable information and evidence of business activity in organizations. ISO/TC 46/SC 11 is currently developing six 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	/		
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	3		
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'. 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 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. Moreover, two dedicated technical reports for the biometric access and Video surveillance were initiated. Recently, the committee discussed the need for a standard that would define the requirements related to the professional activity in the field of processing and protecting of personal data. The decision to develop such a standard is subject to the outcomes of a ballot in progress. As of September 2018 it was agreed to concentrate the privacy-related standardization activities in another committee, which will be CEN/CLC/JTC 13/WG 5 (see 3.5.2.5 for more information). Thus, after the approval by CEN-CENELEC BT, the CEN/CLC/JTC 8 will be disbanded and its program of work transferred to CEN/CLC/JTC 13/WG 5.			

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	ENISA; SHiELD Project		
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	19		
Involvement of Luxembourg			
1 delegate - Mr. Jean Lancrenon ANEC G.I.E.			

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.

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	DTCE, VISA EUROPE		
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	68		
Standards under development	7		
Involvement of Luxembourg			
2 delegates - Mr. Benoit Poletti (Chairman) INCERT GIE - Mrs. Shenglan Hu POST Telecom PSF			

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

3.5.2.7. ETSI/TC CYBER

General information			
Committee	**ETSI/TC CYBER**	**Title**	**Cyber Security**
Creation date	2014	**MEMBERS** 	162 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 - Provision of security mechanisms to protect privacy - Creation of security specifications and alignment with work done in other TCs.		
Structure	TC CYBER/WG-QSC Quantum-Safe Cryptography		
Standardization work			
Published standards	38		
Standards under development	23		
Involvement of Luxembourg			
2 organizations - Luxtrust - ILNAS 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 includes 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; - DTS/CYBER-0027-5, CYBER; Middlebox Security Protocol; Part 5: Enterprise Network Security; - DMI/CYBER-0030; ETSI mcTLS protocol demonstration; - DTS/CYBER-0044, CYBER; External encodings for the Advanced Encryption Standard;		

- DTR/CYBER-0045, CYBER; Guide to Identity Based Encryption;
- DMI/CYBER-QSC-0010, CYBER QSC Extended Roadmap; CYBER QSC Extended Roadmap Related Material;
- DTS/CYBER-QSC-0015, CYBER Quantum-Safe Hybrid Key Exchanges;
- 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 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 TS 103 643, CYBER; 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;
- ETSI TS 103 651, CYBER; Critical Security Controls for MSP middlebox defence;
- ETSI EN 303 645, 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 , related services and trust service Infrastructures, to protect electronic transactions and ensure trust and confidence with business partners, including the preparation of reports and other necessary activities, by: - Developing generic standards, guides and reports; - Liaising with other ETSI bodies; - Liaising with bodies external to ETSI; - Establishing a continuing work plan.		
Structure	/		
Standardization work			
Published standards	182		
Standards under development	30		
Involvement of Luxembourg			
4 companies - eWitness S.A. - Luxtrust - Nowina Solutions - POST Luxembourg Note: ILNAS 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 is notably responsible to maintain standards and specifications published in response to European Commission (EC) Mandate M/460 on Electronic Signature Standardization.

3.6. Fora and Consortia Related to Digital Trust

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

In connection with the "National Cybersecurity Strategy III", a list of relevant Fora and Consortia working in the Digital Trust area (and notably in relation with Smart ICT technologies) is provided in this section. This information intends to help national stakeholders to identify, in addition to the standardization technical committees described in Section 3.5.2, organizations that can be relevant to their needs in the Digital Trust area.

In addition to this list, national stakeholders can refer to the ETSI Technical Report 103 306 "CYBER; Global Cyber Security Ecosystem"[94], which provides the global cybersecurity ecosystem and notably specifies the relevant organizations of the cybersecurity ecosystem at national level.

3.6.1. 3GPP - 3rd Generation Partnership Project

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

3.6.2. BSI - Bundesamt für Sicherheit in der Informationstechnik

	BSI	Bundesamt für Sicherheit in der Informationstechnik
Scope	The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry.	

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

Activities	Standards Development, Education, Certification, Research
Topics	Cybersecurity, Cryptography, Critical Infrastructure Protection, Secure Electronic Identities, Security in Digitalization, Incident Response
Website	https://www.bsi.bund.de

3.6.3. CSA - Cloud Security Alliance

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

3.6.4. EC-Council - International Council of E-Commerce Consultants

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

3.6.5. EuroCloud

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

3.6.6. GIAC - Global Information Assurance Certification

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

3.6.7. IEEE SA - Institute for Electrical and Electronic Engineers Standards Association

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

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

3.6.8. IETF - Internet Engineering Task Force

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

3.6.9. GSMA - GSM Association

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

3.6.10. IIC - Industrial Internet Consortium

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

3.6.11. ISACA - Information Systems Audit and Control Association

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

3.6.12. (ISC)^2 - International Information System Security Certification Consortium

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

3.6.13. ISECOM - Institute for Security and Open Methodologies

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

3.6.14. NIST - National Institute of Standards and Technology

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

3.6.15. OASIS - Organization for the Advancement of Structured Information Standards

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

3.6.16. OCF - Open Connectivity Foundation

	OCF	Open Connectivity Foundation
Scope	OCF's Mission is Twofold: - Provide specifications, code and a certification program to enable manufacturers to bring OCF Certified products to the market that can interoperate with current IoT devices and legacy systems. - Make the end user's experience better by seamlessly bridging to other ecosystems within a user's smart home and ensure interoperability with OCF compliant devices.	
Activities	Standards Development, Certification	
Topics	IoT	
Website	https://openconnectivity.org	

3.6.17. OMG - Object Management Group

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

3.6.18. oneM2M

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

3.6.19. OWASP - The Open Web Application Security Project

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

3.6.20. PCI-SSC - PCI Security Standards Council

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

3.6.21. SNIA - Storage Networking Industry Association

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

3.6.22. TCG - Trusted Computing Group

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

3.6.23. W3C - World Wide Web Consortium

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

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. The purpose of this Standards Analysis "Smart Secure ICT Luxembourg" is to encourage the participation of national stakeholders in technical standardization. It will directly contribute to support and stimulate the ICT sector in terms of competitiveness, visibility and performance. Many national organizations are now engaged on the path of Smart ICT technical standardization, which offers them unique opportunities to participate in the process and helps in designing the future global Smart Secure ICT landscape. In particular, this chapter provides an overview of ILNAS developments aiming at facilitating the involvement of stakeholders in the technical standardization process, for the benefit of the national Economy.

The ICT sector is, at a national level, the most active standardization sector. Luxembourg is a "P-member"[95] of ISO/IEC JTC 1 and represents national interests in its plenary meetings. As mentioned earlier 91 delegates[96] from the country are currently involved in international and European technical standardization committees. Among them, 74 are involved in Smart ICT and Digital Trust related technical committees, such as Internet of Things: 18; Cloud Computing: 15; Artificial Intelligence: 23; Blockchain: 22, Digital Trust: 38. However, considering the rich and vibrant ecosystem of organizations involved in the ICT sector in Luxembourg, ILNAS believes that active technical committees in Smart ICT standardization could still attract more national stakeholders and make them benefit from related opportunities of technical standardization. In this way, ILNAS, with the support of ANEC G.I.E., is following closely Smart ICT related technical committees in order to provide the most relevant information to the national ICT community. Moreover, ANEC G.I.E. standardization officers are managing, as national chairpersons, the technical committees listed below to facilitate the involvement of national stakeholders in the technical committees and represent the interests of the Grand Duchy of Luxembourg in the international plenary meetings[97].

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

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

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

[95] 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)

[96] Some experts are participating in more than one technical committee.

[97] More information on: https://portail-qualite.public.lu/fr/normes-normalisation/secteurs/tic.html

with ANEC G.I.E., workshops in the framework of ICT prospective and, more specifically in the “Smart Secure ICT” domain.

For instance, breakfasts dedicated to the promotion of Smart Secure ICT standardization were organized in 2018 and 2019 in order to discuss Smart ICT and widespread use of such technologies in a secure way. Beyond the technical aspects, latest related standardization developments were presented to highlight their importance for the establishment of a trusted digital environment. These breakfasts reviewed various Smart ICT technologies, focusing mainly on Cloud Computing, Internet of Things, Artificial Intelligence, and Blockchain. They were organized to bring together national stakeholders of dedicated Smart ICT subsectors and to provide them with the relevant standardization knowledge and facilitate their engagement in the standards development process. In this manner, ILNAS organizes information sessions dedicated to technical standardization of a specific Smart ICT subsector, on a regular basis[98]. Similarly, in 2018, ILNAS, with the support of ANEC G.I.E., published two White Papers dedicated to Blockchain[99] and to Internet of Things[100], in order to make national stakeholders 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[101] and the IoT White Paper was released during the ILNAS-ETSI Workshop 2018[102].

Moreover, as mentioned in the introduction of this chapter, standardization officers of ANEC G.I.E. are chairing, in support of ILNAS, the National Mirror Committees (NMCs) that gather national experts dedicated to Smart ICT (IoT, Cloud Computing, Artificial Intelligence, and Blockchain). This involvement aims at reinforcing Luxembourg’s positioning in these areas and NMC meetings are regularly organized to allow interested national stakeholders to strengthen their commitment into the process of technical standardization (interested people who are not already delegates of technical committees can also participate to be informed and analyze the benefits of taking part in the development of standards). In this context, ANEC G.I.E. participated in five international plenary meetings of technical committees in 2018. This participation continues during 2019[103]. In this context, it organized NMC meetings to prepare, debrief and exchange on the topics dealt during these plenary meetings with the 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.

---

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

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

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

101 https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2018/retour-evenement-presentation-white-paper-blockchain-and-distributed-ledgers.html

102 https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2018/workshop-ilnas-etsi-2018-quelles-avancees-pour-la-normalisation-technique-internet-of-things.html

103 Participation in three more plenary meetings is planned in 2019

To facilitate the organization of such awareness, interested stakeholders can fill a declaration of interest in ICT standardization[104] to be contacted by ILNAS and ANEC G.I.E.

4.1.3. Smart ICT Standards Watch

The objective of the Standards Analysis "Smart Secure ICT Luxembourg" is to facilitate the identification of technical committees in the Smart ICT area that meet organizations' potential interests. Moreover, ILNAS, with the support of ANEC G.I.E., can execute, on demand, a focused standards watch to answer the needs of a national 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 Dissemination

ILNAS, with the support of ANEC G.I.E., publishes and disseminates reports and White Papers at the national level in order to provide valuable information on Smart ICT standardization topics to national stakeholders. In addition to the White Papers described below, ILNAS plans to publish two new National Technical Standardization Reports, on Internet of Things and Blockchain, as well as a White Paper on Artificial Intelligence, in 2020.

- **White Paper Internet of Things and Technical Standardization**[105]

ILNAS and ANEC G.I.E. published, with the support of the Ministry of the Economy, a White Paper Internet of Things and Technical Standardization in July 2018. The IoT, a network of connected objects capable of collecting and exchanging data, is one of the most promising concepts emerging from the 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**[106]

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

[104] https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/normes-normalisation/declarations-interet/declaration-interet-normalisation-tic/declaration-interest-standardization-it.pdf
[105] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf
[106] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-blockchain-june-2018.pdf

- **White Paper Digital Trust for Smart ICT** [107]

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

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

- **White Paper Green Computing**[108]

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**[109]

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

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

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

[109] 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

ILNAS offers the free consultation of its entire standards' database (including more than 180 000 normative documents from ILNAS, DIN, CEN, CENELEC, ETSI, ISO and IEC) through reading stations located in six different places in Luxembourg[110]:

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

This service allows, for example, interested organizations or individuals to consult a standard before its purchase. The ILNAS e-Shop[111] 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[112], to reinforce the collaboration of the organizations in the domain of Smart Secure ICT for Business Innovation through Technical Standardization. The research program is intended to analyze and extend standardization and Digital Trust knowledge in three Smart ICT domains, namely Cloud Computing, Internet of Things and Artificial Intelligence/Big Data. In this frame, three PhD students are performing research activities in the above-mentioned Smart ICT domains. The team received the "Security Project of the Year" award during the Information Security Day 2019[113] for the results they already obtained. On the one hand, the results of this research program will support the evolution of the academic program of the Certificate "*Smart ICT for Business Innovation*" (see Section 4.2.2). On the other hand, it will serve as a basis for a future professional Master Program "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*" (expected in 2020).

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

White Paper Data Protection and Privacy in Smart ICT[114]

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

110 https://portail-qualite.public.lu/fr/normes-normalisation/achat-consultation-normes.html
111 https://ilnas.services-publics.lu/
112 https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2017/ul-ilnas-investissent-smart-ict.html
113 https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team
114 https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf

This White Paper has been extended in October 2019 with the publication of three Technical Reports delivering gap analyses between scientific research and technical standardization for the three Smart ICT domains studied in the context of the research program.

4.2. Training in Standardization

4.2.1. Training on Smart ICT Standardization

ILNAS, with the support of ANEC G.I.E., develops a training catalogue[115] annually, which is updated according to market expectations. Since 2018, in addition to general trainings about standards and standardization, technical trainings on Smart ICT standardization and related digital trust challenges are proposed:

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

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

4.2.2. Project of Professional "Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions"

ILNAS, supported by ANEC G.I.E., is collaborating with the University of Luxembourg to develop a professional Master entitled "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*". It is designed for experienced professionals who wish to develop their technological skills in the field of Smart Secure ICT and technopreneurship. It is planned to launch this professional Master in September 2020.

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

This program will provide lectures from three points of views:

- Technical: providing the fundamentals of Smart ICT technologies and security techniques and the latest scientific developments;
- Technopreneurship: in order to highlight major opportunities for technical innovation;
- Technical standardization, which plays a key role, as an important source of knowledge and good practices, while defining the future ICT. Concretely, technical standardization remains a

[115] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2019/Training-Catalogue-ILNAS-ANEC-2019-v16.pdf

main keystone between the Smart ICT technologies, the related digital trust needs, and the development of business innovation, as it points the way forward.

The Master will rely on previous successful projects led by ILNAS in collaboration with the University of Luxembourg, notably the University certificate "*Smart ICT for Business Innovation*"[116], which will be integrated in the future Master program.

4.3. Involvement in Standardization

4.3.1. Becoming a National Delegate in Standardization

4.3.1.1. Benefits of Participation in Smart ICT standardization technical committees

In Luxembourg, registration in technical committees from ISO, IEC, CEN or CENELEC is free of charge[117]. 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;
- Valuing your organization at national and international level;
- Identifying development opportunities;
- Making your organization competitive in the market.

4.3.1.2. Participating in the Training for New delegates in standardization

ILNAS regularly organizes trainings for newcomers in technical standardization[118], who have registered in a technical committee. They are encouraged to participate in order, 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.

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

117 https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html

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

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;
  - Keep informed about the future professional "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*" (forecast in September 2020).

- 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[119].

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

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

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

As described in the national standardization strategy 2014-2020[120], 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, which has high-quality communication infrastructures, hosts several world-leading ICT companies as well as many start-ups[121], and is composed of a market of many companies, associations, administrations, and experts. Luxembourg is also particularly active in creating a secure environment for developing a trusted data-driven economy.

ILNAS, with the support of ANEC G.I.E., is constantly analyzing Smart ICT technical standardization developments and actively supports national stakeholders who want to be involved in this area, according to the "Luxembourg's Policy on ICT technical standardization 2015-2020"[122]. The main objectives of this policy are to foster and strengthen the national ICT sector's involvement in standardization work. To achieve this, ILNAS is conducting three intertwined projects:

a) 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. This Standards Analysis also provides a monitoring of technical committees active in the Digital Trust area, as well as a list of relevant Fora and Consortia working in the cybersecurity domain, to meet the objectives of the "National Cybersecurity

[120] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf
[121] https://www.tradeandinvest.lu/business-sector/ict/
[122] 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

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

Similarly, for the second project, ILNAS, aided by ANEC G.I.E., is offering its support to different industries/organizations through standardization according to the nature of their business at the national level. Smart ICT and/or Digital Trust related technical committees already benefit from a good national representation with 74 national delegates currently registered to participate in one or several of these normative domains (Internet of Things: 18; Cloud Computing: 15; Artificial Intelligence: 23; Blockchain: 22, Digital Trust: 38)[123]. This figure demonstrates the interest of individuals, industries/organizations in technical standardization.

Finally, conforming to the third project, ILNAS, with the support of ANEC G.I.E., has undertaken concrete developments for strengthening education and research activities in the area of technical standardization. It includes the launch of a University certificate dedicated to Smart ICT[124], focusing on 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 CEN-CENELEC, was the first step towards the ambitious project of creating a Master program dedicated to Smart Secure ICT. This professional Master "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*" is forecast to be launched in September 2020. ILNAS and the University of Luxembourg are also implementing a research program[125] 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/Artificial Intelligence. In this context, three PhD students are performing research activities in the above-mentioned Smart ICT domains. As a first result of this collaboration, ILNAS and the University of Luxembourg published a White Paper "Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization"[126] in October 2018. The work performed by the research team was also rewarded with the "Security Project of the Year" award during the Information Security Day 2019[127]. The research results of this program will facilitate the development of the Master.

In parallel, ILNAS, with the support of ANEC G.I.E., has also published White Papers on Smart ICT and Digital Trust, notably on Blockchain and Distributed Ledger Technology[128] and Internet of Things[129] in 2018, aiming at creating awareness and interest concerning relevant standardization developments within the national market. ILNAS is pursuing this research activity with the development of National Technical Standardization Reports on IoT and Blockchain, and of a White Paper on Artificial Intelligence, which are planned to be published in 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 with 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" [130], ILNAS, with the support of ANEC G.I.E., stands ready to encourage and assist each initiative in this process.

---

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

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

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

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

[127] https://wwwfr.uni.lu/snt/news_events/security_project_of_the_year_award_for_snt_team

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

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

[130] 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 20924:2018	Internet of Things (IoT) - Vocabulary
ISO/IEC JTC 1	ISO/IEC 21823-1:2019	Internet of Things (IoT) - Interoperability for IoT systems - Part 1: Framework
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)
ISO/IEC JTC 1	ISO/IEC 14543-3-10:2019	Information technology - Home electronic system (HES) architecture - Part 3-10: Wireless short-packet (WSP) protocol optimised for energy harvesting - Architecture and lower layer protocols
ISO/IEC JTC 1	ISO/IEC 14543-5-12:2019	Information technology – Home electronic system (HES) architecture –Part 5-12: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access test and verification
ETSI	ETSI TR 103 290 V1.1.1 (04/2015)	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
ETSI	ETSI TR 103 375 V1.1.1 (10/2016)	SmartM2M; IoT Standards landscape and future evolutions
ETSI	ETSI TR 103 376 V1.1.1 (10/2016)	SmartM2M; IoT LSP use cases and standards gaps
ETSI	ETSI TR 103 467 V1.1.1 (06/2018)	Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem
ETSI	ETSI TR 103 527 V1.1.1 (07/2018)	SmartM2M; Virtualized IoT Architectures with Cloud Back-ends
ETSI	ETSI TR 103 528 V1.1.1 (08/2018)	SmartM2M; Landscape for open source and standards for cloud native software applicable for a Virtualized IoT service layer
ETSI	ETSI TR 103 529 V1.1.1 (08/2018)	SmartM2M; IoT over Cloud back-ends: A Proof of Concept
ETSI	ETSI TS 118 101 V2.10.0 (10/2016)	oneM2M; Functional Architecture (oneM2M TS-0001 version 2.10.0 Release 2)

SDO	Reference	Title
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 118 108 V1.1.0 (03/2016)	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 1.3.2 Release 1)
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)
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)
ETSI	ETSI GR IP6 008 V1.1.1 (06/2017)	IPv6-based Internet of Things; Deployment of IPv6-based Internet of Things
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 Q.4060 (10/2018)	The structure of the testing of heterogeneous Internet of Things gateways in a laboratory environment
ITU-T	ITU-T Y.4000 / Y.2060 (06/2012)	Overview of Internet of Things

SDO	Reference	Title
ITU-T	ITU-T Y.4003 (06/2018)	Overview of Smart Manufacturing in the context of Industrial 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 (10/2017)	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.4117 (10/2017)	Requirements and capabilities of Internet of Things for support of wearable devices and related services
ITU-T	ITU-T Y.4118 (06/2018)	Internet of Things requirements and technical capabilities for support of accounting and charging
ITU-T	ITU-T Y.4120 (06/2018)	Requirements of Internet of things applications for smart retail stores
ITU-T	ITU-T Y.4121 (06/2018)	Requirements of an Internet of Things enabled network for support of applications for global processes of the Earth
ITU-T	ITU-T Y.4203 (02/2019)	Requirements of things description in the Internet of Things
ITU-T	ITU-T Y.4204 (02/2019)	Accessibility requirements for the Internet of things applications and services
ITU-T	ITU-T Y.4401 / Y.2068 (03/2015)	Functional framework and capabilities of the Internet of Things
ITU-T	ITU-T Y.4416 (06/2018)	Architecture of the Internet of Things based on NGNe
ITU-T	ITU-T Y.4417 (06/2018)	Framework of self-organization network in the IoT environments
ITU-T	ITU-T Y.4418 (06/2018)	Functional architecture of gateway for Internet of things applications
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.4555 (02/2019)	Service Functionalities of Self-quantification over 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 V2.12.1 (04/2019)	oneM2M; Security solutions (oneM2M TS-0003 version 2.12.1 Release 2A)
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
ETSI	ETSI TR 103 533 V1.1.1 (08/2019)	SmartM2M; Security; Standards Landscape and best practices
ETSI	ETSI TR 103 534-1 V1.1.1 (08/2019)	SmartM2M; Teaching material; Part 1: Security
ETSI	ETSI TS 103 645 V1.1.1 (2019-02)	CYBER; Cyber Security for Consumer Internet of Things
ITU-T	ITU-T X.1361 (09/2018)	Security framework for the Internet of things based on the gateway model
ITU-T	ITU-T Y.4806 (11/2017)	Security capabilities supporting safety of the Internet of Things

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 14543-5-102	Information technology -- Home electronic system (HES) architecture -- Part 5-102: Intelligent grouping and resource sharing -- Remote universal management profile
ISO/IEC JTC 1	ISO/IEC DIS 14543-5-101	Information technology -- Home electronic systems (HES) architecture -- Part 5-101:Intelligent grouping and resource sharing remote AV access profile
ISO/IEC JTC 1	ISO/IEC CD 15045-3-1	Information technology — Home Electronic System (HES) gateway — Part 3-1: Introduction to privacy, security, and safety
ISO/IEC JTC 1	ISO/IEC CD 21823-2	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 2: Transport interoperability
ISO/IEC JTC 1	ISO/IEC CD 21823-3	Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 3: Semantic interoperability
ISO/IEC JTC 1	ISO/IEC CD 30161	Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services
ISO/IEC JTC 1	ISO/IEC CD 30162	Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems
ISO/IEC JTC 1	ISO/IEC CD 30163	Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services

SDO	Reference	Title
ISO/IEC JTC 1	ISO/IEC PDTR 30164	Internet of things (IoT) -- Edge Computing
ISO/IEC JTC 1	ISO/IEC CD 30165	Internet of Things (IoT) -- Real-time IoT framework
ISO/IEC JTC 1	ISO/IEC CD 30166	Internet of Things (IoT) – Industrial IoT
ISO/IEC JTC 1	PWI TR JTC1-SC41-1	Internet of Things (IoT) - Underwater Communication Technologies for IoT
ISO/IEC JTC 1	PWI TR JTC1-SC41-2	Internet of Things (IoT) - Guidance on the application of the IoT Reference Architecture to Wearables and Implantables based IoT Systems
ISO/IEC JTC 1	PNW JTC1-SC41-112	Internet of Things (IoT) - Interoperability for Internet of Things Systems –Part 4: Syntactic interoperability
CEN	prEN 17099	Information technology - Fish and fish products - requirements for labelling of distribution units and pallets in the trade of seafood products;
CEN	FprEN 17230	Information technology – RFID in rail.
ETSI	ETSI TS 118 101	oneM2M; Functional Architecture (oneM2M TS-0001 version 3.9.0 Release 3)
ETSI	ETSI TS 118 102	oneM2M Requirements (oneM2M TS-0002 version 3.1.0 Release 3)
ETSI	ETSI TS 118 104	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 3.9.0 Release 3)
ETSI	ETSI TS 118 105	oneM2M; Management Enablement (OMA) (oneM2M TS-0005 version 3.4.0 Release 3)
ETSI	ETSI TS 118 106	oneM2M; Management Enablement (BBF) (oneM2M TS-0006 version 3.6.0 Release 3)
ETSI	ETSI TS 118 107	oneM2M; Service Components (oneM2M TS-0007 version 2.0.2 Release 2A)
ETSI	ETSI TS 118 108	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 3.2.0 Release 3)
ETSI	ETSI TS 118 109	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 3.1.0 Release 3)
ETSI	ETSI TS 118 110	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 3.0.0 Release 3)
ETSI	ETSI TS 118 111	oneM2M; Common Terminology (oneM2M TS-0011 version 3.0.0 Release 3)
ETSI	ETSI TS 118 112	oneM2M; Base Ontology (oneM2M TS-0012 version 3.7.1 Release 3)
ETSI	ETSI TS 118 114	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 3.1.0 Release 3)
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 (oneM2M TS-0017 version 2.1.1 Release 2)
ETSI	ETSI TS 118 118	oneM2M Test Suite Structure and Test Purposes (oneM2M TS-0018 version 2.13.0 Release 2)
ETSI	ETSI TS 118 119	oneM2M Abstract Test Suite and Implementation eXtra Information for Test (oneM2M TS-0019 version 2.3.0 Release 2)

SDO	Reference	Title
ETSI	ETSI TS 118 120	oneM2M; WebSocket Protocol Binding (oneM2M TS-0020 version 2.1.1 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 2.3.0 Release 2A)
ETSI	ETSI TS 118 123	oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023 version 3.7.1 Release 3)
ETSI	ETSI TS 118 124	oneM2M; OIC Interworking (oneM2M TS-0024 version 3.2.0 Release 3)
ETSI	ETSI TS 118 130	oneM2M Ontology based Interworking (oneM2M TS-0030 v3.0.1 Release 3)
ETSI	ETSI TR 118 501	oneM2M; Use Case collection (oneM2M TR-0001 version 2.4.1 Release 2A)
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 Version 2.11.1 Release 2A)
ETSI	ETSI TR 118 513	oneM2M Home Domain Enablement
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 2.5.1 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 E.IoT-NNAI	Internet of Things Naming Numbering Addressing and Identifiers
ITU-T	ITU-T Draft Y.Sup.AI4IoT (ex TR.AI4IoT; Y.AI4SC)	Unlocking Internet of things with artificial intelligence: Where we are and where we could be
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.Accessibility-IoT	Accessibility requirements for the Internet of things applications and services

SDO	Reference	Title
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 Supp-Y.IPv6-IoT	IPv6 Potential for the Internet of Things and Smart Cities
ITU-T	ITU-T Draft X.nb-iot	Security Requirements and Framework for Narrow Band Internet of Things
ITU-T	ITU-T Draft Supp-Y.IoT-Use-Cases	IoT Use Cases

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 WD 30147	Information technology -- Internet of things -- Methodology for trustworthiness of IoT system/service
ISO/IEC JTC 1	ISO/IEC WD 30149	Internet of Things (IoT) -- Trustworthiness framework
ETSI	ETSI TS 118 103	oneM2M; Security solutions (oneM2M TS-0003 version 3.10.0 Release 3)
ETSI	ETSI TS 118 116	oneM2M; Secure Environment Abstraction (oneM2M TS-0016 version 3.0.0 Release 3)
ETSI	ETSI TS 118 129	oneM2M; Security Abstract Test Suite & Implementation eXtra Information for Test
ETSI	ETSI TR 118 508	oneM2M; Security (oneM2M TR-0008 version 2.0.0 Release 2A)
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.1363	Technical framework of personally identifiable information (PII) handling system in Internet of things (IoT) environment
ITU-T	ITU-T Draft X.1364	Security requirements and framework for narrow band Internet of Things (IoT)
ITU-T	ITU-T Draft X.1365	Security methodology for use of identity-based cryptography in support of IoT services over telecom networks
ITU-T	ITU-T Draft X.iotsec-4	Security requirements for IoT devices and gateway
ITU-T	ITU-T Draft X.sc-iot	Security controls for Internet of Things (IoT) systems
ITU-T	ITU-T Draft X.secup-iot	Secure software update for IoT devices
ITU-T	ITU-T Draft X.ssp-iot	Security requirements and framework for IoT service platform

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 19086-2:2018	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model
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
ISO/IEC JTC 1	ISO/IEC TR 22678:2019	Information technology -- Cloud computing – Guidance for policy development
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

SDO	Reference	Title
ETSI	ETSI GS/NFV-EVE011 V3.1.1 (2018-10)	Network Functions Virtualisation (NFV) Release 3; Software Architecture; Specification of the Classification of Cloud Native VNF implementations
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
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.3071 (01/2018)	Cloud-based network management functional architecture
ITU-T	ITU-T M.3371 (10/2016)	Requirements for service management in cloud-aware telecommunication management system
ITU-T	ITU-T M.3372 (08/2018)	Requirements for resource management in cloud-aware telecommunication management systems
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.3914 (01/2018)	Set of parameters of cloud computing for monitoring
ITU-T	ITU-T Q.4040 (02/2016)	The framework and overview of cloud computing interoperability testing
ITU-T	ITU-T Q.4041.1 (01/2018)	Cloud computing infrastructure capabilities interoperability testing - part 1: Interoperability testing between CSC and CSP
ITU-T	ITU-T Q.4042.1 (12/2018)	Cloud interoperability testing about web application - part 1: Interoperability testing between CSC and CSP
ITU-T	ITU-T Y.3500-series Supplement 46 (11/2017)	Scenarios of Implementing Cloud Computing in networks of developing countries
ITU-T	ITU-T Supplement 49 to ITU-T Y.3500-series (11/2018)	Cloud Computing standardization roadmap
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.3505 (05/2018)	Cloud computing – Overview and functional requirements for data storage federation
ITU-T	ITU-T Y.3506 (05/2018)	Cloud Computing Requirements for Cloud Service Brokerage
ITU-T	ITU-T Y.3507 (12/2018)	Cloud computing-Functional requirements of physical machine
ITU-T	ITU-T Y.3508 (08/2019)	Cloud computing - Overview and high-level requirements of distributed cloud
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

SDO	Reference	Title
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 (07/2017)	Cloud computing - Functional architecture of Network as a Service
ITU-T	ITU-T Y.3516 (09/2017)	Cloud computing - Functional architecture of inter-cloud computing
ITU-T	ITU-T Y.3517 (12/2018)	Cloud Computing - Overview of Inter-Cloud Trust Management
ITU-T	ITU-T Y.3518 (12/2018)	Cloud computing - functional requirements of inter-cloud data management
ITU-T	ITU-T Y.3519 (12/2018)	Cloud computing - Functional architecture of Big Data as a Service
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
ITU-T	ITU-T H.626.2 (12/2017)	Architectural requirements for cloud storage in video surveillance

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
ISO/IEC JTC 1	ISO/IEC 27018:2019	Information technology -- Security techniques – Guidance for the assessment of information security controls
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
ISO/IEC JTC 1	ISO/IEC 21878:2018	Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers
ISO/IEC JTC 1	ISO/IEC 19086-4:2019	Information technology -- Cloud computing – agreement (SLA) framework – Part 4: Components of security and protection of PII
ISO/IEC JTC 1	ISO/IEC TR 23186:2018	Information technology -- Cloud computing -- Framework of trust for processing of multi-sourced data
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

SDO	Reference	Title
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.1603 (03/2018)	Data security requirements for the monitoring service of cloud computing
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	ITU-T Y.3514 (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 CD 22123	Information technology -- Cloud computing -- Concepts and terminology
ISO/IEC JTC 1	ISO/IEC DIS 22624	Information technology -- Cloud Computing -- Taxonomy based data handling for cloud services
ISO/IEC JTC 1	ISO/IEC AWI 23751	Information Technologies -- Cloud Computing and distributed platforms – Data sharing agreement (DSA) framework
ISO/IEC JTC 1	ISO/IEC NP TR 23951	Cloud computing – Best practices for cloud SLA metrics
ISO/IEC JTC 1	ISO/IEC PDTS 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 PDTR 23188	Information technology -- Cloud computing -- Edge computing landscape
ISO/IEC JTC 1	ISO/IEC PDTR 23613	Information technology -- Cloud service metering and billing elements
ISO/IEC JTC 1	ISO/IEC 19944:2017/PDAM 1	Information technology -- Cloud computing -- Cloud services and devices: Data flow, data categories and data use - amendment
ETSI	ETSI GR/NFV-IFA029	Network Functions Virtualisation (NFV); Software Architecture; Report on the Enhancements of the NFV architecture towards “Cloud-native” and "PaaS"
ITU-T	ITU-T Draft H.248.CLOUD	Gateway control protocol: Cloudification of packet gateways
ITU-T	ITU-T Draft H.CCVS	Architecture for cloud computing in visual surveillance
ITU-T	ITU-T Draft Y.cccm-reqts	Cloud Computing - Requirements for Containers
ITU-T	ITU-T Draft Y.BaaS-reqts	Cloud computing - functional requirements for blockchain as a service

SDO	Reference	Title
ITU-T	ITU-T Draft Y.mc-reqts	Cloud Computing -Functional requirements of cloud service partner for multi-cloud
ITU-T	ITU-T Draft Y.MLaaS-reqts	Cloud computing - Functional requirements for machine learning as a service
ITU-T	ITU-T Draft Y.csb-arch	Cloud Computing -Functional architecture for cloud service brokerage
ITU-T	ITU-T Draft Y.dsf-arch	Cloud computing - Functional architecture for data storage federation
ITU-T	ITU-T Draft Y.cccsdaom-reqts	Cloud computing - Requirements for cloud service development and operation management
ITU-T	ITU-T Draft Y.ccfrcm	Cloud Computing - Framework and requirements of container management in inter-cloud
ITU-T	ITU-T Draft Y.ccgmfdc	Global Management Framework of Distributed Cloud
ITU-T	ITU-T Draft Y.ccm-reqts	Cloud computing maturity requirements and framework

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
ITU-T	ITU-T Draft X.1604	Security requirements of Network as a Service (NaaS) in cloud computing
ITU-T	ITU-T Draft X.1605	Security requirements of public infrastructure as a service (IaaS) in cloud computing
ITU-T	ITU-T Draft X.nssa-cc	Requirements of network security situational awareness platform for cloud computing
ITU-T	ITU-T Draft X.sgcc	Security guidelines for container in cloud computing environment
ITU-T	ITU-T Draft X.sgdc	Security guidelines for distributed cloud
ITU-T	ITU-T Draft X.sgmc	Security guidelines for multi-cloud
ITU-T	ITU-T Draft X.sr-cphr	Security requirements of cloud-based platform under low latency and high reliability application scenarios
ITU-T	ITU-T Draft X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment
ITU-T	ITU-T Draft Y.ccrm	Cloud computing - Framework of risk management

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 9075-1:2016	Information technology -- Database languages -- SQL -- Part 1: Framework (SQL/Framework)

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 11179-2:2019	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 19503:2005	Information technology -- XML Metadata Interchange (XMI)
ISO/IEC JTC 1	ISO/IEC 19075-8:2019	Information technology database languages -- SQL technical reports -- Part 8: Multi-dimensional arrays (SQL/MDA)
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
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

SDO	Reference	Title
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
ISO/IEC JTC 1	ISO/IEC 20546:2019	Information technology -- Big Data -- Overview and Vocabulary
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	ITU-T Y.3519 (12/2018)	Cloud computing - Functional architecture of Big Data as a Service
ITU-T	ITU-T Y.3601 (05/2018)	Big data - framework and requirements for data exchange
ITU-T	ITU-T Y.3602 (12/2018)	Big data - Functional requirements for data provenance
ITU-T	ITU-T Y.3650 (01/2018)	Framework of big data driven networking
ITU-T	ITU-T Y.4114 (07/2017)	Specific requirements and capabilities of the IoT for Big Data
ITU-T	ITU-T F.743.7 (05/2019)	Requirements for big data enhanced visual surveillance services

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
ISO/IEC JTC 1	ISO/IEC 20889:2018	Privacy enhancing data de-identification terminology and classification of techniques
ITU-T	ITU-T X.1147 (11/2018)	Security requirements and framework for big data analytics in mobile internet services
ITU-T	ITU-T Y.3602 (12/2018)	Big data - Functional requirements for data provenance

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 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 NP TR 24027	Information technology -- Artificial Intelligence (AI) -- Bias in AI systems and AI aided decision making
ISO/IEC JTC 1	ISO/IEC NP TR 24028	Information technology -- Artificial Intelligence (AI -- Overview of trustworthiness in Artificial Intelligence
ISO/IEC JTC 1	ISO/IEC NP TR 24029-1	Artificial Intelligence (AI) -- Assessment of the robustness of neural networks -- Part 1: Overview
ISO/IEC JTC 1	ISO/IEC NP TR 24030	Information technology -- Artificial Intelligence (AI) -- Use cases
ISO/IEC JTC 1	ISO/IEC NP 23894	Information technology -- Artificial Intelligence (AI) -- Risk management
ISO/IEC JTC 1	ISO/IEC NP TR 24368	Information technology -- Artificial intelligence -- Overview of ethical and societal concerns
ISO/IEC JTC 1	ISO/IEC NP TR 24372	Information technology -- Artificial intelligence (AI) -- Overview of computational approaches for AI systems
ISO/IEC JTC 1	ISO/IEC NP 38507	Information technology -- Governance of IT -- Governance implications of the use of artificial intelligence by organizations
ISO/IEC JTC 1	ISO/IEC DIS 21838-1	Information technology -- Top-level ontologies -- Part 1: Requirements
ISO/IEC JTC 1	ISO/IEC DIS 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 FDIS 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 NP TR 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 NP TR 15944-14	Information technology -- Business operational view -- Part 14: Open-edi, model and cloud computing architecture

SDO	Reference	Title
ISO/IEC JTC 1	ISO/IEC NP TR 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
ISO/IEC JTC 1	ISO/IEC FDIS 9075-15	Information technology -- Database languages -- SQL – Part 15: Multi-dimensional arrays (SQL/MDA)
ETSI	DTR/INT-008_AFI AI Testing	INT WG AFI; Artificial Intelligence (AI) in Test Systems
ITU-T	ITU-T Draft Y.BD-arch	Big data - Reference architecture
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 Y. bDDN-MNTMP	Big data driven mobile network traffic management and planning
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 D.princip_bigdata	Policy framework and principles for data protection in the context of big data relating to international telecommunication services
ITU-T	ITU-T Draft X.mdcv	Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles
ITU-T	ITU-T Draft X.sgBDIP	Security guidelines for big data infrastructure and platform
ITU-T	ITU-T Draft X.sgtBD	Security guidelines of lifecycle management for telecom big data
ITU-T	ITU-T Draft F.AFBDI	Assessment framework for big data infrastructure
ITU-T	ITU-T Draft Y.bDDN-FunArch	Functional architecture of big data driven networking
ITU-T	ITU-T Draft H.VSBD	Architecture for Big Data Application in Visual Surveillance System
ITU-T	ITU-T Draft H.CUAV-AIF	Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence
ITU-T	ITU-T Draft F.VS-AIMC	Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence
ITU-T	ITU-T Draft L.DCIM	Specifications of data centre infrastructure management (DCIM) system based on Big Data and AI technology
ITU-T	ITU-T Draft Y.SSC-AISE-arc	Reference architecture of artificial intelligence service exposure for smart sustainable cities
ITU-T	ITU-T Draft Y.Sup.AI4IoT (ex TR.AI4IoT; Y.AI4SC)	Unlocking Internet of things with artificial intelligence: Where we are and where we could be
ITU-T	ITU-T Draft Suppl on Y. Sup.aisr	Artificial Intelligence Standard Roadmap

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 CD 20547-4	Information technology -- Big data reference architecture -- Part 4: Security and privacy
ISO/IEC JTC 1	ISO/IEC NP TR 24028	Information technology -- Artificial Intelligence (AI -- Overview of trustworthiness in Artificial Intelligence
ISO/IEC JTC 1	ISO/IEC NP TR 24029-1	Artificial Intelligence (AI) -- Assessment of the robustness of neural networks -- Part 1: Overview
ISO/IEC JTC 1	ISO/IEC NP 23894	Information technology -- Artificial Intelligence (AI) -- Risk management
ISO/IEC JTC 1	ISO/IEC NP TR 24368	Information technology -- Artificial intelligence -- Overview of ethical and societal concerns
ITU-T	ITU-T Draft X.GSBDaaS	Guidelines on security of Big Data as a Service
ITU-T	ITU-T Draft Y.BDDP-reqts	Big data - Overview and requirements for data preservation
ITU-T	ITU-T Draft D.princip_bigdata	policy framework and principles for data protection in the context of big data relating to international telecommunication services
ITU-T	ITU-T Draft X.mdcv	security-related misbehaviour detection mechanism based on big data analysis for connected vehicles
ITU-T	ITU-T Draft X.sgBDIP	Security guidelines for big data infrastructure and platform
ITU-T	ITU-T Draft X.sgtBD	Security guidelines of lifecycle management for telecom big data

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

ANEC G.I.E.
Southlane Tower I – 1, Avenue du Swing
L-4367 Belvaux

Email: anec@ilnas.etat.lu
Phone: (+352) 24 77 43 70

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

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.

October 2019 · Smart Secure ICT · Version 2.0 · © ILNAS/ANEC · ISSN 2354-483X

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