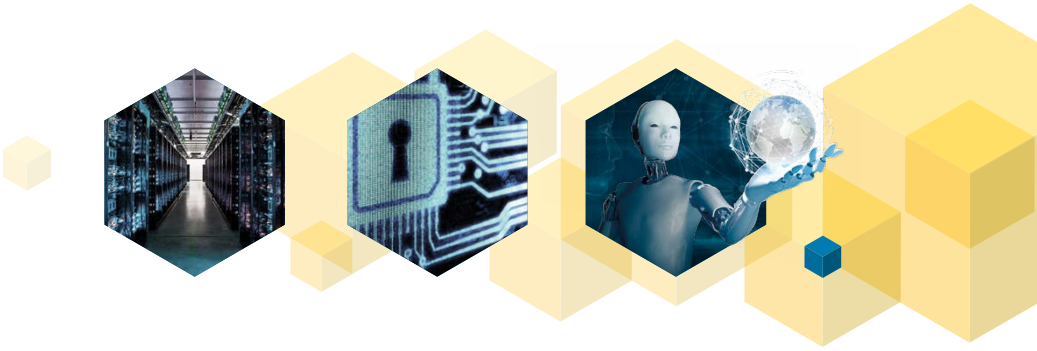
ILNAS

STANDARDS ANALYSIS
SMART ICT
LUXEMBOURG

Version 1.0 · May 2017



ANEC

FOREWORD

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

The ICT sector has gained more and more importance in the society as a whole in the last decades. The rapid evolution of the technologies and their usages in our daily lives are drawing a new paradigm in which ICT will play an increasing role. The ability of all the "things" to be connected, to communicate between each other and to collect information is deeply changing the world we know and we are probably only at the beginning of this transformation, where ICT become Smart. In this way, technical standardization plays a key role to connect all the Smart ICT components, to make them interoperable and prevent vendor lock in, but also to guarantee the security and safety of the next digital world. Standards can support the integration of multiple data sources of Smart ICT technologies; therefore, standards and technical standardization play an important role for data quality, data governance, data protection, data privacy and security.

The Grand-Duchy of Luxembourg has clearly understood this state of fact and an ambitious development strategy is led by the government since several years, not only to be part of this transformation, but also to take a major role in the future of the digital landscape. To support this development, the *"Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services"* (ILNAS) has drawn up the "Luxembourg Standardization Strategy 2014-2020"[1], approved by the Minister of the Economy and based on three pillars in which the ICT sector is one of the cornerstones.

ILNAS carries out different legal missions in the field of ICT. In addition, through the "Luxembourg's policy on ICT technical standardization 2015-2020"[2], ILNAS commissioned the Economic Interest Grouping *"Agence pour la Normalisation et l'Économie de la Connaissance"* (ANEC GIE) to strengthen the national ICT sector involvement in standardization work.

ILNAS, with the support of ANEC GIE, has launched several activities dedicated to strengthen and develop the ICT-related standardization landscape at the national level in terms of education and involvement of stakeholders, such as the creation of a University Certificate Smart ICT for Business Innovation in collaboration with the University of Luxembourg or the current development of a research program on Digital Trust for Smart ICT with the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg. This research program will concentrate on three important pillars of the Smart ICT: Cloud Computing, Internet of Things, Big Data, and Digital Trust related to these technologies, notably with the objective to develop a Master degree *Smart Secure ICT for Business Innovation* at the horizon 2019.

In the frame of the "Luxembourg's policy on ICT technical standardization 2015-2020", one of the main missions of ANEC GIE notably consists in drawing-up yearly a national Standards Analysis for the ICT sector (ANS TIC), whose last version was published in March 2017[3] and constitutes, both with the recently published White Paper "Digital Trust for Smart ICT"[4], the basis of the present Smart ICT Standards Analysis. Directly in line with the previously detailed developments, this report is intended to be used as a practical tool to discover last standardization developments of selected Smart ICT, namely Cloud Computing, Internet of Things and Big Data, as well as the related Digital Trust standards-based evolution. Therefore, the present document will allow national stakeholders to identify relevant standardization technical committees in the Smart 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] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf

[2] 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

[3] ILNAS & ANEC GIE, "Standards Analysis of the ICT Sector" (7th edition), 2017

[4] ILNAS, "White Paper Digital Trust for Smart ICT" (3rd edition), 2016

EXECUTIVE SUMMARY

This Smart ICT Standards Analysis is conceived as a practical guide to all the national stakeholders regarding standardization activities in the field of selected Smart ICT areas (Cloud Computing, Internet of Things, Big Data) and Digital Trust related to these technologies to quickly identify issues and interests for them to join in such technical standardization committees. Beyond this possibility, different opportunities, presented in this report, are available for national stakeholders with the objective to make them able to take advantage of standards and standardization.

In this context, this report, relying on the National Standard Analysis of the ICT sector[5], is designed to develop an information and exchange network for Smart ICT standardization knowledge in the Grand Duchy of Luxembourg. The ICT sector is already involved at the national standardization level with 72 national delegates currently registered by ILNAS[6], including 49 who are directly involved in Smart ICT and/or Digital Trust related technical committees (Cloud Computing: 13; Internet of Things: 6; Big Data: 7; Digital Trust: 35).

ILNAS, with the support of ANEC GIE, has already started awareness to attract and involve national delegates into an integrated and innovative approach of standardization in these Smart technologies. 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 a strong development of Smart ICT technical standardization in 2017, with the aim to support the market in the related economic development. ILNAS priorities notably provide the management of the national Smart ICT technical committees, as well as the raising of awareness in national organizations, to foster the national involvement in Smart ICT technical standardization and better position of Luxembourg at the international level.

This report provides information of this Smart ICT standardization development at national level. It introduces the fundamental pillars of Smart ICT along with Digital Trust related to these technologies and standardization activities performed at international, European and national levels. It will provide awareness about Smart ICT technical standardization progress to the national stakeholders and will facilitate their involvement in such activities to take advantage of standards and standardization for their economic development.

[5] https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/standards-analysis-ict-7-0.pdf

[6] National register of standardization delegates (March 2017)

TABLE OF CONTENTS

1 INTRODUCTION

The sector of Information and Communication Technologies (ICT) 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. Cloud Computing, Internet of Things and Big Data 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. Thus, economic growth of and through Smart ICT is tied to the related standardization activities.

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[7]. To enhance these activities also at the academic level, ILNAS is notably working with the University of Luxembourg (UL) to develop standards-related education and research. The University certificate *"Smart ICT for Business Innovation"*, in 2015-2016, was its first step to work closely with academia aiming to provide standards-based knowledge on recent emerging Smart ICT technologies to ICT professionals at national level. The course offered for two semesters was completed successfully with great interest of participations from different industries and a new course of the University certificate will start at the beginning of 2018.

Recently and in line with the University certificate, ILNAS and the UL have developed a research program whose objective is to analyze and extend standardization and Digital Trust knowledge in the Smart ICT sectors such as Cloud Computing, Internet of Things and Big Data. Three PhD students will start their research activities in the mentioned domains of the Smart ICT. The main motivation of this program is to perform standardization-Digital Trust related research to enhance quality of the University certificate and to serve as the base for a future Master Program *Smart Secure ICT for Business Innovation* expected in 2019.

In relation with these recent developments, this Smart ICT Standards Analysis concentrates on three important pillars of the Smart ICT: Cloud Computing, Internet of Things, Big Data. Moreover Digital Trust related to these technologies is also included. This report is directly based on the Luxembourg's Standard Analysis of the ICT sector[8] (ANS TIC) and also relies on White Papers published by ILNAS in the Smart ICT area[9]. The main purpose of this document is to inform national stakeholders about the main standardization activities and technical committees related to Smart ICT with the objective to offer them guidance for a potential future involvement in the standard's development process. It also provides a support to the current and future development of ILNAS standardization at national level (i.e., research and education). The readers are encouraged to consult the ANS TIC to have more information about the standards developments in the other fields of ICT that have been studied at national level, as described in Figure 1.

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

[8] ILNAS & ANEC GIE, "Standards Analysis of the ICT Sector" (7th edition), 2017

[9] White Paper "Digital Trust for Smart ICT" and "Big Data"

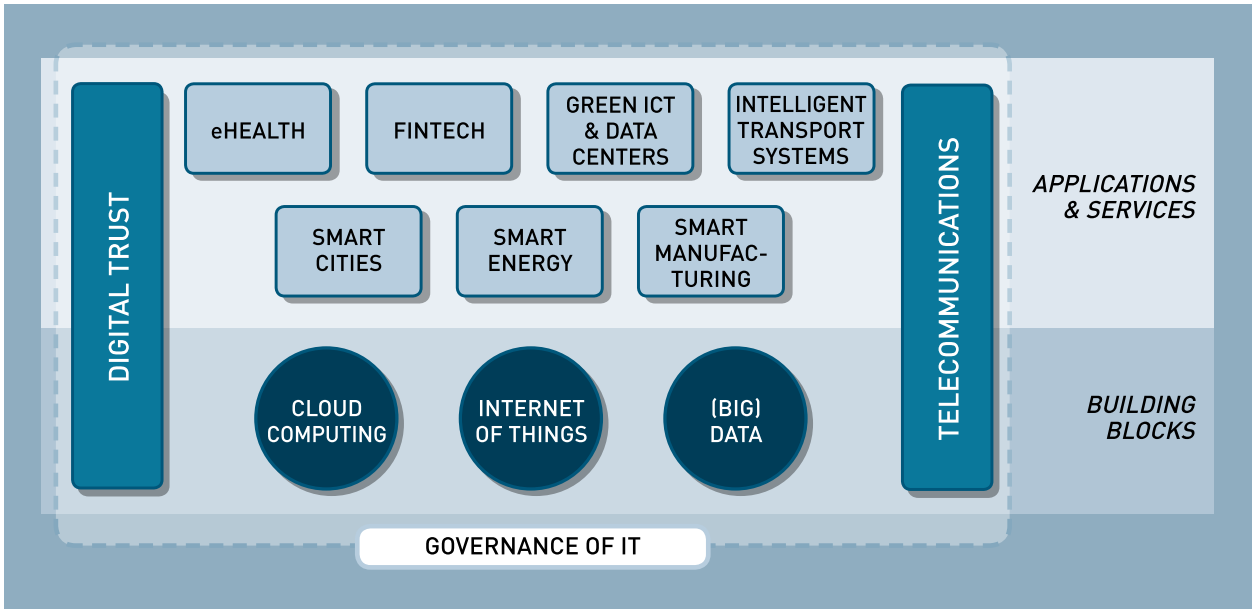


Figure 1: ICT standards analysis subsectors

The report is organized as follows. The importance of standardization along with its objectives and introduction of standardization landscape in national, European and international level have been included in Chapter 2. Chapter 3 is dedicated to definition of Smart ICT, economical overview of ICT and interaction of three pillars of Smart ICT components: Cloud Computing, Internet of Things and Big Data, which are further defined in Chapter 4 with their fundamental characteristics. Detail list of technical standardization committees of each technologies have been also included in this Chapter.

Finally, Chapter 5 presents opportunities related to standardization for national stakeholders. It also introduces how ILNAS is helping national economy thorough standardization. The concluding Chapter provides a summary of the document and reiterates the commitment of ILNAS to assist national entities with their involvement in standardization.

2 STANDARDS AND STANDARDIZATION

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) 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[10].

2.1 STANDARDIZATION OBJECTIVES AND PRINCIPLES

As stated in the Regulation (EU) N°1025/2012 on European standardization, and according to the World Trade Organization (WTO)[11], 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 final 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.

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.

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

[11] Source: Second triennial review of the operation and implementation of the agreement on technical barriers to trade – Annex 4: Decision of the committee on principles for the development of international standards, guides and recommendations

COHERENCE

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

DEVELOPMENT DIMENSION

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

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

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

2.2 STANDARDIZATION LANDSCAPE

In Europe, the three recognized European Standardization Organizations (ESO), as stated in the Regulation (EU) No 1025/2012[12], 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.

[12] Regulation (EU) No 1025/2012 of The European Parliament And of The Council : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF

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

EUROPEAN AND INTERNATIONAL STANDARDIZATION BODIES		DATE OF CREATION	NUMBER OF MEMBERS	NUMBER OF PUBLISHED STANDARDS
ISO	International Organization for Standardization	1946	163	21 133
IEC	International Electrotechnical Commission	1906	84	6 895
ITU-T	International Telecommunication Union's Telecommunication Standardization Sector	1865	258[13]	5 201
CEN	European Committee for Standardization	1961	34	15 985
CENELEC	European Committee for Electrotechnical Standardization	1973	34	6 937
ETSI	European Telecommunications Standards Institute	1988	814[13] (68 countries)	15 336

Table 1: Characteristics of European and International Standardization Organizations[14]

At national levels, one or several 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, ISO, IEC and ETSI.

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 2).

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

[14] Source: Websites of organizations - March 2017

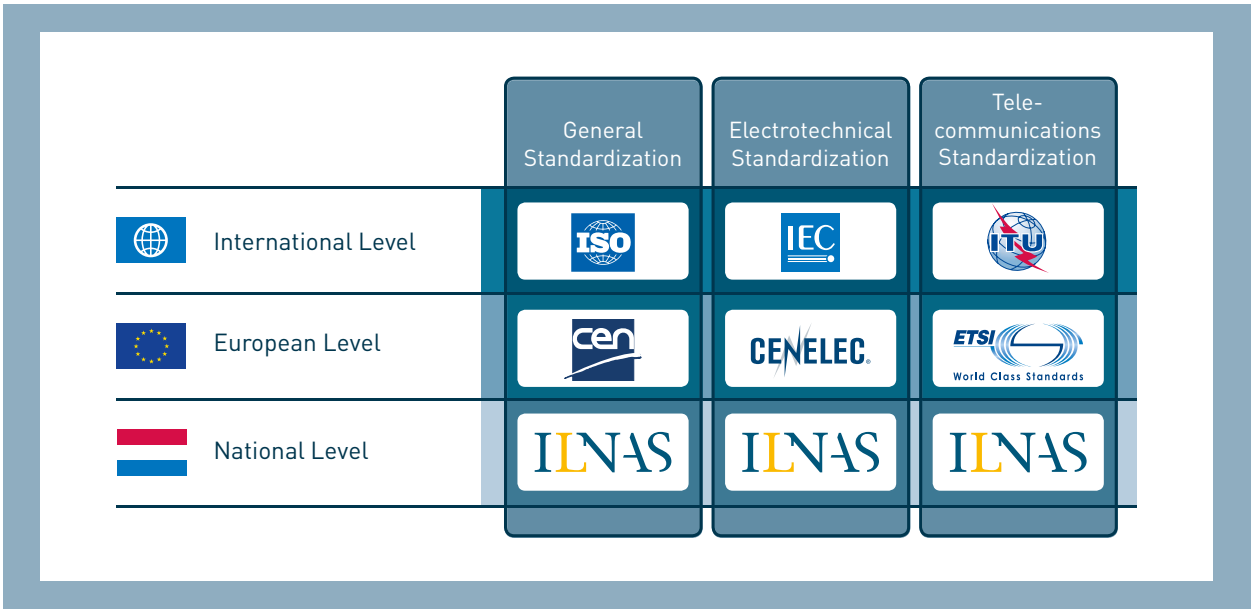


Figure 2: Interactions between the Standardization Organizations

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[15], 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);
- Standardization documents should be approved between the two organizations.

Similarly, CENELEC and IEC signed the Dresden Agreement[16] in 1996 with the aim of developing intensive consultations in the electrotechnical field. This agreement has been replaced by the Frankfurt Agreement in 2016 with the aim to simplify the parallel voting processes, and increases 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);
- Ballots for documents made in parallel at IEC and CENELEC.

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

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

Under both agreements, 32% of all European standards ratified by CEN, as well as 72% of those ratified by CENELEC, are respectively identical to ISO or IEC standards[17]; in that respect, the European and international organizations do not duplicate work.

Finally, ITU-T and ETSI have agreed on a Memorandum of Understanding (MoU) in 2012[18] (replacing the former MoU signed in 2000) that paves the way for European regional standards, developed by ETSI, to be recognized internationally.

Agreements also exist between the standards organizations to facilitate their cooperation. For example, ISO and IEC have the possibility to sign conventions to create Joint Technical Committees (JTC) or Joint Project Committees (JPC) when the area of work is overlapping the two organizations. It is to avoid the creation of duplicative or incompatible standards. In this frame, the Joint Technical Committee ISO/IEC JTC 1 "Information Technology" has been created in 1987.

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[19]. Similarly, the cooperation between CEN and CENELEC aims to create a European standardization system that is open, flexible and dynamic.

[17] CEN-CENELEC Quarterly Statistical Pack – 2017 Q1

[18] Memorandum of understanding between ETSI and ITU

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

3 SMART ICT LANDSCAPE

3.1 SMART ICT DEFINITION AND ECONOMICAL OVERVIEW

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

Dynamism in the ICT based technology is driving innovation processes. New tools and technologies are now adopted in ICT business to enhance its effectiveness in the governmental and industrial sector. These technologies add more smartness and are closely interconnected with each other. They are also referred as Smart ICT technologies. For example, Cloud Computing, Internet of Things, and Big Data are already offering previously unimagined possibilities for innovation and business development.

DEFINITION:

Smart ICT

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, Robotic and new ways of gathering data, such as social media and crowdsourcing.[20]

In terms of economic impact, the IT products and services were estimated to represent worldwide revenue of $ 2.4 trillion in 2016 according to IDC and this figure could reach $ 2.7 trillion in 2020[21]. Research & Development investment in the ICT sector is still very important, for example global Software and Hardware activities have increased by 12.3% and 7.6% respectively in 2015[22]. Moreover, the coming trends show that the sector is still innovating with the development of technologies such as Intelligent Things, Artificial Intelligence and Advanced Machine Learning, Virtual Reality and Augmented Reality, Blockchains and Distributed Ledger Technologies, etc.[23]

At the European level, the ICT sector has been directly responsible for 4.5% of GVA[24] (Gross Value Added), with a market value of EUR 529 billion in 2013[25], but it contributes far more to the overall productivity growth. This is not only due to the high levels of dynamism and innovation inherent in this sector, but also due to the enabler role this sector plays, in changing how other sectors do business. At the same time,

[20] 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").

[21] http://www.businesswire.com/news/home/20160829005519/en/Worldwide-Spending-Forecast-Reach-2.7-Trillion-2020

[22] The 2016 EU Industrial R&D Investment Scoreboard

[23] Source: Gartner (October 2016)

[24] 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)

[25] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_nace10_c&lang=en (source: Eurostat)

the social impact of ICT has become significant. This is supported by European statistics of 2016, with 85% (Luxembourg: 97%) of households having a broadband connection[26], 79% (Luxembourg: 97%) of individuals using the Internet on a regular basis[27] of which 67% (Luxembourg: 82%) used a mobile device to connect to the Internet away from home or work[28].

The European Commission 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 reduction of energy consumption, support to ageing citizens' lives, revolution of health services and delivery of better public services. ICT can also drive the digitization of Europe's cultural heritage forward by providing online access to all. Currently, ICT plays a crucial role in[29]:

- Advanced research to uncover radically new technological possibilities and ICT contributions to research and innovation;
- Research and innovation activities on generic ICT technologies either driven by industrial roadmaps or through a bottom up approach;
- Multi-disciplinary application-driven research and innovation leveraging ICT to tackle societal challenges.

Finally, at the national level, ICT is considered as a key economic sector. Within the National Government Program[30], having a developed ICT sector is a cornerstone, especially to support other economic sectors: eco-technologies (e.g. Smart Grid, IT management), logistics (e.g. e-commerce), biotechnologies (e.g. Archiving, Data Management), industrial and financial sector (e.g. Cloud Computing).

The ICT sector is already a competitive sector in Luxembourg, which ranks 10th out of the 28 EU Member States in the "European Commission Digital Economy and Society Index" (DESI) 2016[31]. The country is particularly running ahead in terms of connectivity, human capital (ranks 1st in Europe for Internet users and digital skills) and use of the Internet. The ICT sector represents more than 2,000 companies in 2014 or 4.23% of the total employment in 2016[32]. Moreover, the ICT sector has contributed to 6.2% of GVA in Luxembourg in 2013[33].

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

- The "Digital Lëtzebuerg" initiative[34], launched in autumn 2014 to provide a common umbrella for the numerous public and private initiatives that make up the country's digital economy and society;
- The "Digital (4) Education" strategy[35], presented in May 2015 with the objective to reinforce digital skills in the educative system and answer the growing demand for skilled ICT professionals;
- The strategic study on the "Third Industrial Revolution"[36], 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".

[26] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en (source : Eurostat)

[27] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=tin00091&lang=en (source : Eurostat)

[28] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=tin00083&lang=en (source : Eurostat)

[29] https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20A4%20Sept2016.pdf

[30] http://www.gouvernement.lu/3322796/Programme-gouvernemental.pdf

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

[32] Source: STATEC

[33] Source: Eurostat (online data code: nama_nace10_c)

[34] http://www.digital-luxembourg.public.lu/en/index.html

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

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

3.2 SMART ICT COMPONENTS AND THEIR INTERACTIONS

Although many terminologies come in mind while talking about Smart ICT, but three technologies, namely, Cloud Computing, Internet of Things and Big Data are the major elements of the current ICT market. Moreover, these Smart technologies have now become entangled and closely linked with each other. The Internet of Things produces both raw and pre-processed data. Big Data stores, analyses and provides mechanisms for operating and understanding the large amount of data produced. Cloud Computing supports these environments by providing the processing power and infrastructure to allow the capture, storage, analysis of the data (see Figure 3).

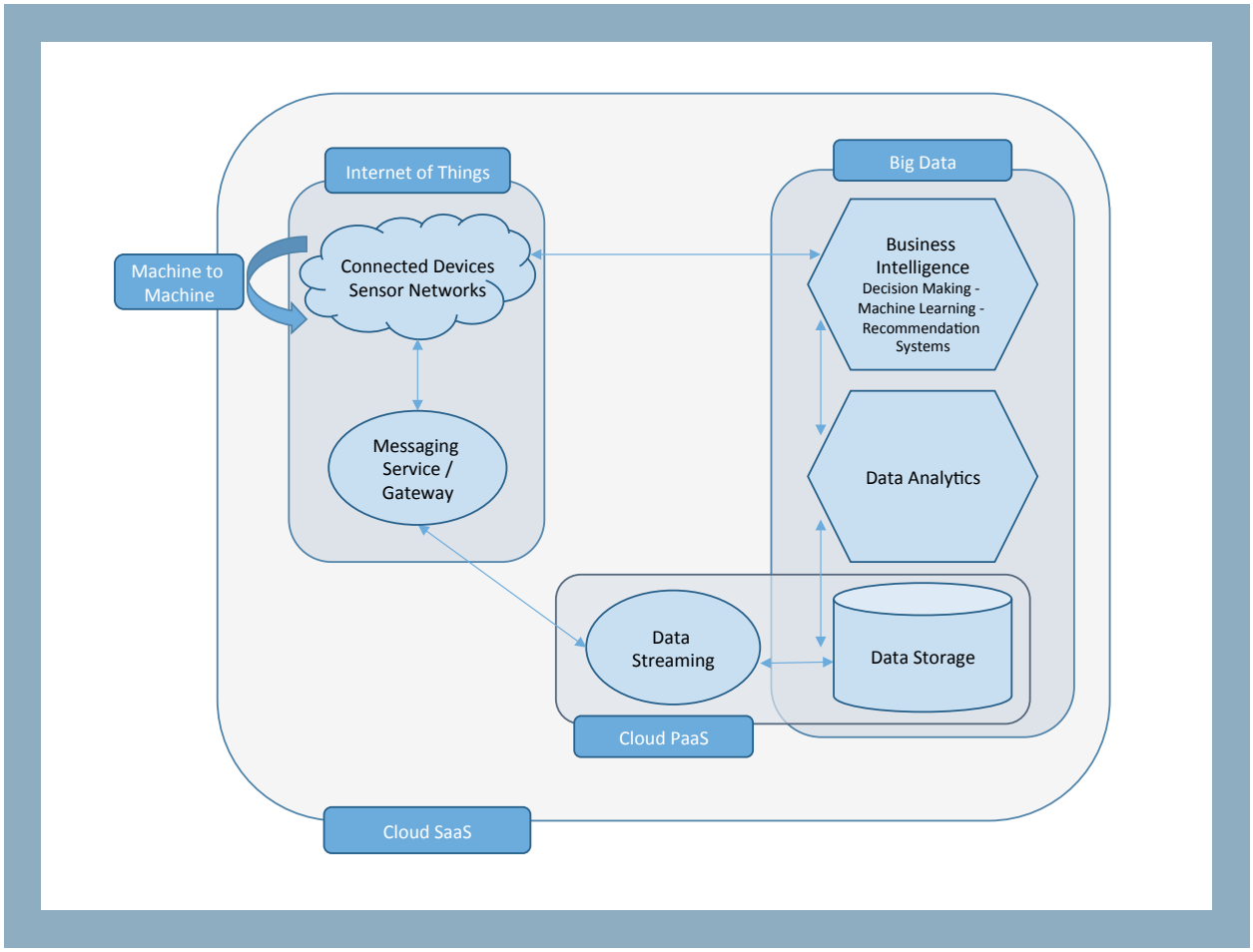


Figure 3: Smart ICT Components and their Interactions[37]

To better understand how these technologies work and interact together, the next section provides an introduction of the three pillars of the Smart ICT: Cloud Computing, Internet of Things (IoT), Big Data and Digital Trust related to these three technologies; and in particular why and how standardization is an important challenge for these technologies.

[37] ILNAS, "White Paper Digital Trust for Smart ICT" (3rd edition), 2016

4 SMART ICT STANDARDS WATCH

The objective of the standards analysis is to facilitate the involvement of the national organizations in the technical standardization process. In this way, this chapter introduces the three pillars of the Smart ICT: Cloud Computing, Internet of Things (IoT), Big Data and Digital Trust related to these three technologies, and details the relevant technical committees for each of them. This information is based on the standard's watch realized in the frame of the development of the Luxembourg's Standard Analysis of the ICT sector[38]. Moreover, a list of standards both published and under development for the three selected Smart ICT technologies is also provided in each concerned subsection. This chapter focuses on the formal standards bodies active in the Smart ICT area, both at European and international levels:

ISO/IEC

ISO is the world's dominant developer and publisher of International Standards in terms of scope. It has around 21,000 standards published and more than 4,700 standards under development[39]. ISO is in charge of developing International Standards for all industry sectors. IEC prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology". To prevent an overlap in standardization work related to information technology, ISO and IEC formed a Joint Technical Committee in 1987 known as ISO/IEC JTC 1.

ISO/IEC JTC 1 has taken a leading role in Smart ICT standardization since a couple of years with the creation of working groups and technical committees directly responsible for the development of International Standards in the Smart ICT areas.

CEN

CEN, the European Committee for Standardization, is the European counterpart of ISO. The ICT sector is an active standardization domain for the CEN, which has 14 technical committees and additional other groups directly concerned under its supervision[40]. The other ICT-related topics are principally being tackled at the international level by ISO/IEC JTC 1, complying with the "Vienna Agreement" set up between CEN and ISO, as detailed in section 2.2.

The standardization activities of the European Standardization Organizations, including CEN, are detailed in an annual common Work Program, which was published in December 2016 for the year 2017[41]. It has foreseen to be active in several ICT-related areas covering both the Digital & Information Society and the Smart Technologies.

ETSI - EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE

The European Telecommunications Standards Institute (ETSI) produces globally applicable standards for ICT including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI is officially recognized by the European Union as a European Standardization Organization.

In this chapter, specific technical committees of ETSI are detailed due to their particular importance for Digital Trust (e.g.: ETSI/TC ESI and ETSI/TC CYBER).

[38] https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2017/standards-analysis-ict-7-0.pdf

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

[40] According to: ILNAS & ANEC GIE, "Standards Analysis of the ICT Sector" (7th edition), 2017

[41] http://www.cencenelec.eu/News/Publications/Publications/cen-cenelec-wp2017_en.pdf

ITU-T - INTERNATIONAL TELECOMMUNICATION UNION - TELECOMMUNICATION STANDARDIZATION SECTOR

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) is an "intergovernmental public-private partnership organization" which brings together experts from around the world to develop international standards known as ITU-T Recommendations which represents defining elements in the global infrastructure of ICT.

This chapter does not include ITU-T study groups (equivalent to technical committees) but the organization is still introduced since it actively collaborates in the development of many ISO/IEC standards. Moreover, a list of ITU-T Recommendations (both published and under development) relevant in the context of the selected Smart ICT is provided in the Appendix.

4.1 CLOUD COMPUTING

There are many definitions of cloud computing, we introduce here the definition of recommendation ITU-T Y.3500 | ISO/IEC 17788[42]:

"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".

Another definition of National Institute of Standards[43], which has gained broad support from the industry:

"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."

4.1.1 CHARACTERISTICS

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. There are four deployments models, namely, Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. The fundamental characteristics of Cloud Computing are[44]:

4.1.1.1 BROAD NETWORK ACCESS

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms as well as other traditional or Cloud-based software services.

4.1.1.2 RAPID ELASTICITY

Capabilities can be rapidly and elastically provisioned to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

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

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

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

4.1.1.3 MEASURED SERVICE

Cloud systems automatically control and optimize resource usage by leveraging a metering of e.g. storage, processing, bandwidth, or active user accounts. It provides transparency for both the provider and consumer of the service by means of monitoring, controlling and reporting.

4.1.1.4 ON DEMAND SERVICE

A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically without requiring human interaction with a service provider.

4.1.1.5 MULTI TENANCY

With the capabilities of multi-tenancy of a Cloud resource, physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another.

4.1.1.6 RESOURCE POOLING

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

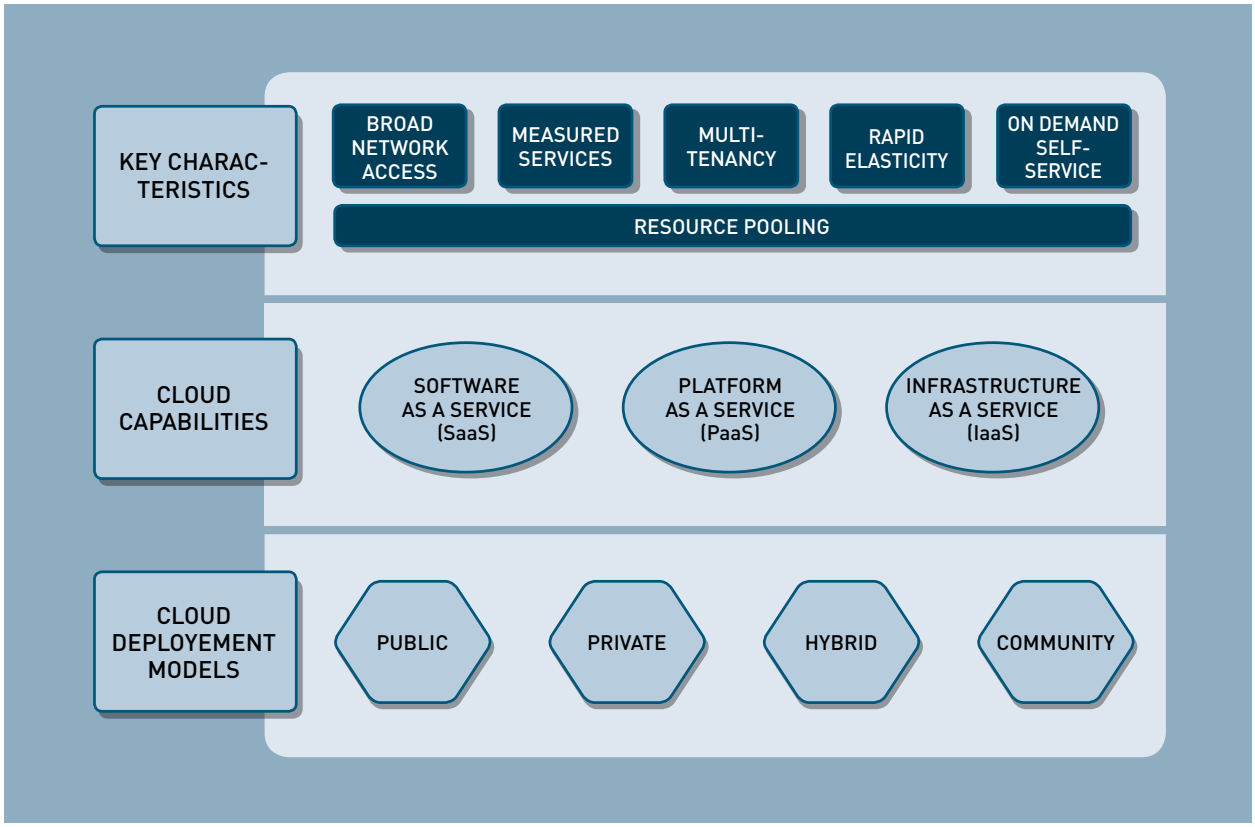


Figure 4: Visual Model of ISO/IEC Cloud Computing Definition[45]

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

4.1.2 CLOUD COMPUTING STANDARDS AND STANDARDIZATION TECHNICAL COMMITTEES

The standards landscape for Cloud Computing is extensive, since many standards developing organizations are active in the Cloud Computing subsector and many standards and specifications have been developed. As specified by the European Commission in its European Cloud Computing Strategy[46], it is necessary to cut "through the jungle of standards" in order to identify existing solutions, market needs and, finally, to increase Cloud Computing adoption. This section provides an overview of the Cloud Computing related technical committees and standards currently active in the recognized Standardization Organizations.

4.1.2.1 TECHNICAL COMMITTEES

4.1.2.1.1 ISO/IEC JTC 1/SC 38

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/SC 38**	**TITLE**	**Cloud Computing and Distributed Platforms**
CREATION DATE	2009	**MEMBERS** 	**Participating Countries (30):** United States, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Republic of Korea, **Luxembourg**, Netherlands, Pakistan, Panama, Poland, Russian Federation, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, United Kingdom
SECRETARIAT	ANSI (USA)		
SECRETARY	Ms. Lisa Rajchel		
CHAIRPERSON	Dr. Donald Deutsch		
ORGANIZATIONS IN LIAISON	CSCC, Cloud security alliance, DMTF, Ecma International, INLAC, ITU, OASIS, OGF, SNIA, EC, EuroCloud, TM Forum		**Observing Countries (10):** Argentina, Bosnia and Herzegovina, Czech Republic, Hong Kong, Norway, Portugal, Serbia, Turkey, Uruguay, Zambia
WEB SITE	https://www.iso.org/committee/601355.html		
SCOPE	Standardization in the area of Cloud Computing and Distributed Platforms including but not limited to: • Service Oriented Architecture (SOA); • Service Level Agreement; • Interoperability and Portability; • Data and their Flow Across Devices and Cloud Services.		
STRUCTURE	TC 1/SC 38/WG 3	Cloud Computing Service Level Agreements (CCSLA)	
	JTC 1/SC 38/WG 4	Cloud Computing Interoperability and Portability (CCIP)	
	JTC 1/SC 38/WG 5	Cloud Computing Data and its Flow (CCDF)	
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 38 (number includes updates): 10		

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

STANDARDS UNDER DEVELOPMENT	6	
INVOLVEMENT OF LUXEMBOURG		
13 DELEGATES	Mr. Johnatan Pecero (Chairman)	ANEC GIE
	Mr. Michel Ayme	Atos Luxembourg PSF S.A.
	Mr. Christophe Delogne	BGL BNP Paribas
	Mr. Cyril Cassagnes	KPMG Luxembourg S.à r.l.
	Mrs. Myriam Djerouni	Banque de Luxembourg S.A.
	Mrs. Shenglan Hu	POST Telecom PSF S.A.
	Mrs. Digambal Nayagum	AS AVOCATS
	Mr. Shyam Wagle	ANEC GIE
	Mr. Joost Pisters	LuxCloud S.A.
	Mr. Jean Rapp	Actimage S.A.
	Mr. Jean-Michel Remiche	POST Telecom S.A.
	Mrs. Ana-Maria Simionovici	University of Luxembourg
	Mr. Qiang Tang	Luxembourg Institute of Science and Technology (LIST)

COMMENTS

ISO/IEC JTC 1/SC 38, Cloud Computing and Distributed Platforms, is responsible for the development of standards to support distributed computing paradigms- especially in the area of Cloud Computing. 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 DIS 19086-2, Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model;
- ISO/IEC FDIS 19086-3, Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements;
- ISO/IEC DIS 19941, Information Technology -- Cloud Computing -- Interoperability and portability;
- ISO/IEC FDIS 19944, Information Technology -- Cloud Computing – Cloud services and devices: data flow, data categories and data use;
- ISO/IEC AWI 22123, Information Technology -- Cloud Computing -- Concepts and Terminology;
- ISO/IEC NP TR 22678, Information Technologies -- Cloud Computing -- Guidance for Policy Development.

Moreover, projects related to Cloud Computing security are under the direct responsibility of ISO/IEC JTC 1/SC 27. In this frame, several International Standards have already been published, like ISO/IEC 27017:2015 or ISO/IEC 27018:2014, which respectively define code of practice for information security controls based on ISO/IEC 27002 for Cloud services and for protection of personally identifiable information (PII) in public Clouds acting as PII processors.

Currently, ISO/IEC JTC 1/SC 27 is developing the fourth part of ISO/IEC 19086, concerning the security and privacy aspects of the SLA framework and technology.

4.1.2.2 STANDARDS

4.1.2.2.1 Published Standards

This section details the standards already published by the recognized SDO regarding Cloud Computing (non-exhaustive list). The linked standards below are publicly available.

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 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 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 / 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 27018:2014	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC JTC 1	ISO/IEC 27036-4:2016	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ETSI	ETSI TR 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 TR 103 304 V1.1.1 (07/2016)	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
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 003 391 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Interoperability and Security 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

4.1.2.2.2 Standards under development

This section details the standards under development regarding Cloud Computing in the recognized SDO (non-exhaustive list).

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 DIS 19086-2	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric Model
ISO/IEC JTC 1	ISO/IEC FDIS 19086-3	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 3: Core conformance requirements
ISO/IEC JTC 1	ISO/IEC CD 19086-4	Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy
ISO/IEC JTC 1	ISO/IEC DIS 19941	Information technology -- Cloud computing -- Interoperability and portability
ISO/IEC JTC 1	ISO/IEC FDIS 19944	Information technology -- Cloud computing -- Cloud services and devices: data flow, data categories and data use
ISO/IEC JTC 1	ISO/IEC AWI 22123	Information technology -- Cloud computing -- Concepts and terminology
ISO/IEC JTC 1	ISO/IEC NP TR 22678	Information Technologies -- Cloud Computing -- Guidance for Policy Development
ETSI	ETSI DGS/NFV-EVE011	Network Functions Virtualisation (NFV) Release 3; Software Architecture; Specification of the Classification of Cloud Native VNF implementations
ETSI	ETSI DGR/NFV-IFA029	Network Functions Virtualisation (NFV); Software Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"
ETSI	ETSI TS 103 458	CYBER; Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services
ETSI	ETSI GS IP6 007	IPv6-based Cloud Computing; IPv6-based Deployment of Cloud Computing

4.2 INTERNET OF THINGS (IOT)

The internet of things (IoT) has been defined in Recommendation ITU-T Y.2060[47] as:

"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".

"Thing: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks."

Another definition by IEEE communication Magazine[48] links the IoT back to Cloud services:

"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."

4.2.1 CHARACTERISTICS

The concept of IoT is broad and still in the process of defining. Characteristics of IoT can be defined from the perspectives of IoT components/devices used, services provided, usability, and security. However, it will be too early to characterize all the features of such evolving technologies, some fundamental characteristics defined in ITU-T Recommendation Y.2060 are as follows:

4.2.1.1 INTERCONNECTIVITY

With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

4.2.1.2 THINGS-RELATED SERVICES

The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

4.2.1.3 HETEROGENEITY

The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

[47] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items
[48] http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps

4.2.1.4 DYNAMIC CHANGES

The state of devices change dynamically, e.g., 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.

4.2.1.5 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 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 data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

4.2.2 IOT STANDARDS AND 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[49]. The urgent need for standardization and necessary improvements in interoperability are critical success factors for accelerated adoption of IoT systems[50]. This section provides an overview of the IoT related technical committees and standards currently active in the recognized Standardization Organizations to fill the gap in IoT standardization.

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

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

4.2.2.1 TECHNICAL COMMITTEES

4.2.2.1.1 ISO/IEC JTC 1/WG 7

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/WG 7**	**TITLE**	**Sensor networks**
CREATION DATE	2009	**MEMBERS** 	**Participating countries (24):** Republic of Korea, Australia, Austria, Canada, China, Finland, France, Germany, India, Israel, Japan, **Luxembourg**, Mexico, Netherlands, Norway, Pakistan, Saudi Arabia. Singapore, Slovenia, South Africa, Spain, Sweden, United Kingdom, United States
SECRETARIAT	KATS (Republic of Korea)		
SECRETARY	Ms. Jooran Lee		
CHAIRPERSON	Dr. Yongjin Kim		
ORGANIZATIONS IN LIAISON	DEWI, OGC, IEEE Instrumentation and Measurement Society TC 9, ITU-T SG 20		**Observing Countries (10):** Argentina, Bosnia and Herzegovina, Czech Republic, Hong Kong, Norway, Portugal, Serbia, Turkey, Uruguay, Zambia
WEB SITE	http://isotc.iso.org/livelink/livelink/open/jtc1wg7		
SCOPE	The ISO/IEC JTC 1/WG 7 has been established with the following Terms of Reference: 1) In the area of generic solutions for sensor networks, undertake standardization activities that support and can be applied to the technical work of all relevant JTC 1 entities and to other standards organizations. This includes activities in sensor networks such as the following: • Standardization of terminology; • Development of a taxonomy; • Standardization of reference architectures; • Development of guidelines for interoperability; • Standardization of specific aspects of sensor networks. 2) In the area of application - oriented sensor networks, identify gaps and commonalities that may impact standardization activities within the scope of JTC 1. Further, share this information with relevant entities within and outside of JTC 1. Unless better pursued within another JTC 1 entity, the following standardization activities may be pursued as projects by this Working Group: • Addressing the technology gaps within the scope of JTC 1 entities; • Exploiting technology opportunities where it is desirable to provide common approaches to the use of sensor networks across application domains; • Addressing emerging areas related to M2M and IoT. 3) In order to foster communication and sharing of information between groups working in the field of sensor networks: • Seek liaison relationships with all relevant JTC 1 SCs/WGs; • Seek liaison relationships with other organizations outside JTC 1 including but not limited to: relevant ISO TCs, IEC TCs and ITUĐT SGs, IEEE 1451, IEEE 1588, IEEE P2030, IEEE 802.15, Open Geospatial Consortium, ZigBee Alliance, IETF 6LoWPAN, IETF ROLL WG, ETSI, IPSO Alliance, EPCglobal, ISA 100, LONMARK, KNX Association, Zwave Alliance; • Consider the possibility of conducting joint projects with relevant ITUĐT SG; • Seek input from relevant research projects and *consortia.*		

STRUCTURE	/	
STANDARDIZATION WORK		
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/WG 7 (number includes updates): 12	
STANDARDS UNDER DEVELOPMENT	5	
INVOLVEMENT OF LUXEMBOURG		
1 DELEGATE	Mr. Shyam Wagle	ANEC GIE

COMMENTS

JTC 1/WG 7 has delivered International Standards on sensor networks since November 2009 when the Working Group was established directly under JTC 1. Initial and outstanding achievements of JTC 1/WG 7 are development and publication of Sensor Network Reference Architecture (SNRA): ISO/IEC 29182 Part 1 to Part 7. ISO/IEC 29182 series gives general overview, requirements, terminologies, views, entity models, interfaces to any users of sensor networks. Sensor Network and its Interface for Smart Grid System (ISO/IEC 30101:2014), Generic Sensor Network Application Interface (ISO/IEC 30128:2014), and Sensor Network Testing Framework (ISO/IEC 19637:2016) are also JTC 1/WG 7's main achievements.

JTC 1/WG 7 is currently developing International Standards on Underwater Acoustic Sensor Network (UWASN) and it will also, in cooperation with its Category C liaison DEWI (Dependable Embedded Wireless Infrastructure), develop Technical Reports on use-cases of sensor networks applications: aerospace, rail, building and automotive[51].

The current work program includes:

- ISO/IEC PDTR 22560, Information technology -- Sensor networks -- Use cases of aeronautics industry: Active Air-flow Control;
- ISO/IEC DIS 30140-1, Information technology -- Underwater acoustic sensor network (UWASN) -- Part 1: Overview and requirements;
- ISO/IEC FDIS 30140-2, Information technology -- Underwater acoustics sensor network (UWASN) -- Part 2: Reference architecture;
- ISO/IEC CD 30140-3, Information technology -- Underwater acoustics sensor network (UWASN) -- Part 3: Entities and interface;
- ISO/IEC CD 30140-4, Information technology -- Underwater acoustics sensor network (UWASN) -- Part 4: Interoperability.

Resolution 12 of the 31st Meeting of ISO/IEC JTC 1 (November 2017) establishes a new JTC 1/SC 41 "Internet of Things and related technologies" that will include JTC 1/WG 7. JTC 1/WG 7 activities will continue until the first JTC 1/SC 41 Plenary Meeting scheduled in June 2017.

Scope of JTC 1/SC 41

- 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.

[51] Source: BUSINESS PLAN FOR JTC 1/WG 7, Sensor networks for the Period: September 2016 to August 2017

4.2.2.1.2 ISO/IEC JTC 1/WG 10

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/WG 10**	TITLE	**Internet of Things (IoT)**
CREATION DATE	2014	MEMBERS 	**Participating countries (31):** Republic of Korea, Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, Germany, Hungary, India, Ireland, Israel, Italy, Japan, **Luxembourg**, Mexico, Netherlands, New Zealand, Norway, Russian Federation, Singapore, Slovenia, South Africa, Spain, Sweden, Switzerland, United Kingdom, United States
SECRETARIAT	KATS (Republic of Korea)		
SECRETARY	Ms. Yaeseul Park		
CHAIRPERSON	Mr. Sangkeun Yoo		
ORGANIZATIONS IN LIAISON	AIM Global, AIOTI/WG 3, ETSI, GS1, IEEE P2413, IIC, ITU-T, NIST CPS PWG, OGC, OMA DM, OMG, oneM2M, The Open Group, OCF, W3C		**Observing Countries (10):** Argentina, Bosnia and Herzegovina, Czech Republic, Hong Kong, Norway, Portugal, Serbia, Turkey, Uruguay, Zambia
WEB SITE	http://isotc.iso.org/livelink/livelink/open/jtc1wg10		

SCOPE	The ISO/IEC JTC 1/WG 10 has been established with the following Terms of Reference:
	• Serve as a focus of and proponent for JTC 1's IoT standardization program.
	• Develop foundational standards for IoT related to JTC 1 for guiding IoT efforts throughout JTC 1 upon which other standards can be developed.
	• The work will cover:
	  • Developing Terms and Definitions for JTC 1 IoT Vocabulary
	  • Developing IoT Reference Architecture and other foundational specifications as JTC 1 standards
	  • Continuing the work begun in SWG on IoT on standardization gaps
	  • Establishing a liaison with JTC 1, ISO, IEC or other entities undertaking work related to IoT
	  • Encouraging the prompt and efficient exchange of information within JTC 1 and with ISO, IEC, or other entities working on IoT, as appropriate
	  • Monitoring the ongoing IoT regulatory, market, business and technology requirements
	  • Developing other IoT standards that build on the foundational standards when relevant JTC 1 subgroups that could address these standards do not exist or are unable to develop them.		

STRUCTURE	/		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/WG 10 (number includes updates): 0		
STANDARDS UNDER DEVELOPMENT	4		

INVOLVEMENT OF LUXEMBOURG		
5 DELEGATES	Mr. Shyam Wagle	ANEC GIE
	Mr. Cyril Cassagnes	KPMG Luxembourg S.à r.l.
	Mr. Hervé Collignon	e-TIC Consulting S.à r.l.
	Mr. Jean Lancrenon	itrust consulting S.à r.l.
	Mr. Sankalp Ghatpande	itrust consulting S.à r.l.

COMMENTS

WG 10 is developing foundational standards for the Internet of Things (IoT) to meet IT industry requirements as well as user requirements.

In 2017, WG 10 will deliver two standards of note. One is the IoT Reference Architecture (IoT RA: ISO/IEC 30141) that defines reference models and architectural views, which can be used to create the architecture of a specific IoT system. Second is the Definition and Vocabulary for IoT (ISO/IEC 20924). Also, a Technical Report on IoT use cases will be published. The TR on IoT use cases will be continuously updated to collect additional use cases including interoperability, smart manufacturing and smart wearable devices[51].

The current WG 10 work program includes the following projects:

- ISO/IEC CD 20924, Information technology -- Internet of Things -- Definition and Vocabulary;
- ISO/IEC PDTR 22417, Information technology -- Internet of things (IoT) use cases;
- ISO/IEC CD 30141, Information technology -- Internet of Things -- Internet of Things Reference Architecture (IoT RA);
- ISO/IEC AWI 21823-1, Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework.

Resolution 12 of the 31st Meeting of ISO/IEC JTC 1 (November 2017) establishes a new JTC 1/SC 41 "Internet of Things and related technologies" that will include JTC 1/WG 10. JTC 1/WG 10 activities will continue until the first JTC 1/SC 41 Plenary Meeting scheduled in June 2017.

Scope of JTC 1/SC 41

- 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.

[52] Source: BUSINESS PLAN FOR ISO/IEC JTC 1/WG 10, Internet of Things (IoT) for the PERIOD COVERED: January 2017 – December 2017

4.2.2.1.3 ISO/IEC JTC 1/SC 31

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/SC 31**	TITLE	**Automatic identification and data capture techniques**
CREATION DATE	1996	MEMBERS 	**Participating Countries (25):** United States, Austria, Belgium, Brazil, Canada, China, Czech Republic, Denmark, France, Germany, India, Ireland, Israel, Japan, Kazakhstan, Republic of Korea, Netherlands, Peru, Philippines, Russian Federation, Slovakia, South Africa, Sweden, Switzerland, United Kingdom
SECRETARIAT	ANSI (United States)		
SECRETARY	Mr. Eddy Merrill		
CHAIRPERSON	Mr. Dan Kimball		
ORGANIZATIONS IN LIAISON	AIM Global, ETSI, Ecma International, GS1, IATA, ITU, OGC, UPU, NATO		**Observing Countries (21):** Argentina, Bosnia and Herzegovina, Colombia, Finland, Ghana, Hong Kong, Hungary, Indonesia, Islamic Republic of Iran, Italy, Kenya, **Luxembourg**, Malaysia, New Zealand, Romania, Serbia, Singapore, Spain, Thailand, Turkmenistan, Ukraine
WEB SITE	https://www.iso.org/committee/45332.html		
SCOPE	Standardization of data formats, data syntax, data structures, data encoding, and technologies for the process of automatic identification and data capture and of associated devices utilized in inter-industry applications and international business interchanges and for mobile applications.		
STRUCTURE	JTC 1/SC 31/WG 1 JTC 1/SC 31/WG 2 JTC 1/SC 31/WG 4	Data carrier Data structure Radio communications	
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 31 (number includes updates): 117		
STANDARDS UNDER DEVELOPMENT	30		
INVOLVEMENT OF LUXEMBOURG			
1 DELEGATE	Mrs. Maria Sotiri	POST Telecom S.A.	
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.

AIDC is an industry term that describes the identification and/or direct collection of data into a microprocessor-controlled device, such as a computer system or a programmable logic controller (PLC), without the use of a keyboard. AIDC technologies provide a reliable means not only to identify but also to track items. It is possible to encode a wide range of information, beginning with a basic item or the identification of a person, to comprehensive details about the item or person, e.g. item description, size, weight, color, etc.

ISO/IEC JTC 1/SC 31, Automatic identification and data capture techniques, is responsible for more than 100 published or in-progress standards in this area. These standards address bar code symbologies (how a bar code is created and read), RFID air interface (how an RFID tag is read), real-time locating systems, and mobile item identification (which explains how a device such as a phone is used to read and access data as well as providing standards to define how the data associated with the technology are stored and read).

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

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

It is also important to note that SC 31 is currently developing four standards regarding the Internet of Things in the supply chain:

- ISO/IEC AWI 18574, Information technology -- Internet of Things (IoT) in the supply chain -- Containerized cargo;
- ISO/IEC AWI 18575, Information technology -- Internet of Things (IoT) in the supply chain -- Products & product packages;
- ISO/IEC AWI 18576, Information technology -- Internet of Things (IoT) in the supply chain -- Returnable transport items (RTIs);
- ISO/IEC AWI 18577, Information technology -- Internet of Things (IoT) in the supply chain -- Transport units.

Moreover, SC 31 already published another standard 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.

4.2.2.1.4 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 (17):** Republic of Korea, Austria, Belgium, Canada, China, Denmark, Finland, France, India, Italy, Japan, Malaysia, Netherlands, Russian Federation, Sweden, United Kingdom, United States
SECRETARIAT	KATS (Republic of Korea)		
SECRETARY	Ms. Jooran Lee		
CHAIRPERSON	Mr François Coallier		
ORGANIZATIONS IN LIAISON	/		**Observing Countries (5):** Argentina, Ireland, **Luxembourg**, Mexico, Saudi Arabia
WEB SITE	http://www.iec.ch/dyn/www/f?p=103:29:2698958918431::::FSP_ORG_ID,FSP_LANG_ID:20486,25#3		
SCOPE	Standardization in the area of Internet of Things and related technologies. 1. Serve as the focus and proponent for JTC 1's standardization program on the Internet of Things and related technologies, including Sensor Networks and Wearables technologies. 2. Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things related applications.		
STRUCTURE	JTC 1/SC 41/WG 1 Sensor Networks JTC 1/SC 41/WG 2 Internet of Things		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 41 (number includes updates): 0		
STANDARDS UNDER DEVELOPMENT	0		
INVOLVEMENT OF LUXEMBOURG			
1 DELEGATE	Mr. Shyam Wagle	ANEC GIE	
COMMENTS			

ISO/IEC JTC 1/SC 41 "Internet of Things and related technologies", is still under construction. It has been established on the basis of the Resolution 12 of the 31st Meeting of ISO/IEC JTC 1 (November 2017).

Its work program will include, at the beginning, the current work programs of ISO/IEC JTC 1/WG 7 and WG10. The activities of the WGs will continue until the first JTC 1/SC 41 Plenary Meeting scheduled in June 2017.

A Study Group on Wearables should also be created in the SC 41. Some discussions also suggest the possibility to create a WG dedicated to Smart Manufacturing. The final structure, scope and work program will be discussed during the first plenary meeting of JTC 1/SC 41, as well as the liaisons to be established. Registration in this SC is already opened for interested national stakeholders.

4.2.2.2 STANDARDS

4.2.2.2.1 Published Standards

This section details the standards already published by the recognized SDO regarding Internet of Things (non-exhaustive list). The linked standards below are publicly available.

SDO	REFERENCE	TITLE
ISO/IEC JTC 1	ISO/IEC 29161:2016	Information technology -- Data structure -- Unique identification for the Internet of Things
ETSI	ETSI TR 103 290 (04/2015)	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
ETSI	ETSI TR 103 375 (10/2016)	SmartM2M; IoT Standards landscape and future evolutions
ETSI	ETSI TR 103 376 (10/2016)	SmartM2M; IoT LSP use cases and standards gaps

4.2.2.2.2. Standards under development

This section details the standards under development regarding Internet of Things in the recognized SDO (non-exhaustive list).

SDO	REFERENCE	TITLE
ISO/IEC JTC 1	ISO/IEC CD 20924	Information technology -- Internet of Things -- Definition and Vocabulary
ISO/IEC JTC 1	ISO/IEC AWI 21823-1	Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework
ISO/IEC JTC 1	ISO/IEC PDTR 22417	Information technology -- Internet of things (IoT) use cases
ISO/IEC JTC 1	ISO/IEC CD 30141	Information technology -- Internet of Things -- Internet of Things Reference Architecture (IoT RA)
ISO/IEC JTC 1	ISO/IEC AWI 18574	Information technology -- Internet of Things (IoT) in the supply chain -- Containerized cargo
ISO/IEC JTC 1	ISO/IEC AWI 18575	Information technology -- Internet of Things (IoT) in the supply chain -- Products & product packages
ISO/IEC JTC 1	ISO/IEC AWI 18576	Information technology -- Internet of Things (IoT) in the supply chain -- Returnable transport items (RTIs)
ISO/IEC JTC 1	ISO/IEC AWI 18577	Information technology -- Internet of Things (IoT) in the supply chain -- Transport units
ETSI	ETSI GR IP6 008	IPv6-based Internet of Things; Deployment of IPv6-based Internet of Things
ETSI	ETSI TR 118 519	oneM2M Dynamic Authorization for IoT
ETSI	ETSI TR 103 467	Speech and multimedia Transmission Quality (STQ); Quality of Service aspects for IoT; Discussion of QoS aspects of services related to the IoT ecosystem
ETSI	ETSI SR 003 438	USER; User centric approach in IoT
ETSI	ETSI PWI BOARDM2M IOT 1501 v1	SmartM2M; oneM2M platform for AIOTI (Alliance for Internet of Things Innovation), a common interworking framework for information sharing

4.3 BIG DATA

The Big Data is 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"[53].

In the definition of Big Data specified in 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[54] is as follow:

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

4.3.1 CHARACTERISTICS[55]

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[56]. 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[57]. 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[58]. This additional V in combination with the original 3Vs will be used in this report to refer to the characteristics of Big Data, which are depicted and described in Table 2 and Figure 5 respectively.

[53] 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.

[54] ISO/IEC 20546:Information technology — Big data — Definition and vocabulary

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

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

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

[58] 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
Volume	How much data: the amount of data that organizations try to harness to improve decision-making across the enterprise.
Velocity	How fast data is created: the speed of incoming data and how quickly it can be made available for analysis (e.g. payment data from credit cards and location data from mobile phones).
Variety	The various types of data: the different types of structured and unstructured data that an organization can collect, such as transaction-level data, text and log files and audio or video.
Veracity	How accurate the data is: the trust in the data which might be impaired by the data being uncertain, imprecise or inherently unpredictable (e.g. trustworthiness, origin, and reputation of the data source).

Table 2: The four characteristics of Big Data

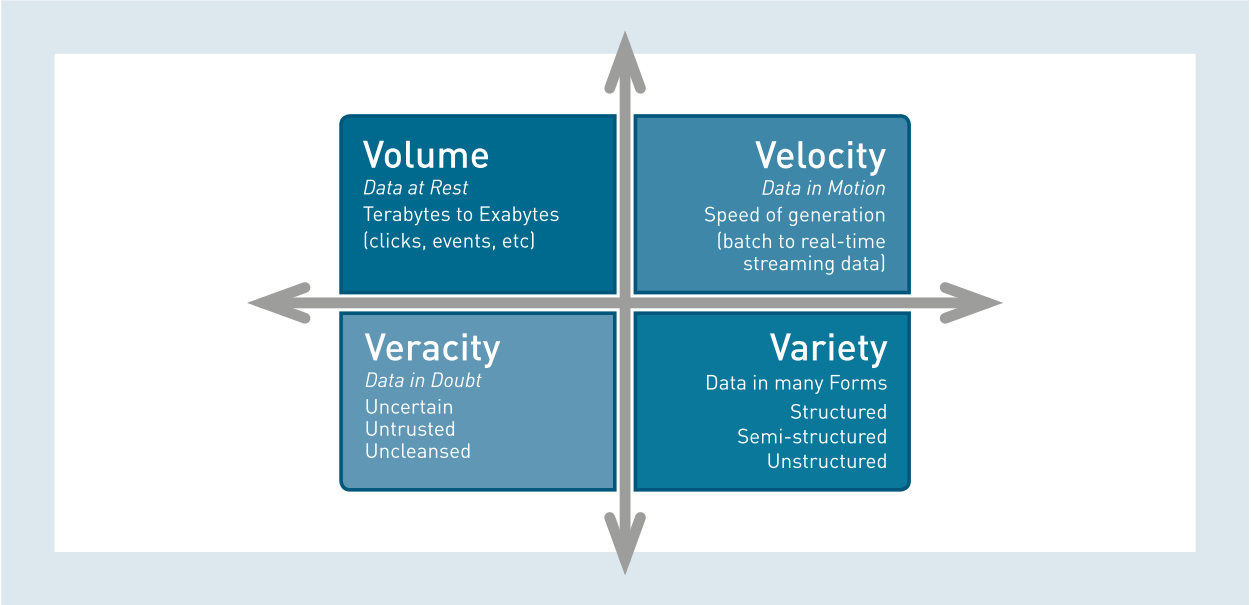


Figure 5: The four Vs of Big Data

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 [59]:

- **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.

[59] 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[60].

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

4.3.2 BIG DATA STANDARDS AND STANDARDIZATION TECHNICAL COMMITTEES

Standards for 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 Big Data. This occurs when analytics designers tweak a model repeatedly to fit the data and begin to interpret noise or randomness as truth. Another potential benefit of standardization for Big Data is the ability to support the integration of multiple data sources. Security and Privacy are of paramount importance for both data quality and for protection. Some of the large volume of data come from social media and medical records and inherently contain private information. Analysis of such data, particularly in conjunction with its context, must protect privacy. 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. This section provides an overview of the Big Data related technical committees and standards currently active in the recognized Standardization Organizations.

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

4.3.2.1 TECHNICAL COMMITTEES

4.3.2.1.1 ISO/IEC JTC 1/WG 9

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/WG 9**	TITLE	**Big Data**
CREATION DATE	2014	MEMBERS 	**Participating countries (26):** United States, Australia, Austria, Brazil, Canada, China, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Republic of Korea, **Luxembourg**, Mexico, Netherlands, Norway , Russian Federation, Singapore, Slovenia, South Africa, Spain, Sweden, United Kingdom
SECRETARIAT	United States (ANSI)		
SECRETARY	Ms. Sally Seitz		
CHAIRPERSON	Mr. Wo Chang		
ORGANIZATIONS IN LIAISON	OGC, IIC, ITU-T SG 13		
WEB SITE	http://isotc.iso.org/livelink/livelink/open/jtc1wg9		
SCOPE	The ISO/IEC JTC 1/WG 9 has been established with the following Terms of Reference: • Serve as the focus of and proponent for JTC 1's Big Data standardization program. • Develop foundational standards for Big Data ---including reference architecture and vocabulary standards---for guiding Big Data efforts throughout JTC 1 upon which other standards can be developed. • Develop other Big Data standards that build on the foundational standards when relevant JTC 1 subgroups that could address these standards do not exist or are unable to develop them. • Identify gaps in Big Data standardization. • Develop and maintain liaisons with all relevant JTC 1 entities as well as with any other JTC 1 subgroup that may propose work related to Big Data in the future. • Identify JTC 1 (and other organization) entities that are developing standards and related material that contribute to Big Data, and where appropriate, investigate ongoing and potential new work that contributes to Big Data. • Engage with the community outside of JTC 1 to grow the awareness of and encourage engagement in JTC 1 Big Data standardization efforts within JTC 1, forming liaisons as is needed.		
STRUCTURE	/		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/WG 9 (number includes updates): 0		
STANDARDS UNDER DEVELOPMENT	5		

INVOLVEMENT OF LUXEMBOURG		
7 DELEGATES	Mr. Johnatan Pecero	ANEC GIE
	Mr. Shyam Wagle	ANEC GIE
	Mr. Christophe Delogne	BGL BNP Paribas
	Mr. Cyril Cassagnes	KPMG Luxembourg S.à r.l.
	Mr. Emmanuel Kieffer	University of Luxembourg
	Mrs. Aida Horaniet	Docler Holding S.à r.l.
	Mrs. Natalia Cassagnes	Actimage S.A.

COMMENTS

The current WG 9 work program includes the development of two foundational International Standard:

- ISO/IEC CD 20546, Big Data -- Definition and Vocabulary;
- ISO/IEC 20547, which specifies the Big Data Reference Architecture (BDRA) and includes the Big Data roles, activities, and functional components and their relationships. It is composed of 5 parts:
  - ISO/IEC AWI TR 20547-1, Information technology -- Big Data Reference Architecture -- Part 1: Framework and Application Process;
  - ISO/IEC PDTR 20547-2, Information technology -- Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements;
  - ISO/IEC AWI 20547-3, Information technology -- Big Data Reference Architecture -- Part 3: Reference Architecture;
  - ISO/IEC AWI 20547-4, Information technology -- Big Data Reference Architecture -- Part 4: Security and Privacy Fabric (under the responsibility of JTC 1/SC 27);
  - ISO/IEC PDTR 20547-5, Information technology -- Big Data Reference Architecture -- Part 5: Standards Roadmap.

It has to be noted that the 4th part of ISO/IEC 20547, dedicated to security and privacy aspects of the BDRA, is developed under the direct responsibility of ISO/IEC JTC 1/SC 27 (IT security techniques) in close collaboration with ISO/IEC JTC 1/WG 9.

4.3.2.1.2 ISO/IEC JTC 1/SC 32

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/SC 32**	TITLE	**Data management and interchange**
CREATION DATE	1997	MEMBERS 	**Participating Countries (14):** United States, Canada, China, Czech Republic, Côte d'Ivoire, Egypt, Finland, Germany, India, Japan, Kazakhstan, Republic of Korea, Russian Federation, United Kingdom
SECRETARIAT	ANSI (USA)		
SECRETARY	Ms. Michaela Miller		
CHAIRPERSON	Mr. Jim Melton		
ORGANIZATIONS IN LIAISON	Infoterm, UNECE		**Observing Countries (22):** Argentina, Austria, Belgium, Bosnia and Herzegovina, France, Ghana, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Italy, **Luxembourg**, Netherlands, Poland, Portugal, Romania, Serbia, Spain, Switzerland, Turkey, Ukraine
WEB SITE	https://www.iso.org/committee/45342.html		
SCOPE	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 JTC 1/SC 32/WG 4 SQL/Multimedia and application packages		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 32 (number includes updates): 77		
STANDARDS UNDER DEVELOPMENT	26		
INVOLVEMENT OF LUXEMBOURG			
1 DELEGATE	Mr. Johnatan Pecero (Acting as Chairman) ANEC GIE		

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 9075-1:2011, Information technology -- Database languages -- SQL -- Part 1: Framework (SQL/ Framework) (under revision); • ISO/IEC 11179-1:2004, Information technology -- Metadata registries (MDR) -- Part 1: Framework (under revision); • ISO/IEC 19503:2005, Information technology -- XML Metadata Interchange (XMI); • ISO/IEC 19763-1:2015, Information technology -- Metamodel framework for interoperability (MFI) -- Part 1: Framework. Current work program of JTC 1/SC 32 includes for example: • The revision of the ISO/IEC 9075 series of standards concerning the SQL database language; • The development of ISO/IEC AWI 21838 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 topics of next generation analytics and big data appear frequently both in computing industry and more general news reports. SC 32 initiated a study group in these areas and delivered a preliminary report to JTC 1 that identified existing SC 32 standards that support these technologies and opportunities for enhancing work in these areas. SC 32 is well-represented in meetings of JTC 1/WG 9.

4.3.2.2 STANDARDS

4.3.2.2.1 Published Standards

There are currently no published standards directly related to Big Data.

4.3.2.2.2 Standards under development

This section details the standards under development regarding Big Data in the recognized SDO (non-exhaustive list).

SDO	REFERENCE	TITLE
ISO/IEC JTC 1	ISO/IEC NP 20546	Information technology -- Big Data -- Overview and Vocabulary
ISO/IEC JTC 1	ISO/IEC NP 20547-1	Information technology -- Big Data -- Reference Architecture -- Part 1: Framework and Application Process
ISO/IEC JTC 1	ISO/IEC NP 20547-2	Information technology – Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
ISO/IEC JTC 1	ISO/IEC NP 20547-3	Information technology -- Big Data Reference Architecture – Part 3: Reference Architecture
ISO/IEC JTC 1	ISO/IEC NP 20547-4	Information technology -- Big Data Reference Architecture – Part 4: Security and Privacy Fabric
ISO/IEC JTC 1	ISO/IEC NP 20547-5	Information technology – Big Data Reference Architecture -- Part 5: Standards Roadmap

4.4 DIGITAL TRUST IN SMART ICT

Trust in Information and Communications Technology (ICT) systems can be explained as a computational construct whose value depends on the context and is likely to change over time[61]. 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 the initial state. Thus, building and maintaining trust is essential and requires a constant effort from the ICT service providers.

Apart from the general technical challenges of developing interconnected Smart technologies related to Cloud Computing, Internet of Things and Big Data, Digital Trust is steadily becoming an increasingly significant challenge that must be addressed[62]. 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. 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.

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[63]. This section presents the basic components of Digital Trust that are involved in any ICT system: Privacy, Data, and Information Security and Interoperability.

4.4.1 BASIC COMPONENTS OF DIGITAL TRUST

4.4.1.1 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[64]. In a study about privacy behaviors regarding information technology, Acquisti *et al.*[65] 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[66] and if other individuals have already agreed to share the information[67]. Privacy is **malleable**, meaning that the acceptable level of privacy is often determined by a *construction* instead of a

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

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

[63] 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.

[64] 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.

[65] 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

[66] 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.

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

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

4.4.1.2 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 paper 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[68] 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[69]. 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.

4.4.1.3 INTEROPERABILITY

Interoperability of 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[70] [12]. However, in its various definitions, system interoperability is mainly composed of two criteria:

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

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

[69] 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.

[70] 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

4.4.2 STANDARDIZATION TECHNICAL COMMITTEES IN DIGITAL TRUST

This section provides an overview of the Digital Trust related technical committees, from the perspective of three pillars of Smart ICT: Cloud Computing, Internet of Things and Big Data, currently active in the recognized Standardization Organizations.

4.4.2.1 ISO/IEC JTC 1/SC 17

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/SC 17**	**TITLE**	**Cards and personal identification**
CREATION DATE	1987	**MEMBERS** 	**Participating Countries (33):** United Kingdom, Armenia, Australia, Austria, Belgium, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Israel, Italy, Japan, Kenya, Republic of Korea, **Luxembourg**, Malaysia, Netherlands, Norway, Poland, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, United States
SECRETARIAT	BSI (United Kingdom)		
SECRETARY	Ms. Jean Stride		
CHAIRPERSON	Mr. Peter Waggett		
ORGANIZATIONS IN LIAISON	AMEX, CCETT, Ecma International, IATA, ICAO, ICMA, ILO, MasterCard International, MasterCard Europe, VISA, VISA EUROPE, NFC Forum, UNECE, JAVA CARD FORUM, EUDCA		**Observing Countries (19):** Argentina, Bosnia and Herzegovina, Croatia, Ghana, Hong Kong, Hungary, Iceland, Indonesia, Islamic Republic of Iran, Ireland, Kazakhstan, Lithuania, New Zealand, Portugal, Serbia, Thailand, Turkey, Ukraine, Viet Nam
WEB SITE	https://www.iso.org/committee/45144.html		
SCOPE	The current area of work for JTC 1/SC 17 consists of: • Identification and related documents; • Cards; • Devices associated with their use in inter-industry applications and international interchange.		
STRUCTURE	JTC 1/SC 17/CAG 1	Chairman advisory group	
	JTC 1/SC 17/WG 1	Physical characteristics and test methods for ID-cards	
	JTC 1/SC 17/WG 3	Identification cards - Machine readable travel documents	
	JTC 1/SC 17/WG 4	Integrated circuit card with contacts	
	JTC 1/SC 17/WG 5	Registration Management Group (RMG)	
	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 Standardization work	

STANDARDIZATION WORK		
PUBLISHED STANDARDS	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 17 (number includes updates): 110	
STANDARDS UNDER DEVELOPMENT	42	
INVOLVEMENT OF LUXEMBOURG		
4 DELEGATES	Mr. Valentin Lacave (Chairman)	Telindus Luxembourg S.A.
	Mr. Benoit Poletti	INCERT GIE
	Mr. Abdelkrim Nehari	INCERT GIE
	Mr. Enrico Ozzano	BIL S.A.

COMMENTS

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

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

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

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

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

Current work 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.

4.4.2.2 ISO/IEC JTC 1/SC 27

GENERAL INFORMATION			
COMMITTEE	**ISO/IEC JTC 1/SC 27**	**TITLE**	**IT Security techniques**
CREATION DATE	1989	**MEMBERS** 	**Participating Countries (55):** Germany, Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, Côte d'Ivoire, Cyprus, Czech Republic, Denmark, Finland, France, India, Indonesia, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, Republic of Korea, Lebanon, **Luxembourg**, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, Rwanda, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay
SECRETARIAT	DIN (Germany)		
SECRETARY	Ms. Krystyna Passia		
CHAIRPERSON	Mr. Walter Fumy		**Observing Countries (20):** Belarus, Bosnia and Herzegovina, Costa Rica, El Salvador, Estonia, Ghana, Hong Kong, Hungary, Iceland, Islamic Republic of Iran, Lithuania, Morocco, State of Palestine, Portugal, Saudi Arabia, Serbia, Slovenia, Swaziland, Thailand, Turkey
ORGANIZATIONS IN LIAISON	(ISC)2, CCETT, Cloud security alliance, ECBS, ENISA, EPC, ETSI, Ecma International, IEEE, ISACA, ISSEA, ITU, MasterCard International, MasterCard Europe, CCBD, TCG, Opengroup UK, TMForum, ISA, ABC4Trust, CSCC, INLAC, TAS3, Cyber Security, PRACTICE, ISF, OECD, FIRST, OIDF, PQCCRYPTO, WITDOM, Kantara Initiative, ISCI, PRIPARE, EuroCloud, PICOS, Article 29 Data Protection Working Party, Interpol, ETSI, TREsPASS, EUDCA		
WEB SITE	https://www.iso.org/committee/45306.html		
SCOPE	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: • Security requirements capture methodology; • Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls and services; • Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; • Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; • Security aspects of identity management, biometrics and privacy; • Conformance assessment, accreditation and auditing requirements in the area of information security; • Security evaluation criteria and methodology. SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.		

STRUCTURE	JTC 1/SC 27/SWG-M	Special Working Group on Management
	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	Number of published ISO/IEC standards under the direct responsibility of JTC 1/SC 27 (number includes updates): 164	
STANDARDS UNDER DEVELOPMENT	63	
INVOLVEMENT OF LUXEMBOURG		
28 DELEGATES	Mr. Benoit Poletti (Chairman)	INCERT GIE
	Mr. Cédric Mauny (Vice-Chairman)	Telindus Luxembourg S.A.
	Mr. Carlo Harpes (Vice-Chairman)	itrust consulting S.à.r.l.
	Mr. Tom Leclerc	Telindus Luxembourg S.A.
	Mr. Peter Schaffer	Ernst & Young Business Advisory Services S.à.r.l.
	Mr. Olivier Montee	Cours@home Luxembourg S.à.r.l. Luxembourg
	Mr. Stéphane Cortina	Institute of Science and Technology (LIST)
	Mr. Hervé Cholez	LIST
	Mr. Nicolas Mayer	LIST
	Mr. Qiang Tang	LIST
	Mr. René Saint-Germain	ALTIRIAN S.A.
	Mr. Sébastien Poggi	Victor Buck Services S.A.
	Mr. Alex Mckinnon	itrust consulting S.à.r.l.
	Mr. Matthieu Aubigny	itrust consulting S.à.r.l.
	Mr. Jean Lancrenon	itrust consulting S.à.r.l.
	Mr. Sankalp Ghatpande	itrust consulting S.à.r.l.
	Mrs. Shenglan Hu	POST Telecom PSF S.A.
	Mrs. Myriam Djerouni	Banque de Luxembourg S.A.
	Mrs. Emelyne Baudrier	Luxembourg Conseil S.à.r.l.
	Mr. David Naramski	NOWINA SOLUTIONS S.à.r.l.
	Mrs. Mélanie Gagnon	MGSI S.à.r.l.
	Mr. Serge Raucq	Vectif ACF S.A.
	Mr. Clement Gorlt	INCERT GIE
	Mrs. Hatice Baskaya	INCERT GIE
	Mr. Gaëtan Pradel	INCERT GIE
	Mr. Enrico Ozzano	BIL S.A.
	Mr. Benoit Bertholon	COINPLUS S.A.
	Mr. Nicolas Domenjoud	ANEC GIE

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

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.

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.).

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.

The WG 4 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).

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

Standards

The best-known standard developed by SC 27 are ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements and ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls. Organizations setting up an ISMS certified compliant with ISO/IEC 27001 are increasingly numerous[71].

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

- ISO/IEC 27018:2014, Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 27017:2015, Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27036-4:2016, Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services;
- ISO/IEC CD 19086-4, Information technology -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Security and privacy.
- Similarly, a standard concerning Big Data security and privacy is currently under development in JTC 1/SC 27, in close collaboration with ISO/IEC JTC 1/WG 9 on Big Data:
- ISO/IEC AWI 20547-4, Information technology -- Big data reference architecture -- Part 4: Security and privacy fabric.

[71] Source: ISO survey 2015

4.4.2.3 ISO/TC 46/SC 11

GENERAL INFORMATION			
COMMITTEE	**ISO/TC 46/SC 11**	TITLE	**Archives/records management**
CREATION DATE	1998	MEMBERS 	**Participating Countries (31):** Australia, Belgium, Bulgaria, Canada, Chile, China, Colombia, Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Japan, Kenya, Republic of Korea, **Luxembourg**, Malaysia, Netherlands, New Zealand, Norway, Portugal, Russian Federation, South Africa, Spain, Sweden, Switzerland, Ukraine, United Kingdom, United States
SECRETARIAT	SA (Australia)		
SECRETARY	Ms. Clare Hobern		
CHAIRPERSON	Ms. Judith Ellis		
ORGANIZATIONS IN LIAISON	ICA, IRMT, InterPARES		**Observing Countries (17):** Argentina, Austria, Brazil, Cuba, Denmark, Greece, Iceland, Islamic Republic of Iran, Lithuania, Poland, Romania, Serbia, Singapore, Slovakia, Slovenia, Sri Lanka, Thailand
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/WG 1	Metadata	
	TC 46/SC 11/WG 7	Digital Records preservation	
	TC 46/SC 11/WG 8	Management of systems for records	
	TC 46/SC 11/WG 10	Implementation Guidelines for the disposition of records	
	TC 46/SC 11/WG 14	Records requirements in enterprise Architecture	
	TC 46/SC 11/WG 15	Appraisal for Managing Records	
	TC 46/SC 11/WG 16	Systems design for records	
	TC 46/SC 11/WG 17	Records in the cloud	
STANDARDIZATION WORK			
PUBLISHED STANDARDS	Number of published ISO standards under the direct responsibility of TC 46/SC 11 (number includes updates): 17		
STANDARDS UNDER DEVELOPMENT	4		
INVOLVEMENT OF LUXEMBOURG			
6 DELEGATES	Mr. Lucas Colet (Chairman)	PricewaterhouseCoopers SC	
	Mrs. Sylvie Forastier	Linklaters LLP	
	Mr. Alain Wahl	ILNAS	
	Mr. Serge Raucq	Vectis ACF S.A.	
	Mr. Michel Picard	Luxembourg Institute of Science and Technology (LIST)	
	Mr. Henri Montin	*Centre des Technologies de l'Information de l'Etat*	

COMMENTS
ISO/TC 46/SC 11 is responsible for the standardization of 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 the following standards: • ISO/FDIS 17068, Information and documentation -- Trusted third party repository for digital records (revision); • ISO/FDIS 23081-1, Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles; • ISO/NP TR 21965, Information and documentation -- Records management in enterprise architecture; • ISO/NP TS 21946, Information and documentation -- Appraisal for managing records.

4.4.2.4 ETSI/TC CYBER

GENERAL INFORMATION			
COMMITTEE	**ETSI/TC CYBER**	TITLE	**Cyber Security**
CREATION DATE	2014	MEMBERS 	134 member organizations of ETSI
CHAIRPERSON	Mr. Charles Brookson		
ORGANIZATIONS IN LIAISON	CEN, CENELEC, ENISA, Eurosmart, GIFSI, ISO/IEC JTC 1, TCG, TTA		
WEB SITE	https://portal.etsi.org/cyber		
SCOPE	The activities of ETSI TC CYBER include the following broad areas: • Cyber Security • Security of infrastructures, devices, services and protocols • Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators • Security tools and techniques to ensure security • Creation of security specifications and alignment with work done in other TCs.		
STRUCTURE	/		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	18		
STANDARDS UNDER DEVELOPMENT	14		
INVOLVEMENT OF LUXEMBOURG			
Note: ILNAS is monitoring the developments of the ETSI/TC CYBER.			

COMMENTS

ETSI/TC CYBER is responsible for the standardization of cyber security and for providing a center of relevant security expertise. In addition, TC CYBER is working in cooperation with the CEN and the CENELEC in response to European Commission (EC) Mandate M/530 on Privacy by Design.

The work program of TC CYBER include the following projects:

- DTR/CYBER-QSC-007, CYBER; Quantum safe key exchanges;
- DTR/CYBER-QSC-008, CYBER; Quantum Safe Signatures;
- DTR/CYBER-QSC-009, CYBER; Quantum Safe Virtual Private Networks;
- DTS/CYBER-0024, CYBER; Critical Infrastructure Metrics for Identification of CI;
- DTS/CYBER-0025, CYBER; Attribute Based Encryption for Attribute Based Access Control;
- ETSI TS 102 165-1, CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA);
- ETSI TS 102 165-2, CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures;
- ETSI TR 103 370, CYBER; Practical introductory guide to privacy;
- ETSI TR 103 421, CYBER; Network Gateway Cyber Defence;
- ETSI TR 103 456, CYBER; Implementation of the Network and Information Security (NIS) Directive
- ETSI TS 103 457, CYBER; Specifying a common interface to transfer sensitive functions to a trusted domain;
- ETSI TS 103 458, CYBER; Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services
- 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, CYBER; Middlebox Security Protocol.

4.4.2.5 ETSI/TC ESI

GENERAL INFORMATION			
COMMITTEE	**ETSI/TC ESI**	TITLE	**Electronic Signatures and Infrastructures**
CREATION DATE	/	MEMBERS 	71 member organizations of ETSI
CHAIRPERSON	Mr. Riccardo Genghini		
ORGANIZATIONS IN LIAISON	CAB Forum, CEN, CENELEC, EA, ENISA, Eurosmart, ISO, ISO/IEC JTC 1, ISOC/IETF, ITU, OASIS, SAFE-BioPharma, TTA, UNECE, UPU		
WEB SITE	http://portal.etsi.org/esi		
SCOPE	TC ESI is the lead body within ETSI in relation to Electronic Signatures and Infrastructures, including the preparation of reports and other necessary activities, by: • Developing generic standards, guides and reports relating to electronic signatures and related trust infrastructures to protect electronic transactions and ensure trust and confidence with business partners; • Liaising with other ETSI bodies in relation to electronic signatures and related trust infrastructures; • Liaising with bodies external to ETSI in relation to electronic signatures and related trust infrastructures; • Establishing a continuing work plan in relation to electronic signatures and related trust infrastructures.		
STRUCTURE	/		
STANDARDIZATION WORK			
PUBLISHED STANDARDS	201		
STANDARDS UNDER DEVELOPMENT	51		
INVOLVEMENT OF LUXEMBOURG			
3 COMPANIES	• eWitness S.A. • Luxtrust • POST Luxembourg Note: ILNAS is also monitoring the 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. The ETSI strategy is in line with, and endorsed by the initiative of the EU Commission to establish a harmonized infrastructure for electronic signatures. In this frame, ETSI/TC ESI works, in collaboration will CEN TC 224, on the execution of EC Mandate M/460 to provide a rationalized framework for digital signatures standardization.

4.4.2.6 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. Caroline De Condé		
CHAIRPERSON	Mr. Franck Leroy		
ORGANIZATIONS IN LIAISON	ANEC, FRONTEX, GlobalPlatform, UIC		
WEB SITE	http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_LANG_ID,FSP_ORG_ID:25,6205&cs=1A98C573151AB3D7A22712120D94364C1#1		
SCOPE	The development of standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy in a multi sectorial environment. It covers: • Operations such as applications and services like electronic identification, electronic signature, payment and charging, access and border control; • Personal devices with secure elements independently of their form factor, such as cards, mobile devices, and their related interfaces; • Security services including authentication, confidentiality, integrity, biometrics, protection of personal and sensitive data; • System components such as accepting devices, servers, cryptographic modules; CEN/TC 224 multi-sectorial environment involves sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and providers from the supply side such as card manufacturers, security technology, conformity assessment body, software manufacturers.		
STRUCTURE	CEN/TC 224/WG 6	User Interface	
	CEN/TC 224/WG 11	Transport applications	
	CEN/TC 224/WG 15	European citizen card	
	CEN/TC 224/WG 16	Application Interface for smart cards used as Secure Signature Creation Devices	
	CEN/TC 224/WG 17	Protection Profiles in the context of SSCD	
	CEN/TC 224/WG 18	Biometrics	
	CEN/TC 224/WG 19	Breeder Documents	
STANDARDIZATION WORK			
PUBLISHED STANDARDS	51		
STANDARDS UNDER DEVELOPMENT	22		

INVOLVEMENT OF LUXEMBOURG		
3 DELEGATES	Mr. Benoit Poletti (Chairman)	INCERT GIE
	Mrs. Shenglan Hu	POST Telecom PSF
	Mr. Enrico Ozzano	BIL S.A.

COMMENTS

As a matter of principle, CEN/TC 224 does not duplicate the work of ISO/IEC JTC 1/SC 17 but, either transposes some of the related International Standards or uses them as the basis for specific European works. In a number of cases, the ultimate objective of the work of CEN/TC 224 is to contribute to international standardization.

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

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

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

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

CEN/TC 224 is particularly involved in the development of standards under the standardization mandate M/460 concerning Electronic Signatures. In this context, it is currently developing standards on protection profiles for signature creation and verification application (EN 419111 series), an application interface for secure elements for electronic identification, authentication and Trusted Services (EN 419212 series), and trustworthy systems supporting server signing (EN 419241 series).

5 OPPORTUNITIES FOR THE NATIONAL MARKET

The previous Chapters highlight that world market trend is following three ICT technologies: Cloud Computing, Internet of Things and Big Data in the ICT sector and Luxembourg is also not apart from it. In this report, these three elements are presented as the main pillars of Smart ICT technology. Standardization is important to make all these Smart ICT components interoperable, but also to guarantee the security and safety of the next digital world, for example with the support of Digital Trust related standards.

The purpose of this sector-based standards analysis is to involve identified national stakeholders in a standardization approach 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 and standardization offers them unique opportunities to participate in designing the future global ICT landscape.

The ICT sector is, at national level, the most mature standardization sector. Luxembourg is notably registered as "O-member"[72] of ISO/IEC JTC 1, and 72 delegates from Luxembourg are currently involved in international and European technical committees from the ICT sector. Among them, 49 are directly involved in Smart ICT and/or Digital Trust related technical committees (Cloud Computing: 13; Internet of Things: 6; Big Data: 7; Digital Trust: 35). However, considering the rich and vibrant ecosystem of organizations involved in the ICT sector in Luxembourg, ILNAS believes that the active technical committees in Smart ICT standardization could still attract more national stakeholders and make them benefit from related opportunities. In this way, ILNAS, with the support of ANEC GIE, is following closely the Smart ICT related technical committees, listed below, in order to provide the most relevant information to the national ICT community and to facilitate their involvement in the technical committees.

- ISO/IEC JTC 1 SC 38 Cloud Computing and Distributed Platforms
- ISO/IEC JTC 1 WG 7 Sensor Networks (will be integrated to ISO/IEC JTC 1 SC 41 in the beginning of June 2017)
- ISO/IEC JTC 1 WG 10 Internet of Things (will be integrated to ISO/IEC JTC 1 SC 41 in the beginning of June 2017)
- ISO/IEC JTC 1 SC 41 Internet of Things and related Technologies
- ISO/IEC JTC 1 WG 9 Big Data
- And the committees related to Digital Trust

ILNAS, with the support of ANEC GIE, actively contributes to inform them and support their normative steps. The opportunities presented in this Chapter should be seen by national stakeholders as a series of proposals, which could lead to go further and to engage in future actions in order to more rapidly 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.

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

5.1 INFORMATION ABOUT STANDARDIZATION

5.1.1 SMART ICT WORKSHOPS

In order to disseminate the ICT standardization knowledge with the related community in Luxembourg (ISO/IEC JTC 1, ETSI, ICT fora and consortia, etc.), ILNAS organizes, at national level in collaboration with ANEC GIE, workshops in the framework of ICT prospective and, more specifically in the domain of "Smart ICT".

For instance, the organization of a series of breakfasts dedicated to the promotion of Smart ICT standardization and Digital Trust in 2016 and 2017. Indeed, in relation with the publication of the White Paper "Digital Trust for Smart ICT", four workshops were organized from October 2016 to March 2017 in order to discuss the role of Digital Trust topic in the adoption and widespread use of Smart ICT. Beyond the technical aspects, latest related standardization developments are presented to highlight their importance for the establishment of a trusted digital environment. This series of breakfasts review various Smart technologies, focusing on the Cloud Computing, Internet of Things, and Big Data, the three topics developed in the White Paper, through the prisms of Digital Trust and standardization. They were organized to bring together national stakeholders of dedicated Smart ICT subsectors and to provide them with the relevant standardization knowledge and facilitate their engagement in the standards development process. In this manner, ILNAS organizes information sessions dedicated to technical standardization of a specific Smart ICT subsector, on a regular basis.

Moreover, ILNAS aims at managing and reinforcing the National Mirror Committees dedicated to Smart ICT (e.g.: ISO/IEC JTC 1/WG 9 for Big Data, ISO/IEC JTC 1/SC 38 for Cloud Computing, ISO/IEC JTC 1/SC 41 for IoT and related technologies, etc.). In this frame, the institute will organize meetings of these NMC, which represent a good opportunity for interested national stakeholders to strengthen their commitment into the process of technical standardization.

5.1.2 AWARENESS SESSIONS

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

To facilitate the organization of such awareness, interested stakeholders can fill a declaration of interest in ICT standardization[73] to be contacted by ILNAS and ANEC GIE.

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

5.1.3 SMART ICT STANDARDS WATCH

The primary objective of this report is to facilitate the identification of technical committees in the Smart ICT area that meet organizations' potential interests. The Luxembourg's Standard Analysis of the ICT Sector (ANS TIC V7.0[74]) gives a wider overview of related standardization technical committees in the ICT sector. The main objective of the standards analysis of the ICT sector is to present the most appropriate document to quickly get an overview of the ICT standardization landscape and select the technical committees to be followed.

Moreover, ILNAS, with the support of ANEC GIE, 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 final result and some additional steps can be proposed by ILNAS and ANEC GIE, like the registration in a technical committee to allow the follow-up of the relevant standardization developments by the requesting organization.

5.1.4 PUBLICATIONS AND DISSEMINATIONS

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

THE WHITE PAPER "DIGITAL TRUST FOR SMART ICT"[75]

ILNAS published, with the support of the Ministry of the Economy, the White Paper "Digital Trust for Smart ICT" at the end of 2016 to bring into perspective, through technical, economic, prospective and standard analysis, the market needs in terms of Digital Trust in order to facilitate the adoption and widespread use of Smart ICT, and more specifically the Internet of Things (IoT), Cloud Computing and Big Data. It aims to provide 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 have been published by ILNAS in 2016:

THE WHITE PAPER "GREEN COMPUTING"[76]

This White Paper surveys, 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

[74] ILNAS & ANEC GIE, "Standards Analysis of the ICT Sector" (7th edition), 2017

[75] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/confiance-numerique/etudes-nationales/white-paper-digital-trust-october-2016/White-Paper-Digital-Trust-October-2016.pdf

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

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.

THE WHITE PAPER "BIG DATA"[77]

This document aims 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 document 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.

5.1.5 FREE CONSULTATION OF THE STANDARDS

ILNAS offer the free consultation of its entire standards' database (including more than 160 000 normative documents from ILNAS, DIN, CEN, CENELEC, ETSI, ISO and IEC) through lecture stations located in six different places in Luxembourg:

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

This service allows, for example, interested organizations or individuals to peruse a standard before its purchase. The ILNAS e-Shop[78] offers then the possibility to buy the relevant standards in electronic format at competitive prices.

5.1.6 SMART ICT STANDARDIZATION RESEARCH RESULTS

ILNAS is currently developing a joint research program with the University of Luxembourg (Interdisciplinary Centre for Security, Reliability and Trust – SnT). It will be dedicated to reinforce the collaboration in the domain of Smart ICT for Business Innovation through Technical Standardization and will focus on Digital Trust for Smart ICT. From one side, through the results of the research, this program will support the

[77] 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

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

evolution of the academic program of the Certificate *Smart ICT for Business Innovation*. From the other side, it will serve as a basis for a future Master Program *Smart Secure ICT for Business Innovation* (expected in 2019). In this context, three PhD students will be involved for research work on dedicated Smart ICT topics: Cloud Computing, Internet of Things and Big Data.

National stakeholders active in the Smart ICT landscape will have the opportunity to benefit from the results of this research program, for example by supporting the registration of some of their employees in the University certificate, described in the next section, or in the future Master degree. They will also be informed through the different information channels of ILNAS described previously.

5.2 TRAINING IN STANDARDIZATION

5.2.1 ONE-DAY TRAINING ON DIGITAL TRUST

ILNAS, with the support of ANEC GIE, is planning to propose a training dedicated to Digital Trust for Smart ICT. In particular, this one-day training offers a general overview of Digital Trust requirements, challenges and opportunities for Smart ICT technologies. The training course will mainly focus on Digital Trust for Cloud Computing, Internet of Things and Big Data.

5.2.2 UNIVERSITY CERTIFICATE SMART ICT FOR BUSINESS INNOVATION

ILNAS, in collaboration with the University of Luxembourg, has developed the University certificate *Smart ICT for Business Innovation*, which represent an innovative way to better understand Smart ICT standardization and develop new related skills.

This diploma allows the students to take a broad view of the cutting-edge Smart ICT concepts and tools at their disposal in order to develop their sense of innovation. Overall, the Certificate focuses on important aspects of Smart ICT and their applications, such as the development of Smart Cities, Big Data, Internet of Things and Cloud Computing. The program also proposes an overview of some challenges to fully exploit the potential of Smart ICT:

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

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

5.3 INVOLVEMENT IN STANDARDIZATION

5.3.1 BECOME NATIONAL DELEGATE IN STANDARDIZATION

5.3.1.1 BENEFITS OF PARTICIPATION IN SMART ICT STANDARDIZATION TECHNICAL COMMITTEES

Participating in Smart ICT standardization technical committees offers a broad set of opportunities and benefits:

- 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;
- Collaborating with strategic partners and international experts;
- Valuing your organization at national and international level;
- Identifying development opportunities;
- Placing your organization in the competition.

5.3.1.2 PARTICIPATION IN THE TRAINING "NEW DELEGATES IN STANDARDIZATION"

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

5.3.1.3 SUPPORT TO NATIONAL DELEGATES

As the national standards body, ILNAS provides 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 to enhance the organization and development of the ICT technical standardization representation at the national level.

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

5.3.1.4. STRONGER COMMITMENT AS A NATIONAL DELEGATE (CHAIRMAN, HEAD OF DELEGATION, EDITOR OF EUROPEAN OR INTERNATIONAL STANDARDS)

Registration as a national delegate offers the possibility to assume different levels of involvement:

- 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 this

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 delegates 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 editor or coeditor. 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).

5.3.2 COMMENT STANDARDS UNDER PUBLIC ENQUIRY

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

5.3.3 PROPOSE NEW STANDARDS PROJECTS

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

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

5.3.4 MONITOR THE STANDARDIZATION WORK PERFORMED BY THE EUROPEAN MULTI-STAKEHOLDER PLATFORM ON ICT STANDARDIZATION (MSP)

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

In this context, interested stakeholders can contact the 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 the national Smart ICT workshops;
  - Benefit from dedicated awareness session;
  - Identify the most relevant Smart ICT standardization technical committees and standards projects with the Smart ICT standards watch;
  - Consult the 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 trained in standardization
  - Participate in a one-day training on Digital Trust;
  - Register in the University certificate Smart ICT for Business Innovation.
- To be involved in standardization
  - Become national standardization delegate
    - Participate in ICT technical committees,
    - Register in the training "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),
  - 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 GIE, can provide an active contribution and support.

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 GIE are specifically dedicated to these aspects and are able to efficiently support and inform the future national delegates[79].

To reinforce this support, persons are appointed as specific points of contact for delegates of the Smart ICT sector. As such, the information and support provided would also stay as close as possible to the issues related to this sector.

[79] Declaration of interest in ICT standardization

6 CONCLUSIONS

Smart ICT is already one of the most active sectors, at both national level and worldwide. It is now evolving towards smarter technological products and services. Through the development of new and innovative digital products and services, Smart ICT constitutes a major source of economic development and it directly participates in the resolution of current environmental and social concerns. Moreover, Smart ICT building blocks, like Cloud Computing, Internet of Things and Big Data play a crucial role to support innovation and foster the development of related subsectors where Smart ICT applications and services offer new opportunities.

In this context, standards are essential not only to develop ICT, but also to support its interoperability with other sectors. Therefore, there is an increasing interest of standards in these enhancing technologies. Technical standardization plays an important role not only giving a first-hand insight into latest developments, thus supporting innovation, but also contributing to harmonization of systems and procedures, opening access to external markets and ensuring constant progress. On the other hand, standards contribute to promote and share good practices and techniques available in the market. They ensure the quality 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[80], ICT is a horizontal sector supporting many innovative or smart developments. ILNAS, with the support of ANEC GIE, will therefore constantly analyze these developments and support national stakeholders according to „Luxembourg's Policy on ICT technical standardization 2015-2020"[81]. ICT is indeed one of the most competitive economic sectors in the Grand Duchy of Luxembourg, having communication infrastructures of high quality, hosting European headquarters of several world-leading ICT companies[82] and with a market composed of many companies, associations, administrations and experts.

ILNAS, with the support of ANEC GIE, has already undertaken concrete developments, through the standardization, for participating to strengthen digital economy of Luxembourg. It includes the launch of a University certificate dedicated to Smart ICT, focusing on the Cloud Computing, Internet of Things, Big Data and Digital Trust related to these technologies. This educational program, supported by the Ministry of the Economy, ETSI and the CEN-CENELEC, is the first step towards a more ambitious project of creating a research program and a Master program dedicated to (Secure) Smart ICT (Cloud Computing, IoT and Big Data) and Digital Trust related to these technologies.

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

[81] 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

[82] http://ict.investinluxembourg.lu/sectors/media-entertainment-e-gaming

ILNAS, with the support of ANEC GIE, is working on and open to support different industries/organizations through standardization according to their nature of business at the national level. Attraction of local individuals, industries/organizations towards the technical standardization committees, University Certificate course, breakfast meetings and workshops organized by ILNAS, with the support of ANEC GIE, signifies that it has already reached to the level of success to aware the importance of standardization in the national market. 49 national standardization delegates are already involved in Smart ICT and/or Digital Trust related technical committees (Cloud Computing: 13; Internet of Things: 6; Big Data: 7; Digital Trust: 35) shows the interest of individuals, industries/organizations towards the technical standardization.

It is worth noting that the different actions taken by ILNAS, with the support of ANEC GIE, for the development of Education about Standardization at national level are also participating in the branding of Luxembourg internationally and particularly at European level. Indeed, the CEN-CENELEC and ETSI are both partners of the University certificate Smart ICT for Business Innovation and actively support the development of this educational program. For instance, Mr. Ashok Ganesh and Mr. Hermann Brand, respectively Director Innovation of CEN-CENELEC and Director Innovation of ETSI, are lecturers in the University certificate, which clearly demonstrates the strong interest of the European Standardization Organizations in the development of such activities.

In this framework, this version of standard analysis, Smart ICT Standards Analysis, constitutes a complementary tool to foster the positioning of Luxembourg in the Smart ICT standardization landscape. It highlights the potential interest for the national stakeholders and the opportunities for the national market to participate in the standardization process especially in main three pillars of Smart ICT, namely Cloud Computing, Internet of Things, Big Data and Digital Trust related to these technologies. However, standardization is performed on a voluntary basis and each stakeholder is free to get involved and to define his/her level of commitment. Proper understanding of the stakes associated to Smart ICT standardization is necessary to adopt the appropriate position across the standardization landscape and benefit from all the related opportunities. Driven by the motto of the national standardization strategy 2014-2020: *"Technical standardization as a service"*, ILNAS, with the support of ANEC GIE, stands ready to encourage and assist each initiative in this process.

7 APPENDIX - SMART ICT STANDARDS AND PROJECTS IN ITU-T

This appendix details the Smart ICT related standards both published and under development in the ITU-T[83]. These documents, called Recommendations, are freely available after their publication in most of the case and constitute valuable and recognized source of information for national stakeholders in the Smart ICT landscape.

7.1 CLOUD COMPUTING

7.1.1 PUBLISHED RECOMMENDATIONS

REFERENCE	TITLE
ITU-T F.743.2 (07/2016)	Requirements for cloud storage in visual surveillance
ITU-T FG Cloud TR Part 1 (02/2012)	Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements
ITU-T FG Cloud TR Part 2 (02/2012)	Technical Report: Part 2: Functional requirements and reference architecture
ITU-T FG Cloud TR Part 3 (02/2012)	Technical Report: Part 3: Requirements and framework architecture of cloud infrastructure
ITU-T FG Cloud TR Part 4 (02/2012)	Technical Report: Part 4: Cloud Resource Management Gap Analysis
ITU-T FG Cloud TR Part 5 (02/2012)	Technical Report: Part 5: Cloud security
ITU-T FG Cloud TR Part 6 (02/2012)	Technical Report: Part 6: Overview of SDOs involved in cloud computing
ITU-T FG Cloud TR Part 7 (02/2012)	Technical Report: Part 7: Cloud computing benefits from telecommunication and ICT perspectives
ITU-T M.3371 (10/2016)	Requirements for service management in cloud-aware telecommunication management system
ITU-T Q Suppl. 65 (07/2014)	Draft Q Supplement 65 to Q.39xx-series Recommendations (Q.Supp-CCI) Cloud computing interoperability activities
ITU-T Q.4040 (02/2016)	The framework and overview of cloud computing interoperability testing
ITU-T X.1601 (10/2015)	Security framework for cloud computing (edition 2 under development)
ITU-T X.1602 (03/2016)	Security requirements for software as a service application environments
ITU-T X.1631 (07/2015) / ISO/IEC 27017:2015	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ITU-T X.1641 (09/2016)	Guidelines for cloud service customer data security
ITU-T X.1642 (03/2016)	Guidelines of operational security for cloud computing

[83] For more information on ITU-T membership, refer to the website of the organization: http://www.itu.int/en/ITU-T/membership/Pages/default.aspx.

ITU-T Y.3500 (08/2014) / ISO/IEC 17788:2014	Information technology -- Cloud computing -- Overview and vocabulary
ITU-T Y.3501 (06/2016)	Cloud computing framework and high-level requirements (edition 2 under development)
ITU-T Y.3502 (08/2014) / ISO/IEC 17789:2014	Information technology -- Cloud computing -- Reference architecture
ITU-T Y.3503 (05/2014)	Requirements for desktop as a service
ITU-T Y.3504 (06/2016)	Functional architecture for Desktop as a Service
ITU-T Y.3510 (02/2016)	Cloud computing infrastructure requirements (edition 2 under development)
ITU-T Y.3511 (03/2014)	Framework of inter-cloud computing
ITU-T Y.3512 (08/2014)	Cloud computing - Functional requirements of Network as a Service
ITU-T Y.3513 (08/2014)	Cloud computing - Functional requirements of Infrastructure as a Service
ITU-T Y.3520 (09/2015)	Cloud computing framework for end to end resource management (edition 2 under development)
ITU-T Y.3521/M.3070 (03/2016)	Overview of end-to-end cloud computing management
ITU-T Y.3522 (09/2016)	End-to-end cloud service lifecycle management requirements
ITU-T Y.3600 (11/2015)	Big data – Cloud computing based requirements and capabilities

7.1.2 RECOMMENDATIONS UNDER DEVELOPMENT

REFERENCE	TITLE
ITU-T Draft H.248.CLOUD	Gateway control protocol: Cloudification of packet gateways
ITU-T Draft H.CSVS-Arch	Architectural requirements for cloud storage in video surveillance
ITU-T Draft H.VSCC	Architecture for cloud computing in visual surveillance
ITU-T Draft M.cbnmsa	Cloud-based network management system architecture
ITU-T Draft Q.CCP	Set of parameters of cloud computing for monitoring
ITU-T Draft Q.wa-iop	Cloud Interoperability testing about Web Application
ITU-T Draft Supp-Y.Cloud Computing Scenarios for Developing Countries	Scenarios of Implementing Cloud Computing in networks of developing countries
ITU-T Draft X.dsms	Data security requirements for the monitoring service of cloud computing
ITU-T Draft X.SRIaaS	Security requirements of public infrastructure as a service (IaaS) in cloud computing
ITU-T Draft X.SRNaaS	Security requirements of Network as a Service (NaaS) in cloud computing
ITU-T Draft Y.BDaaS-arch	Cloud computing - Functional architecture of Big Data as a Service
ITU-T Draft Y.cccm-reqts	Cloud Computing - Requirements for Containers and Micro-services
ITU-T Draft Y.ccdc-reqts	Distributed cloud overview and high-level requirements
ITU-T Draft Y.CCIC-arch	Cloud computing - Functional Architecture of inter-cloud computing

ITU-T Draft Y.CCICDM-Req	Cloud Computing - Requirements for Inter-Cloud Data Management
ITU-T Draft Y.CCICTM	Cloud Computing - Overview of Inter-Cloud Trust Management
ITU-T Draft Y.ccpm-reqts	Cloud computing-Functional requirements of physical machine
ITU-T Draft Y.csb-reqts	Cloud Computing Requirements for Cloud Service Brokerage
ITU-T Draft Y.cslm-metadata	Metadata framework for cloud service lifecycle management
ITU-T Draft Y.sup.ccsr	Supplement on Cloud Computing Standardization Roadmap

7.2 INTERNET OF THINGS

7.2.1 PUBLISHED RECOMMENDATIONS

REFERENCE	TITLE
ITU-T Q.3913 (08/2014)	Set of parameters for monitoring internet of things devices
ITU-T Y.4000 / Y.2060 (06/2012)	Overview of Internet of Things
ITU-T Y.4050 / Y.2069 (07/2012)	Terms and definitions for Internet of Things
ITU-T Y.4100 / Y.2066 (06/2014)	Common requirements of Internet of Things
ITU-T Y.4101/ Y.2067 (06/2014)	Common requirements and capabilities of a gateway for Internet of Things applications
ITU-T Y.4102 / Y.2074 (01/2015)	Requirements for Internet of Things devices and operation of Internet of Things applications during disaster
ITU-T Y.4103 / F.748.0 (10/2014)	Common requirements for Internet of Things (IoT) applications
ITU-T Y.4111 / Y.2076 (02/2016)	Semantics based requirements and framework of the Internet of Things
ITU-T Y.4112 / Y.2077 (02/2016)	Requirements of the Plug and Play capability of the Internet of Things
ITU-T Y.4113 (09/2016)	Requirements of the network for the Internet of Things
ITU-T Y.4401 / Y.2068 (03/2015)	Functional framework and capabilities of the Internet of Things
ITU-T Y.4552 / Y.2078 (02/2016)	Application support models of the Internet of Things
ITU-T Y.4702 (03/2016)	Common requirements and capabilities of device management in the Internet of Things

7.2.2 RECOMMENDATIONS UNDER DEVELOPMENT

REFERENCE	TITLE
ITU-T Draft D.IoTRoaming	Roaming for the Internet of Things (IoT)
ITU-T Draft E.IoT-NNAI	NNAI for Internet of Things
ITU-T Draft Q.Het_IoT_ Gateway_Test	The structure of the testing of heterogeneous Internet of Things gateways in a laboratory environment
ITU-T Draft TR.AI4SC	Artificial Intelligence and Internet of Things
ITU-T Draft X.1362	Simple encryption procedure for Internet of things (IoT) environments
ITU-T Draft X.iotsec-2	Security framework for Internet of things
ITU-T Draft X.oiddev	Object identifier assignments for the Internet of things
ITU-T Draft X.oid-iot	ITU-T X.660 - Supplement on Guidelines for using object identifiers for the Internet of things
ITU-T Draft Supp.-Y.IoT Scenarios for Developing Countries	Scenarios of Implementing Internet of Things in networks of developing countries
ITU-T Draft Y.2067	Common requirements and capabilities of a gateway for Internet of Things applications
ITU-T Draft Y.Accessibility-IoT	Accessibility requirements for the Internet of things applications and services
ITU-T Draft Y.IoT-AC-reqts	Requirements for accounting and charging capabilities of the Internet of Things
ITU-T Draft Y.IoT-ITS-framework	Framework of Cooperative Intelligent Transport Systems based on the Internet of Things
ITU-T Draft Y.IoT-NCM-reqts	Requirements and capabilities of network connectivity management in the Internet of Things
ITU-T Draft Y.IoT-things-description-reqts	Requirements of things description in the Internet of Things
ITU-T Draft Y.IoT-WDS-Reqts	Requirements and capabilities of Internet of Things for support of wearable devices and related services
ITU-T Draft Y.SmartMan-IIoT-overview	Overview of Smart Manufacturing in the context of Industrial Internet of Things
ITU-T Draft Supp-Y.IPv6-IoT	IPv6 Potential for the Internet of Things and Smart Cities
ITU-T Draft Y.IPv6RefModel	Reference Model of IPv6 Subnet Addressing Plan for Internet of Things Deployment
ITU-T Draft Y.IPv6-suite	Reference Model of Protocol Suite for IPV6 interoperable Internet of Things Deployments
ITU-T Draft Y.NGNe-IoT-arch	Architecture of the Internet of Things based on NGNe
ITU-T Draft Y.IoT-SQ-fns	Service Functionalities of Self-quantification over Internet of things
ITU-T Draft Y.IoT-sec-safety	Security capabilities supporting safety of the Internet of Things

7.3 BIG DATA

7.3.1 PUBLISHED RECOMMENDATIONS

REFERENCE	TITLE
ITU-T Y.3600 (11/2015)	Big data - Cloud computing based requirements and capabilities
ITU-T Y.3600-series Supplement 40 (07/2016)	Big Data Standardization Roadmap

7.3.2 RECOMMENDATIONS UNDER DEVELOPMENT

REFERENCE	TITLE
ITU-T Draft F.VSBD	Requirements for big data application in visual surveillance system
ITU-T Draft X.GSBDaaS	Guidelines on security of Big Data as a Service
ITU-T Draft X.srfb	Security Requirements and Framework for Big Data Analytics in mobile Internet services
ITU-T Draft Y.4114	Specific requirements and capabilities of the IoT for Big Data
ITU-T Draft Y. bDDN-MNTMP	Big data driven mobile network traffic management and planning
ITU-T Draft Y.BDaaS-arch	Cloud computing - Functional architecture of Big Data as a Service
ITU-T Draft Y.bDDN-fr	Framework of big data driven networking based on Deep Packet Inspection
ITU-T Draft Y.bDDN-req	Requirement of big data-driven networking
ITU-T Draft Y.BDDP-reqts	Big data - Overview and requirements for data preservation
ITU-T Draft Y.bdi-reqts	Big Data - Overview and functional requirements for data integration
ITU-T Draft Y.bdm-sch	Big data - Metadata framework and conceptual model
ITU-T Draft Y.bDPI-Mec	Mechanism of deep packet inspection applied in network big data context
ITU-T Draft Y.bdp-reqts	Big data - Requirements for data provenance
ITU-T Draft Y.BigDataEX-reqts	Big data exchange framework and requirements
ITU-T Draft Y.Sup-bDDN-usecase	Supplement for use cases and application scenarios of big data driven networking

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 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 GIE
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 GIE) was created in October 2010 by ILNAS, "Chambre de Commerce", "Chambre des Métiers" and STATEC. It is divided into 3 departments: Standardization, Knowledge-based Economy and Metrology. The role of the standardization department of ANEC GIE is to implement the national standardization strategy established by ILNAS in order to support the development of standardization activities at national level and to promote the benefits of participating in the standardization process.

ILNAS

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

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