Welcome

Bienvenue

Willkommen

ILNAS

ILNAS Breakfast “Smart Secure ICT and Technical Standardization”

19th March 2019

ILNAS Breakfast “Smart Secure ICT and Technical Standardization”

AGENDA

09:30 – 09:40	**Reception of participants**
09:40 – 09:55	**Technical Standardization & Smart Secure ICT – Overview and outlook** ***Dr. Jean-Philippe HUMBERT - ****ILNAS*
09:55 – 10:05	**Presentation of the Standards Analysis - Smart Secure ICT Luxembourg** ***Mr. Nicolas DOMENJOUD – ****OLN*
10:05 – 11:05	**Standardization in the ICT sector** • Cloud Computing **- Dr. Johnatan PECERO -** GIE ANEC • Internet of Things **- Dr. Shyam WAGLE -** GIE ANEC • Blockchain & Distributed Ledgers **- Dr. Johnatan PECERO -** GIE ANEC • Artificial Intelligence **- Ms. Natalia CASSAGNES -** GIE ANEC
11:05 – 11:10	**How to become a Delegate in Technical Standardization?** ***Mr. Nicolas DOMENJOUD – ****OLN*
11:10 – 11:30	**Questions and open discussion**

ILNAS

Technical Standardization & Smart Secure ICT

Overview and outlook

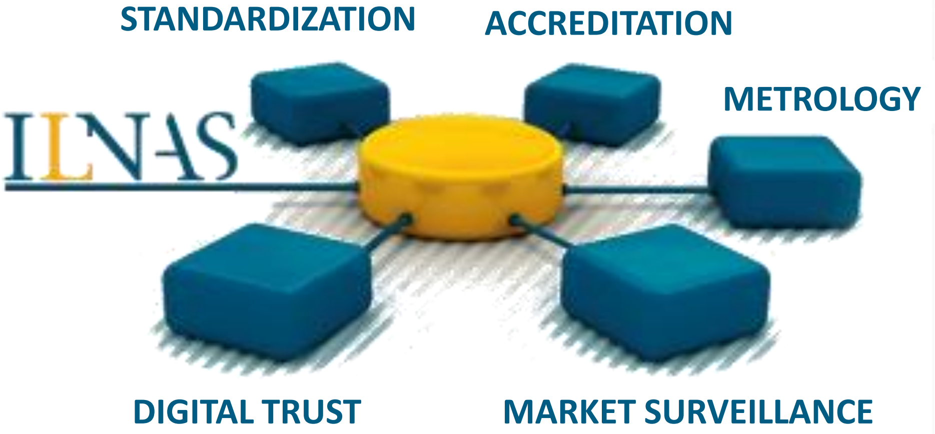
INTRODUCTION OF ILNAS

GENERAL PRESENTATION

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

- **Creation:** law dated July 14, 2014 (repealing the amended Law of May 20, 2008) and law dated February 17, 2017
- **Legal form:** Public administration under the authority of the Minister of the Economy
- **Total staff:** 48 (March 2019)
- **Website:** www.portail-qualite.lu

PORTAIL-QUALITE.LU
QUALITE · SECURITE · CONFORMITE

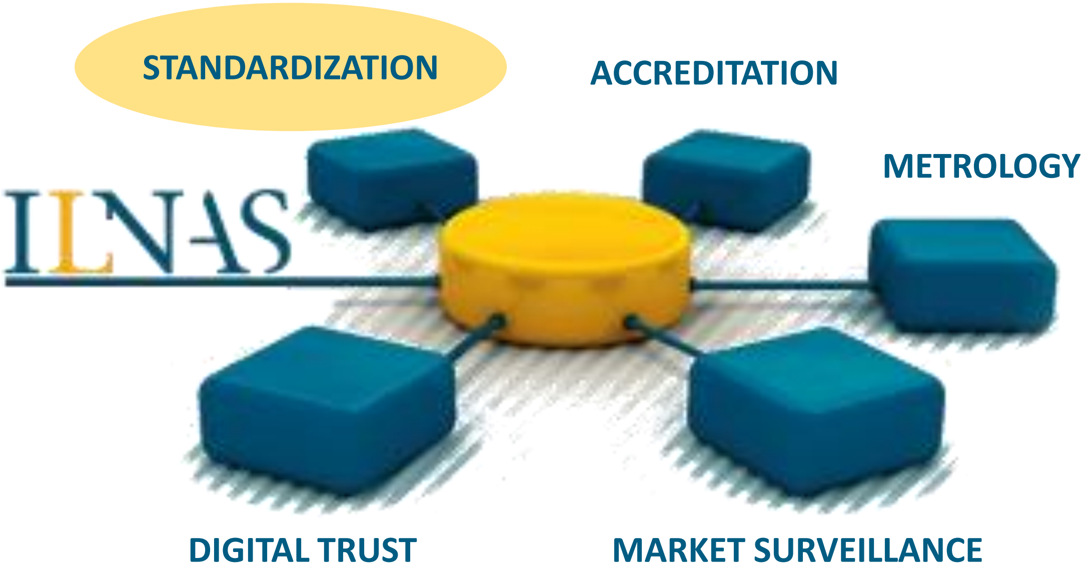


A FRAMEWORK

ILNAS – THE NATIONAL STANDARDS BODY

– **OLN - *Organisme luxembourgeois de normalisation***

- Composed of 6 persons
- Close collaboration with the G.I.E. ANEC-N (5 persons)



A FRAMEWORK

AGENCY FOR STANDARDIZATION AND KNOWLEDGE-BASED ECONOMY

ANEC

- **Creation:** October 4, 2010
- **Status:** Economic Interest Grouping (EIG)
- **Objectives:** Promotion, awareness raising and training, applied research in the field of standardization and metrology in order to support companies' competitiveness in Luxembourg
- **Human resources:** 8 employees (March 2019)
- **Partners:**

ILNAS

CHAMBRE DES METIERS Luxembourg

CHAMBRE DE COMMERCE LUXEMBOURG

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

TECHNICAL STANDARDIZATION - AIM AND COMMITMENT

NATIONAL STANDARDIZATION STRATEGY

LUXEMBOURG

STANDARDIZATION STRATEGY

2014-2020

"Technical standardization as a service"

ILNAS

– THREE PILLARS:

PILLAR 1	**Information and communication technologies (ICT)**
PILLAR 2	**National influence and compliance with legal attributions**
PILLAR 3	**Products and services**

- https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-2014-2020.html

TECHNICAL STANDARDIZATION - AIM AND COMMITMENT

NATIONAL STANDARDIZATION STRATEGY

LUXEMBOURG
STANDARDIZATION STRATEGY
2014-2020

"Technical standar

ILN

Policy on ICT technical
standardization (2015-2020)

ILNAS

1, avenue du Swing, L-4367 Belvaux
Tel.: 247 743 - 70 / anec@ilnas.etat.lu / www.portail-qualite.lu

Pillar 1: Information and communication technologies (ICT)

1. Developing the interest and the involvement of the market
2. Promoting and reinforcing market participation
3. Supporting and strengthening the EaS and related research activities

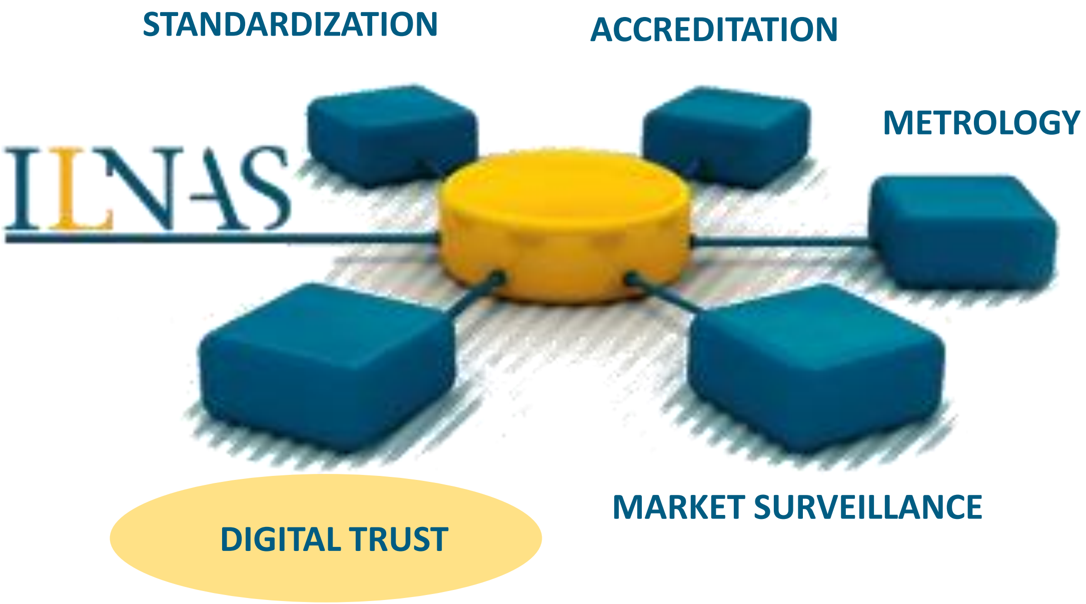
- https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-2014-2020.html
- https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-TIC-2015-2020.html

A FRAMEWORK

ILNAS – DIGITAL TRUST DEPARTMENT

– Digital Trust Department

- Composed of 4 persons
- National digital trust supervisory body



SMART SECURE ICT - OVERVIEW

WHITE PAPER « DIGITAL TRUST FOR SMART ICT » - SEPTEMBER 2017 – THE BASELINE

It surveys current advances in Digital Trust from three complementary points of view:

- A technical analysis
- A business and economic prospective analysis
- A technical standardization perspective

From the technical analysis

- It reviews the basic concepts of the technology and the existing work supporting the development of Digital Trust
- It presents some technical challenges related to Digital Trust

From business and economic prospective

- It highlights the interest for Digital Trust
- It stresses the need of Digital Trust for each Smart ICT concepts

From standards point of view technical standardization

- It considers both as an important tool to support Digital Trust for Smart ICT

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

SMART SECURE ICT - OVERVIEW

WHITE PAPERS ON SMART ICT

ILNAS
White Paper
BLOCKCHAIN AND DISTRIBUTED LEDGERS
TECHNOLOGY, ECONOMIC IMPACT AND TECHNICAL STANDARDIZATION
ILNAS
White Paper
INTERNET OF THINGS (IoT)
TECHNOLOGY, ECONOMIC VIEW AND TECHNICAL STANDARDIZATION
ANEC

- **White Paper “Blockchain and Distributed Ledgers - Technology, Economic Impact and Technical Standardization” – June 2018**
  - Developed with the support of the Ministry of the Economy
  - Provides a comprehensive analysis of the developments in the areas of blockchain and distributed ledger technologies
  - Published on June 23, 2018 – Organization of an event at the Ministry of the Economy
  - 2 more events organized at ILNAS premises to answer market demand
- **White Paper “Internet of Things (IoT) - Technology, Economic View and Technical Standardization” – July 2018**
  - Developed with the support of the Ministry of the Economy
  - Provides a broad view of the developments around IoT and related technologies
  - Published on July 06, 2018 during the ILNAS-ETSI Workshop
- **White Paper “Data Protection and Privacy in Smart ICT” – October 2018**
- **All the White Papers are going to be updated during 2019-2020**

- https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-blockchain-june-2018.pdf
- https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf

SMART SECURE ICT - OVERVIEW

STANDARDS ANALYSIS “SMART SECURE ICT”

Developing the interest and the involvement of the market in ICT Technical Standardization

- **Drawing up a yearly national standards analysis for the ICT sector**
  - Standards watch of the related sector
  - Identification of relevant technical committees and Fora/Consortia
  - Preparation of the final report of analysis and opportunities
  - **FOCUS ON SMART ICT AND DIGITAL TRUST**
    - Cloud Computing, Internet of Things, Big Data, Artificial Intelligence, Blockchain, Digital Trust related developments

- **Defining a national implementation plan for ICT technical standardization**
  - To involve targeted stakeholders of the Grand Duchy of Luxembourg in a global approach to standardization
  - Enhancing the international recognition of the Grand Duchy of Luxembourg

SMART SECURE ICT - OVERVIEW

RESEARCH PROGRAM ILNAS-UNIVERSITY OF LUXEMBOURG (IOT, CLOUD COMPUTING, BIG DATA)

The University of Luxembourg and ILNAS are strengthening their collaboration in the field of Smart ICT and standardization. A ceremony was held on May 17, 2017 at the Ministry of Economy to formally conclude the partnership

In the rear row, from left to right: Jean-Philippe Humbert, Pascal Bouvry, Paul Heuschling, Yves Elsen, Björn Ottersten;
In the front row, from left to right: Ludwig Neyses, Francine Closener, Jean-Marie Reiff

SMART SECURE ICT - OVERVIEW

RESEARCH PROGRAM ILNAS-UNIVERSITY OF LUXEMBOURG (IOT, CLOUD COMPUTING, BIG DATA)

Research Program (2017-2020) on “Digital Trust for Smart ICT”

- **Joint collaboration between ILNAS & SnT-UL to reinforce the collaboration in the domain of Smart ICT for Business Innovation through Technical Standardization**
  - ○ Partnership and contract between ILNAS and SnT have been signed in March 2017

- **3 PhD students are involved in “Digital Trust for Smart ICT”**
  - ○ Cloud Computing
  - ○ Big Data and Analytics
  - ○ Internet of Things

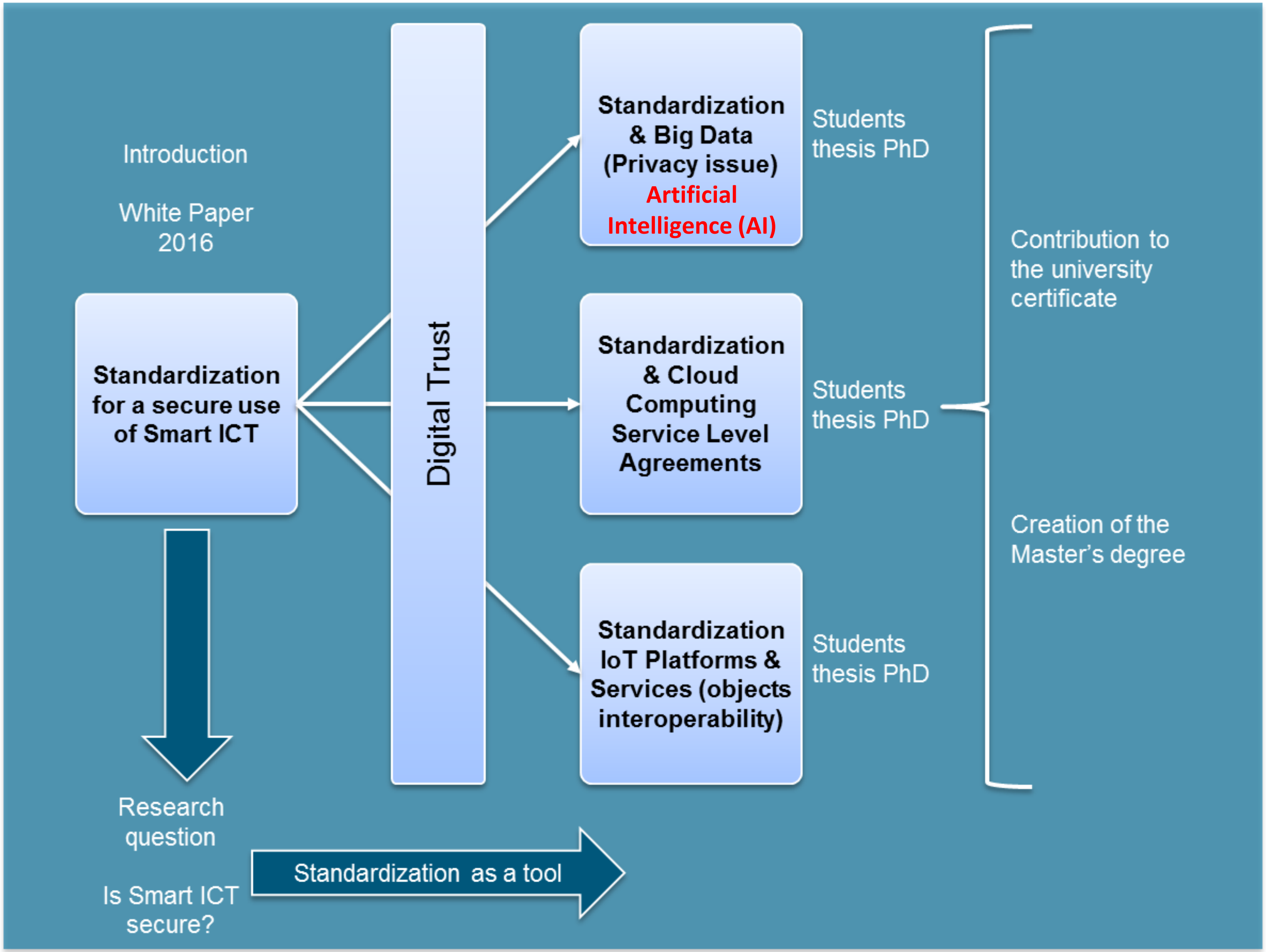
securityandtrust.lu

- **Supported the evolution of the University certificate course program for the class 2018-2019**

- **Other main targets of the research program**
  - ○ To serve as a basis for the development of the Master Program “Smart Secure ICT for Business Innovation”
  - ○ To update the White Paper “Digital trust in Smart ICT”
    - ❑ Update 2018 on Privacy (common problematic to the three Smart ICT domains: Cloud Computing, Big Data and Internet of Things), in collaboration with the Ministry of the Economy → White Paper on “Data Protection and Privacy in Smart ICT” (DPP)
    - ❑ Update 2019 - Evolution of the White Paper DPP

SMART SECURE ICT - OVERVIEW

RESEARCH PROGRAM ILNAS-UNIVERSITY OF LUXEMBOURG (IOT, CLOUD COMPUTING, BIG DATA)



Introduction

White Paper 2016

Standardization for a secure use of Smart ICT

Digital Trust

Standardization & Big Data (Privacy issue) Artificial Intelligence (AI)

Students thesis PhD

Standardization & Cloud Computing Service Level Agreements

Students thesis PhD

Standardization IoT Platforms & Services (objects interoperability)

Students thesis PhD

Contribution to the university certificate

Creation of the Master's degree

Research question

Is Smart ICT secure?

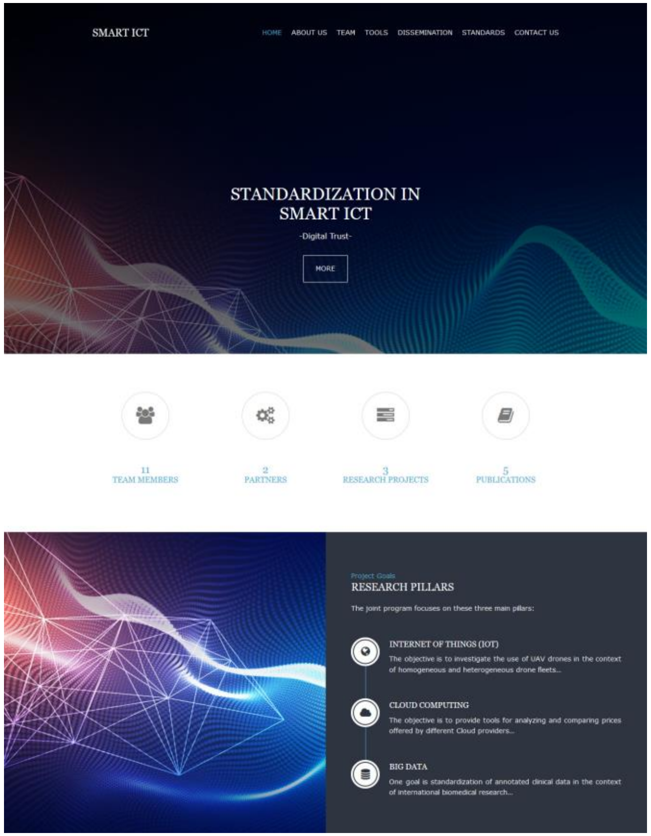
Standardization as a tool

securityandtrust.lu

SMART SECURE ICT - OVERVIEW

RESEARCH PROGRAM ILNAS-UNIVERSITY OF LUXEMBOURG (IOT, CLOUD COMPUTING, BIG DATA)

Research Program Website (UL) - https://smartict.gforge.uni.lu/



STANDARDIZATION IN SMART ICT

-Digital Trust-

11 TEAM MEMBERS

2 PARTNERS

3 RESEARCH PROJECTS

5 PUBLICATIONS

Project Goals

RESEARCH PILLARS

The joint program focuses on these three main pillars:

INTERNET OF THINGS (IOT)

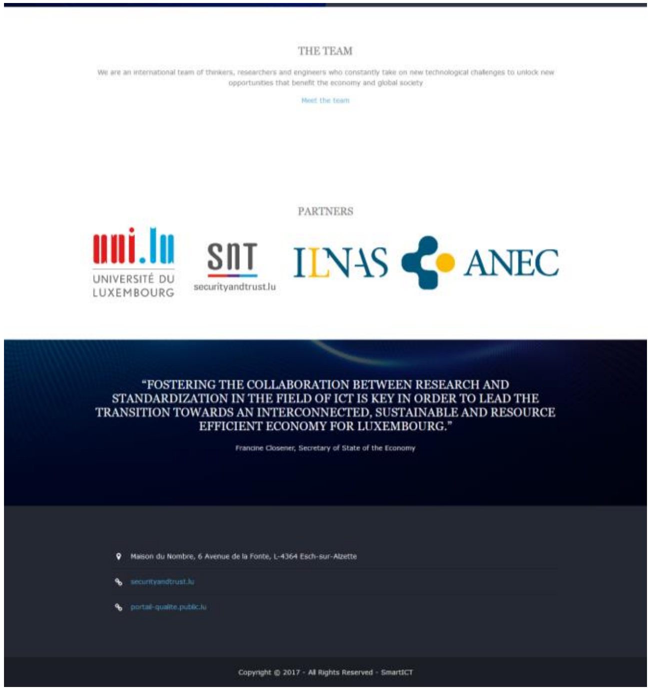
The objective is to investigate the use of UAV drones in the context of homogeneous and heterogeneous drone fleets...

CLOUD COMPUTING

The objective is to provide tools for analyzing and comparing prices offered by different Cloud providers...

BIG DATA

One goal is standardization of annotated clinical data in the context of international biomedical research...



THE TEAM

We are an international team of thinkers, researchers and engineers who constantly take on new technological challenges to unlock new opportunities that benefit the economy and global society

PARTNERS

uni.lu UNIVERSITÉ DU LUXEMBOURG

SnT securityandtrust.lu

ILNAS

ANEC

"FOSTERING THE COLLABORATION BETWEEN RESEARCH AND STANDARDIZATION IN THE FIELD OF ICT IS KEY IN ORDER TO LEAD THE TRANSITION TOWARDS AN INTERCONNECTED, SUSTAINABLE AND RESOURCE EFFICIENT ECONOMY FOR LUXEMBOURG."

Francine Closener, Secretary of State of the Economy

Maison du Nombre, 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette

securityandtrust.lu

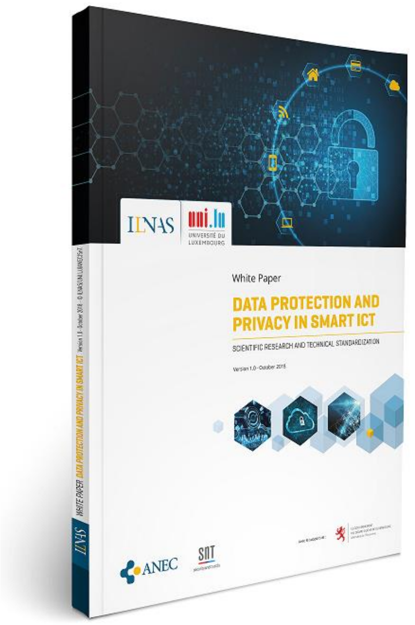
portail-qualite.public.lu

Copyright © 2017 - All Rights Reserved - SmartICT

SMART SECURE ICT - OVERVIEW

RESEARCH PROGRAM ILNAS-UNIVERSITY OF LUXEMBOURG (IOT, CLOUD COMPUTING, BIG DATA)

White Paper “DATA PROTECTION AND PRIVACY IN SMART ICT - SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION”


ILNAS
uni.lu
UNIVERSITÉ DU LUXEMBOURG
White Paper
DATA PROTECTION AND PRIVACY IN SMART ICT
SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION
Version 1.0 - October 2018
ANEC
SNT

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

– **First result of the Research Program**
  - White Paper “Data Protection & Privacy in Smart ICT”
  - Common development between ILNAS and the University of Luxembourg with the support of the Ministry of the Economy
  - Published on 12th October 2018 (World Standards Day)

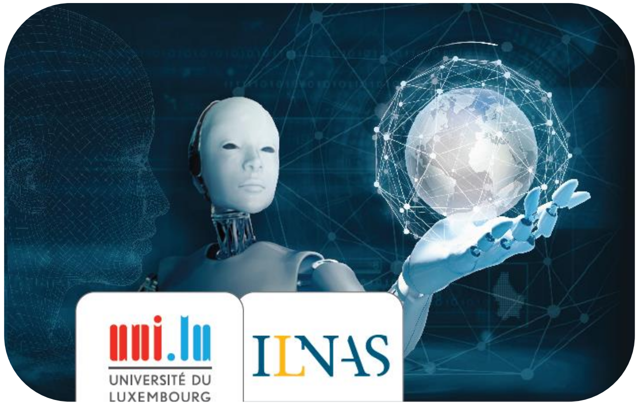
– **For better understanding of Data Protection and Privacy in Smart ICT Data**
  - Scientific and technological challenges
  - Economic potential
  - Understanding related standardization needs and efforts

– **Objective**
  - Analyze the state-of-the-art from research and technical standardization perspectives
  - One of the goals of performing this analysis is to understand the links between research and standardization

SMART SECURE ICT - OUTLOOK

MASTER PROGRAM "SMART SECURE ICT FOR BUSINESS INNOVATION"

Strengthening ILNAS's relations with academic partners with the aim of structuring education about standardization and ad-hoc research in the Grand Duchy of Luxembourg



- **Origin:**
  - Pilot project conducted between September 2015 and September 2016: "Smart ICT for Business Innovation" university certificate in partnership with the University of Luxembourg
  - Second promotion: February 2018 to February 2019

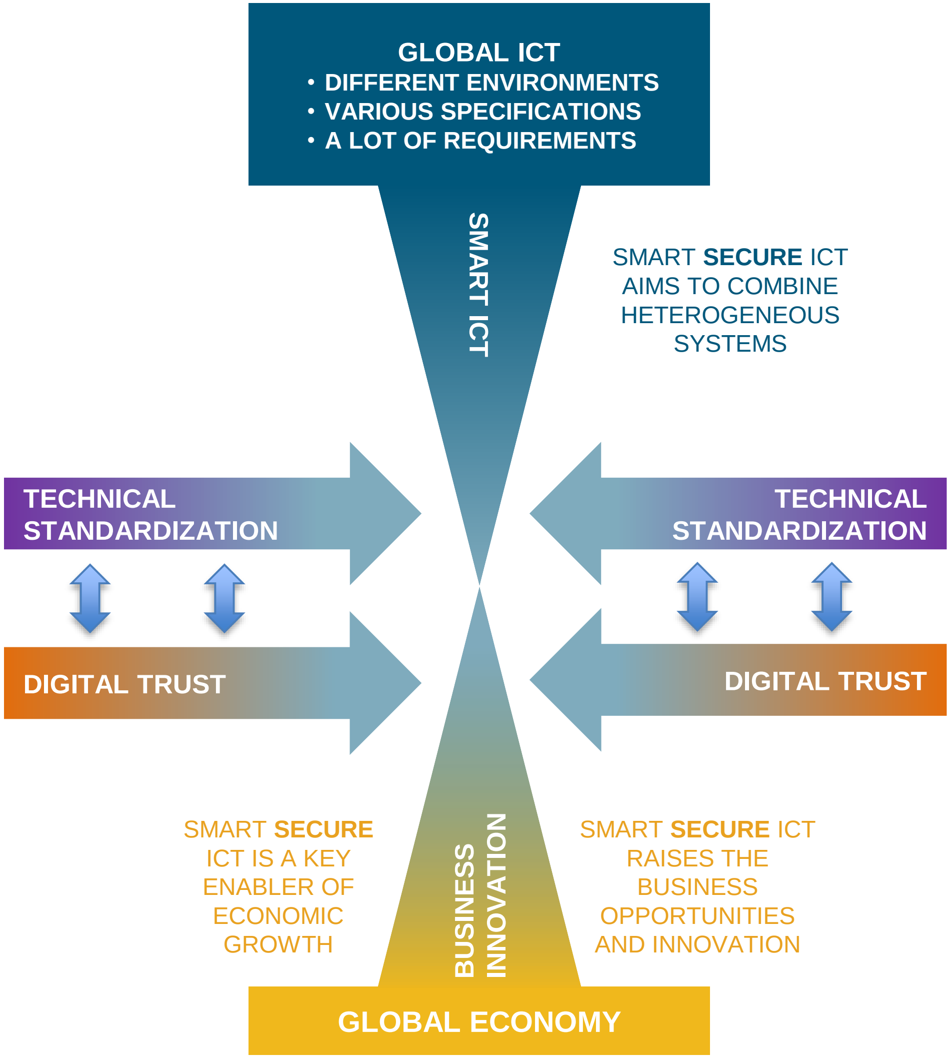
- **Objective: University Master on technical standardization and digital trust (horizon 2020)**
  - Will answer national priorities related to "Smart Secure ICT" topics, providing a smart way to link technology, standards and the business world, while creating an additional means of innovation at the national level

SMART SECURE ICT - OUTLOOK

MASTER PROGRAM “SMART SECURE ICT FOR BUSINESS INNOVATION”

- (NEW) READING GRID

EFFECTIVENESS AND GROWTH OF THE ICT INDUSTRY ARE DETERMINED BY THE ABILITY OF THE COMPONENT PARTS TO **SECURELY** “TALK” TO EACH OTHER – TO INTEROPERATE



GLOBAL ICT
- DIFFERENT ENVIRONMENTS
- VARIOUS SPECIFICATIONS
- A LOT OF REQUIREMENTS

SMART ICT

SMART **SECURE** ICT AIMS TO COMBINE HETEROGENEOUS SYSTEMS

TECHNICAL STANDARDIZATION

TECHNICAL STANDARDIZATION

DIGITAL TRUST

DIGITAL TRUST

SMART **SECURE** ICT IS A KEY ENABLER OF ECONOMIC GROWTH

BUSINESS INNOVATION

SMART **SECURE** ICT RAISES THE BUSINESS OPPORTUNITIES AND INNOVATION

GLOBAL ECONOMY

TECHNICAL STANDARDIZATION:

- COMMON LANGUAGES
- INTERNATIONAL OUTCOMES
- CONSENSUS
- BUSINESS-DRIVEN

A FORCE MULTIPLIER FOR ICT INNOVATION …

SMART SECURE ICT - OUTLOOK

MASTER PROGRAM "SMART SECURE ICT FOR BUSINESS INNOVATION"

New Digital Trust Layer

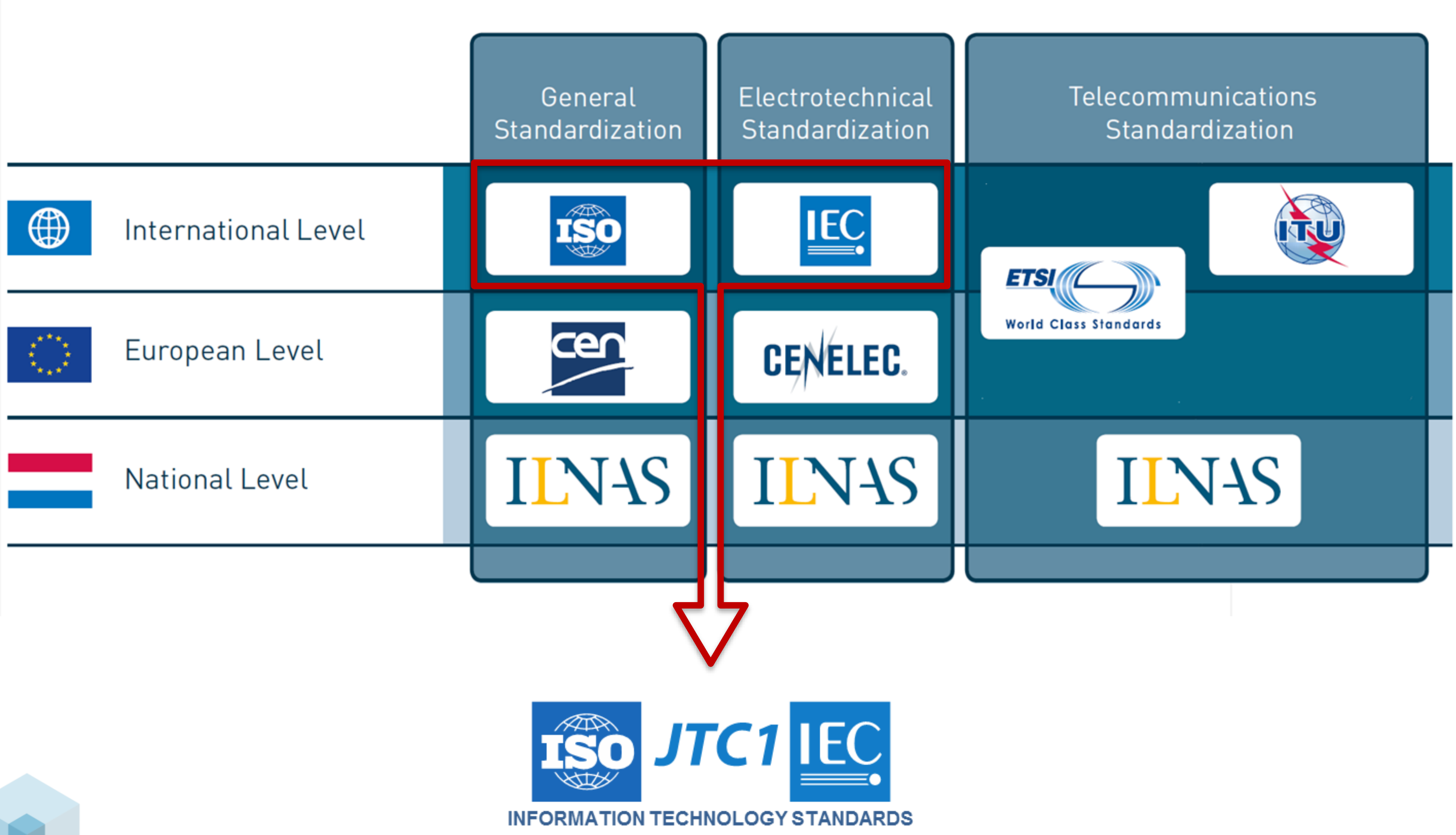
- **Smart ICT is fueling new business models, opportunities and innovation at large**
  - This domain becomes less tangible, more distributed, and more vulnerable to (cyber) threats and attacks
  - Digital Trust must be an essential part of Smart ICT

- **Digital Trust indicates a positive and verifiable belief about the perceived reliability of a digital information source, product or service, leading to an intention to use. It is not a technology, nor a process, it is an outcome exemplified by:**
  - Reliability
  - Accountability
  - Privacy
  - Transparency
  - Security
  - Quality
  - Integrity
  - …

- **Attainment of Digital Trust is driven by how Smart ICT technologies are both secured and used, and it helps to increase the broad adoption of innovative services, products, and the Smart ICT technologies → SMART SECURE ICT**
  - Digital Trust for Cloud Computing
  - Digital Trust for IoT
  - Digital Trust for Artificial Intelligence
  - Digital Trust for Big Data
  - …

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 – INFORMATION TECHNOLOGY



	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
International Level	ISO	IEC	ITU
European Level	CEN	CENELEC	ETSI World Class Standards
National Level	ILNAS	ILNAS	ILNAS

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS

– **ISO/IEC JTC 1 – Information technology**

  - JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications

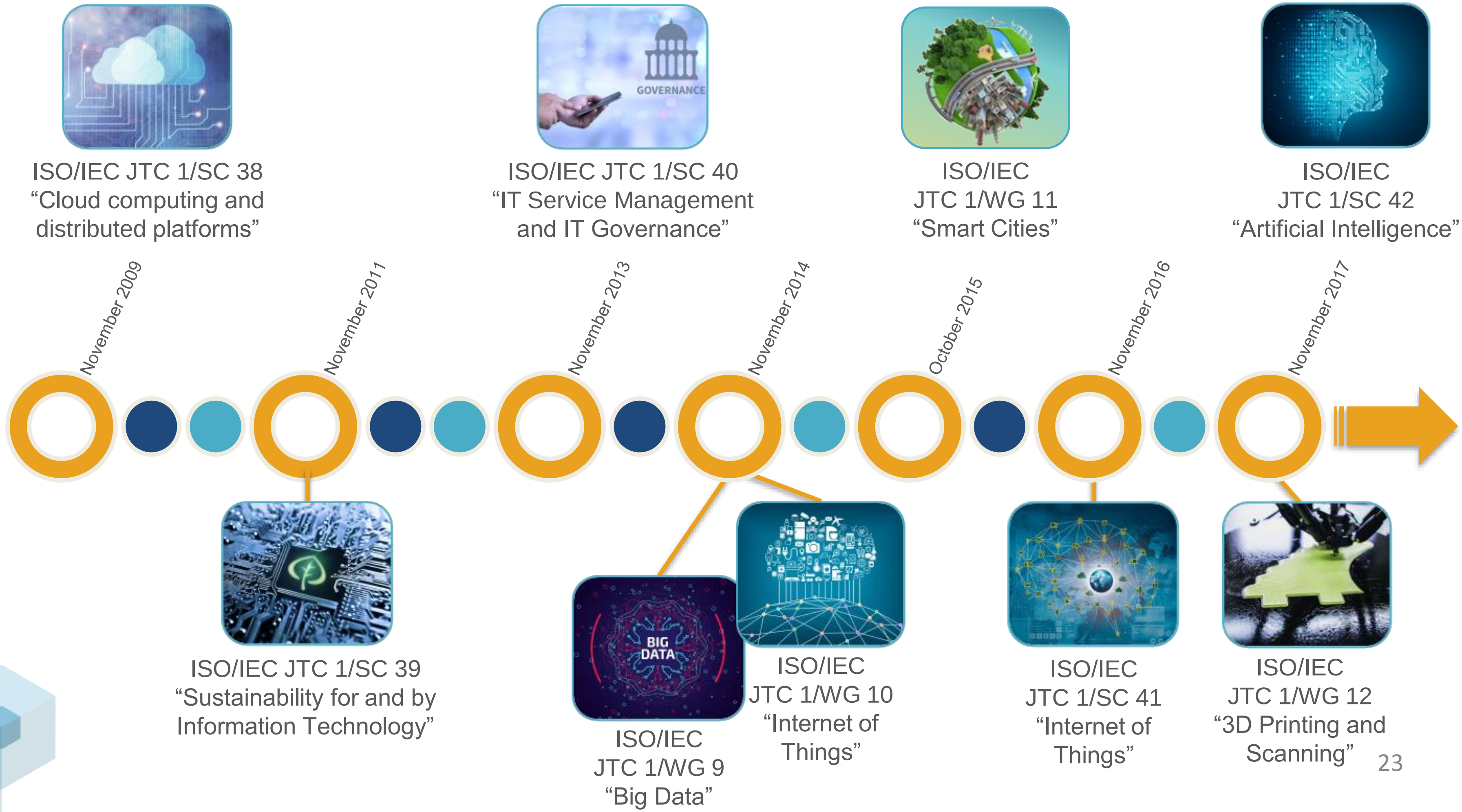
– **ILNAS**

  - Presidency of the National Mirror Committee
  - Participation in the annual Plenary Meetings
  - The Grand-Duchy of Luxembourg is Participating Member (P-Member)
  - Transmission of relevant information to the market
  - Use of relevant information to develop "Education and research" in standardization
  - Enhances the visibility of the Grand Duchy of Luxembourg at international level / ICT technical standardization
  - Stronger positioning to vote and comment standardization projects
  - Added value for the digital and general economy

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS

ISO/IEC JTC 1 - A technical committee in constant evolution to follow the technological progress and answer market needs



November 2009

ISO/IEC JTC 1/SC 38
"Cloud computing and distributed platforms"

November 2011

ISO/IEC JTC 1/SC 39
"Sustainability for and by Information Technology"

November 2013

ISO/IEC JTC 1/SC 40
"IT Service Management and IT Governance"

November 2014

ISO/IEC
JTC 1/WG 9
"Big Data"

ISO/IEC
JTC 1/WG 10
"Internet of Things"

October 2015

ISO/IEC
JTC 1/WG 11
"Smart Cities"

November 2016

ISO/IEC
JTC 1/SC 41
"Internet of Things"

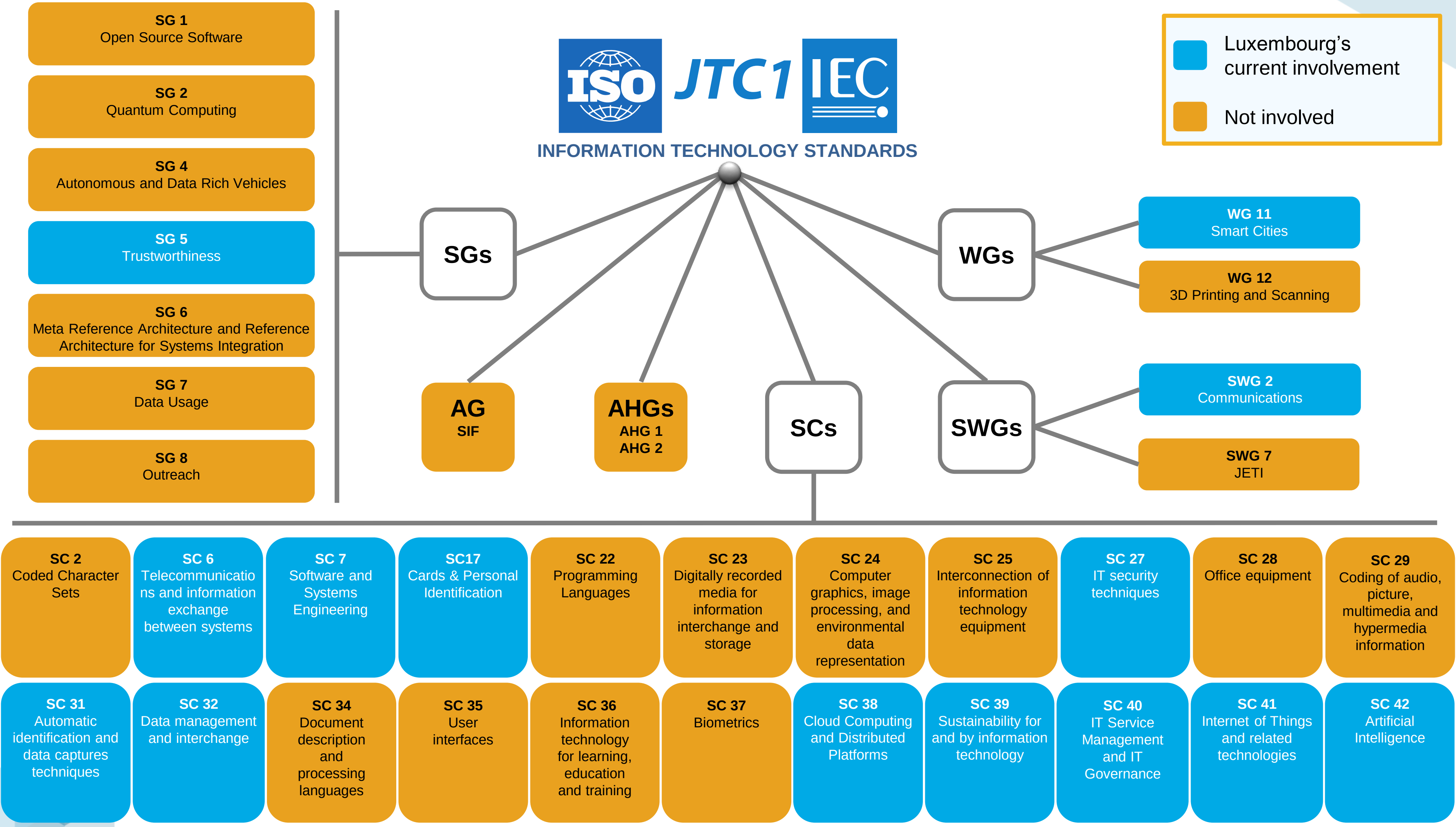
November 2017

ISO/IEC
JTC 1/SC 42
"Artificial Intelligence"

ISO/IEC
JTC 1/WG 12
"3D Printing and Scanning"

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS



🟦 Luxembourg's current involvement

🟧 Not involved

INFORMATION TECHNOLOGY STANDARDS

SGs
- 🟧 SG 1 Open Source Software
- 🟧 SG 2 Quantum Computing
- 🟧 SG 4 Autonomous and Data Rich Vehicles
- 🟦 SG 5 Trustworthiness
- 🟧 SG 6 Meta Reference Architecture and Reference Architecture for Systems Integration
- 🟧 SG 7 Data Usage
- 🟧 SG 8 Outreach

WGs
- 🟦 WG 11 Smart Cities
- 🟧 WG 12 3D Printing and Scanning

🟧 AG SIF

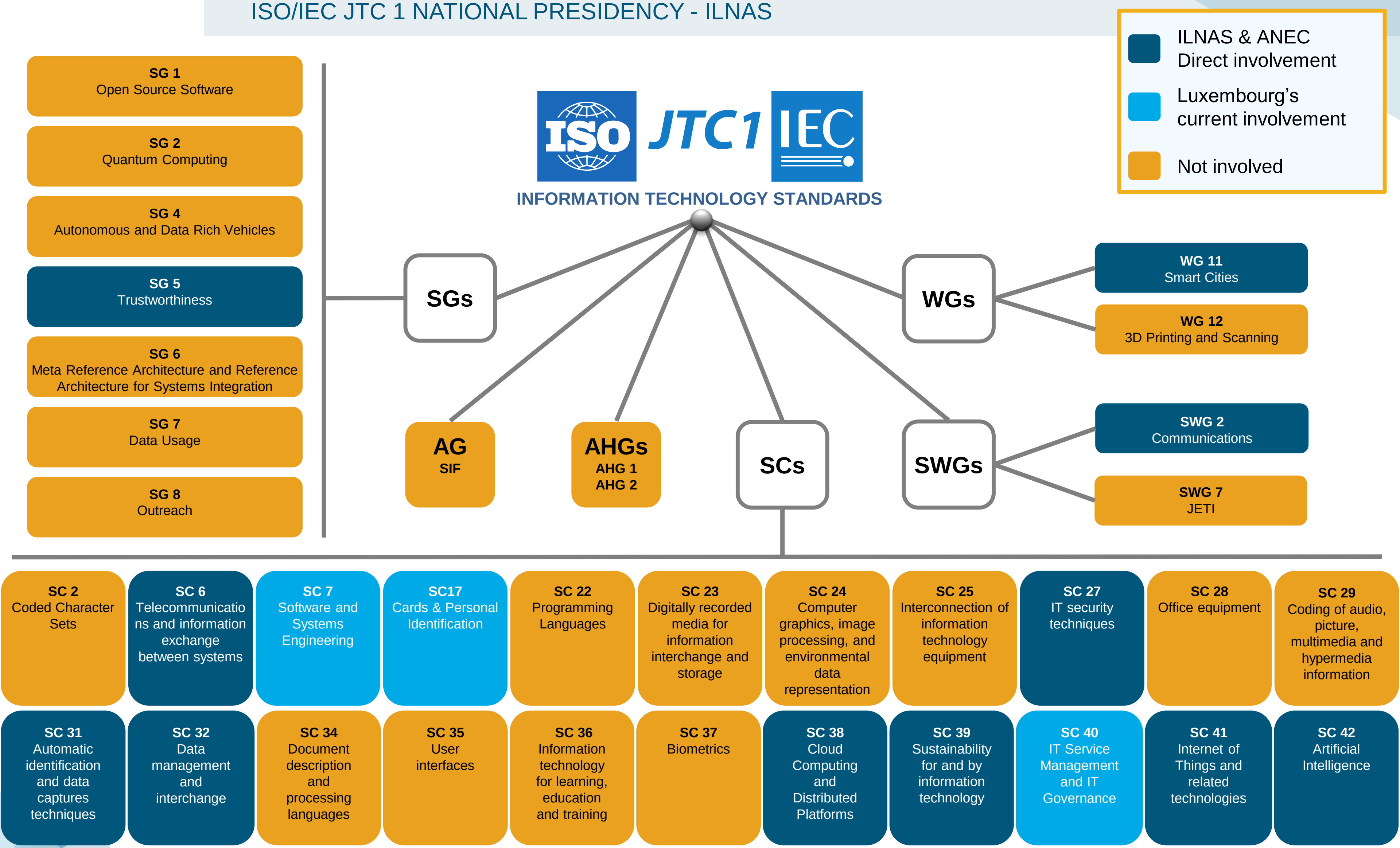
🟧 AHGs AHG 1 AHG 2

SWGs
- 🟦 SWG 2 Communications
- 🟧 SWG 7 JETI

SCs
- 🟧 SC 2 Coded Character Sets
- 🟦 SC 6 Telecommunications and information exchange between systems
- 🟦 SC 7 Software and Systems Engineering
- 🟦 SC17 Cards & Personal Identification
- 🟧 SC 22 Programming Languages
- 🟧 SC 23 Digitally recorded media for information interchange and storage
- 🟧 SC 24 Computer graphics, image processing, and environmental data representation
- 🟧 SC 25 Interconnection of information technology equipment
- 🟦 SC 27 IT security techniques
- 🟧 SC 28 Office equipment
- 🟧 SC 29 Coding of audio, picture, multimedia and hypermedia information
- 🟦 SC 31 Automatic identification and data captures techniques
- 🟦 SC 32 Data management and interchange
- 🟧 SC 34 Document description and processing languages
- 🟧 SC 35 User interfaces
- 🟧 SC 36 Information technology for learning, education and training
- 🟧 SC 37 Biometrics
- 🟦 SC 38 Cloud Computing and Distributed Platforms
- 🟦 SC 39 Sustainability for and by information technology
- 🟦 SC 40 IT Service Management and IT Governance
- 🟦 SC 41 Internet of Things and related technologies
- 🟦 SC 42 Artificial Intelligence

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS



🟦 ILNAS & ANEC Direct involvement

🔷 Luxembourg's current involvement

🟧 Not involved

ISO JTC1 IEC

INFORMATION TECHNOLOGY STANDARDS

SGs

- SG 1 Open Source Software
- SG 2 Quantum Computing
- SG 4 Autonomous and Data Rich Vehicles
- SG 5 Trustworthiness
- SG 6 Meta Reference Architecture and Reference Architecture for Systems Integration
- SG 7 Data Usage
- SG 8 Outreach

AG SIF

AHGs AHG 1 AHG 2

WGs

- WG 11 Smart Cities
- WG 12 3D Printing and Scanning

SWGs

- SWG 2 Communications
- SWG 7 JETI

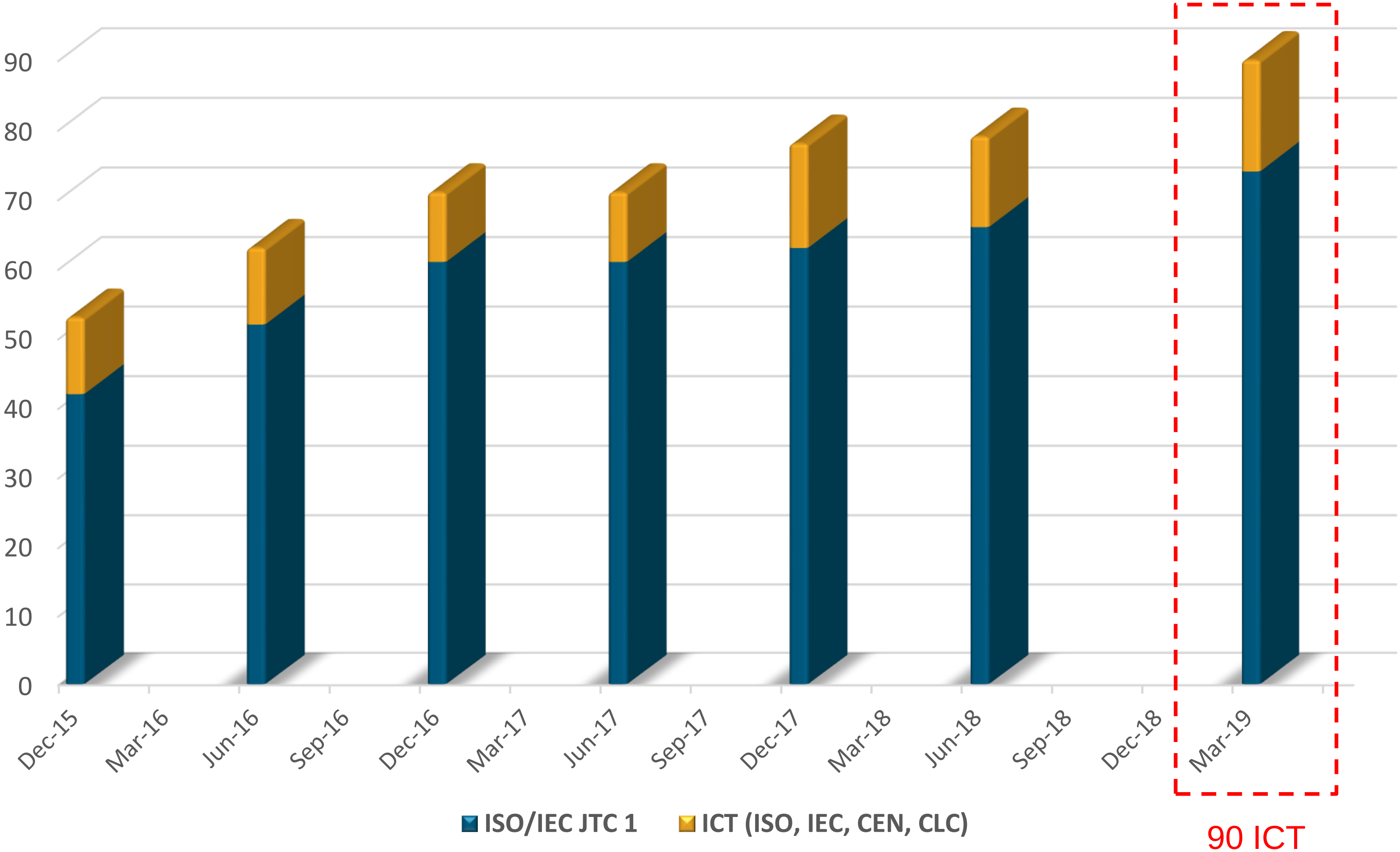
SCs

SC 2 Coded Character Sets	SC 6 Telecommunications and information exchange between systems	SC 7 Software and Systems Engineering	SC17 Cards & Personal Identification	SC 22 Programming Languages	SC 23 Digitally recorded media for information interchange and storage	SC 24 Computer graphics, image processing, and environmental data representation	SC 25 Interconnection of information technology equipment	SC 27 IT security techniques	SC 28 Office equipment	SC 29 Coding of audio, picture, multimedia and hypermedia information
SC 31 Automatic identification and data captures techniques	SC 32 Data management and interchange	SC 34 Document description and processing languages	SC 35 User interfaces	SC 36 Information technology for learning, education and training	SC 37 Biometrics	SC 38 Cloud Computing and Distributed Platforms	SC 39 Sustainability for and by information technology	SC 40 IT Service Management and IT Governance	SC 41 Internet of Things and related technologies	SC 42 Artificial Intelligence

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS

Evolution of the number of standardization delegates in the ICT sector

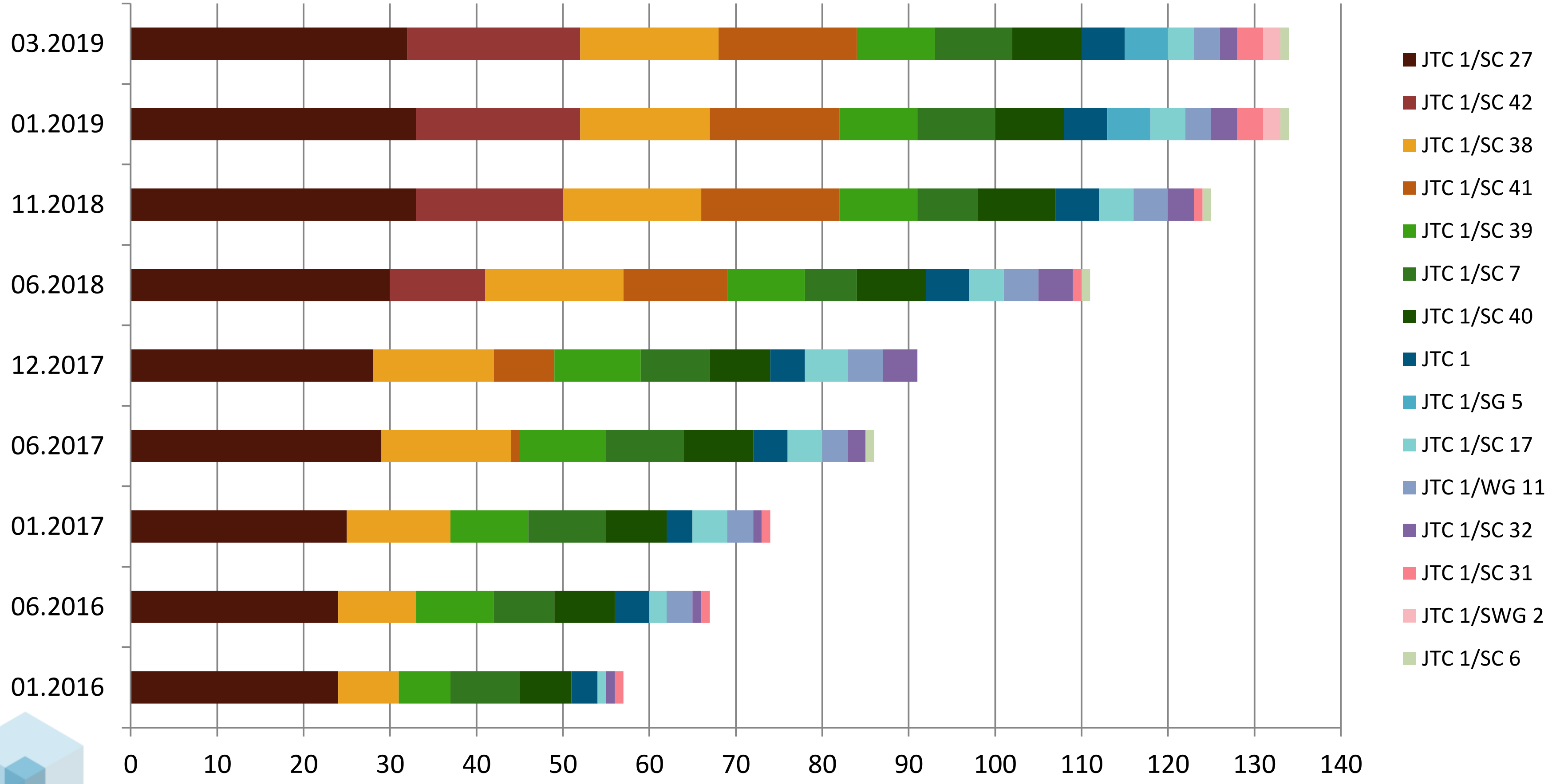


90 ICT delegates

SMART SECURE ICT - AN ECOSYSTEM

ISO/IEC JTC 1 NATIONAL PRESIDENCY - ILNAS

- **Top representation in JTC 1:**
  - 32 delegates in the IT security domain
  - 16 delegates in the Cloud Computing domain
  - 16 delegates in the IoT domain
  - 20 delegates in the Artificial Intelligence / Big Data domains



Registre national des délégués en normalisation - March 2019

Presentation of the Standards Analysis Smart Secure ICT Luxembourg

CONTENT

I - Context and objectives of the Standards Analysis Smart Secure ICT

II - Results of the Standards Analysis

III - Opportunities for the national market

CONTENT

I - Context and objectives of the Standards Analysis Smart Secure ICT

II - Results of the Standards Analysis

III - Opportunities for the national market

I. Context and objectives of the Standards Analysis Smart Secure ICT

A. Context

LUXEMBOURG
STANDARDIZATION STRATEGY
2014-2020

"Technical standardization as a service"

Policy on ICT technical standardization (2015-2020)

ILNAS

Pillar 1: Information and communication technologies (ICT)

1 Developing the interest and the involvement of the market

2 Promoting and reinforcing market participation

3 Supporting and strengthening the EaS and related research activities

- https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-2014-2020.html
- https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-TIC-2015-2020.html

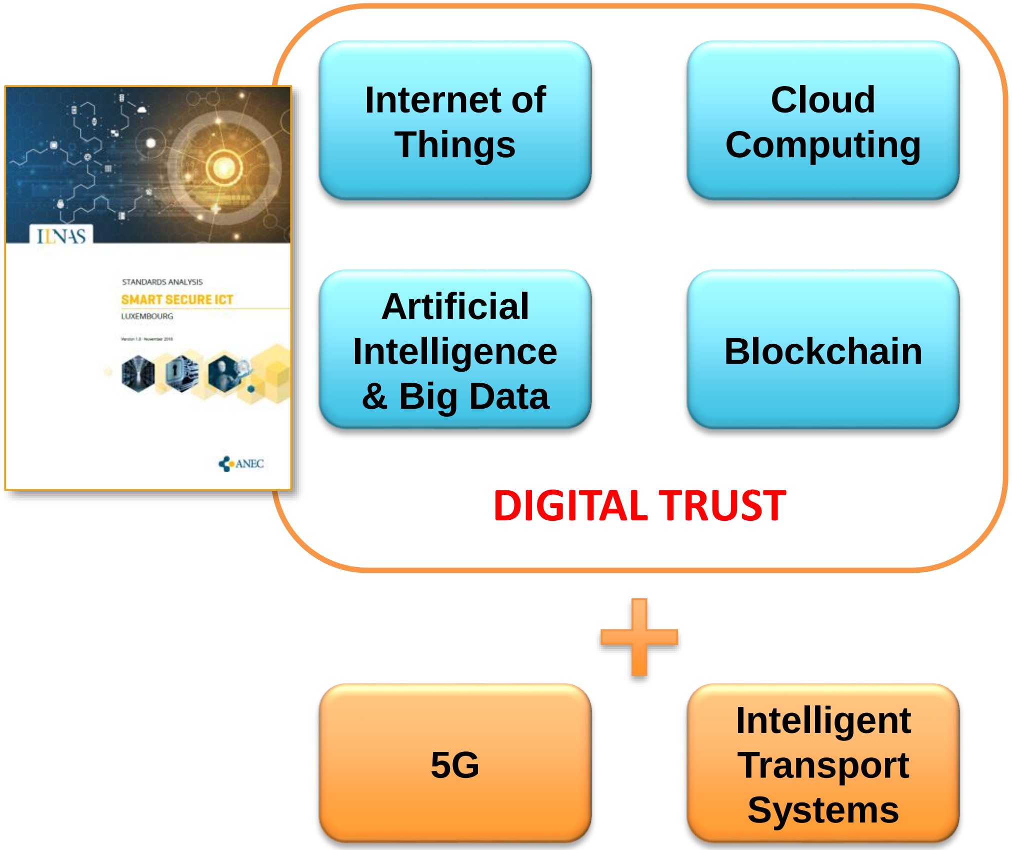
I. Context and objectives of the Standards Analysis Smart Secure ICT

A. Context

→ Relies on previous ILNAS Smart ICT publications

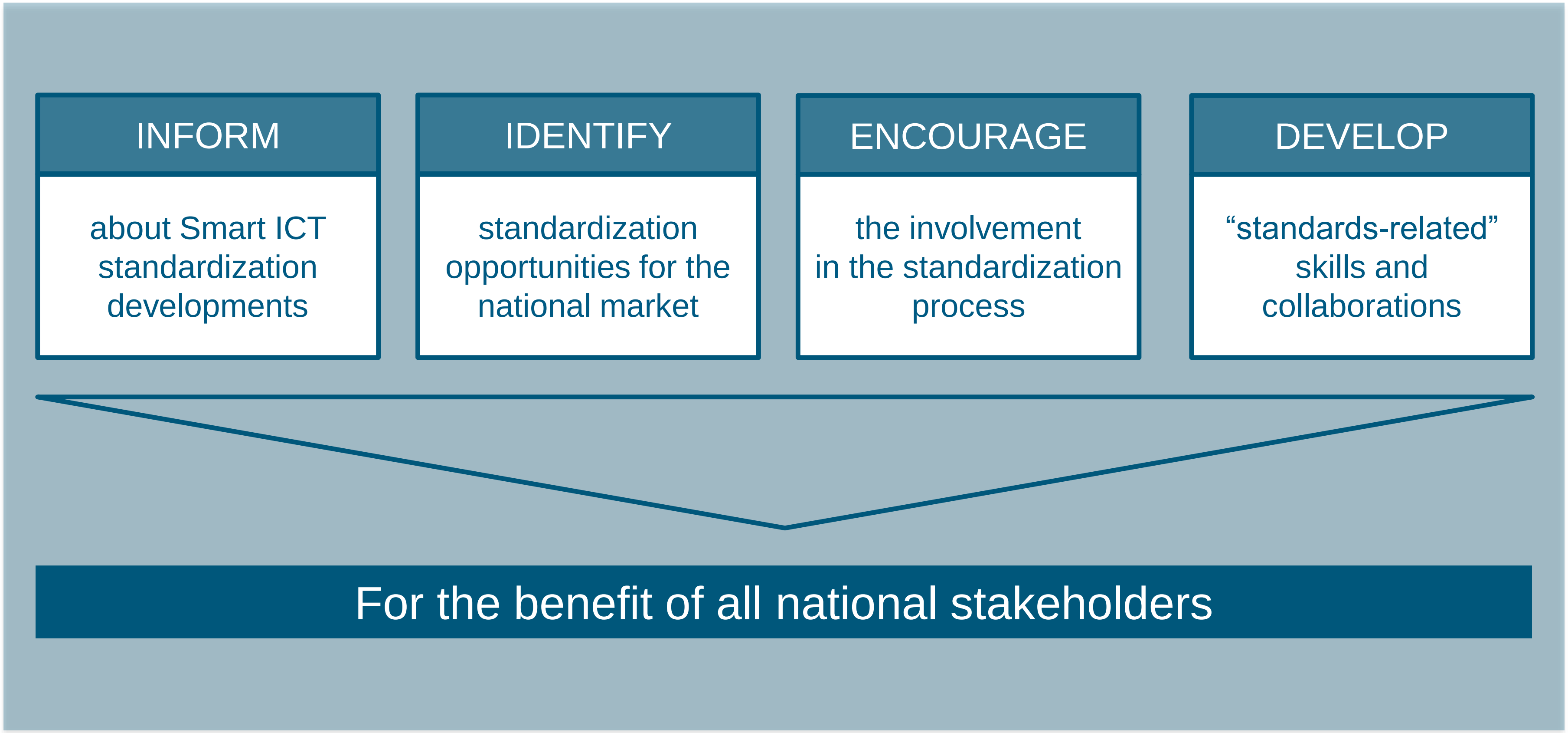
→ Focuses on **four Smart ICT areas**, considering **related Digital Trust** challenges and developments from a standardization perspective

→ Introduces **two new topics** currently receiving particular interest from the market and highly interrelated with Smart ICT



I. Context and objectives of the Standards Analysis Smart Secure ICT

B. Objectives



INFORM

about Smart ICT standardization developments

IDENTIFY

standardization opportunities for the national market

ENCOURAGE

the involvement in the standardization process

DEVELOP

“standards-related” skills and collaborations

For the benefit of all national stakeholders

I. Context and objectives of the Standards Analysis Smart Secure ICT

C. Scope of the Standards Analysis

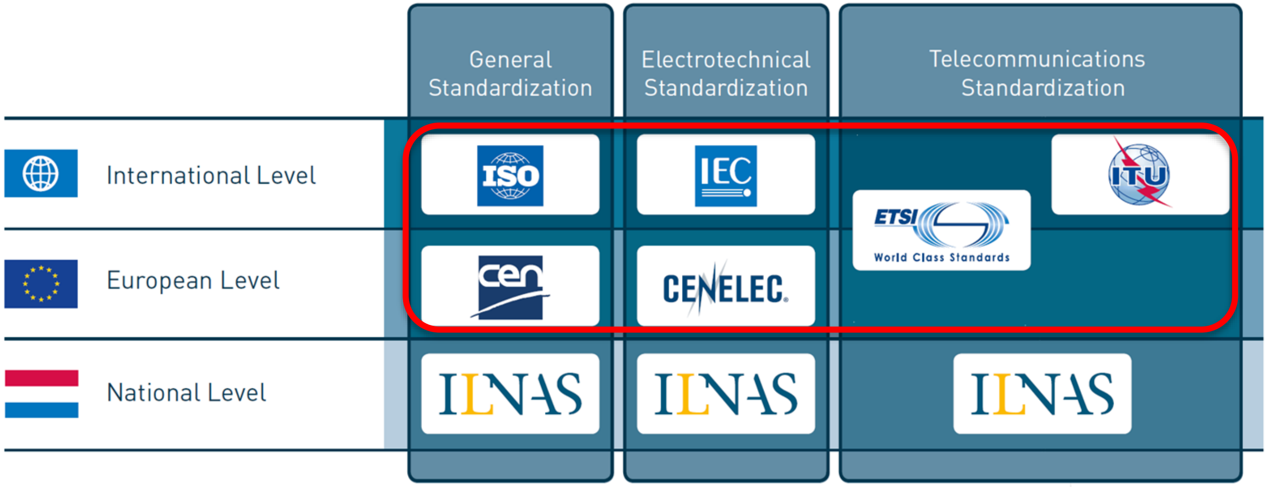
- **Introduction of Smart ICT technologies main characteristics**

- **Identification and presentation of relevant standardization technical committees**

- **Introduction of basic components of Digital Trust for Smart ICT**

- **Identification and presentation of standards published or in development in the selected Smart ICT areas as well as Digital Trust standards developments related to these areas**

- **Identification and presentation of standardization opportunities offered to the national stakeholders in Luxembourg**



	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
International Level	ISO	IEC	ITU
European Level	cen	CENELEC	ETSI World Class Standards
National Level	ILNAS	ILNAS	ILNAS

CONTENT

I - Context and objectives of the Standards Analysis Smart Secure ICT

II - Results of the Standards Analysis

III - Opportunities for the national market

II. Results of the Standards Analysis

A. Presentation of the results

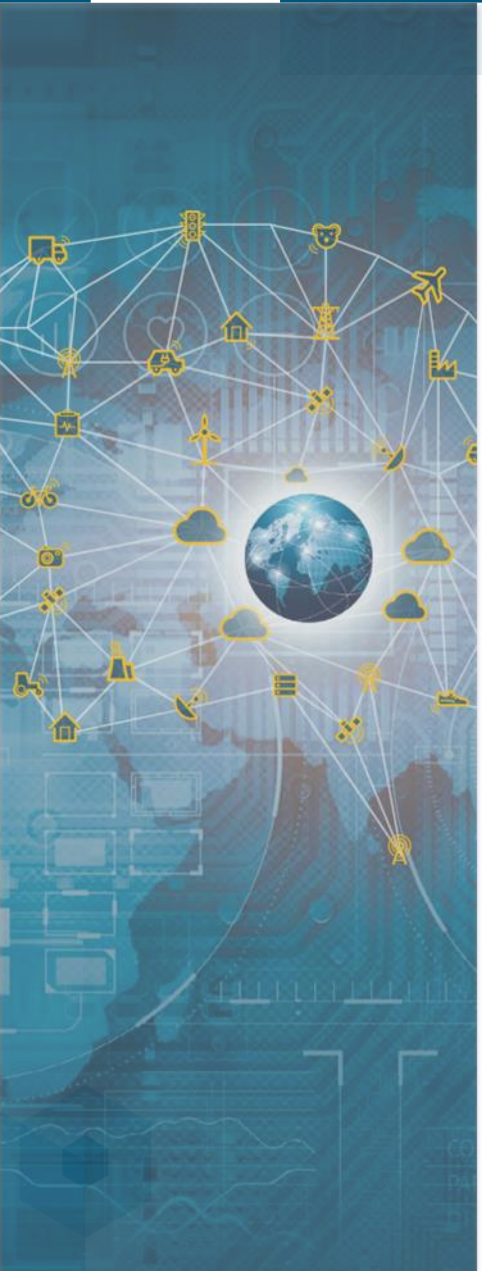
- **Smart ICT definition**

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

- **Introduction of fundamental concepts of Smart ICT and related Digital Trust aspects based on standards**
  - **Internet of Things**: ISO/IEC 20924:2018, Definitions and vocabulary (*new*)
  - **Cloud Computing**: ISO/IEC 17788:2014, Overview and vocabulary
  - **Artificial Intelligence and Big Data**:
    - ISO/IEC 20546:2019, Big Data -- Definition and Vocabulary (*new*)
    - ISO/IEC 22989, Artificial Intelligence Concepts and Terminology (*under development*)
  - **Blockchain and Distributed Ledger Technologies**: ISO 22739, Terminology and concepts (*under development*)
  - **Basic Components of Digital Trust**
    - **Privacy**
    - **Data and Information Security**
    - **Interoperability**

II. Results of the Standards Analysis

B. Internet of Things



- **TECHNICAL COMMITTEES (6)**
  - ISO/IEC JTC 1/SC 41 “Internet of Things and related technologies”
  - ISO/IEC JTC 1/SC 31 “Automatic identification and data capture techniques”
  - ISO/IEC JTC 1/SC 25 “Interconnection of information technology equipment”
  - CEN/TC 225 “AIDC Technologies”
  - ETSI/TC SmartM2M “Smart Machine-to-Machine Communication”
  - ITU-T/SG 20 “Internet of Things, smart cities and communities”

- **PUBLISHED STANDARDS (43)**
  - ISO/IEC 30141:2018, Information technology -- Internet of Things -- Internet of Things Reference Architecture (IoT RA)
  - ISO/IEC TR 22417:2017, Information technology - Internet of things (IoT) - IoT use cases
  - ISO/IEC 21823-1:2019, Internet of things (IoT) -- Interoperability for Internet of things systems -- Part 1: Framework (*new*)
  - …

- **STANDARDS UNDER DEVELOPMENT (79)**
  - ISO/IEC NP 30161, Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services
  - …

II. Results of the Standards Analysis

C. Cloud Computing

- **TECHNICAL COMMITTEES (2)**
  - ISO/IEC JTC 1/SC 38 “Cloud Computing and Distributed Platforms”
  - ITU-T/SG 13 “Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures”

- **PUBLISHED STANDARDS (40)**
  - ISO/IEC 19941:2017, Information technology -- Cloud computing – Interoperability and portability
  - ISO/IEC 19944:2017, Information technology -- Cloud computing -- Cloud services and devices: Data flow, data categories and data use
  - ISO/IEC TR 22678:2019, Information Technologies -- Cloud Computing -- Guidance for Policy Development (*new*)
  - …

- **STANDARDS UNDER DEVELOPMENT (28)**
  - ISO/IEC CD 22123, Information technology -- Cloud computing -- Concepts and terminology
  - ISO/IEC NP TR 23951, Cloud computing -- Best practices for cloud SLA metrics (*new*)
  - …

II. Results of the Standards Analysis

D. Artificial Intelligence and Big Data

- **TECHNICAL COMMITTEES (2)**
  - ISO/IEC JTC 1/SC 42 “Artificial Intelligence”
  - ISO/IEC JTC 1/SC 32 “Data management and interchange”

- **PUBLISHED STANDARDS (26)**
  - ISO/IEC 20546:2019, Information technology -- Big Data -- Overview and Vocabulary (*new*)
  - ISO/IEC TR 20547-2:2018, Information technology – Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
  - ISO/IEC TR 20547-5:2018, Information technology -- Big data reference architecture -- Part 5: Standards roadmap
  - …

- **STANDARDS UNDER DEVELOPMENT (28)**
  - ISO/IEC WD 22989, Artificial Intelligence -- Concepts and Terminology
  - ISO/IEC WD 23053, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
  - ISO/IEC NP TR 24030, Information technology -- Artificial Intelligence (AI) -- Use cases (*new*)
  - …

II. Results of the Standards Analysis

E. Blockchain and Distributed Ledger Technologies

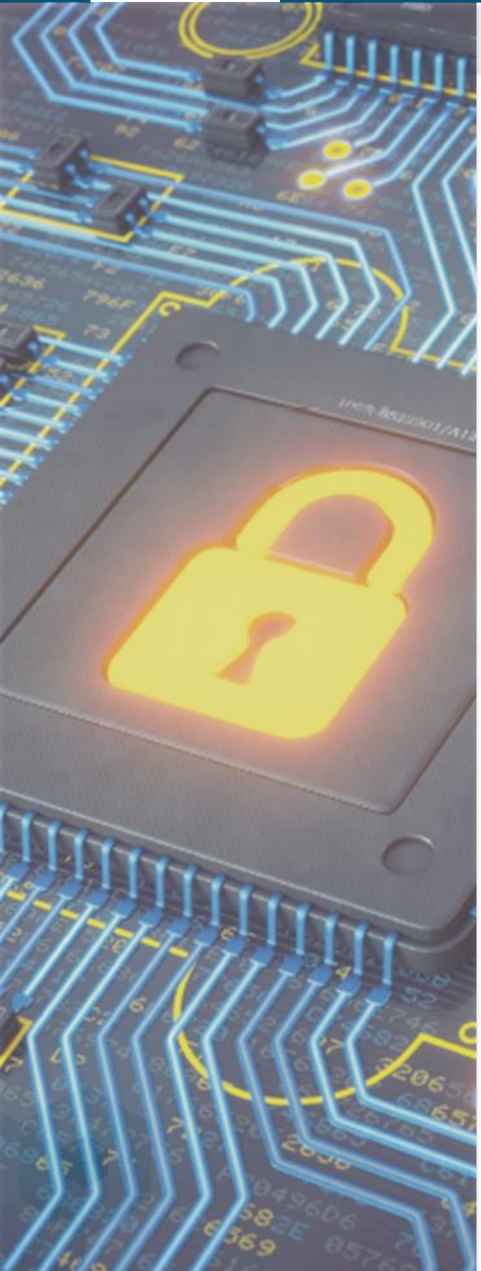
- **TECHNICAL COMMITTEES (2)**
  - ISO/TC 307 “Blockchain and distributed ledger technologies”
  - ITU-T/FG-DLT “Focus Group on Application of Distributed Ledger Technology”

- **PUBLISHED STANDARDS (0)**

- **STANDARDS UNDER DEVELOPMENT (11)**
  - ISO/CD 22739, Blockchain and distributed ledger technologies – Terminology
  - ISO/AWI TS 23259, Blockchain and distributed ledger technologies -- Legally binding smart contracts
  - ISO/NP TR 23246, Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies
  - …

II. Results of the Standards Analysis

F. Digital Trust in Smart ICT



- **TECHNICAL COMMITTEES (8)**
  - ISO/IEC JTC 1/SC 17 “Cards and personal identification”
  - ISO/IEC JTC 1/SC 27 “IT Security techniques”
  - CEN/CLC/JTC 13 “Cybersecurity and Data Protection”
  - ETSI/TC CYBER “Cyber Security”
  - …

- **PUBLISHED STANDARDS (20) → Digital Trust aspects of Smart ICT**
  - **IoT:** ETSI TS 118 103 V2.4.1 (09/2016), oneM2M; Security solutions (oneM2M TS-0003 version 2.4.1 Release 2)
  - **Cloud Computing:**
    - 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 19086-4:2019, Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy (*new*)
  - …

- **STANDARDS UNDER DEVELOPMENT (28)**
  - **Internet of Things:**
    - ISO/IEC 30149, Trustworthiness framework
    - ISO/IEC WD 27030, Security techniques -- Guidelines for security and privacy in Internet of Things (*new*)
  - **Big Data:** ISO/IEC CD 20547-4, Information technology -- Big data reference architecture -- Part 4: Security and privacy
  - …

II. Results of the Standards Analysis

G. Introduction on 5G and ITS

→ **Introduction on 2 topics that could significantly transform the economy and society in relation with Smart ICT development**

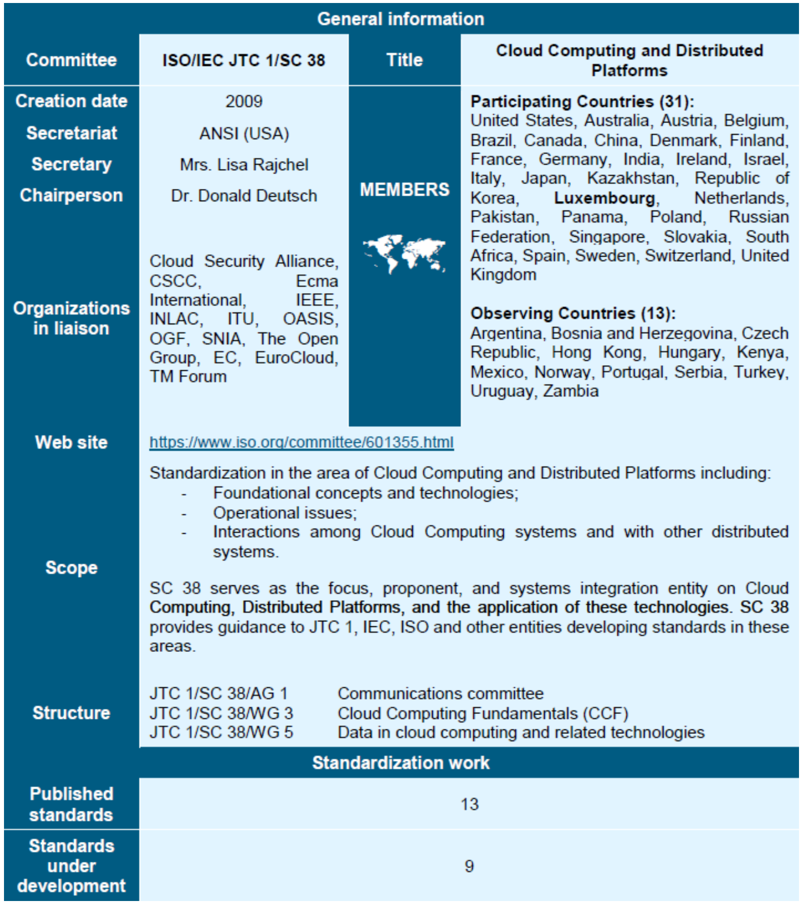
- **5G Technical standardization**
  - 1 Technical Committee
    - ITU-T/FG NET-2030 “Focus Group Technologies for Network 2030 (FG NET-2030)”

- **Intelligent Transport Systems Technical Standardization**
  - 3 Technical Committees
    - ISO/TC 204 “Intelligent transport systems”
    - CEN/TC 278 “Intelligent transport systems”
    - ETSI/TC ITS “Automotive Intelligent Transport”

II. Results of the Standards Analysis

H. Presentation of the results

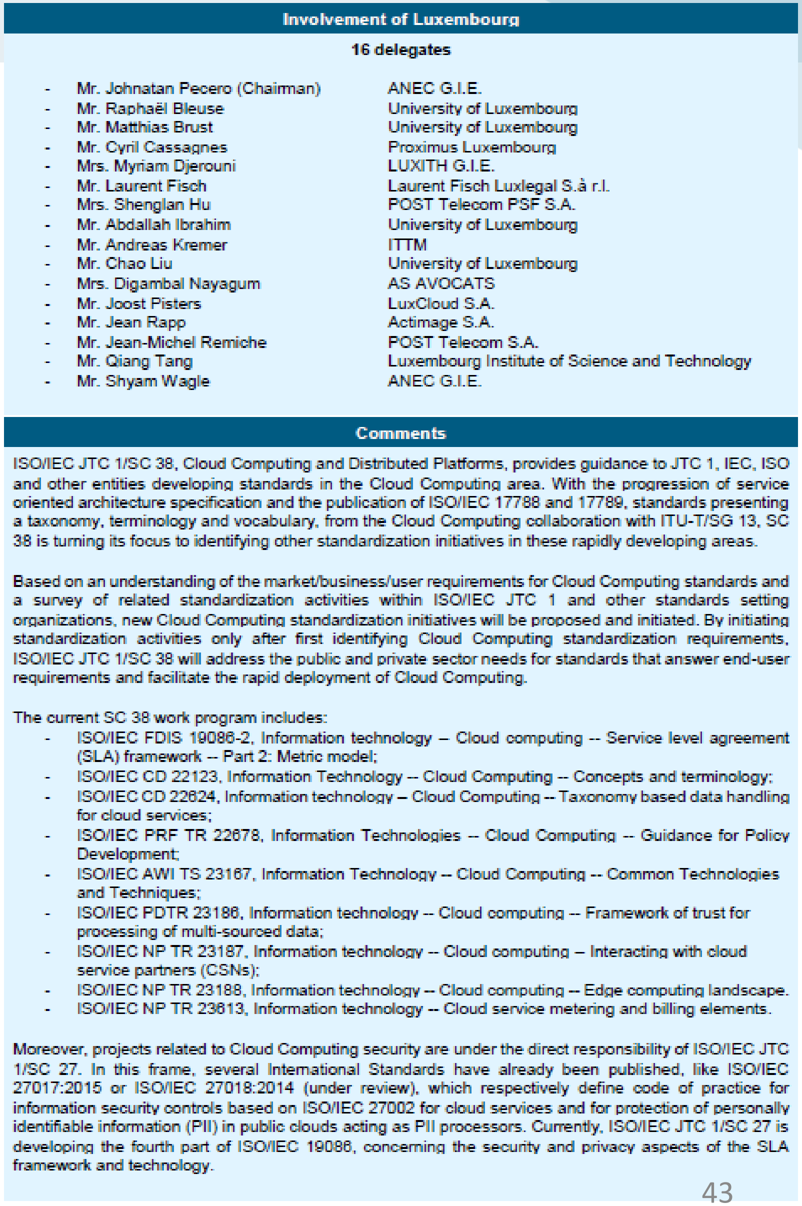
- **Presentation of the technical committees using ID-Cards**



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

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

Secretariat	ANSI (USA)		
Secretary	Mrs. Lisa Rajchel		
Chairperson	Dr. Donald Deutsch		
Organizations in liaison	Cloud Security Alliance, CSCC, Ecma International, IEEE, INLAC, ITU, OASIS, OGF, SNIA, The Open Group, EC, EuroCloud, TM Forum		
Web site	https://www.iso.org/committee/601355.html		
Scope	Standardization in the area of Cloud Computing and Distributed Platforms including: - Foundational concepts and technologies; - Operational issues; - Interactions among Cloud Computing systems and with other distributed systems. SC 38 serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in these areas.		
Structure	JTC 1/SC 38/AG 1 Communications committee JTC 1/SC 38/WG 3 Cloud Computing Fundamentals (CCF) JTC 1/SC 38/WG 5 Data in cloud computing and related technologies		
	Standardization work		
Published standards	13		
Standards under development	9		



Involvement of Luxembourg

16 delegates

- Mr. Johnatan Pecero (Chairman)	ANEC G.I.E.
- Mr. Raphaël Bleuse	University of Luxembourg
- Mr. Matthias Brust	University of Luxembourg
- Mr. Cyril Cassagnes	Proximus Luxembourg
- Mrs. Myriam Djerouni	LUXITH G.I.E.
- Mr. Laurent Fisch	Laurent Fisch Luxlegal S.à r.l.
- Mrs. Shenglan Hu	POST Telecom PSF S.A.
- Mr. Abdallah Ibrahim	University of Luxembourg
- Mr. Andreas Kremer	ITTM
- Mr. Chao Liu	University of Luxembourg
- Mrs. Digambal Nayagum	AS AVOCATS
- Mr. Joost Pisters	LuxCloud S.A.
- Mr. Jean Rapp	Actimage S.A.
- Mr. Jean-Michel Remiche	POST Telecom S.A.
- Mr. Qiang Tang	Luxembourg Institute of Science and Technology
- Mr. Shyam Wagle	ANEC G.I.E.

Comments

ISO/IEC JTC 1/SC 38, Cloud Computing and Distributed Platforms, provides guidance to JTC 1, IEC, ISO and other entities developing standards in the Cloud Computing area. With the progression of service oriented architecture specification and the publication of ISO/IEC 17788 and 17789, standards presenting a taxonomy, terminology and vocabulary, from the Cloud Computing collaboration with ITU-T/SG 13, SC 38 is turning its focus to identifying other standardization initiatives in these rapidly developing areas.

Based on an understanding of the market/business/user requirements for Cloud Computing standards and a survey of related standardization activities within ISO/IEC JTC 1 and other standards setting organizations, new Cloud Computing standardization initiatives will be proposed and initiated. By initiating standardization activities only after first identifying Cloud Computing standardization requirements, ISO/IEC JTC 1/SC 38 will address the public and private sector needs for standards that answer end-user requirements and facilitate the rapid deployment of Cloud Computing.

The current SC 38 work program includes:

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

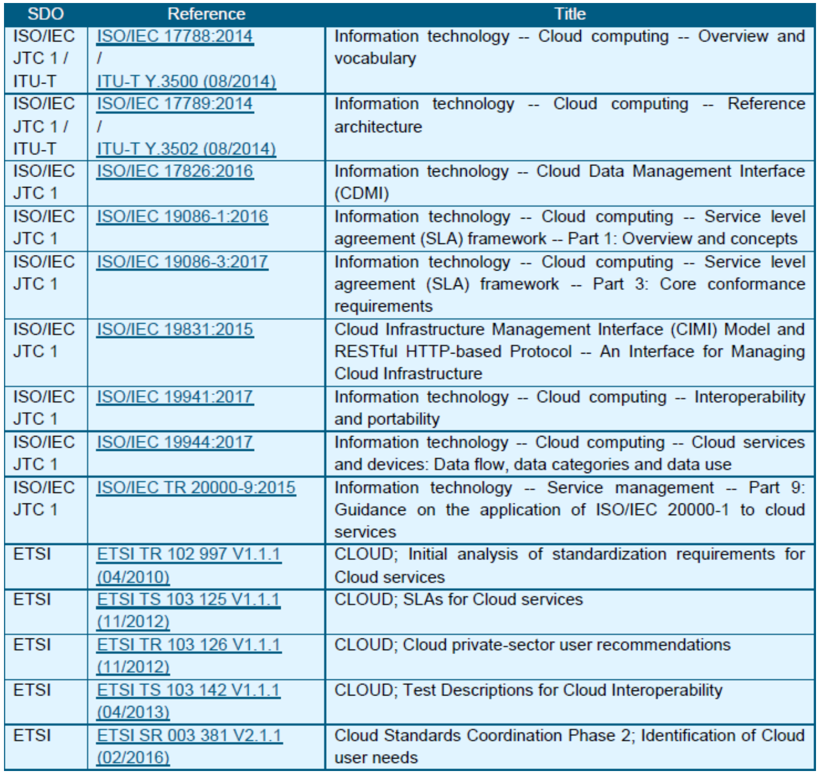
Moreover, projects related to Cloud Computing security are under the direct responsibility of ISO/IEC JTC 1/SC 27. In this frame, several International Standards have already been published, like ISO/IEC 27017:2015 or ISO/IEC 27018:2014 (under review), which respectively define code of practice for information security controls based on ISO/IEC 27002 for cloud services and for protection of personally identifiable information (PII) in public clouds acting as PII processors. Currently, ISO/IEC JTC 1/SC 27 is developing the fourth part of ISO/IEC 19086, concerning the security and privacy aspects of the SLA framework and technology.

II. Results of the Standards Analysis

H. Presentation of the results

- **Published standards and standards projects listed in the Appendix**
  - Areas concerned: IoT, Cloud Computing, Artificial Intelligence and Big Data
  - Information provided:
    - Standards (published / under development)
    - **Digital Trust related standards (published / under development)**

e.g.: Cloud Computing



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

CONTENT

I - Context and objectives of the Standards Analysis Smart Secure ICT

II - Results of the Standards Analysis

III - Opportunities for the national market

III. Opportunities for the national market

Overview

INFORMATION ABOUT STANDARDIZATION

- Smart ICT workshops
- Awareness sessions
- Smart ICT standards watch
- Publications and disseminations
- Free consultation of the standards
- Smart ICT standardization research results

TRAININGS IN STANDARDIZATION

- Trainings on Smart ICT Standardization
- University certificate Smart ICT for Business Innovation

INVOLVEMENT IN STANDARDIZATION

- Become national delegate in standardization
- Comment standards under public enquiry
- Propose new standards projects
- Monitor the standardization work performed by the European Multi-Stakeholder Platform on ICT Standardization (MSP)

ILNAS

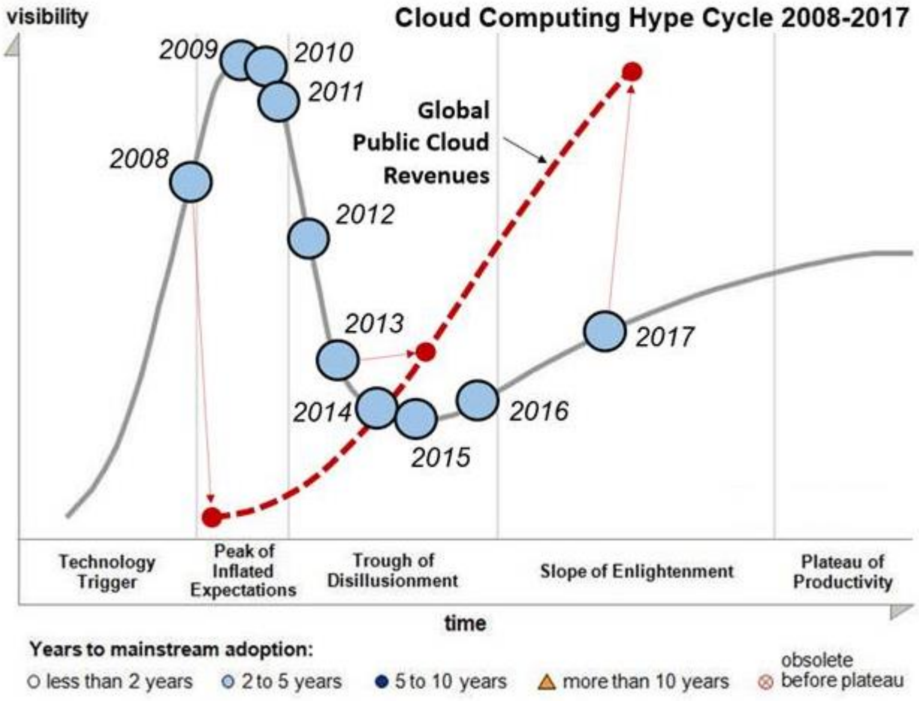
Smart Secure ICT and Technical Standardisation

Cloud Computing and Distributed Platforms

ILNAS ANEC

Cloud Computing – Currents Status

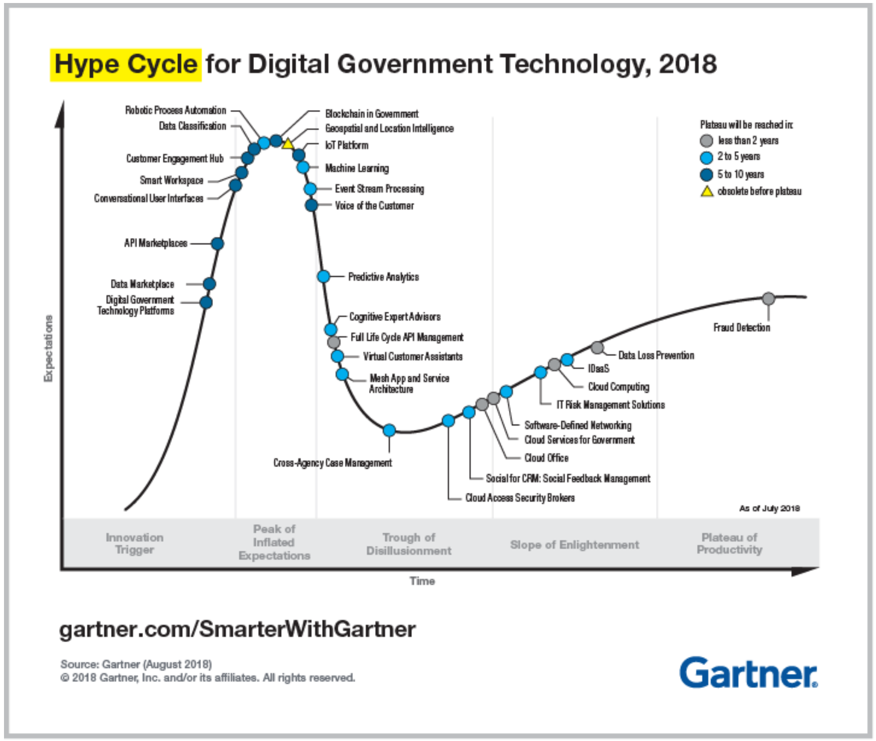
Where Cloud Computing is today


Cloud Computing Hype Cycle 2008-2017

©Sources: Gartner, Forrester Research and Phillip Nones' Blog, consulted 12/03/2019

- **Cloud Computing passed the Peak of Inflated Expectations and crossed the Through of Disillusionment**
- **Cloud Computing is approaching to the Slope of Enlightenment & Plateau of Productivity**

- **Cloud Computing is no longer the new shiny object it was 9 years ago**

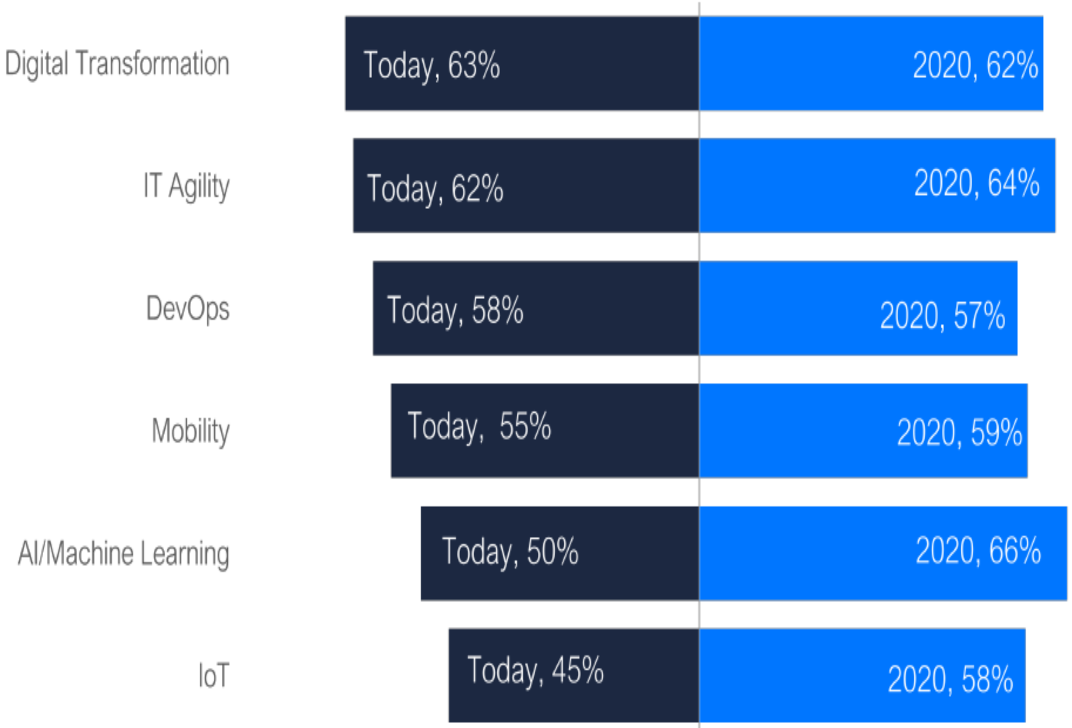

Hype Cycle for Digital Government Technology, 2018

gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Cloud Computing – The Future of Cloud 2020

Public Cloud Drivers



Source: Cloud Vision 2020: The future of the Cloud – A survey of Industry Influencers by LogicMonitor, consulted 12/03/2019

- **Cloud Computing is now becoming the back-end for all forms of computing, including the ubiquitous Internet of Things**
- **New ways of organizing compute, such as containerization and DevOps are inseparable from Cloud and accelerating the adoption of cloud**
- **Digitally transforming enterprises is the leading factor driving greater public Cloud engagement or adoption today**
- **IT agility is the second major interest from companies to move to Cloud Computing**

- **A report (LogicMonitor 2018) estimates that 83% of Enterprise Workloads will be in the Cloud by 2020**
  - 41% will run on public Cloud platforms
  - Additional 20% are predicted to be private Cloud-based
  - 22% will run on hybrid Cloud platforms

- **Artificial Intelligence and Machine Learning will be the leading catalyst driving greater Cloud Computing adoption by 2020**

Digital Trust in Cloud Computing

Cloud Computing: Allocation of responsibilities in the services models

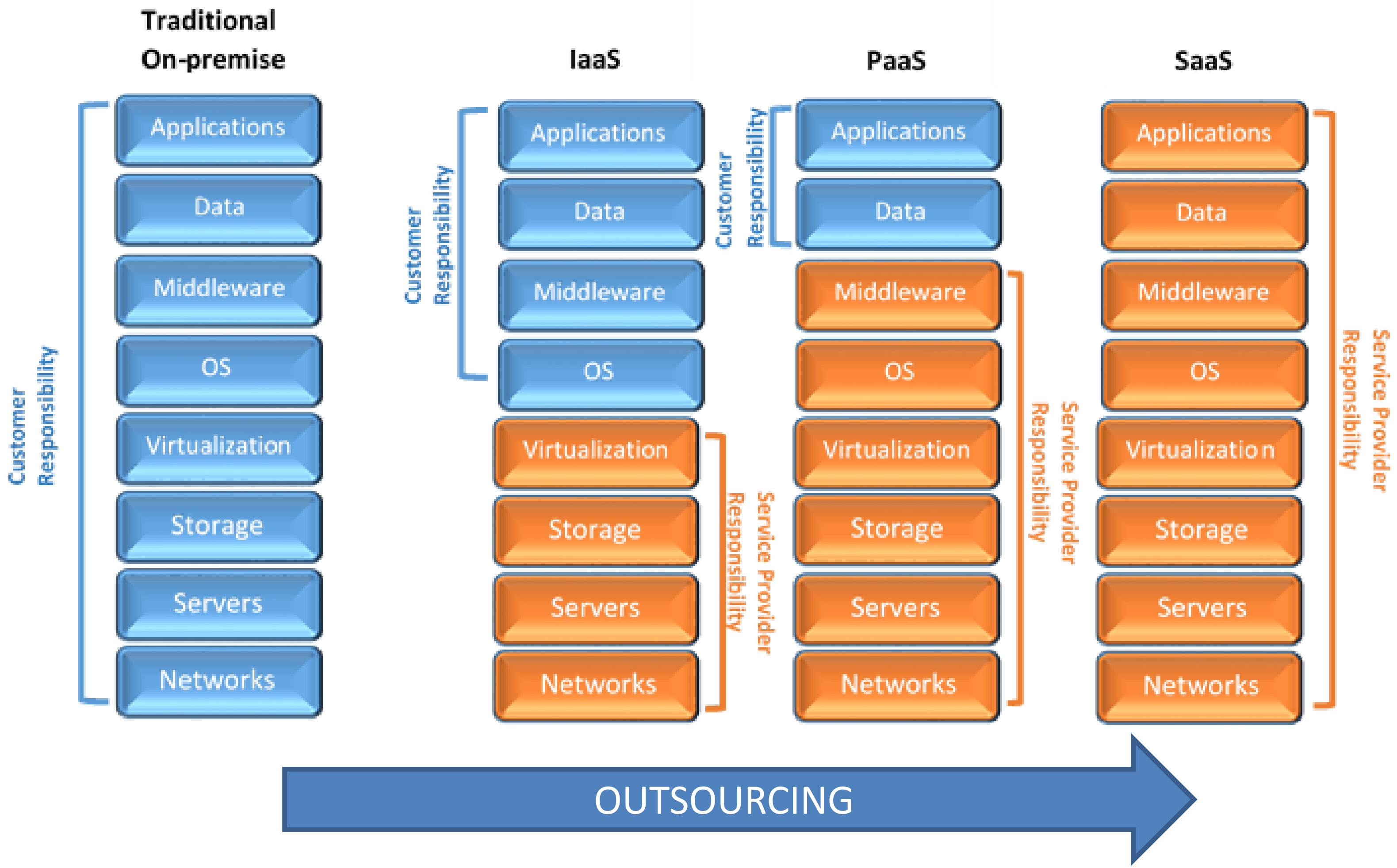


Figure : Allocation of responsibilities in the cloud computing service models

Source: ILNAS white paper: Digital Trust for Smart ICT, version 3.0, September 2017

What is (Digital) Trust for Cloud Computing?

- *“Trust is the extent to which a cloud service consumer is willing to depend on a cloud service provider, provisioning a cloud service and expects certain qualities that the cloud service provider promised to met”*

Source: T.H. Noor, Q.Z. Sheng, A. Bouguettaya: “Trust Management in Cloud Services”, 2014, Springer.

- An effective trust management service helps CSCs and CSPs reap the benefits brought by cloud computing technologies

Pillars of Trust in Cloud Computing

- *Security : Data must be secure*
- *Privacy : The privacy of individuals must be protected*
- *Compliance: national and international laws governing utilizatior and protection of data must be complied*

Trust in Cloud Computing

⇨ **Trust as a human concern**

⇨The major concerns are regarding who has access to the data and where they are physically located

⇨ **Trust as a technical challenge**

⇨Access to data

⇨Use of data

⇨Accountability

⇨ **Trust as a legal puzzle**

⇨Difficult to keep track of what resources are used and in which country

⇨Difficult to be compliance with regulations related to data handling

⇨Lack of clarity which party is responsible for ensuring that legal requirements for personal information are observed, or appropriate data handling standards are set and followed

⇨It is difficult to determine the exposure of data that is being transferred, because information passing through some countries can be accessed by law enforcement agencies

Source: ILNAS white paper: Digital Trust for Smart ICT, version 3.0, September 2017

Digital Trust concerns depending on the deployment model

⇨ **Private Cloud**

⇨Trust management does not represent a main concern if the organization does not rely on a third-party service provider

⇨ **Public Cloud**

⇨Potential risks exist regarding security, privacy and loss of control over data

⇨ **Community Cloud**

⇨If there is a third party involved, the same issues may occur as in the private cloud model, otherwise it is limited to community subjects

⇨ **Hybrid Cloud**

⇨Trust management issues related to the public model relate to the hybrid one as well

Ref: ILNAS white paper: Digital Trust for Smart ICT, version 3.0, September 2017

Digital Trust in Cloud Computing - Challenges

From the perspective of the Cloud Consumer:

1. Data security concerns
2. Reliability of service and business continuity
3. Integration and interoperability with on-premise systems
4. Weak contracts, SLAs and consequences for non-performance
5. Limited transparency
6. Loss of control
7. Immaturity of vendors
8. Vendor lock-in and data portability
9. Long-term costs and TCO uncertainties
10. Legal and regulatory compliance

From the perspective of the Cloud Provider :

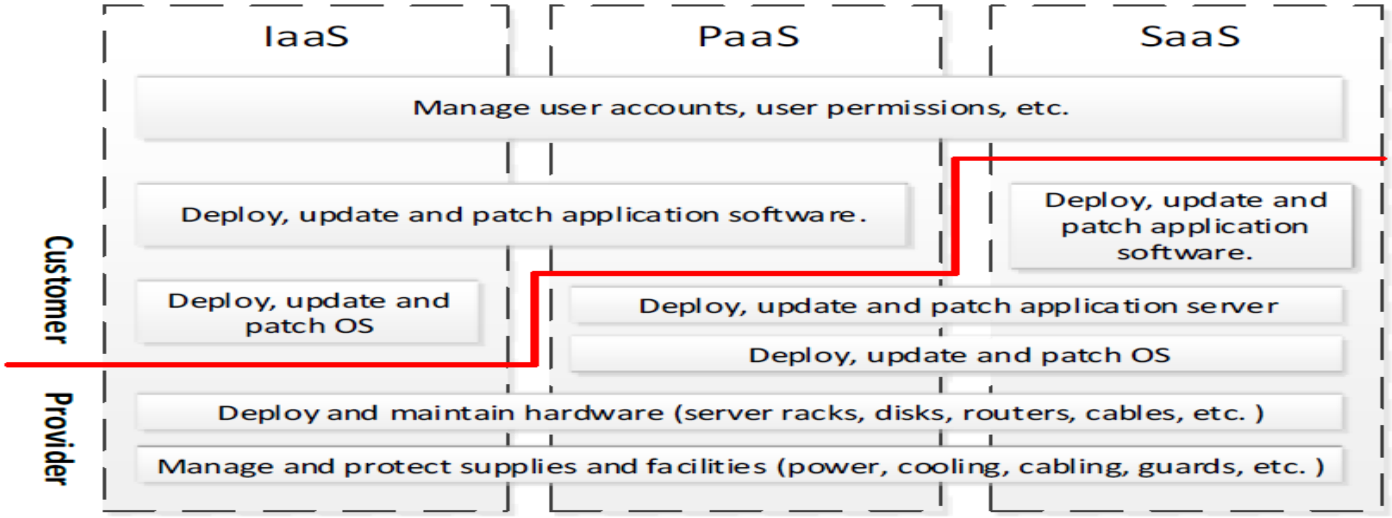
1. Joining the Cloud by users/resources dynamically
2. Different security policies
3. Continuity and provider dependency
4. Compliance with applicable regulations and good practices
5. Trust enhancement through assurance mechanisms

The resulting lack of trust could be an inhibitor for further adoption of Cloud in areas where sensitive to critical information is involved.

[25] R. K. Kalluri and C. G. Rao, “Addressing the Security, Privacy and Trust Challenges of Cloud Computing,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6094–6097, 2014.

[27] J. Mooney, *Essential Practices for Embracing the Inevitability of the Cloud*. MIT Sloan School of Management, Center for Information Systems Research, Boston, {MA}, 2012.

Security tasks outsourced in the services models



IaaS

PaaS

SaaS

Manage user accounts, user permissions, etc.

Deploy, update and patch application software.

Deploy, update and patch application software.

Deploy, update and patch OS

Deploy, update and patch application server

Deploy, update and patch OS

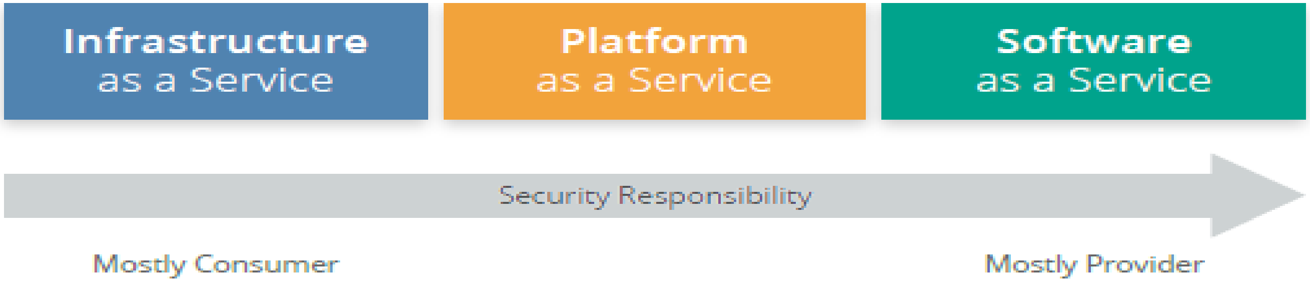
Deploy and maintain hardware (server racks, disks, routers, cables, etc.)

Manage and protect supplies and facilities (power, cooling, cabling, guards, etc.)

Customer

Provider

Figure: Division of certain (non exhaustive list) security tasks on cloud computing service models



Infrastructure as a Service

Platform as a Service

Software as a Service

Security Responsibility

Mostly Consumer

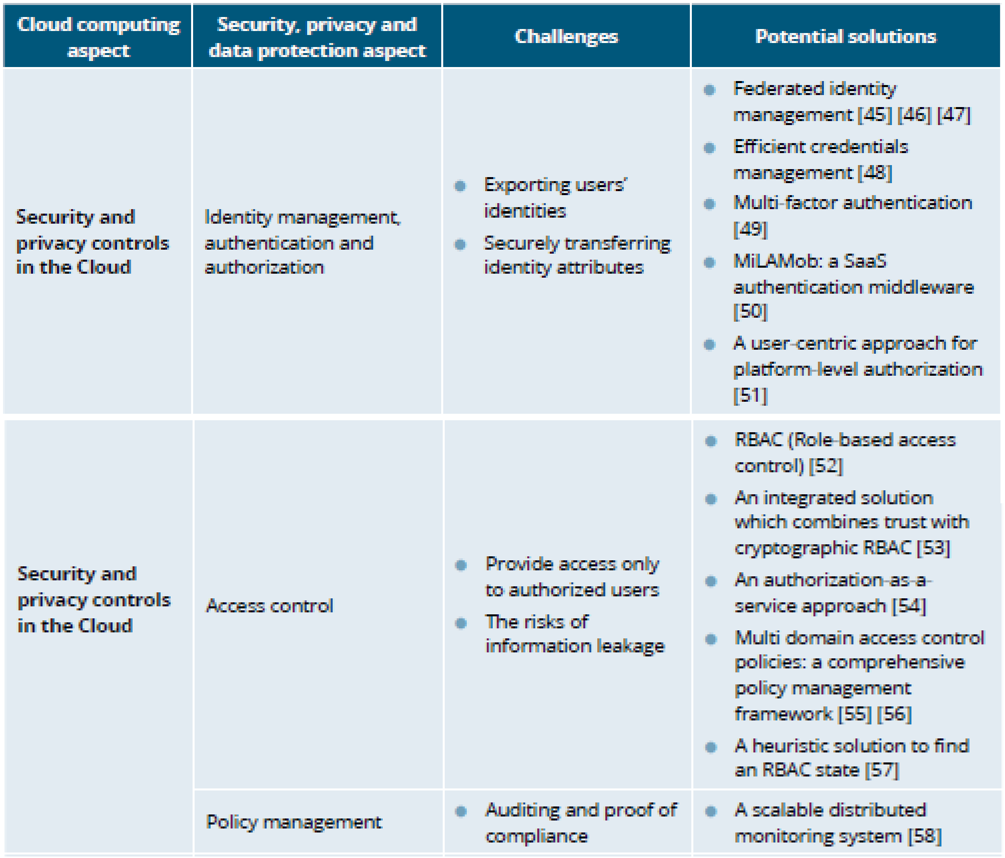
Mostly Provider

https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

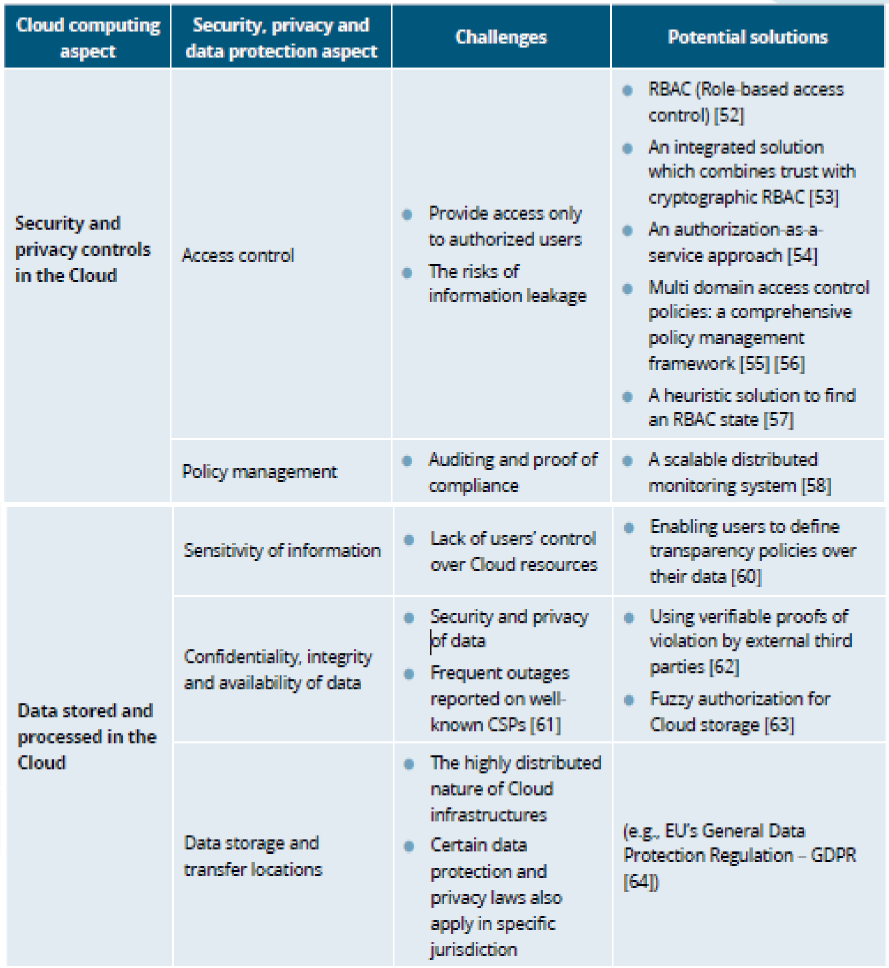
Who is responsible for what?

In practice for SMEs, it is important to carefully assess which security tasks are outsourced to the provider and which security tasks remain under their own responsibilities : who makes backups of data or software, which type of failover/redundancy is offered by the provider and what needs to be done still by the customer.

Digital Trust in Cloud Computing – Security and Data Protection aspects



Cloud computing aspect	Security, privacy and data protection aspect	Challenges	Potential solutions
Security and privacy controls in the Cloud	Identity management, authentication and authorization	• Exporting users' identities • Securely transferring identity attributes	• Federated identity management [45] [46] [47] • Efficient credentials management [48] • Multi-factor authentication [49] • MiLAMob: a SaaS authentication middleware [50] • A user-centric approach for platform-level authorization [51]
Security and privacy controls in the Cloud	Access control	• Provide access only to authorized users • The risks of information leakage	• RBAC (Role-based access control) [52] • An integrated solution which combines trust with cryptographic RBAC [53] • An authorization-as-a-service approach [54] • Multi domain access control policies: a comprehensive policy management framework [55] [56] • A heuristic solution to find an RBAC state [57]
	Policy management	• Auditing and proof of compliance	• A scalable distributed monitoring system [58]



Cloud computing aspect	Security, privacy and data protection aspect	Challenges	Potential solutions
Security and privacy controls in the Cloud	Access control	• Provide access only to authorized users • The risks of information leakage	• RBAC (Role-based access control) [52] • An integrated solution which combines trust with cryptographic RBAC [53] • An authorization-as-a-service approach [54] • Multi domain access control policies: a comprehensive policy management framework [55] [56] • A heuristic solution to find an RBAC state [57]
	Policy management	• Auditing and proof of compliance	• A scalable distributed monitoring system [58]
Data stored and processed in the Cloud	Sensitivity of information	• Lack of users' control over Cloud resources	• Enabling users to define transparency policies over their data [60]
	Confidentiality, integrity and availability of data	• Security and privacy of data • Frequent outages reported on well-known CSPs [61]	• Using verifiable proofs of violation by external third parties [62] • Fuzzy authorization for Cloud storage [63]
	Data storage and transfer locations	• The highly distributed nature of Cloud infrastructures • Certain data protection and privacy laws also apply in specific jurisdiction	(e.g., EU's General Data Protection Regulation – GDPR [64])

Table: Summary of privacy and data protection challenges and corresponding solutions in Cloud Computing

Ref: ILNAS-University of Luxembourg white paper: Data Protection and Privacy in Smart ICT – scientific research and technical standardization, version 1.0 October 2018, pages 33-35

Digital Trust – Standards and Technical Standardization for Cloud

- Standards and technical standardization can help establishing and maintaining Digital Trust in relation to current and future Smart ICT technologies

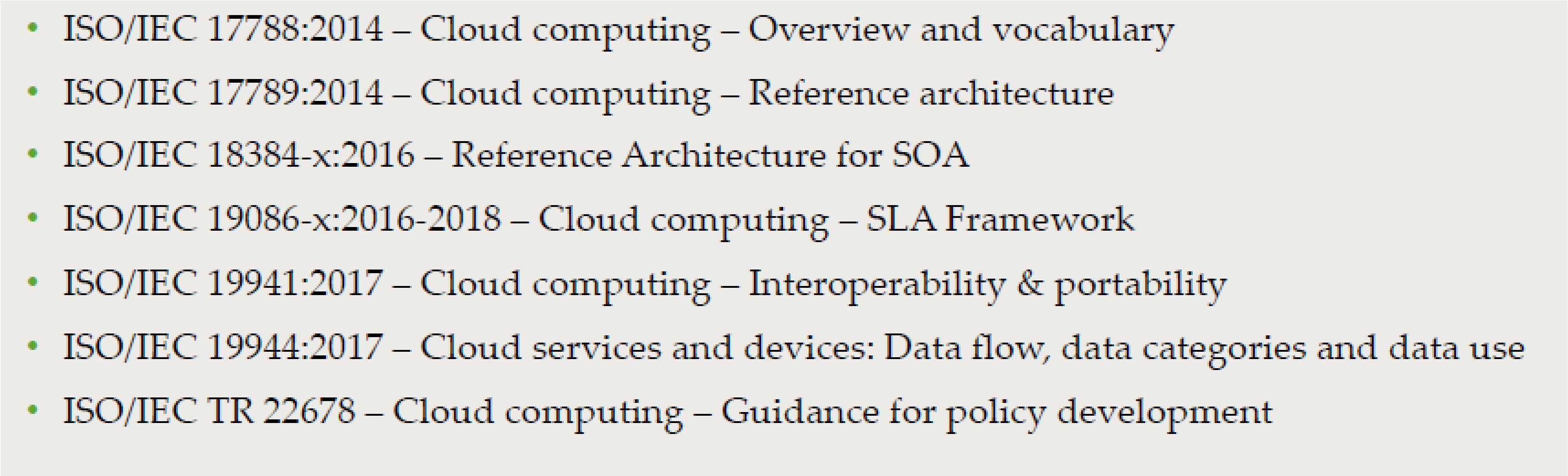
- Standards can provide the tools, techniques, guidelines, and assessment grid necessary to build and nurture relationship between trustor and trustee

- Standards can provide common communication protocols allowing interoperability

- ISO/IEC 19086 1-4 for example are a key element in creating a culture of trust and transparency in cloud SLAs and procurement of cloud services

Cloud Computing – Smart Secure & Technical Standardization

Technical standardization and related standards

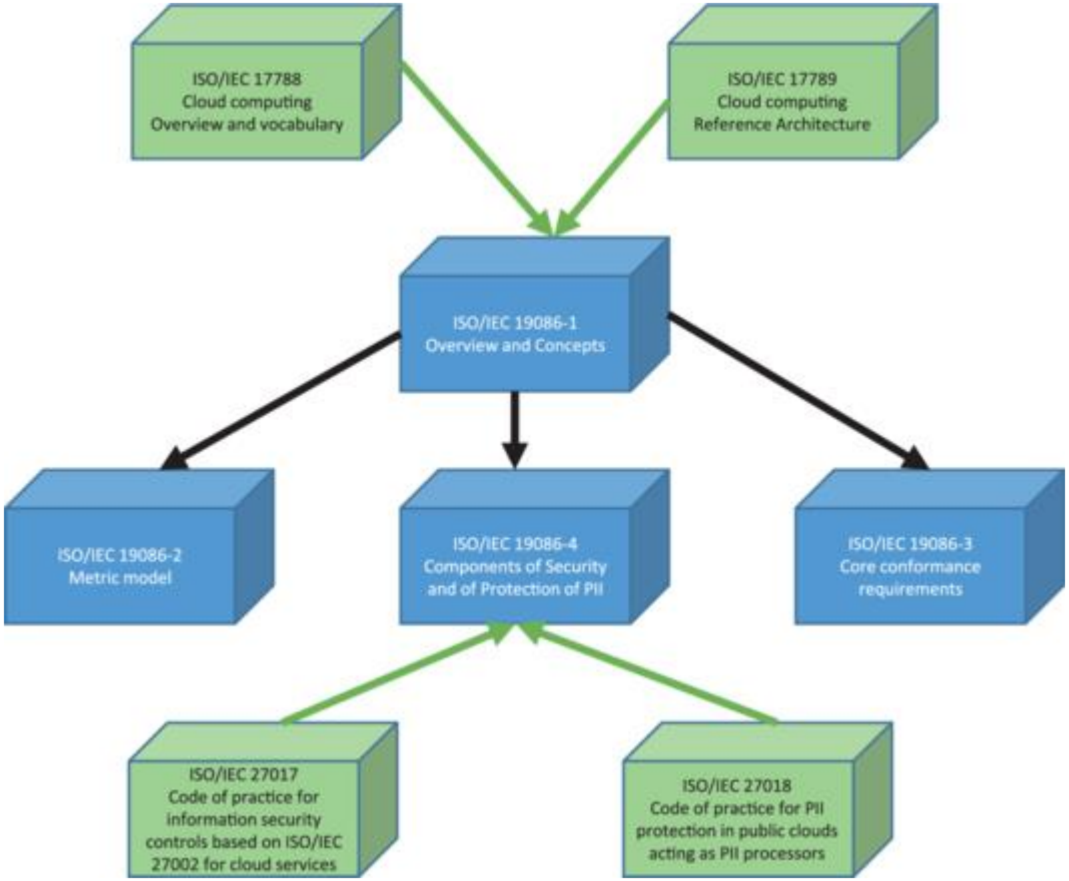


- ISO/IEC 17788:2014 – Cloud computing – Overview and vocabulary
- ISO/IEC 17789:2014 – Cloud computing – Reference architecture
- ISO/IEC 18384-x:2016 – Reference Architecture for SOA
- ISO/IEC 19086-x:2016-2018 – Cloud computing – SLA Framework
- ISO/IEC 19941:2017 – Cloud computing – Interoperability & portability
- ISO/IEC 19944:2017 – Cloud services and devices: Data flow, data categories and data use
- ISO/IEC TR 22678 – Cloud computing – Guidance for policy development

To properly secure the cloud the first step is to understand the cloud. Some foundational standards are being developed and already published . So the main idea is to provide a common language and understanding of cloud for security professionals, begin highlighting the differences between cloud and traditional computing, and help guide security professionals towards adopting cloud-native approaches that result in better security (and those other benefits), instead of creating more risks.

Cloud Computing – Smart Secure & Technical Standardization

Security aspects of Cloud – Related Standards – ISO/IEC 19086-x series



Guidance for Cloud Service Providers who process PII information - Example

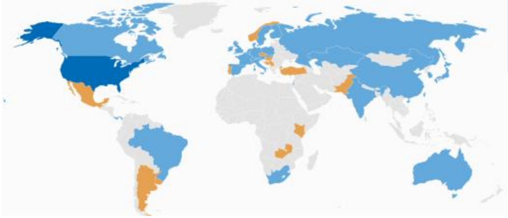
- **ISO/IEC 27018:2019 – Code Of Practice For Protecting Personally Identifiable Information (PII) In Public Clouds**
  - It sets commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in line with the privacy principles found in ISO/IEC 29100:2011
  - It is mean to help the public cloud service provider comply with applicable obligations when acting as a PII processor, assist the cloud service customer and public cloud PII processor in entering into a contractual agreement, and provide cloud service customers with the ability to exercise audit and compliance rights and responsibilities
  - The standard does implement the controls found in ISO/IEC 27002:2013 it augments them for its purposes.
  - By following ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018 :
    - Customers of cloud service providers can know where their data is stored, because ISO/IEC 27018 requires to inform customers of the countries in which their data may be stored, so customers have the visibility they need to comply with any applicable information security rules

Cloud Computing – Smart Secure & Technical Standardization

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

- **Created:** **2009**

- **Main focus areas (adjusted scope in 2017):**
  - Standardization in the areas of Cloud Computing and Distributed Platforms including:
    - Foundational concepts and technologies,
    - Operational issues, and
    - Interactions among Cloud Computing systems and with other distributed systems
- **Highlights:**
  - New Leadership team! New SC 38 Chair: Mr. Steve Holbrook – for a three-year term (beginning 1st January 2019) – IBM program director
  - Status:
    - After 9 years, CC is no longer the new shiny object
  - Accomplishments & Investments (previous 9 years):
    - Freely available foundational publications (some examples):
      - ISO/IEC 17788:2014 – Cloud computing – Overview and vocabulary
      - ISO/IEC 17789:2014 – Cloud computing – Reference architecture
      - ISO/IEC 18384-x:2016 – Reference Architecture for SOA
      - ISO/IEC 19086-x:2016-2018 – Cloud computing – SLA Framework
      - ISO/IEC 19941:2017 – Cloud computing – Interoperability & portability
      - ISO/IEC 19944:2017 – Cloud services and devices: Data flow, data categories and data use
      - ISO/IEC TR 22678 – Cloud computing - Guidance for policy development



Secretariat 🟦
Participating Members (30) 🟦
Observing Members (15) 🟧

- **Key Indicators:**
  - 15 published ISO Standards (under direct responsibility of SC 38)
  - 9 ISO standards under development
  - 30 Participating members (**Luxembourg** among them)
  - 15 Observing members
- **Structure:**
  - WG 3: Cloud Computing Fundamentals
  - WG 5: Data in Cloud Computing and related technologies

ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms - NMC

- **Luxembourg's involvement (16 until now…):**
  - Mr. Matthias BRUST (University of Luxembourg)
  - Mr. Cyril CASSAGNES (University of Luxembourg)
  - Mr. Boonyarit CHANGAIVAL (University of Luxembourg)
  - Mrs. Myriam DJEROUNI (Banque de Luxembourg)
  - Mr. Laurent FISCH (Laurent Fisch Luxlegal S.à.r.l.)
  - Mrs. Shenglan HU (POST)
  - Mr. Abdallah IBRAHIM (University of Luxembourg)
  - Mr. Andreas KREMER (ITTM)
  - Mr. Chao LIU (University of Luxembourg)
  - Ms. Digambal NAYAGUM (AS Avocats)
  - Mr. Jean RAPP (Actimage)
  - Mr. Jean-Michel REMICHE (POST)
  - Mr. Qiang TANG (LIST)
  - Mr. Shyam WAGLE (G.I.E ANEC)
  - Mr. Muhammad Umer WASIM (University of Luxembourg)
  - Mr. Johnatan PECERO (G.I.E ANEC) – **Current Chairman**

Ref: ilnas-oln-register-national-delegues-normalization. Consulted: March 04, 2019

- **Organization and follow-up of projects**
  - A monthly report of open votes and related documents will be sent to ensure the information of all the national delegates of the SC 38
  - To remind : a delegate can focus on one or more project
  - The members of the committee will directly communicate their position/comments to all the other national members to simplify the working process
  - The members will be informed in case a new member would join the NMC
- **Summary of major activities carried out in the context of the NMC in 2018**
  - Votes and comments on standardization projects: 8
  - Participation into standards projects working group meetings: 3
  - NMC f2f meetings: 2
  - Participation into plenary meetings: 1
- **Communication (including NMC)**
  - ➢ https://portail-qualite.public.lu/fr/normes-normalisation/secteurs/tic/cloud-computing.html

Smart Secure ICT and Technical Standardisation

Internet of Things

Internet of Things (IoT)

Basic concept

Things

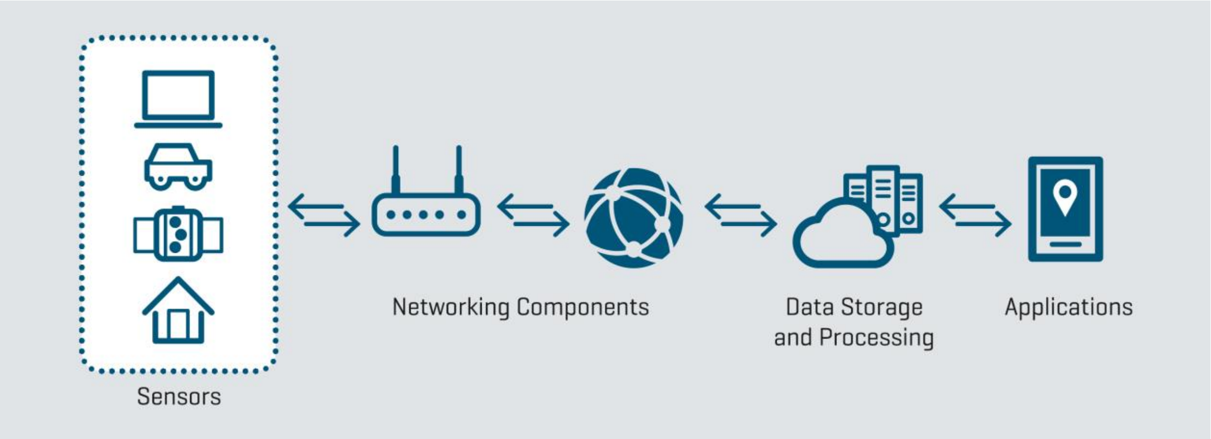
- Surrounded by things – eg. basic electronic devices, smart devices, automated vehicles, smart buildings and so on

Connectivity

- The term IoT is popular to realize the scenario where internet connectivity and computing capability extends to a variety of object

Applications

- Massive volumes of data is processed and turned into valuable information to be utilized by different applications running on the IoT components



Source: ILNAS IoT whitepaper, 2018

Need of technical standardization in IoT

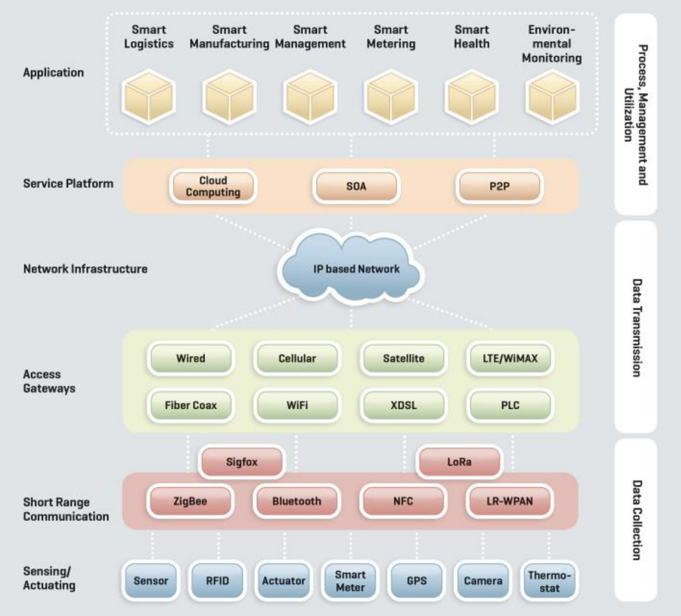
Common language for all stakeholders

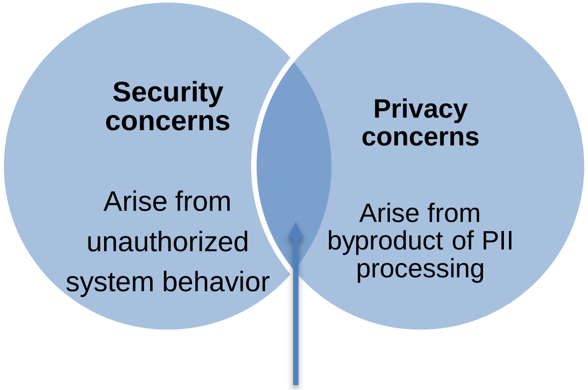
Architecture
- Vocabulary
- Reference architecture

Interoperability
- Within the system
- Out of the system

Applications
- Identify the sectors
- Technology implementation

Security and privacy concerns
- Protection of unauthorized use of...
- Protection of PII
- Building trust





Security concerns

Arise from unauthorized system behavior

Privacy concerns

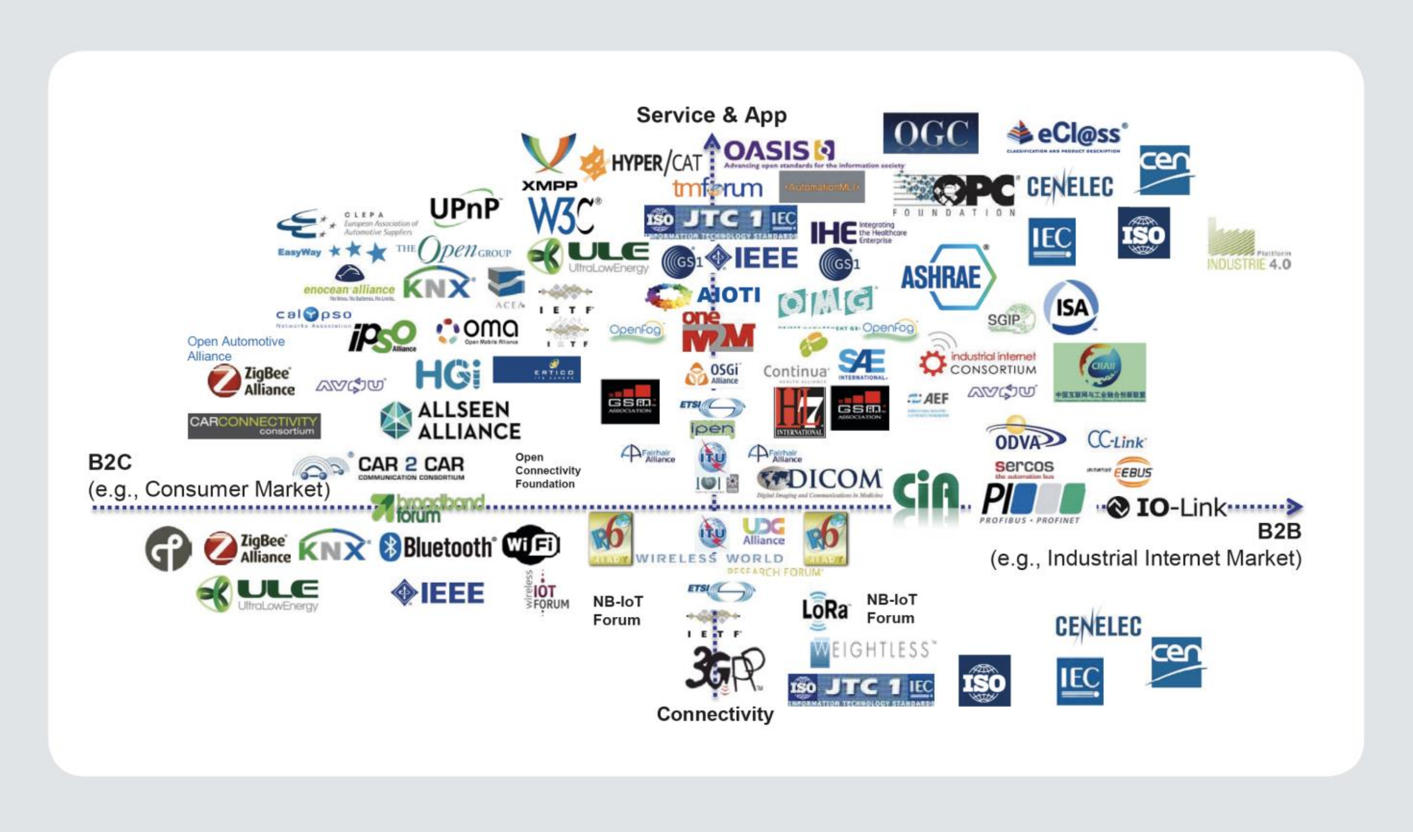
Arise from byproduct of PII processing

Security of PII

Source: 1. ILNAS IoT whitepaper, 2018
2. NIST report, 2018 , https://doi.org/10.6028/NIST.IR.8200

Technical standardization landscape in IoT

IoT alliances and SDOs landscape



- ISO/IEC JTC1/SC 41: Internet of Things and related technologies
- ETSI/TC Smart M2M, ETSI/TC Cyber
- ITU-T SG 20, JCA IoT and SC&C, FG-DPM, ITU-T SG 13
- And other fora and consortia

Source: AIOTI, “IoT LSP Standard Framework Concepts - Release 2.8,” 2017

JTC1 and other initiatives to make secure IoT

Published and ongoing standards

IoT Trustworthiness SC 41

- **ISO/IEC 30149** Internet of Things (IoT) —Trustworthiness framework - ongoing
- **ISO/IEC 30147** Internet of Things (IoT) – Methodology for implementing and maintaining trustworthiness of IoT systems and services - ongoing

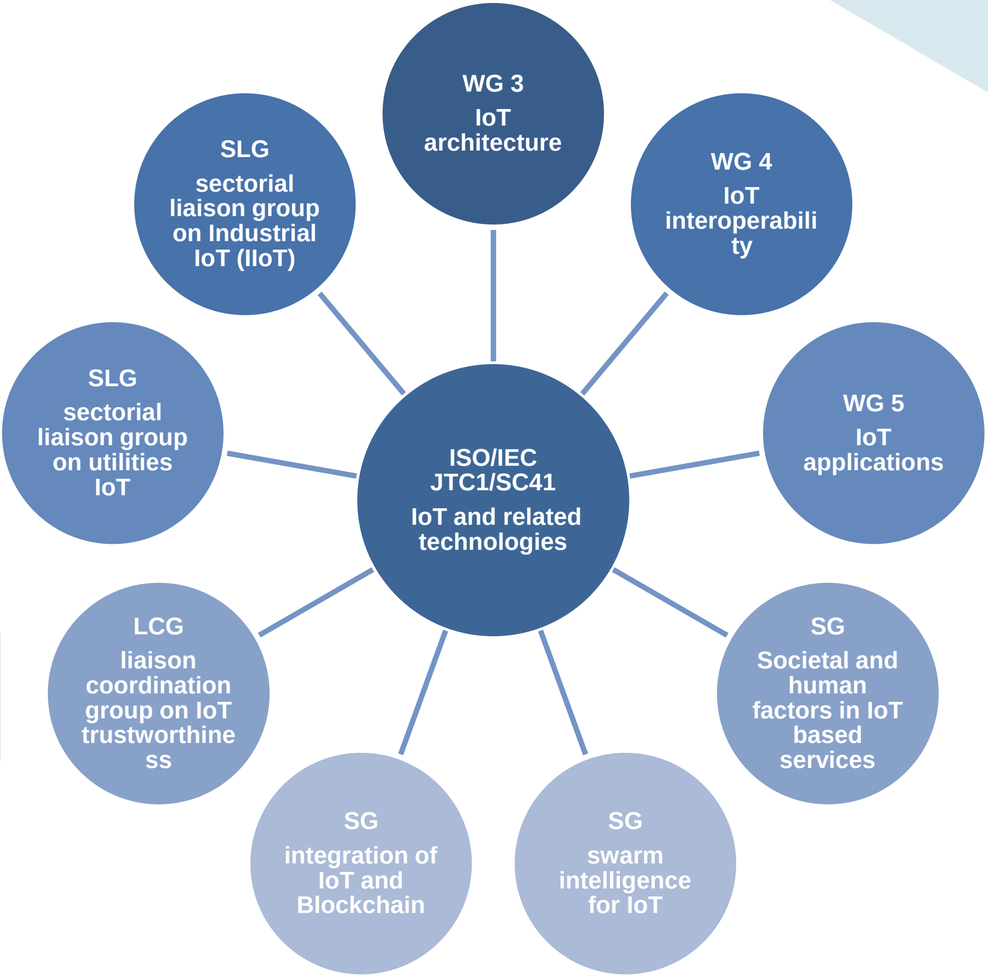
IoT Security SC 27

- **ISO/IEC 27030** Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT) - ongoing
- **ISO/IEC 27032** IT Security Techniques -- Cybersecurity -- Guidelines for Internet Security - ongoing

ETSI, ITU-T, ….

- **ETSI TS 103 645 v.1.1.1 --** Cyber security for Consumer Internet of Things - published
- **ITU-T X.1361** -- Security framework for IoT based on the gateway model - ongoing
- **NIST report** -- Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) - published

IoT security related standards


ISO/IEC JTC1/SC41
IoT and related technologies
WG 3
IoT architecture
WG 4
IoT interoperability
WG 5
IoT applications
SG
Societal and human factors in IoT based services
SG
swarm intelligence for IoT
SG
integration of IoT and Blockchain
LCG
liaison coordination group on IoT trustworthiness
SLG
sectorial liaison group on utilities IoT
SLG
sectorial liaison group on Industrial IoT (IIoT)

Structure: SC 41 – IoT and related technologies

IoT trustworthiness framework

ISO/IEC 30149 Internet of Things (IoT) —Trustworthiness framework
(WD -- in progress under JTC1/SC 41) -- preliminary concept of the project

Security
- Confidentiality
- Integrity
- Availability

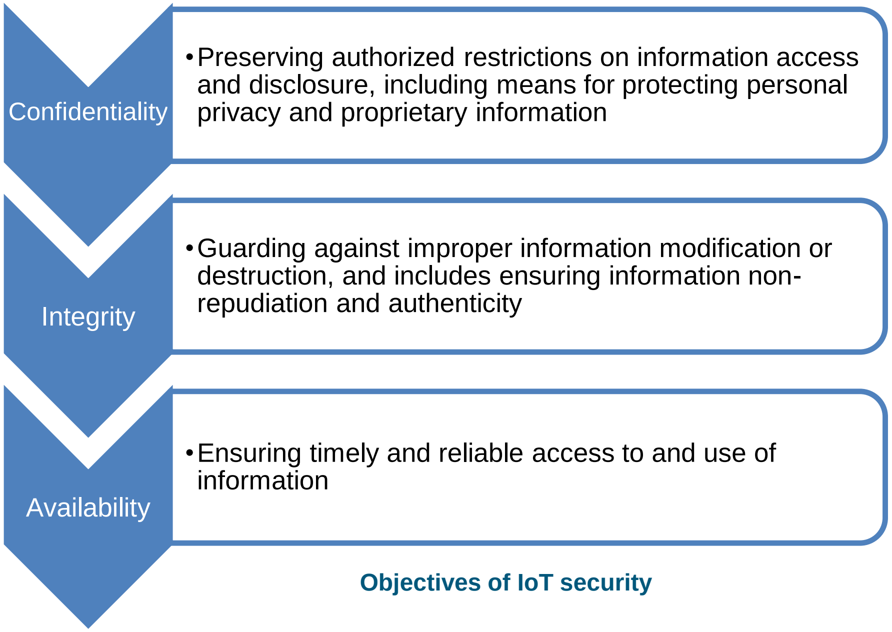
Privacy (PII)
- Privacy framework
- Law & regulations

Safety
- Environmental safety
- Living entity safety
- Operational safety

Reliability
- Trust that the device/system and services/functions provided will be able to perform consistently as expected

Resiliency
- Resiliency – Trust that the device/system can recover quickly or maintain its functionality in spite of difficulties / failures

Factors of trustworthiness in IoT



Confidentiality
- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity
- Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

Availability
- Ensuring timely and reliable access to and use of information

Objectives of IoT security

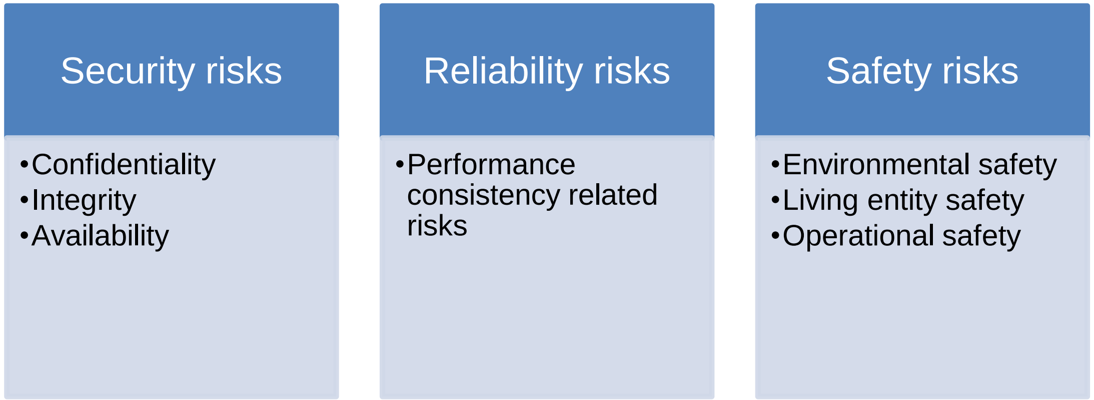
Sources of trustworthiness risks for IoT Solutions
- General
- IoT solution's contexts
  - Business sector
  - Regulatory
  - Technological

Level of Trust
- Targeted Level of Trust (required)
- Expected Level of Trust (predicted)
- Actual Level of Trust (measured)

IoT solutions context and level of trust

Methodologies for IoT Trustworthiness

ISO/IEC 30147 Internet of Things — Methodology for trustworthiness of IoT system/service (WD -- in progress under JTC1/SC 41) -- preliminary concept of the project



Security risks

- Confidentiality
- Integrity
- Availability

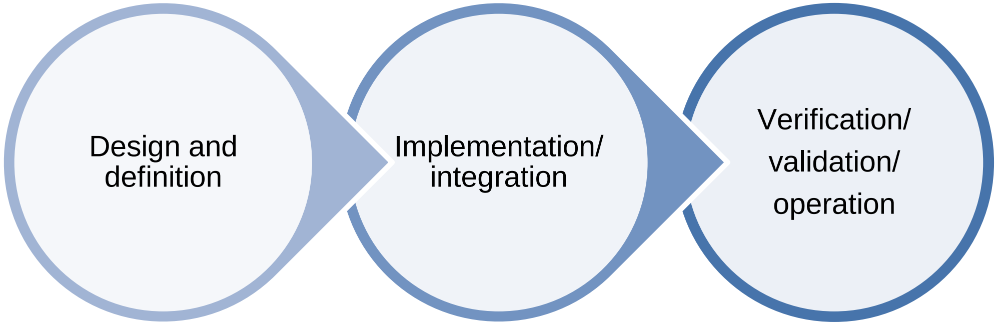
Reliability risks

- Performance consistency related risks

Safety risks

- Environmental safety
- Living entity safety
- Operational safety

Risks in building a trust



Design and definition

Implementation/ integration

Verification/ validation/ operation

Methodology

Guidelines for security and privacy in Internet of Things (IoT)

ISO/IEC 27030 Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT) (WD -- in progress under JTC1/SC 27) -- preliminary concept of the project

IoT service provider

- Roles of stakeholders (eg.):
  - IoT business manager
  - IoT Service delivery manager
  - IoT system operator
  - IoT security analyst
  - IoT operations analyst

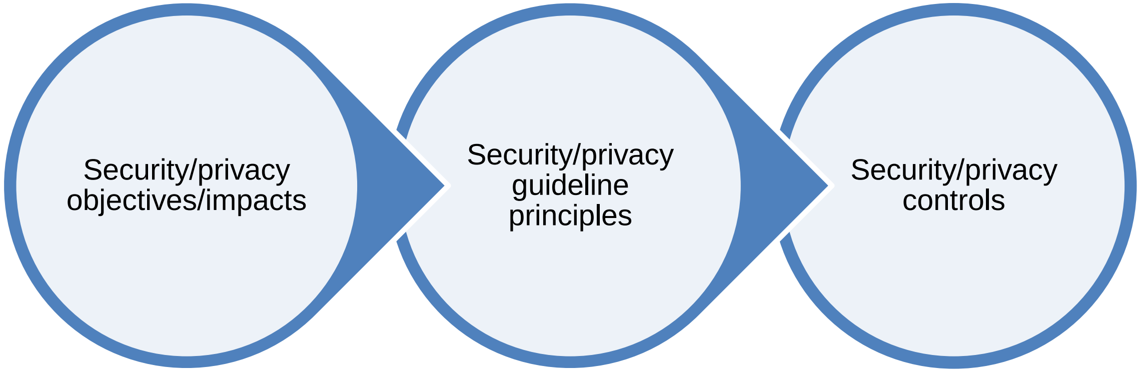
IoT service developer

- Roles of stakeholders (eg.):
  - IoT development operations manager
  - IoT application developer
  - IoT device developer
  - IoT system integrator

IoT user

- Roles of stakeholders (eg.):
  - Human users
  - Digital users (non-human users)

Trustworthiness issues to IoT stakeholders


Security/privacy objectives/impacts
Security/privacy guideline principles
Security/privacy controls

Guidelines on risks, principles and controls for security and privacy of IoT

Cyber security for consumer IoT

ETSI TS 103 645 v.1.1.1 (2019-02)

Scope

- It specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services.

Guidance

- Provides basic guidance for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions

M -- the provision is a mandatory requirement
R -- the provision is a recommendation
M C -- the provision is a mandatory requirement and conditional
R C -- the provision is a recommendation and conditional

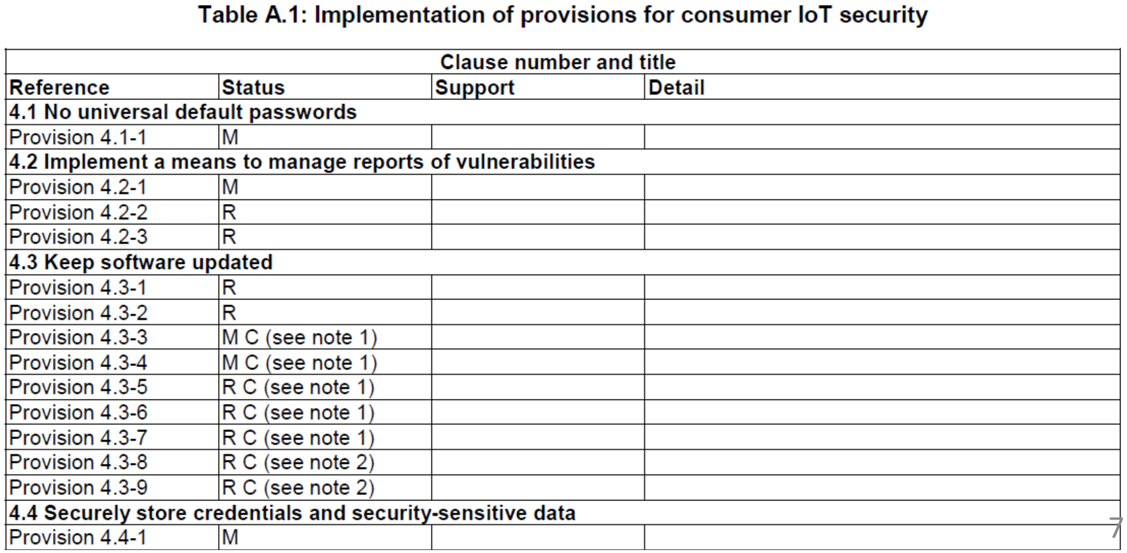


Table A.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
4.1 No universal default passwords			
Provision 4.1-1	M		
4.2 Implement a means to manage reports of vulnerabilities			
Provision 4.2-1	M		
Provision 4.2-2	R		
Provision 4.2-3	R		
4.3 Keep software updated			
Provision 4.3-1	R		
Provision 4.3-2	R		
Provision 4.3-3	M C (see note 1)		
Provision 4.3-4	M C (see note 1)		
Provision 4.3-5	R C (see note 1)		
Provision 4.3-6	R C (see note 1)		
Provision 4.3-7	R C (see note 1)		
Provision 4.3-8	R C (see note 2)		
Provision 4.3-9	R C (see note 2)		
4.4 Securely store credentials and security-sensitive data			
Provision 4.4-1	M		

Conclusions

Many initiatives

- Having every things connected to the global internet infrastructure and things communicating with each other brings many security and privacy problems in the overall IoT ecosystem:
  - More and more things are connected to the internet everyday
  - Users entrust their personal data to the online devices and services
  - A robust system should be designed to withstand security and privacy threats

Still need to do ..

- ILNAS, with the support of ANEC GIE, supporting national stakeholders in IoT related activities
  - Developing market interest and involvement
  - Promoting and reinforcing market participation
  - Supporting and strengthening the education about standardization and related research activities
  - Welcome to JTC1/SC 41 National Mirror Committee (NMC)

SC 41 – National Mirror Committee

Participation to National Mirror Committee

16 registered national delegates*

- ANEC GIE (1)
- vyzVoice (2)
- INCERT GIE (2)
- iTrust (1)
- FANUC Europe S.A. (1)
- LIST (1)
- Tarkett S.A. (1)
- University of Luxembourg (7)

NMC Meeting ISO/IEC JTC 1/SC 41
(17/01/2019)

NMC Meeting ISO/IEC JTC 1/SC 41
(12/12/2017)

Plenary Meeting ISO/IEC JTC 1/SC 41
S. Korea (28/05/17 – 02/06/17)

Plenary Meeting ISO/IEC JTC 1/SC 41
India (13/11/17 – 17/11/17)

Plenary Meeting ISO/IEC JTC 1/SC 41
Japan (26/11/18 – 30/11/18)

* As of March 2019

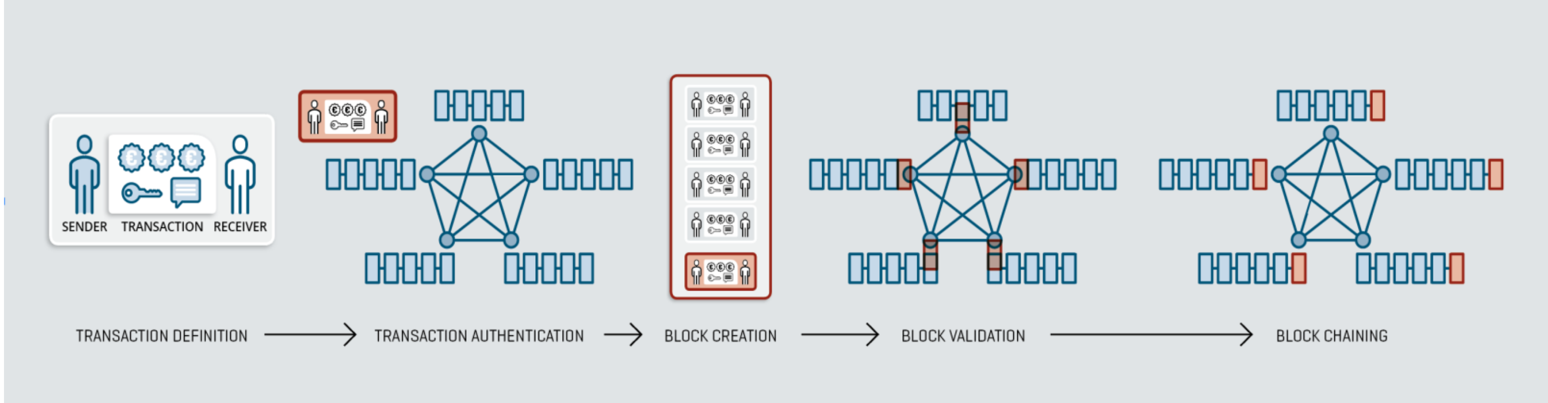
Smart Secure ICT and Technical Standardisation

Blockchain & Distributed Ledgers Technologies

Blockchain and Distributed Ledger Technologies (DLT)

Background

- The process of creating and validating transactions



- The core innovation of the blockchain technology revolves around the notions of:
  - A distributed ledger that allows a network of computers to jointly create, evolve and keep track of a database of records
  - A set of underlying protocols that allow users to reach consensus without having to trust each other

Source: ILNAS white paper: Blockchain and Distributed Ledger Technologies – technology, economic impact, and technical standardization version 1.0 June 2018

Blockchain and Distributed Ledger Technologies (DLT)

Core characteristics

- Decentralization and network model
  - Nodes take different roles (e.g., routing, maintaining blockchain database, mining)
- Blockchain as a database structure
  - Data storage and management
  - Blockchain database structure, ICT ecosystem, and decentralization

- Scope, information access and design choices
  - Public blockchain and private blockchain
  - Permissionless blockchain and permissioned blockchain

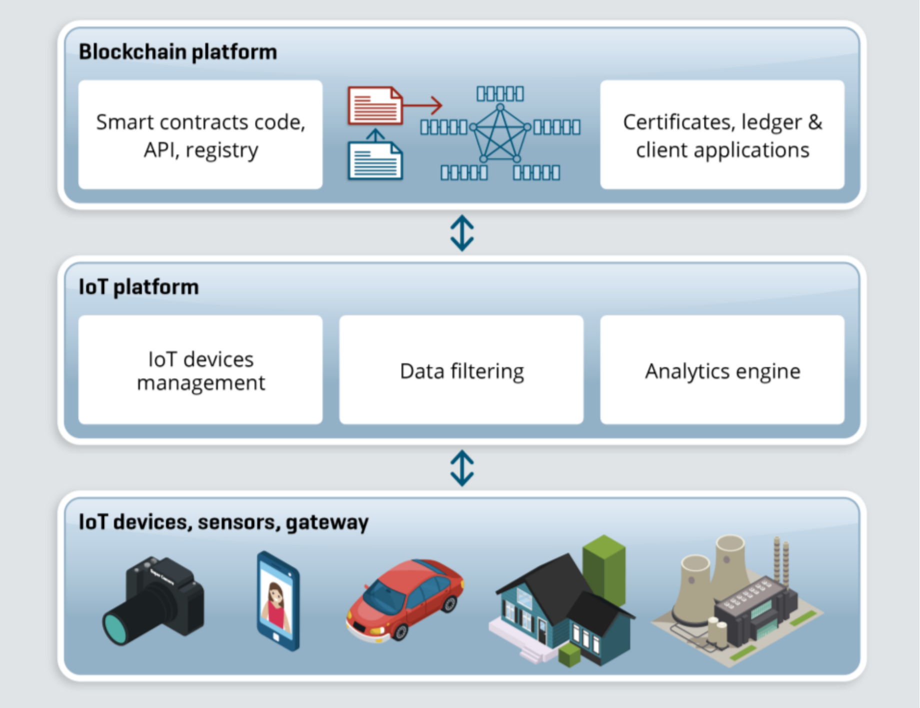
- Consensus methods
  - Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), Proof of Elapsed Time (PoET) and Federated Byzantine Agreement (FBA)

Source: ILNAS white paper: Blockchain and Distributed Ledger Technologies – technology, economic impact, and technical standardization version 1.0 June 2018

Blockchain and Distributed Ledger Technologies (DLT)

Blockchain and DLT and Smart ICT

- Blockchain and Smart ICT
  - Two-way relationship between Cloud computing and blockchain
  - For Big Data and analytics, and for Internet of Things
    - Current (Big Data / IoT) challenges
    - Potential blockchain-based solutions
    - Use cases
    - System architecture


Blockchain platform
Smart contracts code, API, registry
Certificates, ledger & client applications
IoT platform
IoT devices management
Data filtering
Analytics engine
IoT devices, sensors, gateway

Source: ILNAS white paper: Blockchain and Distributed Ledger Technologies – technology, economic impact, and technical standardization version 1.0 June 2018

- Security
  - Risks to core blockchain operations
    (e.g., 51% vulnerability, double spending, private key security)
  - Risks due to smart contracts
    - Taxonomy of smart contract vulnerabilities, their causes, and resulting attacks
    - Examples:
      - The Call to the unknown vulnerability in the Solidity source code could result in the DAO type attack
      - Immutable bugs in EVM Bytecode could result in Rubixi and GovernMental type attacks

Source: ILNAS white paper: Blockchain and Distributed Ledger Technologies – technology, economic impact, and technical standardization version 1.0 June 2018

Blockchain and Distributed Ledger Technologies (DLT)

Blockchain and DLT and Digital Trust

- Privacy
  - Notion of confidentiality and privacy in blockchain
  - Privacy enhancing techniques
    - Examples:
      - Storing sensitive information off-chain
      - One-time addresses and stealth addresses
      - Mixing and coinjoin

- Secure data registry
  - Blockchain could be used for secure exchange of data, which could help in reducing frauds and improving transparency and traceability (e.g., agriculture and food, public services, manufacturing, human resources)

Source: ILNAS white paper: Blockchain and Distributed Ledger Technologies – technology, economic impact, and technical standardization version 1.0 June 2018

Prospective Role of Standards to Support DLT/Blockchain

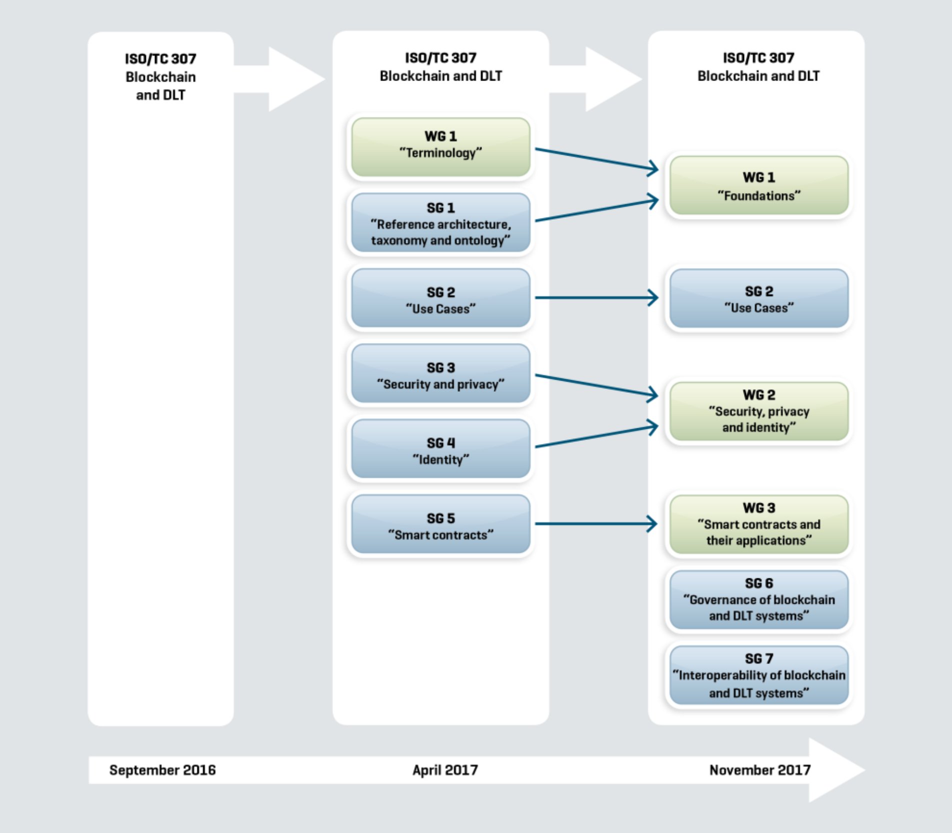
- To ensure interoperability between multiple DLT/Blockchain implementations and, in doing so, could help to reduce risk of a fragmentation of the ecosystem

- Using standards to establish a stronger consensus on consistent terminology and vocabulary could improve understanding of the technology and help progress the market

- Establishing the standards to address the security and resilience of, and the privacy and data governance concerns related to DLT/Blockchain could help create trust in the technology

- Standards could play a role in digital identity management and foster end-user trust in the technology

- ISO/TC 307 Blockchain and distributed ledger technologies
  - Formed in September 2016
  - Four plenary meetings were held so far: April 2017, November 2017, May 2018, October 2018



ISO/TC 307 Blockchain and DLT

ISO/TC 307 Blockchain and DLT

WG 1 "Terminology"

SG 1 "Reference architecture, taxonomy and ontology"

SG 2 "Use Cases"

SG 3 "Security and privacy"

SG 4 "Identity"

SG 5 "Smart contracts"

ISO/TC 307 Blockchain and DLT

WG 1 "Foundations"

SG 2 "Use Cases"

WG 2 "Security, privacy and identity"

WG 3 "Smart contracts and their applications"

SG 6 "Governance of blockchain and DLT systems"

SG 7 "Interoperability of blockchain and DLT systems"

September 2016

April 2017

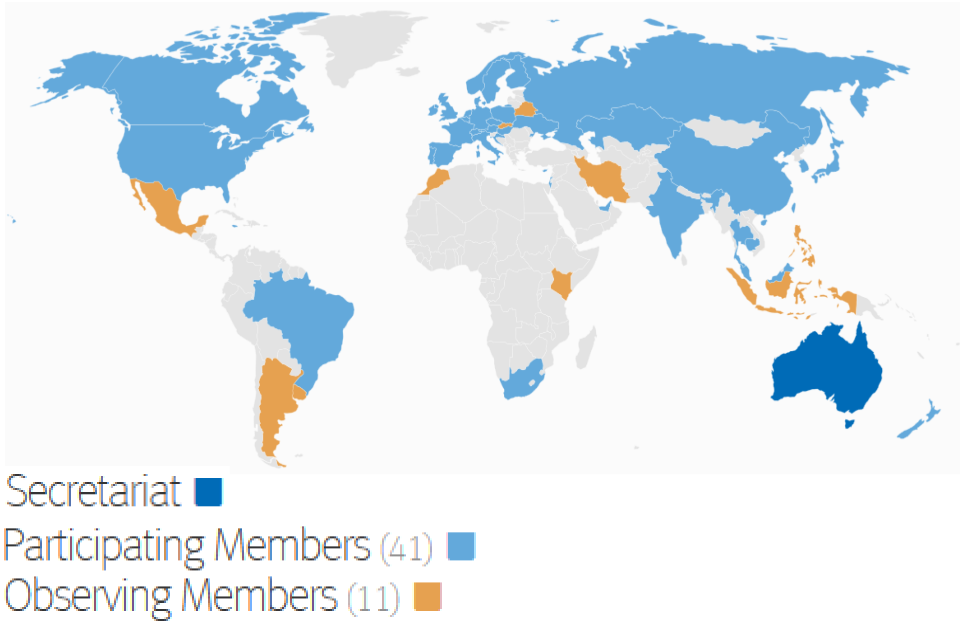
November 2017

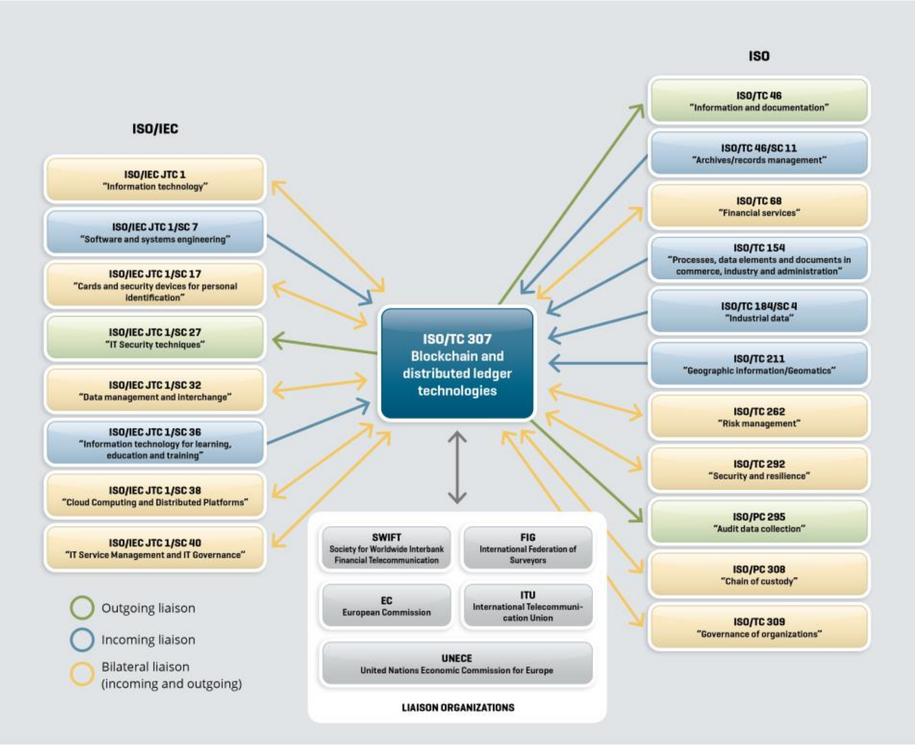
- Scope
  - Standardization of blockchain technologies and distributed ledger technologies to support interoperability and data exchanges between users, applications and systems

Blockchain and Distributed Ledger Technologies (DLT)

Technical Standardization

- ISO/TC 307 Blockchain and distributed ledger technologies
  - 41 Participating members (including Luxembourg) and 11 Observing members
  - To facilitate better coordination in the standards development processes, several liaisons have been established – 23 internal liaisons (IEC, ISO, ISO/IEC): e.g. SC 27, SC 38, SC 40, TC 322 ; 7 liaison organizations: e.g. EC, ITU, SWIFT, FIG, IEEE




ISO/IEC
ISO/IEC JTC 1 "Information technology"
ISO/IEC JTC 1/SC 7 "Software and systems engineering"
ISO/IEC JTC 1/SC 17 "Cards and security devices for personal identification"
ISO/IEC JTC 1/SC 27 "IT Security techniques"
ISO/IEC JTC 1/SC 32 "Data management and interchange"
ISO/IEC JTC 1/SC 36 "Information technology for learning, education and training"
ISO/IEC JTC 1/SC 38 "Cloud Computing and Distributed Platforms"
ISO/IEC JTC 1/SC 40 "IT Service Management and IT Governance"
Outgoing liaison
Incoming liaison
Bilateral liaison (incoming and outgoing)
ISO/TC 307 Blockchain and distributed ledger technologies
SWIFT Society for Worldwide Interbank Financial Telecommunication
FIG International Federation of Surveyors
EC European Commission
ITU International Telecommunication Union
UNECE United Nations Economic Commission for Europe
LIAISON ORGANIZATIONS
ISO
ISO/TC 46 "Information and documentation"
ISO/TC 46/SC 11 "Archives/records management"
ISO/TC 68 "Financial services"
ISO/TC 154 "Processes, data elements and documents in commerce, industry and administration"
ISO/TC 184/SC 4 "Industrial data"
ISO/TC 211 "Geographic information/Geomatics"
ISO/TC 262 "Risk management"
ISO/TC 292 "Security and resilience"
ISO/PC 295 "Audit data collection"
ISO/PC 308 "Chain of custody"
ISO/TC 309 "Governance of organizations"

- ISO/TC 307 Blockchain and distributed ledger technologies - defined objectives
  - Develop a reference architecture (RA) IS that will provide a unified view of blockchain and DLT (target date: 2021)
  - Elaborate on a package of IS and Technical Specifications (TS) to address the compatibility between technology and legal frameworks to aid in adoption of blockchain and DLT by industry and government (target date: 2021)
  - Produce Technical Reports (TR) in the areas of security, privacy and identity then investigate the potential IS that would need to be developed as the aspects are better defined and identified;
  - Address interoperability between different ledger technologies and between ledger technologies and other system components as the aspects are better developed and defined.

- ISO/TC 307 Structure
  - [AG 1] SBP Review Advisory Group
  - [JWG 04] Joint ISO/TC 307 – ISO/IEC JTC 1/SC 27 WG; Blockchain and DTLs and IT Security techniques
  - [SG 02] Use cases
  - [SG 07] Interoperability of blockchain and DLT systems
  - [WG 01] Foundations
  - [WG 02] Security, privacy and identity
  - [WG 03] Smart contracts and their applications
  - [WG 05] Governance

Blockchain and Distributed Ledger Technologies (DLT)

Technical Standardization

- ISO/TC 307 Structure

  - [SG 02] Use cases
    - ***Scope:*** Consider the most common types of use cases, the potential implications of the existing use cases and applications

  - [SG 07] Interoperability of blockchain and DLT systems
    - ***Scope:*** interoperability issues related to cryptocurrencies' platform, utility and transaction tokens, and other cryptographically supported digital assets or proxies for physical and intangible assets

  - [WG 01] Foundations
    - ***Scope:*** Unified terms and basic definitions, foundational elements of blockchain and DLTs technologies

- ISO/TC 307 Structure

  - [WG 02] Security, privacy and identity
    - ***Scope:*** Assess whether there are requirements for security and privacy in relation to blockchain and DLTs; identify the types of identities and entity types needed for data and functionality within blockchains. Identify any regulations that could impact the creation, use and management of identities in relation to blockchains

  - [WG 03] Smart contracts and their applications
    - ***Scope:*** Analysis of the current understanding of smart contracts from both a technical as well as appropriate legal perspective. Interoperability with the law, including but not limited to the verification, enforcement, and life cycle of smart contracts

  - [WG 05] Governance
    - ***Scope:*** To provide guiding principles and a framework for the governance of distributed ledger systems. To provide guidance on the effective, efficient, and acceptable use of distributed ledger systems for the fulfilment of governance objectives including risk and regulatory contexts

Blockchain and Distributed Ledger Technologies (DLT)

Technical Standardization – ISO/TC 307 on-going projects

- WG 1 Foundations
  - ISO/CD 22739 Blockchain and distributed ledger technologies – Terminology (International Standard)
  - ISO/CD 23257 Blockchain and distributed ledger technologies -- Reference architecture (Technical Specification)
  - ISO/AWI TS 23258 Blockchain and distributed ledger technologies -- Taxonomy and Ontology (Technical Specification)
  - ISO/NP TR 23578 Blockchain and distributed ledger technologies -- Discovery issues related to interoperability (Technical Report)
- WG 2 Security, privacy and identity
  - ISO/NP TR 23244 Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations (Technical Report)
  - ISO/NP TR 23245 Blockchain and distributed ledger technologies -- Security risks, threats and vulnerabilities (Technical Report)
  - ISO/NP TR 23246 Blockchain and distributed ledger technologies -- Overview of identity management using blockchain and distributed ledger technologies (Technical Report)
  - ISO/NP TR 23576 Blockchain and distributed ledger technologies -- Security management of digital asset custodians (Technical Report)

Blockchain and Distributed Ledger Technologies (DLT)

Technical Standardization – ISO/TC 307 on-going projects

- WG 3 Smart contracts and their applications
  - ISO/AWI TS 23259 Blockchain and distributed ledger technologies -- Legally binding smart contracts (Technical Specification)
  - ISO/NP TR 23455 Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems (Technical Report)
  - Additionally a study on supply chain and trade facilitation
- WG 5 Governance
  - ISO/NP TS 23635 Blockchain and distributed ledger technologies -- Guidelines for governance (Technical Specification)

Blockchain and Distributed Ledger Technologies (DLT)

Technical Standardization – ISO/TC 307 NMC

- ISO/TC 307 NMC
  - ILNAS manages ISO/TC 307 National Mirror Committee
  - ANEC G.I.E. serves as the presidency for this NMC
  - 19 experts – as of today

- Organize Frequent NMC meetings
  - to discuss about current ballots of the drafts of IS or TR
  - to debrief about the outcomes of the plenary meetings (Next Plenary Meeting will be held in Dublin, Ireland on 27th-31th May 2019)

- ILNAS takes initiatives to keep the national stakeholders informed about various developments

Smart Secure ICT and Technical Standardisation

Artificial Intelligence

Technical standardization and Artificial Intelligence

Background information

- **Artificial Intelligence is not new**
  - Officially appeared in 1956
  - Some work on the topic even before that date

- **Standardization efforts related to AI are not new**
  - Work on related terminology since 1989

Plenary meeting ISO/IEC JTC 1/SC 42
(18.04.18 – 20.04.18)

- **Dedicated technical committee ISO/IEC JTC1/SC42 Artificial Intelligence**
  - Approved in October 2017
  - Work started in April 2018
  - 2 plenary meetings
  - 9 projects under development
  - 36 countries involved
  - National Mirror Committee web page

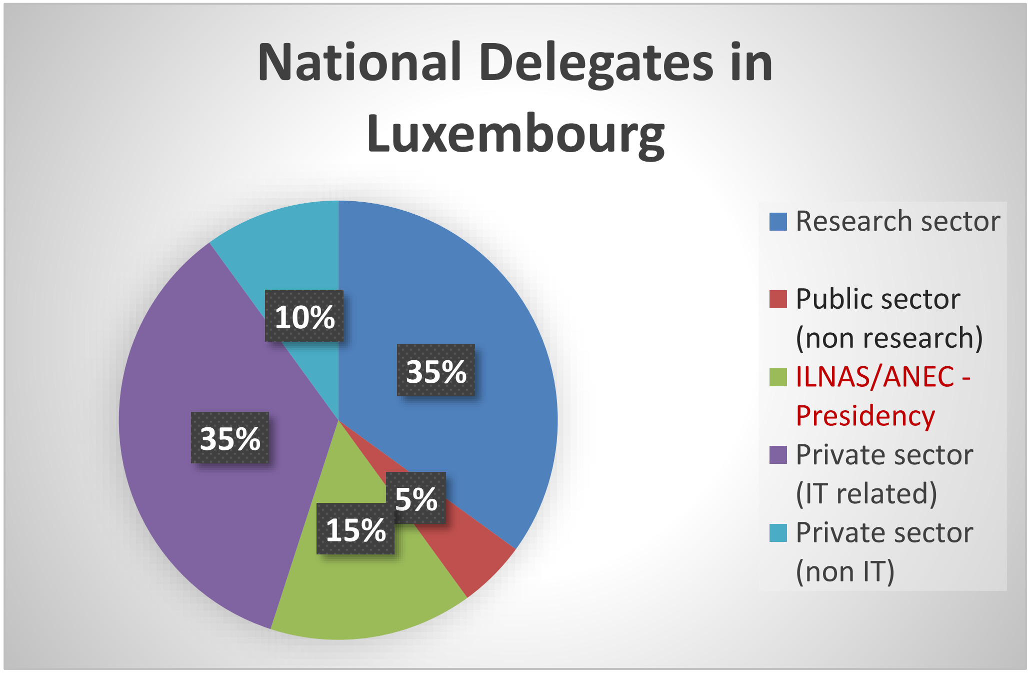
Plenary meeting ISO/IEC JTC 1/SC 42
(08.10.18 – 12.10.18)

Technical standardization and Artificial Intelligence

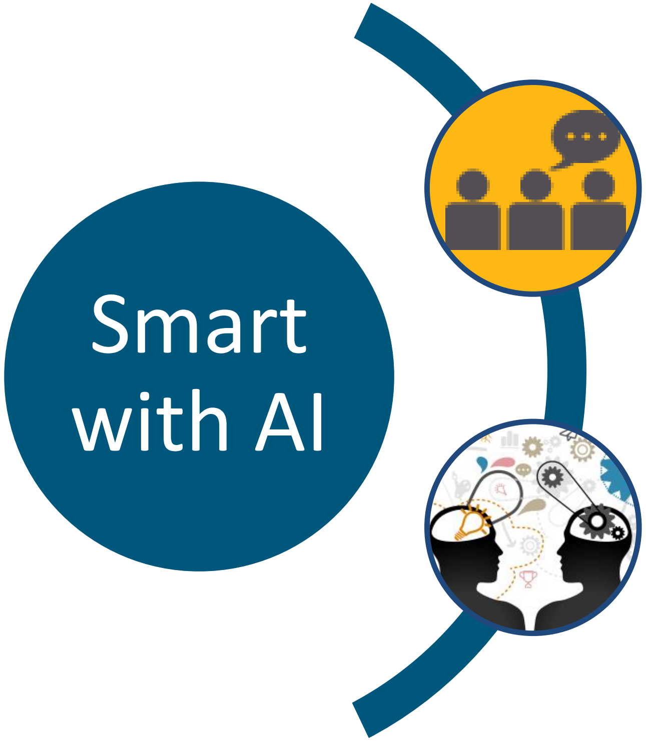
Participation from Luxembourg - National Mirror Committee

- **20 delegates from Luxembourg (Register of national delegates – Mars 2019) + 2 in progress**

  - ANEC GIE (3), Presidency
  - BIL (1)
  - CSSF (1)
  - Everis Spain SLU (1)
  - INCERT GIE (2)
  - ITTM (1)
  - KPMG (1)
  - Laurent Fisch Luxlegal S.a.r.l. (1)
  - LIST (1)
  - PmG SD S.a.r.l. (1)
  - Tarkett S.A. (1)
  - Université du Luxembourg (6)



- **8 delegates contribute directly on the topics related to Secure AI**



Smart with AI

Speak the same language

- ISO/IEC 20546:2019 Information technology -- Big data -- Overview and vocabulary
- ISO/IEC WD 22989 Artificial intelligence -- Concepts and terminology

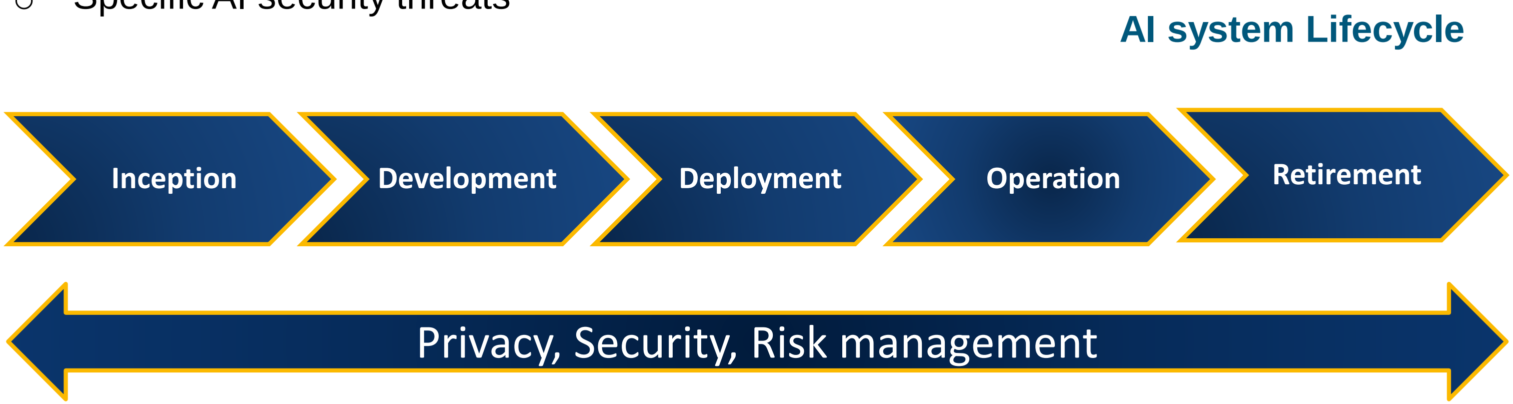
Use good practices

- ISO/IEC DIS 20547-3 Information technology -- Big data reference architecture -- Part 3: Reference architecture
- ISO/IEC WD 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

Technical standardization and Artificial Intelligence

Secure AI

- **Security all along the AI system lifecycle**
  - Common IT security threats
  - Specific AI security threats



- **Security… but not only**
  - Secure - Safe - Trustworthy - Does no harm
    - Different types of harm

Trustworthiness

TR ISO/IEC 24028, Overview of trustworthiness in Artificial Intelligence

- *The goal of this document is to identify possible standardization areas to address **common concerns affecting the trustworthiness of AI systems** by describing possible approaches to address such concerns.*

Bias

TR ISO/IEC 24027, Bias in AI systems and AI aided decision making

- *This document addresses **bias in relation to AI systems**, especially with regards to AI aided decision-making. Measurement techniques and methods for assessing bias are described, with the aim to address bias related vulnerabilities, and mitigation thereof. All AI system lifecycle phases are in scope, including but not limited to data collection, training, continual learning, design, testing, evaluation, and use.*

Robustness

TR ISO/IEC 24029-1, Assessment of the robustness of neural networks

- Part 1: Overview

- *This document provides background about the **existing methods to assess robustness properties** of neural networks.*

Risk management

ISO/IEC 23894, Artificial intelligence - Risk management

- This document provides **guidelines on managing risk faced by organizations** during the development and application, where an organization either just implements or applies or both, of artificial intelligence (AI) techniques and systems, to assist organizations to integrating risk management for AI into significant activities and functions. It moreover describes processes for the effective implementation and integration of AI risk management.
- This document uses the guidelines described in the International Standard ISO 31000 (Risk management – Guidelines) and in addition provides additional **guidance that arises by the application of AI to existing processes in any organization or when an organization provides an AI system for use by others**.

Technical standardization and Artificial Intelligence

Concerns from governance bodies

- **ISO/IEC 38507, Governance implications of the use of artificial intelligence by organizations**

  ○ Scope:

Standardization in the area of governance ***implication of the use of AI by organizations****. This will:*

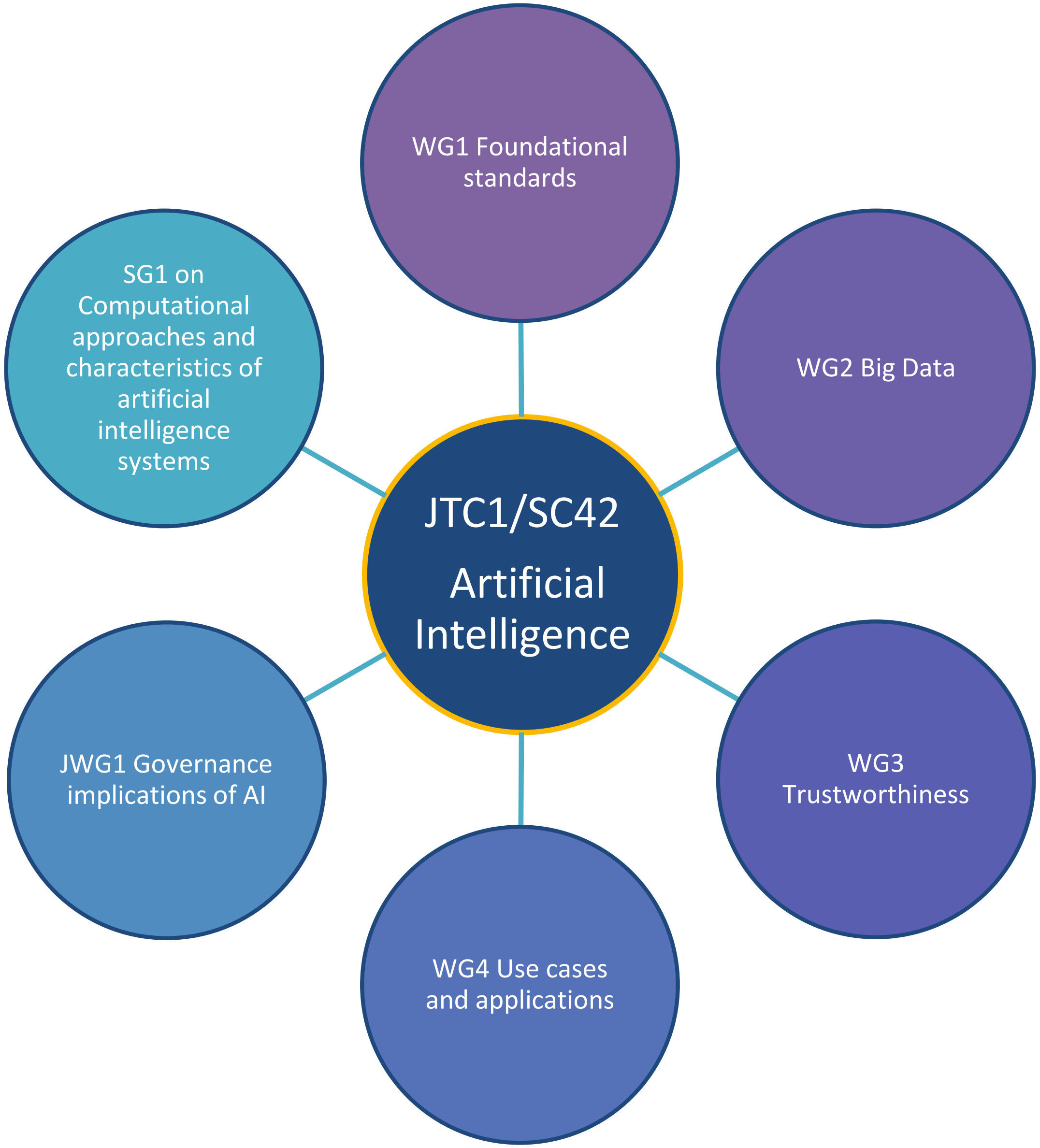
▪ *establish a vocabulary for the governance of AI*

▪ *provide a framework for understanding the implications, in a timely manner, of the use of different AI technologies*

▪ *equip governing bodies to evaluate, direct and monitor the introduction and use of these technologies, applying the governance principles of ISO/IEC 38500.*

Technical standardization and Artificial Intelligence

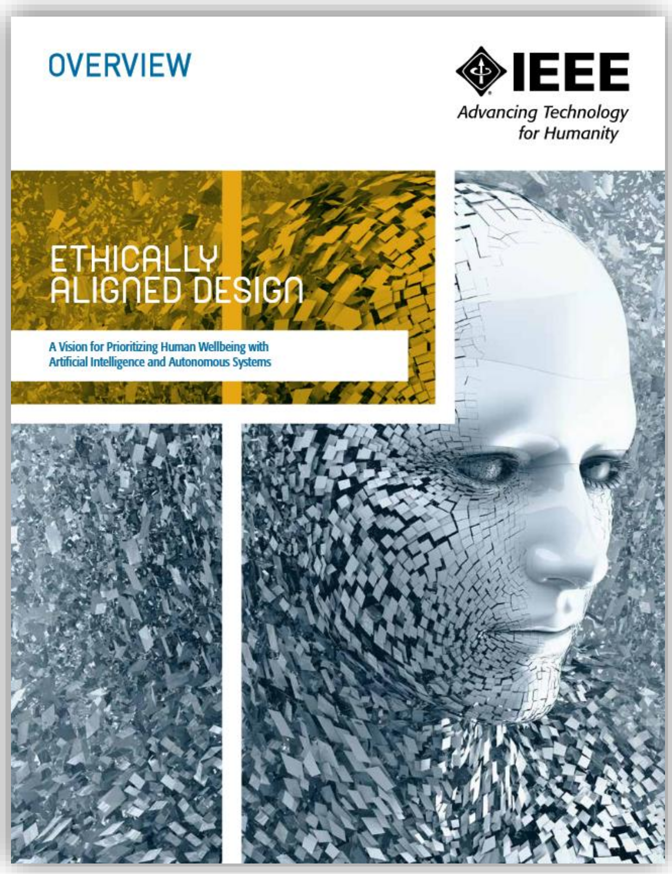
Current Structure of ISO/IEC JTC1/SC42 Artificial Intelligence


WG1 Foundational standards
SG1 on Computational approaches and characteristics of artificial intelligence systems
WG2 Big Data
JTC1/SC42
Artificial Intelligence
JWG1 Governance implications of AI
WG3 Trustworthiness
WG4 Use cases and applications

Technical standardization and Artificial Intelligence

Ethical considerations

- **Ethics is not technical concept**
  - Outside of scope of SC42 Artificial Intelligence
- **IEEE**
  - Global Initiative on Ethics of Autonomous and Intelligent Systems
    - Ethically aligned design v1 and v2
    - IEEE P7000 family of standards



OVERVIEW

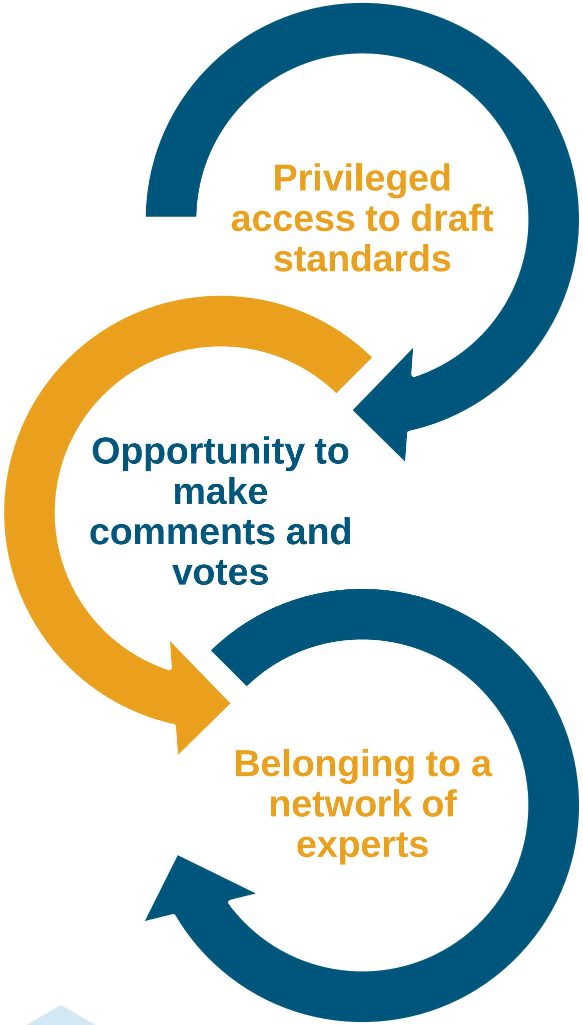
IEEE
Advancing Technology for Humanity

ETHICALLY ALIGNED DESIGN

A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems

How to become delegate in technical standardization

Why to get involved into technical standardization?


Privileged access to draft standards
Opportunity to make comments and votes
Belonging to a network of experts

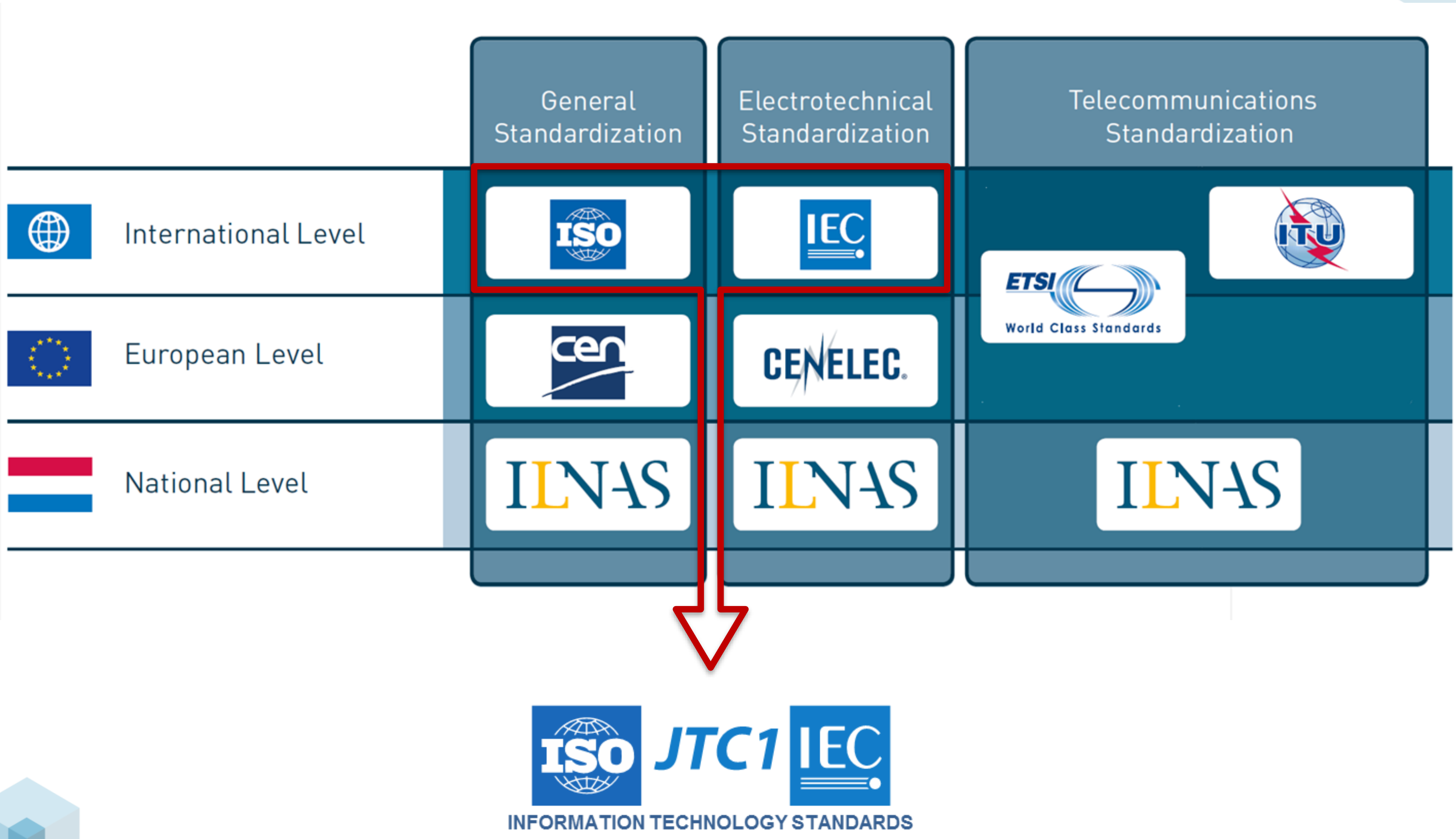
- Live monitoring of the development of draft standards
- Analyze ongoing projects and draft standards
- Anticipate future market rules and best practices

- Defend the interests of your business
- Spread and promote your innovations
- Valuate your know-how as good practices which could serve as a reference in your sector of activity

- Learn about your competitors and their position during the meetings
- Collaborate in order to defend common interests
- Enhance your organization and your skills at national, European and international level in terms of competitiveness

ILNAS

Recognized Standardization Organizations

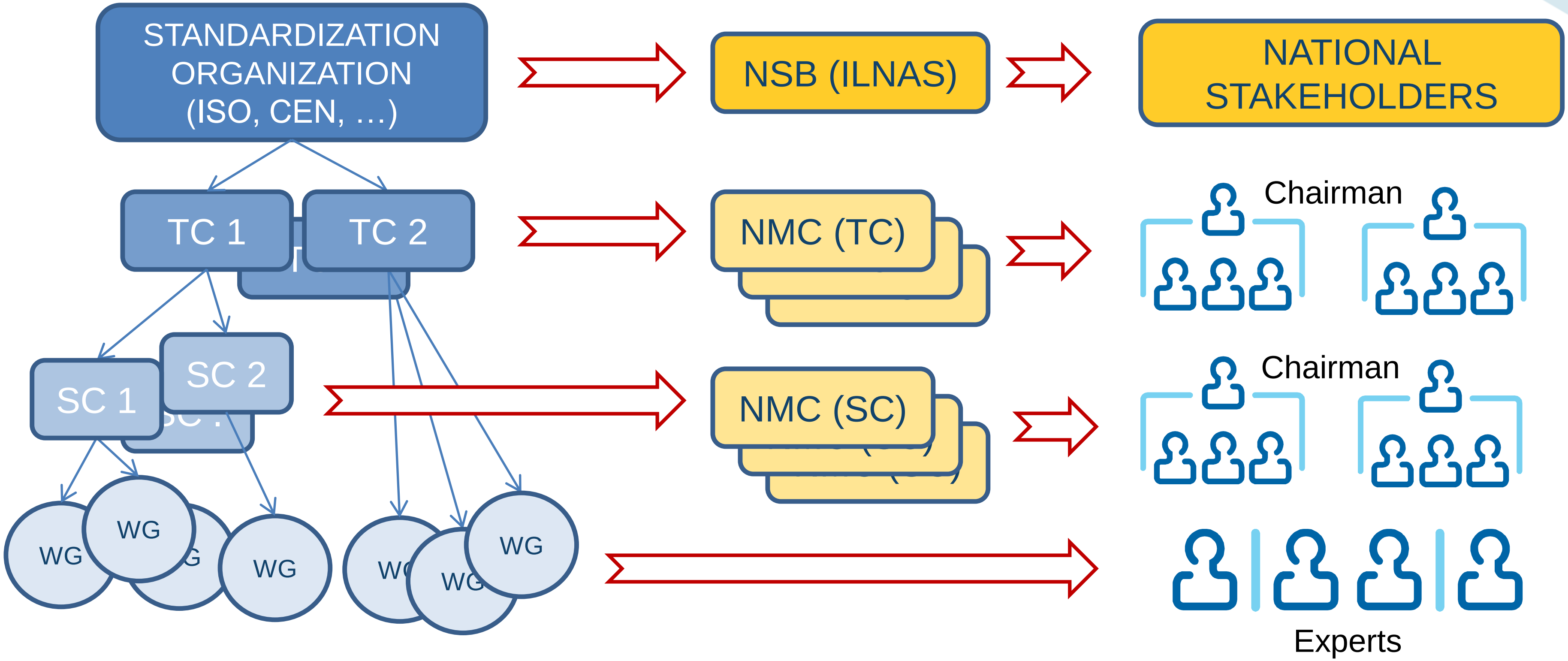


	General Standardization	Electrotechnical Standardization	Telecommunications Standardization
International Level	ISO	IEC	ITU ETSI World Class Standards
European Level	cen	CENELEC.	
National Level	ILNAS	ILNAS	ILNAS

ISO JTC1 IEC

INFORMATION TECHNOLOGY STANDARDS

Organization of the participation at national level



- TC: *Technical committee*
- SC: *Sub-committee*
- WG: *Working group*

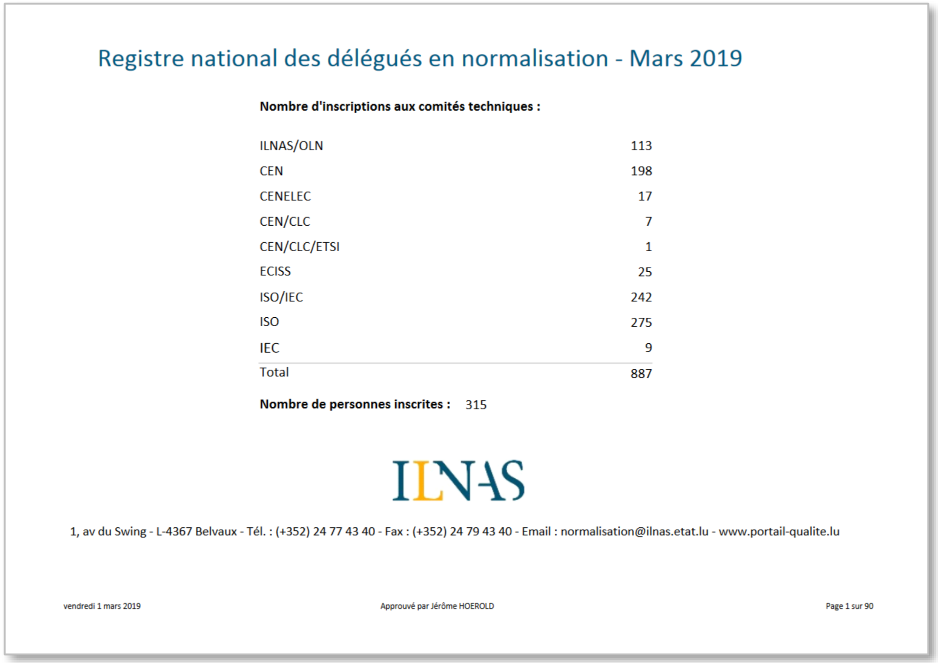
- NSB: *National Standards Body*
- NMC: *National mirror committee*

National register of standardization delegates

- **Who can participate ?**
  - Every socio-economic actor with a certain expertise

- **Cost of participation ?**
  - Free participation in Luxembourg

- **Register of National experts (March 2019)**
  - 315 persons registered
  - 887 registrations in technical committees



Registre national des délégués en normalisation - Mars 2019

Nombre d'inscriptions aux comités techniques :

ILNAS/OLN	113
CEN	198
CENELEC	17
CEN/CLC	7
CEN/CLC/ETSI	1
ECISS	25
ISO/IEC	242
ISO	275
IEC	9
Total	887

Nombre de personnes inscrites : 315

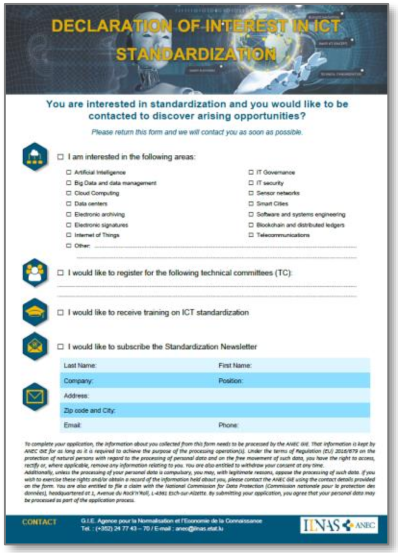
1, av du Swing - L-4367 Belvaux - Tél. : (+352) 24 77 43 40 - Fax : (+352) 24 79 43 40 - Email : normalisation@ilnas.etat.lu - www.portail-qualite.lu

vendredi 1 mars 2019 Approuvé par Jérôme HOEROLD Page 1 sur 90

→ https://gd.lu/cCN7qg

Registration in technical committees

Declaration of interest



DECLARATION OF INTEREST IN ICT STANDARDIZATION

You are interested in standardization and you would like to be contacted to discover arising opportunities?

Please return this form and we will contact you as soon as possible.

☐ I am interested in the following areas:

- ☐ Artificial Intelligence
- ☐ Big Data and data management
- ☐ Cloud Computing
- ☐ Data centers
- ☐ Electronic archiving
- ☐ Electronic signatures
- ☐ Internet of Things
- ☐ Other: ……………………………………………
- ☐ IT Governance
- ☐ IT security
- ☐ Sensor networks
- ☐ Smart Cities
- ☐ Software and systems engineering
- ☐ Blockchain and distributed ledgers
- ☐ Telecommunications

☐ I would like to register for the following technical committees (TC):

……………………………………………

……………………………………………

☐ I would like to receive training on ICT standardization

☐ I would like to subscribe the Standardization Newsletter

Last Name: First Name:

Company: Position:

Address:

Zip code and City:

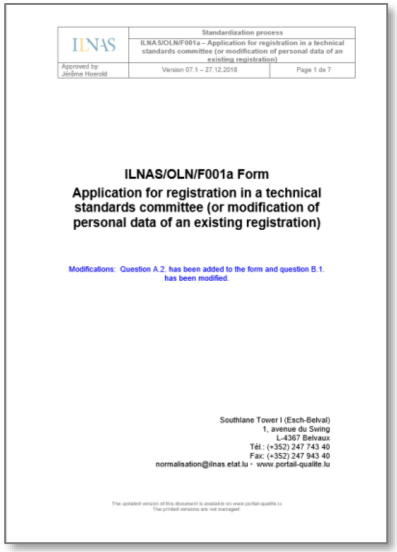
Email: Phone:

To complete your application, the information about you collected from this form needs to be processed by the ANEC GIE. That information is kept by ANEC GIE for as long as it is required to achieve the purpose of the processing operation(s). Under the terms of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, you have the right to access, rectify or, where applicable, remove any information relating to you. You are also entitled to withdraw your consent at any time.
Additionally, unless the processing of your personal data is compulsory, you may, with legitimate reasons, oppose the processing of such data. If you wish to exercise these rights and/or obtain a record of the information held about you, please contact the ANEC GIE using the contact details provided on the form. You are also entitled to file a claim with the National Commission for Data Protection (Commission nationale pour la protection des données), headquartered at 1, Avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette. By submitting your application, you agree that your personal data may be processed as part of the application process.

CONTACT G.I.E. Agence pour la Normalisation et l'Economie de la Connaissance
Tel. : (+352) 24 77 43 – 70 / E-mail : anec@ilnas.etat.lu

→ https://gd.lu/4pCBgW

Registration form



ILNAS	Standardization process	
	ILNAS/OLN/F001a – Application for registration in a technical standards committee (or modification of personal data of an existing registration)	
Approved by: Jérôme Hoerold	Version 07.1 – 27.12.2018	Page 1 de 7

ILNAS/OLN/F001a Form

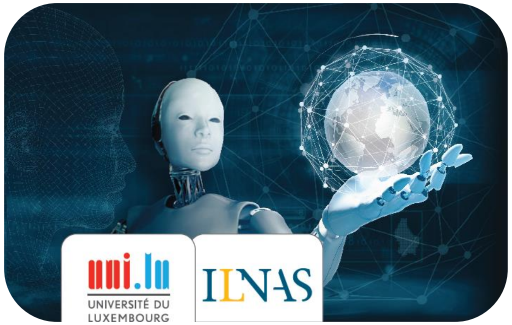
Application for registration in a technical standards committee (or modification of personal data of an existing registration)

Modifications: Question A.2. has been added to the form and question B.1. has been modified.

Southlane Tower I (Esch-Belval)
1, avenue du Swing
L-4367 Belvaux
Tél.: (+352) 247 743 40
Fax: (+352) 247 943 40
normalisation@ilnas.etat.lu · www.portail-qualite.lu

The updated version of this document is available on www.portail-qualite.lu
The printed versions are not managed.

→ https://gd.lu/fzdHMM



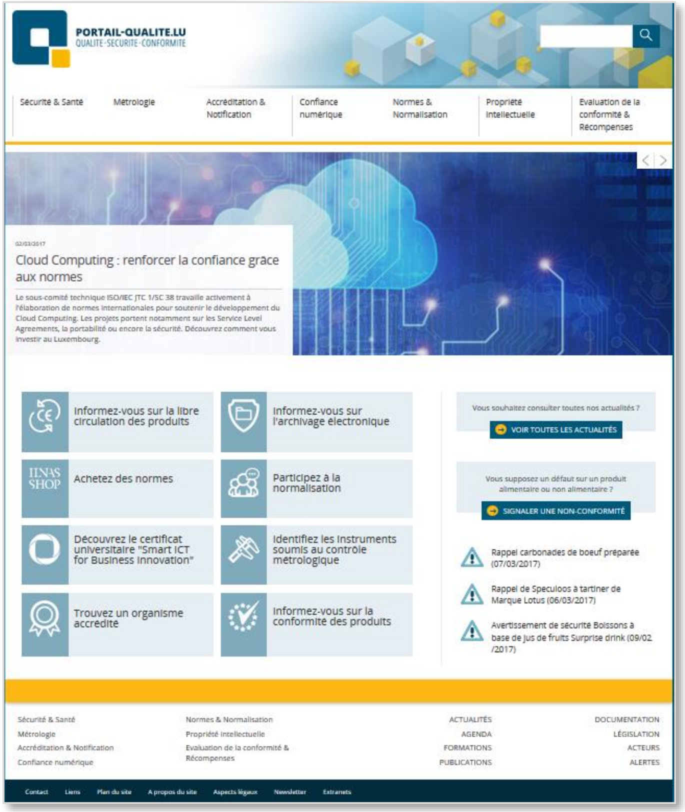
MASTER PROGRAM

"SMART SECURE ICT FOR BUSINESS INNOVATION"

- ➢ Ideal training to prepare for the future Smart Secure ICT ecosystem taking benefits of technical standardization

For more information

→ **Portail qualité:**
www.portail-qualite.lu



PORTAIL-QUALITE.LU
QUALITE·SECURITE·CONFORMITE

Sécurité & Santé | Métrologie | Accréditation & Notification | Confiance numérique | Normes & Normalisation | Propriété intellectuelle | Evaluation de la conformité & Récompenses

02/03/2017

Cloud Computing : renforcer la confiance grace aux normes

Le sous-comité technique ISO/IEC JTC 1/SC 38 travaille activement à l'élaboration de normes internationales pour soutenir le développement du Cloud Computing. Les projets portent notamment sur les Service Level Agreements, la portabilité ou encore la sécurité. Découvrez comment vous investir au Luxembourg.

- Informez-vous sur la libre circulation des produits
- Informez-vous sur l'archivage électronique
- ILNAS SHOP Achetez des normes
- Participez à la normalisation
- Découvrez le certificat universitaire "Smart ICT for Business Innovation"
- Identifiez les instruments soumis au contrôle métrologique
- Trouvez un organisme accrédité
- Informez-vous sur la conformité des produits

Vous souhaitez consulter toutes nos actualités ?

VOIR TOUTES LES ACTUALITÉS

Vous supposez un défaut sur un produit alimentaire ou non alimentaire ?

SIGNALER UNE NON-CONFORMITÉ

- Rappel carbonades de boeuf préparée (07/03/2017)
- Rappel de Speculoos à tartiner de Marque Lotus (06/03/2017)
- Avertissement de sécurité Boissons à base de jus de fruits Surprise drink (09/02/2017)

Sécurité & Santé
Métrologie
Accréditation & Notification
Confiance numérique

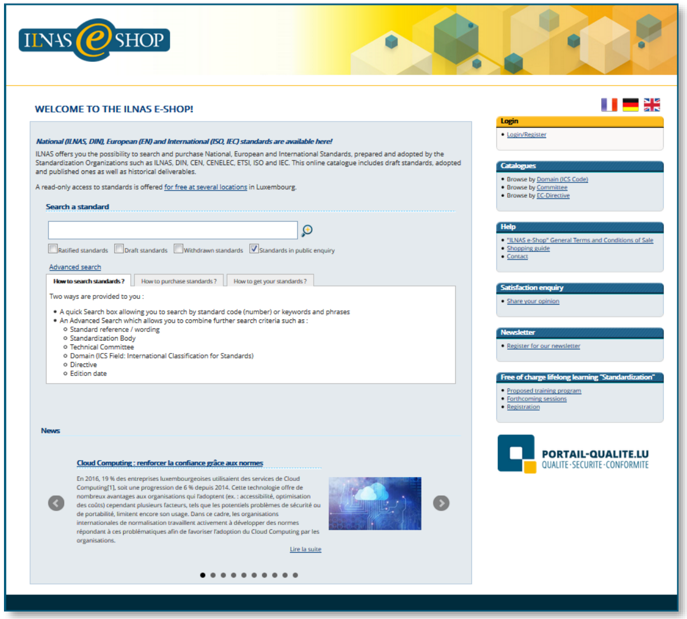
Normes & Normalisation
Propriété intellectuelle
Evaluation de la conformité & Récompenses

ACTUALITÉS
AGENDA
FORMATIONS
PUBLICATIONS

DOCUMENTATION
LÉGISLATION
ACTEURS
ALERTES

Contact | Liens | Plan du site | A propos du site | Aspects légaux | Newsletter | Extranets

→ **ILNAS e-shop:**
https://ilnas.services-publics.lu/



ILNAS e SHOP

WELCOME TO THE ILNAS E-SHOP!

National (ILNAS, DIN), European (EN) and International (ISO, IEC) standards are available here!

ILNAS offers you the possibility to search and purchase National, European and International Standards, prepared and adopted by the Standardization Organizations such as ILNAS, DIN, CEN, CENELEC, ETSI, ISO and IEC. This online catalogue includes draft standards, adopted and published ones as well as historical deliverables.

A read-only access to standards is offered for free at several locations in Luxembourg.

Search a standard

□ Ratified standards □ Draft standards □ Withdrawn standards ☑ Standards in public enquiry

Advanced search

How to search standards ? | How to purchase standards ? | How to get your standards ?

Two ways are provided to you :

- A quick Search box allowing you to search by standard code (number) or keywords and phrases
- An Advanced Search which allows you to combine further search criteria such as :
  - Standard reference / wording
  - Standardization Body
  - Technical Committee
  - Domain (ICS Field: International Classification for Standards)
  - Directive
  - Edition date

News

Cloud Computing : renforcer la confiance grâce aux normes

En 2016, 19 % des entreprises luxembourgeoises utilisaient des services de Cloud Computing[1], soit une progression de 6 % depuis 2014. Cette technologie offre de nombreux avantages aux organisations qui l'adoptent (ex. : accessibilité, optimisation des coûts) cependant plusieurs facteurs, tels que les potentiels problèmes de sécurité ou de portabilité, limitent encore son usage. Dans ce cadre, les organisations internationales de normalisation travaillent activement à développer des normes répondant à ces problématiques afin de favoriser l'adoption du Cloud Computing par les organisations.

Lire la suite

Login
- Login/Register

Catalogues
- Browse by Domain (ICS Code)
- Browse by Committee
- Browse by EC-Directive

Help
- "ILNAS e-Shop" General Terms and Conditions of Sale
- Shopping guide
- Contact

Satisfaction enquiry
- Share your opinion

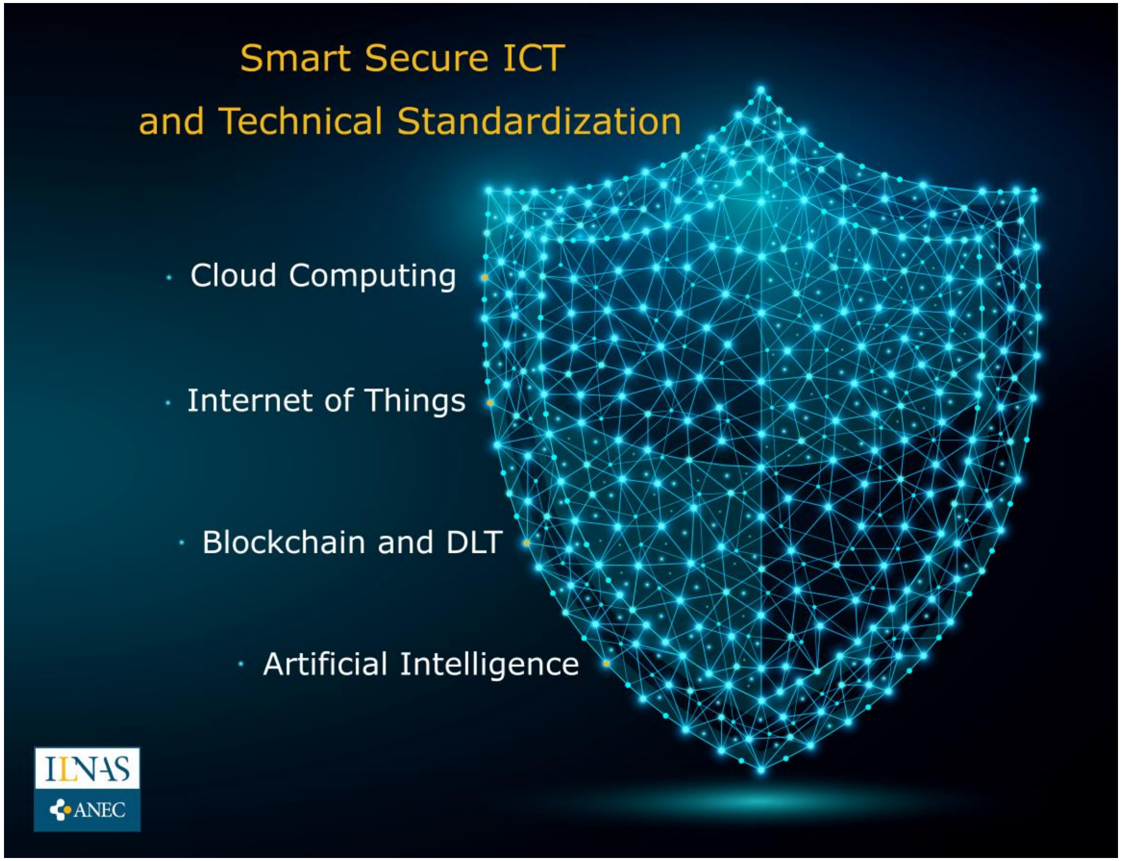
Newsletter
- Register for our newsletter

Free of charge lifelong learning "Standardization"
- Proposed training program
- Forthcoming sessions
- Registration

PORTAIL-QUALITE.LU
QUALITE·SECURITE·CONFORMITE

→ **Newsletters:**
https://portail-qualite.public.lu/fr/support/newsletter.html

QUESTIONS AND OPEN DISCUSSION



Smart Secure ICT

and Technical Standardization

- Cloud Computing
- Internet of Things
- Blockchain and DLT
- Artificial Intelligence

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail: info@ilnas.etat.lu
www.portail-qualite.lu