ILNAS

Welcome

Bienvenue

Willkommen

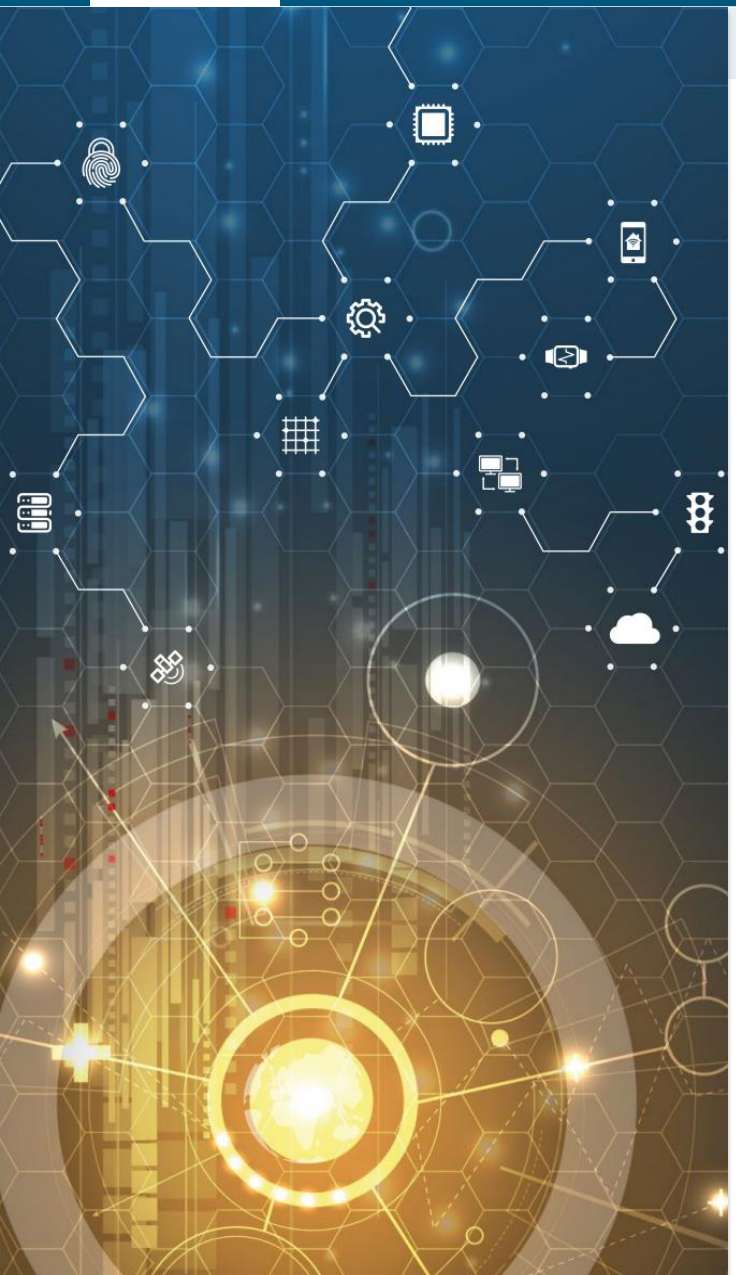
Presentation of the Standards Analysis Smart Secure ICT Luxembourg

Mr. Nicolas Domenjoud

Responsable secteur « TIC & Normalisation » – ILNAS/OLN

21 October 2019

CONTENT

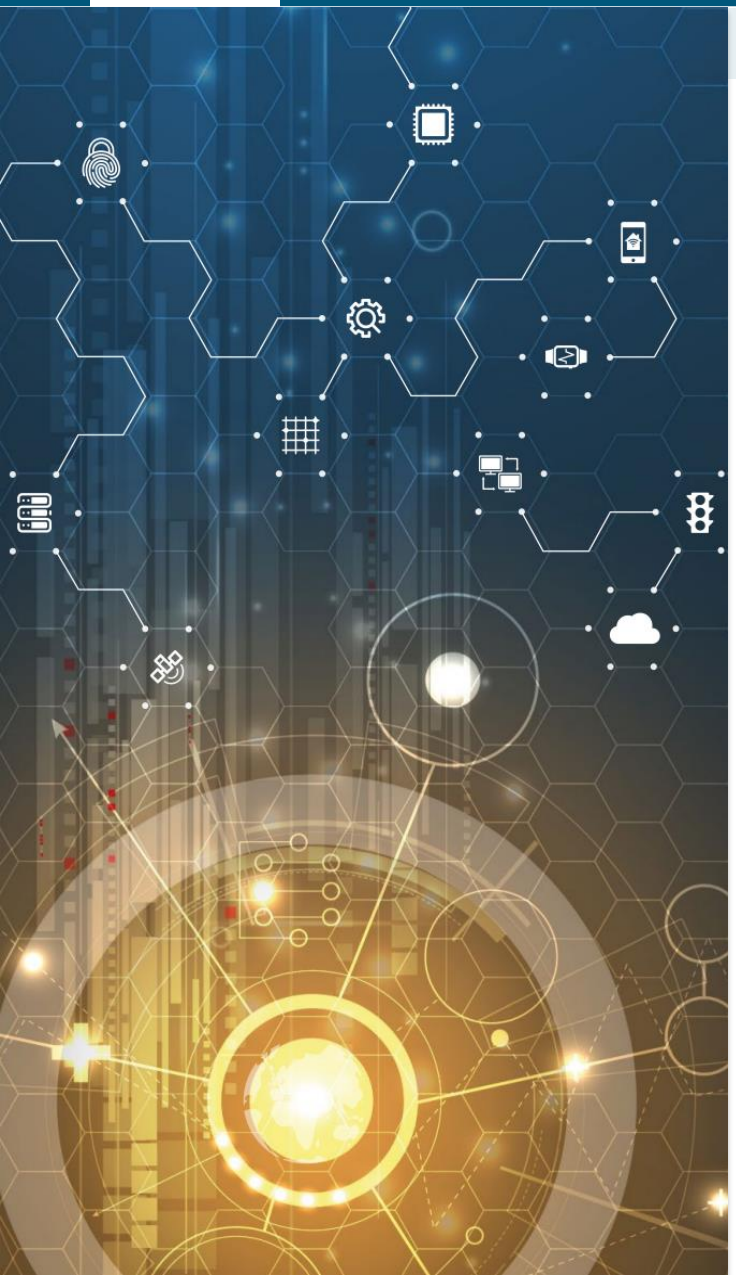


I - Context and objectives of the Standards Analysis Smart Secure ICT

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

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

2. GUIDELINES OF THE NATIONAL CYBERSECURITY STRATEGY

2.1. Guideline No. 1: strengthening public confidence in the digital environment

2.1.1. **Objective 1 :** Knowledge-sharing between all stakeholders
2.1.2. **Objective 2 :** Disseminating information on risks
2.1.3. **Objective 3 :** Raising awareness of all the parties concerned
2.1.4. **Objective 4 :** Responsible disclosure
2.1.5. **Objective 5 :** Combating cybercrime

2.2. Guideline No. 2: digital infrastructure protection

2.2.1. **Objective 1 :** Census of essential and critical digital infrastructure
2.2.2. **Objective 2 :** Security policies
2.2.3. **Objective 3 :** Crisis management
2.2.4. **Objective 4 :** Standardization
2.2.5. **Objective 5 :** Strengthen international cooperation
2.2.6. **Objective 6 :** Cyber defence
2.2.7. **Objective 7 :** Strengthening the resilience of the State's digital infrastructure

OBJECTIVE 4 : STANDARDIZATION

Standardization determines common techni-cal language, both at European and interna-tional level. If applied to the field of cyber-security, this unifying capability allows us to set definitions and needs, the state of the art in this area as well as reference architec-ture, while establishing by consensus require-ments and specifications required to ensure a suitable level of security. This constantly evolving whole facilitates digital ownership, especially for Smart ICT developments (Cloud Computing, Big Data, the Internet of things, Blockchain, etc.).

National monitoring and investment in the development process of standards related to the field of cybersecurity will be strengthened, specifically in order to convert it into a strategic tool for the development of national digital confidence.

This approach will be carried out for formal technical standardization (ISO, IEC, ETSI, CEN-CENELEC, ITU-T), while taking into account the work developed by relevant fora and consortia identified in the context of cybersecurity.

The ILNAS (Luxembourg standardisation body) will unify and develop this strategic monitoring in order to report it at national level, in the interest of the implementation of a "smart nation".

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

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
- → Provides a monitoring of **relevant technical committees and standards**
- → Introduces **Fora and Consortia** identified as relevant in the cybersecurity context

Internet of Things

Cloud Computing

Artificial Intelligence & Big Data

Blockchain

DIGITAL TRUST

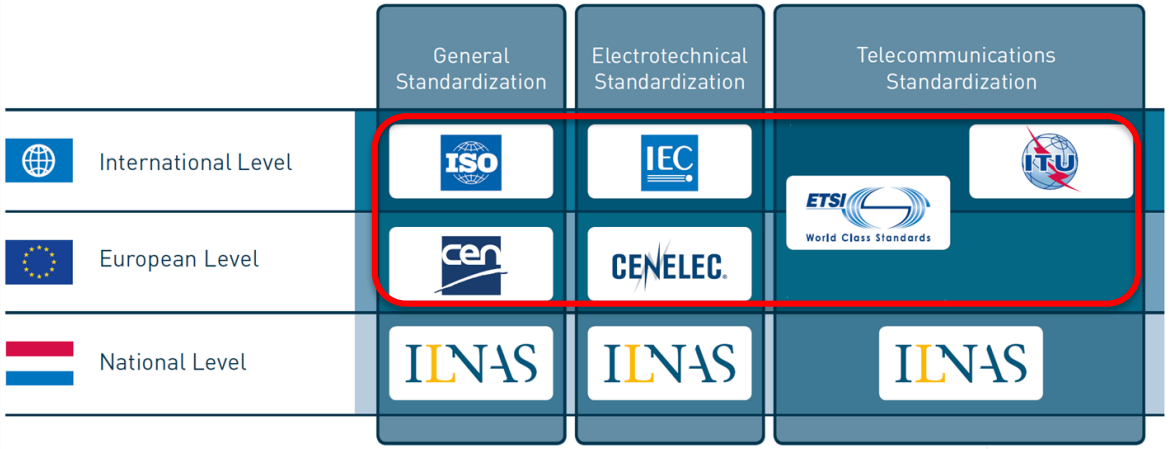
I. Context and objectives of the Standards Analysis Smart Secure ICT

B. Objectives

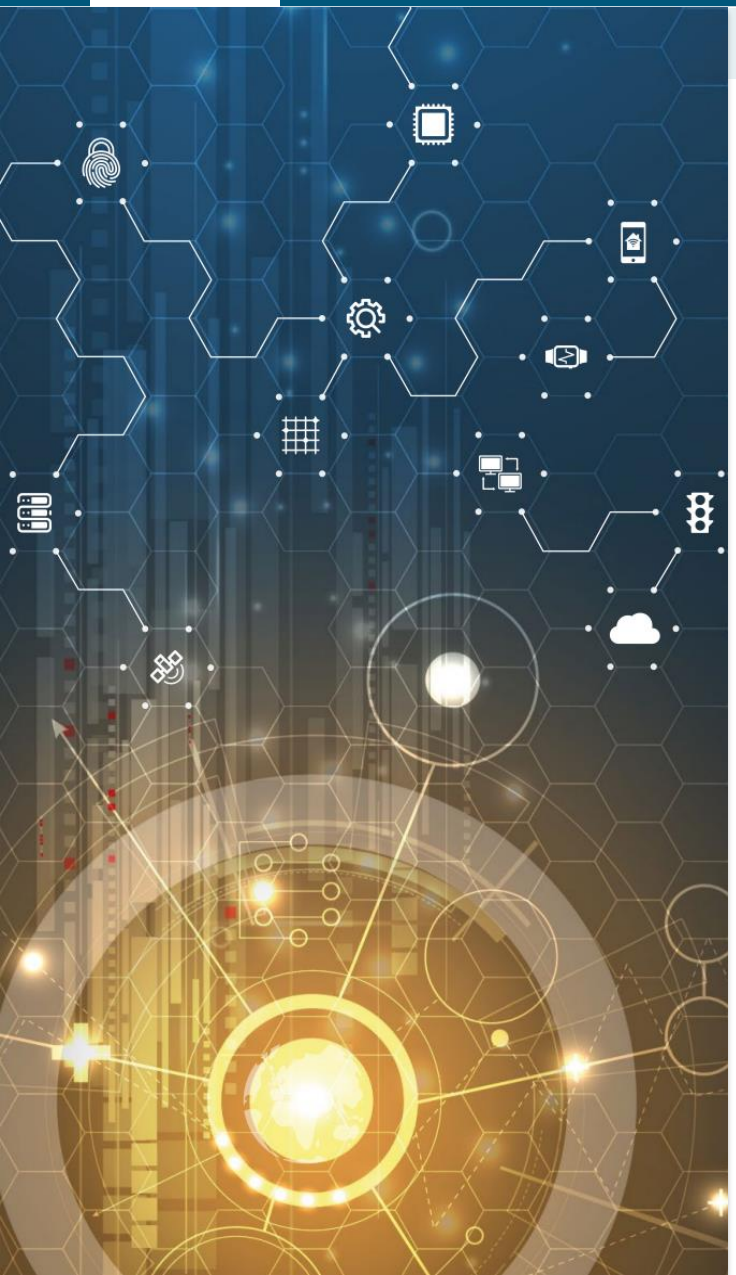
INFORM	IDENTIFY	ENCOURAGE	DEVELOP
about Smart ICT standardization developments	standardization opportunities for the national market	the involvement in the standardization process	"standards-related" skills and collaborations

For the benefit of all national stakeholders

- Introduction of **Smart ICT technologies main characteristics**
- Identification and presentation of **relevant standardization technical committees** as well as identified **Fora and Consortia in the context of cybersecurity**
- 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**



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

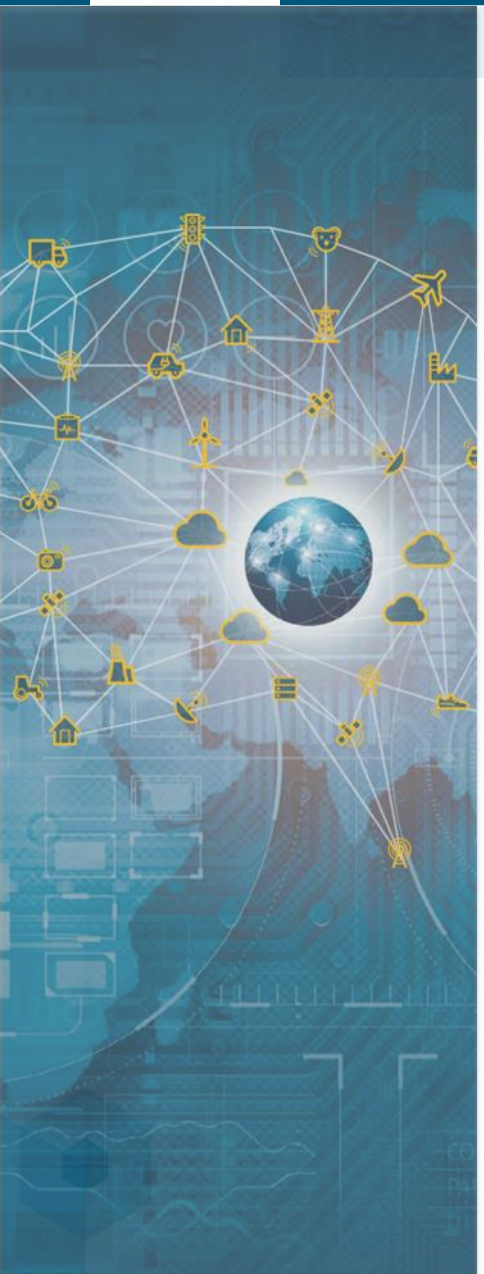
A. Smart (Secure) ICT overview

- **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*)
    - ITU-T Y.4000/Y.2060 (06/2012), Overview of the Internet of things
  - **Cloud Computing**:
    - ISO/IEC 17788:2014 | ITU-T Y.3500, 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**

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 (65)**
  - ISO/IEC 30141:2018, Internet of Things Reference Architecture (IoT RA)
  - ISO/IEC TR 22417:2017, IoT use cases
  - ISO/IEC 21823-1:2019, Interoperability for Internet of things systems -- Part 1: Framework (***new***)
  - …

- **STANDARDS UNDER DEVELOPMENT (66)**
  - ISO/IEC CD 30161, Requirements of IoT data exchange platform for various IoT services
  - ISO/IEC CD 30165, Real-time IoT framework
  - ISO/IEC CD 30166, Industrial IoT (***new***)
  - …

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 (62)**
  - ISO/IEC 19941:2017, Interoperability and portability
  - ISO/IEC 19944:2017, Cloud services and devices: Data flow, data categories and data use
  - ISO/IEC TR 22678:2019, Guidance for Policy Development (***new***)
  - …

- **STANDARDS UNDER DEVELOPMENT (23)**
  - ISO/IEC CD 22123, Concepts and terminology
  - ISO/IEC AWI 23751, Data sharing agreement (DSA) framework (***new***)
  - ISO/IEC NP TR 23951, Best practices for cloud SLA metrics (***new***)
  - …

II. Results of the Standards Analysis

D. Artificial Intelligence and Big Data

- **TECHNICAL COMMITTEES (3)**
  - ISO/IEC JTC 1/SC 42 “Artificial Intelligence”
  - ISO/IEC JTC 1/SC 32 “Data management and interchange”
  - ITU-T/SG 16 “Multimedia coding, systems and applications” (***new***)

- **PUBLISHED STANDARDS (35)**
  - ISO/IEC 20546:2019, Big Data -- Overview and Vocabulary (***new***)
  - ISO/IEC TR 20547-2:2018, Big Data Reference Architecture -- Part 2: Use Cases and Derived Requirements
  - ISO/IEC TR 20547-5:2018, Big data reference architecture -- Part 5: Standards roadmap
  - …

- **STANDARDS UNDER DEVELOPMENT (43)**
  - 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

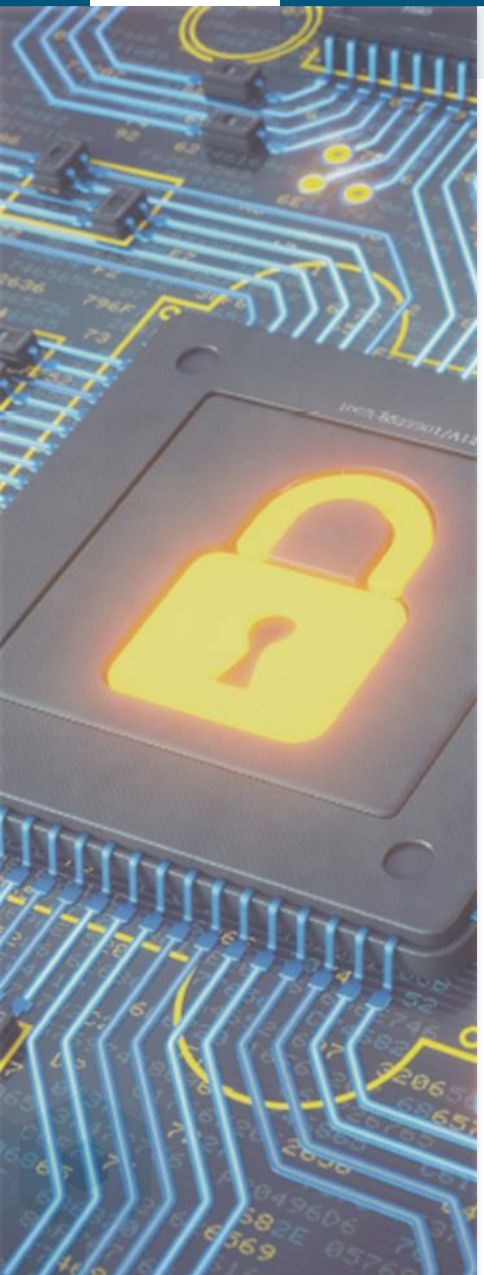
E. Blockchain and Distributed Ledger Technologies

- **TECHNICAL COMMITTEES (1)**
  - ISO/TC 307 “Blockchain and distributed ledger technologies”

- **PUBLISHED STANDARDS (1)**
  - ISO/TR 23455:2019, Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems (***new***)

- **STANDARDS UNDER DEVELOPMENT (10)**
  - ISO/DIS 22739, Terminology
  - ISO/DTR 23245, Security risks, threats and vulnerabilities
  - ISO/NP TR 23246, Overview of identity management using blockchain and distributed ledger technologies
  - ISO/CD 23257, Reference architecture
  - ISO/NP TS 23635, Guidelines for governance
  - …

II. Results of the Standards Analysis



F. Digital Trust in Smart ICT

- **TECHNICAL COMMITTEES (8)**
  - ISO/IEC JTC 1/SC 27 “Information Security, cybersecurity and privacy protection”
  - CEN/CLC/JTC 13 “Cybersecurity and Data Protection”
  - ETSI/TC CYBER “Cyber Security”
  - …

- **PUBLISHED STANDARDS (32) → Digital Trust aspects of Smart ICT**
  - **IoT:** ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things (***new***)
  - **Cloud Computing:** ISO/IEC 27018:2019, Guidance for the assessment of information security controls (***new***)
  - **AI/Big Data**: ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques
  - …

- **STANDARDS UNDER DEVELOPMENT (39)**
  - **IoT:** ISO/IEC 30149, Trustworthiness framework
  - **Cloud Computing**: ITU-T Draft X.sgmc, Security guidelines for multi-cloud (***new***)
  - **AI/Big Data:** ISO/IEC NP TR 24028, Overview of trustworthiness in Artificial Intelligence (***new***)
  - …

II. Results of the Standards Analysis

G. Presentation of the results

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

General information			
Committee	ISO/IEC JTC 1/SC 27	**Title**	**Information Security, cybersecurity and privacy protection**
Creation date	1989		
Secretariat	DIN (Germany)		
Committee Manager	Ms. Krystyna Passia		
Chairperson	Dr. Andreas Wolf		
Organizations in liaison	(ISC)2, CalConnect, CCETT, CSA, ECBS, Ecma International, ENISA, EPC, ETSI, Global Platform, IEEE, ISACA, ISSEA, ITU, MasterCard Int., SBS, ABC4Trust, Article 29 Data Protection Working Party, CCDB, CCUF, CREDENTIAL, CSCC, Cyber Security, EUDCA, EuroCloud, FIDO Alliance, FIRST, IFAA, INLAC, Interpol, ISA – Automation, ISCI, ISF, Kantara Initiative, OASIS-PMRM, OECD, OIDF, Opengroup – United Kingdom, PICOS, PQCRYPTO, PRIPARE, PRISMACLOUD, SAFECode, SAFEcrypto, TAS3, TCG, TMForum, TREsPASS, WITDOM	**MEMBERS**	**Participating Countries (48):** Germany, Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Cyprus, Denmark, Finland, France, India, Indonesia, Islamic Republic of Iran, Ireland, Israel, Italy, Japan, Republic of Korea, Lebanon, **Luxembourg**, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Poland, Romania, Russian Federation, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay **Observing Countries (30):** Belarus, Bosnia and Herzegovina, Bulgaria, Chile, Côte d'Ivoire, Czech Republic, El Salvador, Estonia, Eswatini, Ghana, Hong Kong, Hungary, Iceland, Kazakhstan, Kenya, Lithuania, Morocco, North Macedonia, Pakistan, State of Palestine, Philippines, Portugal, Rwanda, Saudi Arabia, Senegal, Serbia, Slovenia, Thailand, Trinidad and Tobago, Turkey
Web site	https://www.iso.org/committee/45306.html		
Scope	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: - Security requirements capture methodology; - Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls and services; - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; - Security aspects of identity management, biometrics and privacy;		

Structure		
	JTC 1/SC 27/AG 1	Management Advisory Group
	JTC 1/SC 27/SG 1	Data Security
	JTC 1/SC 27/SG 2	Trustworthiness
	JTC 1/SC 27/SG 3	Concepts and Terminology
	JTC 1/SC 27/SWG-T	Transversal Items
	JTC 1/SC 27/WG 1	Information security management systems
	JTC 1/SC 27/WG 2	Cryptography and security mechanisms
	JTC 1/SC 27/WG 3	Security evaluation testing and specification
	JTC 1/SC 27/WG 4	Security controls and services
	JTC 1/SC 27/WG 5	Identity management and privacy technologies

Standardization work	
Published standards	184
Standards under development	80

Involvement of Luxembourg

27 delegates

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

Comments

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

Working Groups

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

II. Results of the Standards Analysis

G. 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.: Digital Trust for Cloud Computing standards

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

II. Results of the Standards Analysis

G. Presentation of the results

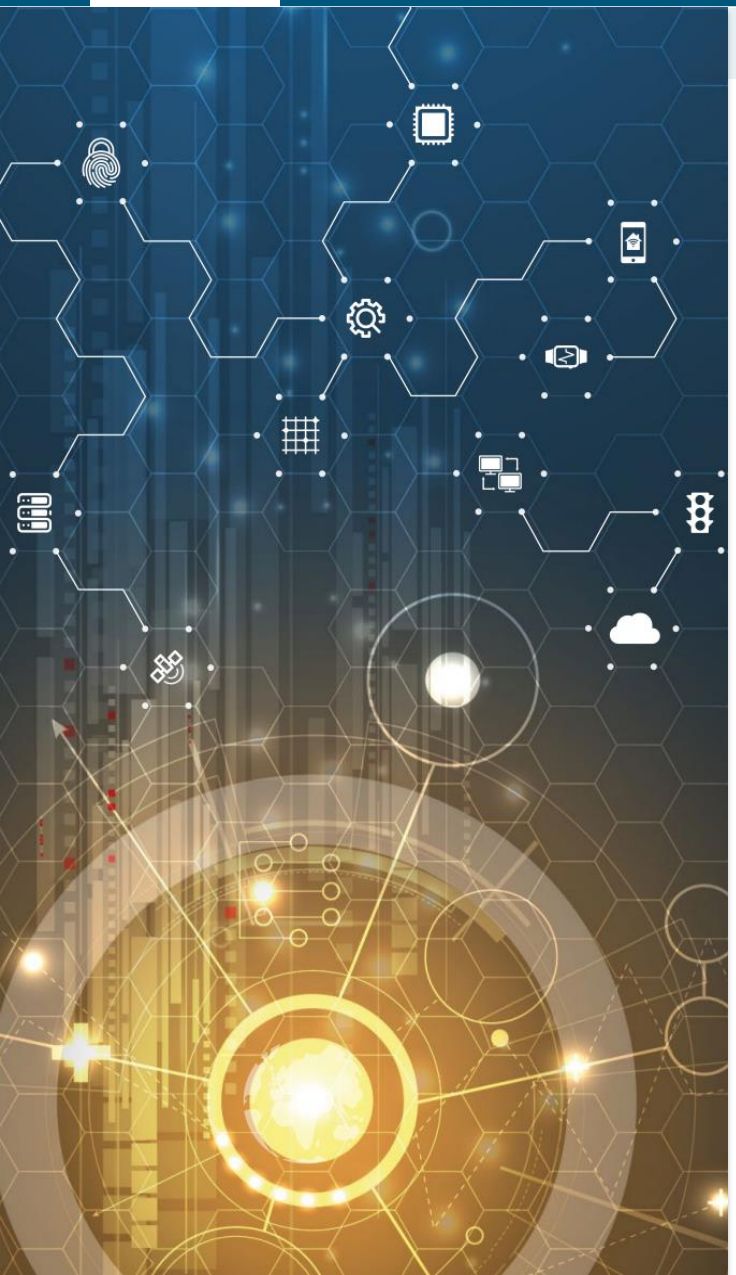
- **A list of relevant Fora and Consortia working in the Digital Trust area (and notably in relation with Smart ICT technologies) is provided (23 Fora and Consortia identified)**

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

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

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

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
- Future professional "*Master in Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions*" (forecast in September 2020)

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

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