StandICT.eu

Supporting European Experts Presence in International Standardisation Activities in ICT

Project Title	Supporting European Experts Presence in International Standardisation Activities in ICT
Project Acronym	StandICT.eu
Grant Agreement No	780439
Instrument	Coordination and Support Action
Thematic Priority	ICT standardisation, ICT Technical specifications, cloud computing, 5G communications, IoT, cybersecurity, data technologies
Start Date of Project	01.01.2018
Duration of Project	24 Months
Project Website	www.standict.eu

D2.1 – REPORT ON RELEVANT ICT STANDARDISATION, POTENTIAL GAPS AND EU PRIORITIES

Work Package	WP2, Prioritisation of global standards for EU
Lead Author (Org)	Wolfgang, Ziegler (Fraunhofer Institute SCAI)
Contributing Author(s) (Org)	Stephanie Parker, Trust-IT
Due Date	01.03.2018
Date	05.04.2019
Version	2.0

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

The work described in this document has been conducted within the project StandICT.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 7804391. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Versioning and Revision History

Version	Date	Author	Notes
0.8	11.03.2018	Wolfgang Ziegler	Initial version for internal review
0.9	29.03.2018	Wolfgang Ziegler	Section 4 additional information for the watch updated, Section 5 changed to include the list of the 2018 Rolling Plan, Section 6 adapted and Annex included
0.10	04.04.2018	Timea Biro	Internal review
1.1	29.03.2019	Wolfgang Ziegler	Revision after EC review: new Section 5 Potential gaps and new Section 6 EU priorities added
1.2	01.04.2019	Wolfgang Ziegler	Cross-linked the new sections with the Standards Watch
1.3	02.04.2019	Silvana Muscella	1st Internal Review
1.4	04.04.2019	Stephanie Parker	Updates on 5G standardisation
1.5	05.04.2019	Stephanie Parker	2nd Internal Review
2.0	05.04.2019	Silvana Muscella	Final version for submission

Table of Contents

List of Tables

List of Figures

Executive Summary of the Project

This deliverable **D2.1 Report on relevant ICT standardisation, potential gaps and EU priorities** is a revised version that was submitted in time for the first year StandICT.eu review which took place in February 2019 in Brussels. This revised report addresses the reviewer recommendations, who rejected the deliverable on the basis of it missing elements around gaps and EU priroities. The consortium has addressed the recommendations by introducing two sections into the report to cover:

- ➔ Section 5 which covers the **Potential Gaps** in 5G communications, Cyber Security, Internet of Things, Cloud Computing, Big Data technologies;
- ➔ Section 6 that covers the **EU priorities** in the areas of 5G communications, Cyber Security, Internet of Things, Cloud Computing, Big Data technologies.

This additional information will serve to introduce the gap analysis into the Standards Watch and will also be reflected in the monthly monitoring report that the funded applicants need to complete, with a drop-down menu to facilitate compilation for the applicant and for the consortium which analyses and monitors the content for impact.

The Digital Single Market (DSM) is aimed at boosting Europe's competitiveness throughout multiple industrial and service sectors. 5 priority domains are highlighted as the building blocks of the DSM: 5G, Cloud Computing, Internet of Things, Cybersecurity and Big Data. The emergence and continuous evolution in these domains compels the establishment of common standards to guarantee interoperable and benchmarked services and technologies to drive the DSM, keep markets open, support innovation and allow a full-service portability.

StandICT.eu, "Supporting European Experts Presence in International Standardisation Activities in ICT", addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene. Through a Standards Watch, StandICT.eu will map and monitor the international ICT standards landscape and liaise with Standards Development Organisations (SDOs) and Standard Setting Organisations (SSOs), as well as industry-led groups, to identify gaps and priorities matching EU DSM objectives These will become the topics for a series of 10 Open calls in the 5 priority domains and a continuous cascading grants process, to be launched by StandICT.eu from March 2018, providing support for European specialists to contribute to ongoing standards development activities, and attend SDO & SSO meetings.

Through the mapping and monitoring process of activities in the EU and globally, over its 24 month work plan, StandICT.eu will provide a Go-To-Platform for the Open Call applications and evaluation, support prioritization of standardisation activities and build a community of Standardisation experts to support knowledge exchange and collaboration and reinforce European presence in the international ICT standardisation scene through 3 structured steps: 1) Monitoring and gathering information on the on-going work from the relevant international and global SDOs; 2) Setting up, managing and facilitating an open call designed to support the participation and contribution of EU specialists in key SDOs; and 3) Creating positive impact on business and research opportunities from ICT standardisation. StandICT.eu's positioning will envisage a trajectory of the ICT standardisation landscape that looks beyond 2020. An influential Expert Advisory Group (EAG) and External Pool of Evaluators (EPE) will support the project's rigorous activities.

The objectives of the project can be summarised as follows:

- To create awareness on the advantages of adopting ICT standards;
- To build strong motivation to businesses and SMEs, in addition to researchers to contribute actively in the shaping of ICT standards;

- To provide input and feedback during the development and evolution phases;
- To deliver the StandICT.eu platform supporting an inclusive transparent, continuous Open Call process and the standardisation landscape overview through the StandICT Watch to ensure effective grants allocations
- To attain global recognition of StandICT.eu is the Go-to-Platform to understand how Europe influences ICT standards efforts;
- Create a lasting legacy a consolidated, relevant European Community database of experts and engaged actors in the project;
- Provide global visibility of the benefits worldwide.

1 Introduction

*This deliverable **D2.1 – Report on relevant ICT standardisation, potential gaps and EU priorities** presents the initial exploration of the standardisation landscape with a focus on the five priority areas (5G, Cyber Security, IoT, Cloud, BiG Data) identified as critical for the Digital Single Market by the European Commission in their report **Rolling Plan for ICT Standardisation 2017 [1], 2018 [8]** and the **COM(2016) 176 on the ICT Standardisation Priorities for the Digital Single Market [2]**.*

1.1 Purpose and Scope

The purpose of this deliverable is twofold: firstly, to provide an overview on standardisation and potential gaps in the five areas and to generate the basic data for StandICT.eu's Standardisation Watch. Secondly, to provide input to a prioritised list of standardisation activities that will be used for the 1st and subsequent calls for experts. These experts will then apply for StandICT.eu grants with proposals addressing standardisation along the topics of the prioritised list.

The scope of the proposal is to consolidate standardisation activities relevant for the five priority areas in one single place that will be initially this deliverable and in the following two years of the project and the time beyond the StandICT.eu Standardisation Watch, an interactive web space accessible through the StandICT.eu portal [7] that will be continuously updated (see section 10 for an introduction into the the StandICT.eu Standardisation Watch). Moreover, the information on Potential gaps in Section EU priorities in Section 5 and EU priorities in Section 6 will also be continuously monitored for changes, updated and accessible through the Standards Watch web pages.

1.2 Relationship to other project outcomes

This deliverable is the basis for a number of other outcomes of the project, namely **D2.2 Interim report on relevant ICT standardisation, EU priorities and business opportunities** to be delivered month 14. This deliverable presents an interim list of relevant SDOs and associated standards for the five priority areas and recommendations and how the standards can bridge opportunities for businesses.

Furthermore, **D2.3 Final recommendations report on relevant ICT standardisation, EU priorities and business opportunities** which is due month 24 will extend both D2.1 and D2.2. As mentioned before, D2.1 also provides the ground for the StandICT.eu standards watch continuous monitoring.

1.3 Structure of the document

The rest of this document is organized as follows:

- Section 2 EC Communication on ICT Standardisation Priorities and Rolling Plan for ICT standardisation.
- Section 3 Approach.
  - Section 4 SDOs and standards in the five priority areas: 5G, Cyber Security, IoT, Cloud and Data.
- Section 5 Potential gaps.
- Section 6 EU Priorities.
- Section 7 Prioritised list for 1st call.
- Section 8 Call priorities.
- Section 9 Role of communities and OSS.
- Section 10 Relation to StandICT.eu standardisation watch.
- Section 11 Conclusions.

2 EC Communication on ICT Standardisation Priorities and Rolling Plan for ICT standardisation

For selection and assessment of relevant SDOs and ongoing standardisation work StandICT.eu's work is oriented along the lines of the following two publications of the EC addressing ICT standardisation relevant for Europe

In their 2016 communication on **ICT Standardisation Priorities for the Digital Single Market** the EC identifies several new challenges for the development of ICT standards for the Digital Single Market that require a focused and sustained European response [2]:

- All sectors of the economy increasingly rely on digital technologies that change ever faster, frequently dramatically exceeding the pace of change in more traditional sectors and industries.
- The value of digital systems increasingly derives from cross-sector applications, data and technology convergence.
- The increasing complexity resulting from a proliferation of standards, and the diversity of technical communities involved in standard setting can slow down innovation.
- There are ever more bodies and organizations involved in standard or technical specification setting around the world.
- European work on standardisation cannot be viewed in isolation.
- The Commission considers that standardisation has not received the necessary level of political support in the European Union.

In response to these challenges the Commission has identified the following priority areas: 5G communications, cloud computing, the internet of things (IoT), (big) data technologies and cybersecurity. These are the essential technology building blocks of the Digital Single Market.

The EC encourages stronger European leadership in standard setting in these areas to increase competitiveness and help European innovations better access the global market.

The **Rolling Plan for ICT Standardisation 2017** [1] and **2018** [8] extend the 2016 communication on ICT Standardisation Priorities providing a deeper analysis on requirements, SDOs with ongoing standardisation in the priority areas, other activities and relevant initiatives. The document includes

per area comments of the European Multi-Stakeholder Platform on ICT Standardisation (MSP)[1] and defines a number of actions per area.

The Rolling Plan defines policy objectives for each of the priority areas which prepare the groundwork for the presentation of relevant SDOs and their standardisation activities in the respective area:

5G (cf [8] p19)

Very high-capacity networks like 5G are identified as a key asset for global competitiveness. 5G is not fully standardised yet but its key specifications and technological foundations are already being developed and tested. The Commission launched a 5G public private-partnership (the 5G PPP[2]) to that end in 2013. The 5G PPP has established several working groups, including one on standardisation (5G Pre-Standardisation WG), and the 5G Infrastructure Association is a market representation partner of 3GPP. The benefits of adopting 5G go beyond the telecom sector to enable a fully mobile and connected society and to empower socio-economic trans-formations in a variety of ways (many of which are not possible at present) including higher productivity, sustainability, well-being and innovation opportunities for smaller actors and start-ups. 5G makes possible a new wave of convergence possible through digital business models reaching non-ICT-native industrial sectors. In that context, the EU sees 5G as a core infrastructure to support the DSM strategy's wider objectives for the digitisation of the industry.

Cloud Computing (cf [8] p21)

Establishing a coherent framework and conditions for cloud computing was one of the key priorities of the Digital Agenda for Europe. The Digital Single Market strategy confirmed the importance of cloud computing, which is driving a paradigm shift in the delivery of digital technologies, enhancing innovation, digital single market and access to content.

Data (cf [8] p25)

With the continuously growing amount of data (often referred to as 'big data') and the increasing amount of open data, interoperability is increasingly a key issue in exploiting the value of this data.

Standardisation at various levels (such as metadata schemes, data representation formats and licensing conditions of open data) is essential to enable broad data integration, data exchange and interoperability with the overall goal of fostering innovation based on data. This refers to all types of (multilingual) data, including both structured and unstructured data, and data from different domains as diverse as geospatial data, statistical data, weather data, public sector information (PSI) and research data, to name just a few.

IoT (cf [8] p29)

The Internet of Things (IoT) is a key priority area of the DSM. The IoT is an emerging technology that connects more objects to the internet — including house-hold equipment, wearable electronics, vehicles and sensors. Besides the innovation potential in many industrial sectors, the IoT also has the potential to help address many societal challenges including climate change, resource and energy efficiency and ageing.

A large number of proprietary or semi-closed solutions to address specific problems have emerged, leading to non-interoperable concepts, based on different architectures and protocols. Consequently, the deployment of truly IoT applications, i.e. where information of connectable "things" can be flexibly aggregated and scaled, has been limited to a set of "intranets of things — or goods".

In the emerging IoT economy, voluntary global standards can accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. A certain level of standardisation can facilitate interoperability, compatibility, reliability, security and effective operations on a global scale

[1] The MSP is a group of experts set-up by Commission with the aim to advise the Commission on all matters related to ICT standardisation. The MSP is composed of all Member States and EFTA countries and all other relevant stakeholders, including standard setting organisations, industry, SMEs and societal stakeholders in the area of ICT standardisation.
[2] https://5g-ppp.eu/.

among different technical solutions, stimulating industry innovation and provide a clearer technology evolution path.

Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges. Therefore, there is a need for a secure solution that is interoperable and scales across a global IoT ecosystem. In this context, the European large-scale pilots (LSP) were the subject of a call for proposals in 2016. The LSPs will support the deployment of IoT solutions, by enhancing and testing their acceptability and adoption by users and the public, and by fostering new market opportunities for suppliers to the EU.

Cyber Security (cf [8] p35)

The European cybersecurity strategy [9] and the Directive on network and information security [10] provide for action to promote the development and take-up of ICT security standards.

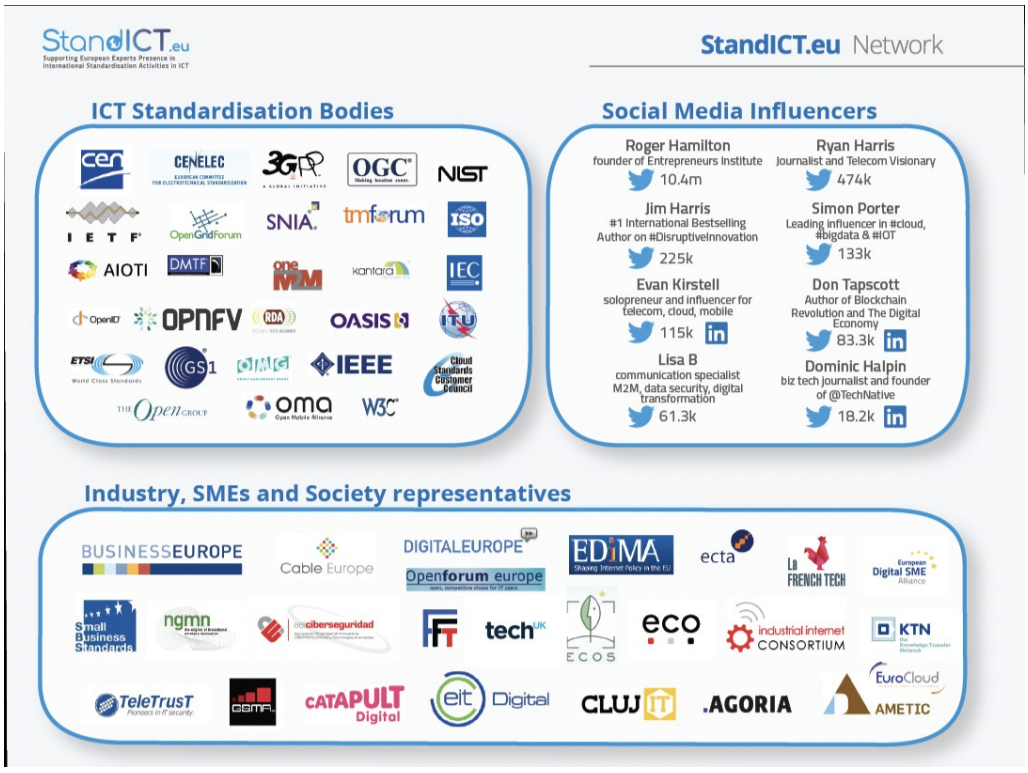
A network and information security public-private platform (NIS Platform) has been set up by the Commission with representation from various stakeholders.

3 Approach

This **Report on relevant ICT standardisation, potential gaps and EU priorities** is a living document and does not claim completeness. It aims at covering as much as possible the broad range of standardisation activities, technical specifications and standards relevant for the five priority areas, based on a systematic analysis of diverse sources as detailed below.

The report is a project document that will have a mid-term update followed by one at the end of the project. Moreover, it will be the base for the online interactive Standardisation Watch that will be collaboratively and regularly reviewed and continuously updated by the project partners and stakeholders, like the Expert Advisory Group.

Besides being stimulated by the SDO and standardisation-related network of the project partners the selection of SDOs and standardisation activities is driven by the two aforementioned sources of the EC, the communication of ICT standardisation priorities and the rolling plan.



As an outcome of the work of first meeting of the EAG, held in Pisa (IT), 28 February 2018, the priorities map outlined focused on 5G, Cyber Security, IoT, Cloud Computing and Data. Following a proposal of the EAG the area Big Data was renamed to Data to make it less restrictive. Data includes, e.g., public sector information, open data, Big Data, and more. 5G (with probably the largest number of ongoing standardisation activities) is followed by Cyber Security as a cross cutting activity, followed by IoT, with a large number of SDOs and ongoing standardisation. Followed by Cloud Computing and Data, both having strong links to IoT.

Figure 1: **The StandICT.eu Network**

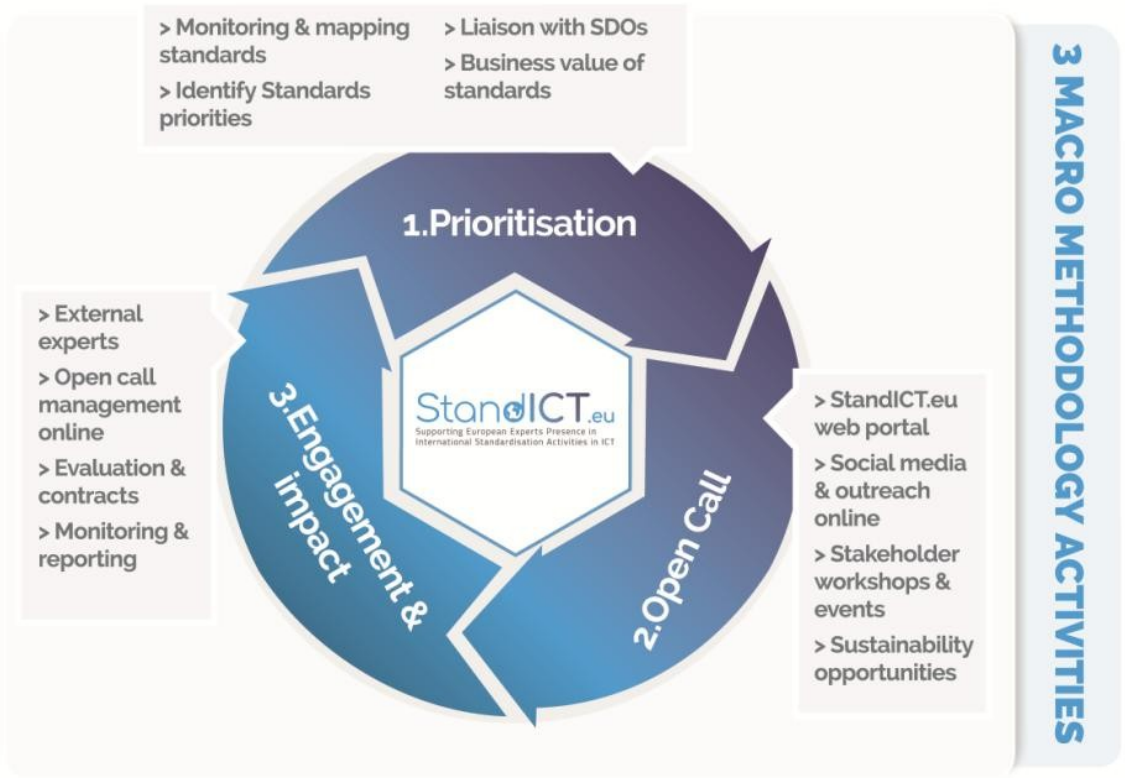


Figure 2: **StandICT.eu overall methodology**

4 SDOs and standards in the five priority areas

Organisation of the information

In the following tables SDOs are referenced in the first column spanning as much rows as needed to include the individual standards of the respective SDO in the third column. The second column references the topic (field) the standard is designated for (if applicable). The fourth column indicates the state of an individual standard.

Additional information for each standard/standardisation activity will be available through StandICT.eu's Standardisation Watch web pages, showcasing, topics:

SDOs (or similar),	**Standards or specifications**	**Topic**
Description	Description	Description
Reference URL	Reference URL	Reference URL
Related Standards / Topics	Related SDOs / Topics	Related SDOs/Topic
Rule of participation / Engagement	Status (ongoing/ draft / finalized / published)	Use cases / Implementations / Communities
Useful links	Useful links	Useful links

Cells are left empty if information is not applicable or not currently available but will be collected and made available for the StandICT.eu's Standardisation Watch web pages and in the next versions of this document.

5G communications

SDO	**Area**	**Standard**	**Status**
3GPP - Third Generation Partnership Project	Worldwide Mobile Communications Standards	Worldwide Spectrum bands definitions and allocations Releases 15, 16, 17 Release 15: mainly focuses on enhanced mobile broadband (eMBB) and ultra reliable low latency (URLCC) Release 16: complementary use cases, related to industry applications. Release 17: mainly focuses on vertical industry applications and services,	ongoing NSA NR released in December 2017 Functional freeze date including stable protocols: September 2018 http://www.3gpp.org/release-15
		3GPP Specification groups: TSG RAN Radio Access Network	

		TSG SA Service & Systems Aspects TSG CT Core Network & Terminals RAN WG1 Radio Layer 1 spec SA WG1 Services CT WG1 MM/CC/SM (lu) RAN WG2 Radio Layer 2 spec Radio Layer 3 RR spec SA WG2 Architecture CT WG3 Interworking with external networks RAN WG3 lub spec, lur spec, lu spec UTRAN O&M requirements SA WG3 Security CT WG4 MAP/GTP/BCH/SS RAN WG4 Radio Performance Protocol aspects SA WG4 Codec CT WG6 Smart Card Application Aspects RAN WG5 Mobile Terminal Conformance Testing SA WG5 Telecom Management RAN WG6 Legacy RAN radio and protocol SA WG6 Mission-critical applications	
ETSI	NFV ISG	*Network Functions Virtualisation*	ongoing
	OS MANO	*Open Source Management and Network Orchestration*	ongoing
	MEC ISG	*Multi-access edge computing*	ongoing
	CIM ISG	*Context Information Management*	ongoing
ITU-T	AI for Future Networks including 5G	IMT-2020 Technologies & Specifications	Technical reports and specifications for machine learning (ML) for future networks, including interfaces, network architectures, protocols, algorithms and data formats.
ITU-R	Worldwide Spectrum bands definitions and		

	allocations		
	IMT-2020 Evaluation	IMT-2020 Technologies & Specifications	WRC-19 to designate mmWave 5G bands & IMT-2020 Specs by early 2020
CEPT-ECC	European spectrum bands harmonization	IEEE 802.1 series on media access control (MAC)	
IEEE		IEEE 802.3 series on Ethernet	
		IEEE 802.11 series on wireless LAN	
		IEEE 802.15 series on wireless personal area networks	
		IEEE 802.16 broadband wireless access	
		IEEE 802.18 radio regulatory technical advisory	
		IEEE 802.19 wireless coexistence	
		IEEE 802.21 series on media independent handover services	
		IEEE 802.22 series on cognitive wireless RAN medium access control (MAC) and physical layer PHY) specifications	
		IEEE 1900 series on dynamic spectrum access	
		IEEE 1903 series on next generation service overlay network (NGSON)	
		IEEE 1904 series	
		IEEE 1911 series on HDBaseT	
		IEEE 2030 series on the Smart Grid, including electric vehicle infrastructure	
IETF	Internet Engineering Task Force	e.g. ccamp WG on Yang data model	

Cyber Security

SDO	Topic	Standard	Status
CEN European Committee for Standardization	Cybersecurity	ISO/IEC JTC1 CEN and CENELEC also cooperate with respectively the International Organization for Standardization (ISO) and the International Electrotechnical Commission	

		(IEC) to reach agreements on common standards that can be applied throughout the whole world, thereby facilitating international trade.	
CENELEC European Committee for Electrotechnical Standardization		ISO/IEC 27000	several ongoing
ISO/IEC International Organization for Standardization/ International Electrical Commission	IT Security techniques	ISO/IEC CD 30111 Vulnerability handling processes 30.60	ongoing
		ISO/IEC CD 29192-7 Lightweight cryptography -- Part 7: Broadcast authentication protocols 30.60	ongoing
		ISO/IEC CD 29192-6 Lightweight cryptography -- Part 6: Message authentication codes (MACs) 30.20	ongoing
		ISO/IEC 29192-2:2012/PDAM 2 30.60	ongoing
		ISO/IEC 29192-2:2012/PDAM 1 30.60	ongoing
		ISO/IEC CD 29184 Guidelines for online privacy notices and consent 30.20	ongoing
		ISO/IEC DIS 29147 Vulnerability disclosure 40.60	ongoing
		ISO/IEC NP 29115 Entity authentication assurance framework 10.99	ongoing
		ISO/IEC DIS 29101 Privacy architecture framework 40.99	ongoing
		ISO/IEC 29100:2011/PRF Amd 1 Clarifications 50.00	ongoing
		ISO/IEC PRF TS 29003 Identity proofing 50.20	ongoing
		ISO/IEC CD 27552 Enhancement to ISO/IEC 27001 for privacy management -- Requirements 30.20	ongoing
		ISO/IEC AWI 27551 Requirements for attribute-based unlinkable entity authentication 20.00	ongoing
		ISO/IEC CD 27550 Privacy engineering 30.20	ongoing
		ISO/IEC TR 27103 Cybersecurity and ISO and IEC Standards 60.00	ongoing
		ISO/IEC AWI 27102 Information security management guidelines for cyber insurance 20.00	ongoing

		ISO/IEC DIS 27050-2 Electronic discovery -- Part 2: Guidance for governance and management of electronic discovery 40.20	ongoing
		ISO/IEC PRF TS 27034-5-1 Application security -- Part 5-1: Protocols and application security controls data structure -- XML schemas 50.00	ongoing
		ISO/IEC FDIS 27034-7 Information technology -- Application security -- Part 7: Assurance prediction framework 50.00	ongoing
		ISO/IEC FDIS 27034-3 Information technology -- Application security -- Part 3: Application security management process 50.00	ongoing
		ISO/IEC NP 27009 Sector-specific application of ISO/IEC 27001 -- Requirements 10.99	ongoing
		ISO/IEC PDTS 27008 Guidelines for the assessment of information security controls 30.20	ongoing
		ISO/IEC FDIS 27005 Information security risk management 50.00	ongoing
		ISO/IEC CD 24761 Authentication context for biometrics 30.20	ongoing
		ISO/IEC 24760-1:2011/DAmd 1.2 Additional terminology and concepts 40.60	ongoing
		ISO/IEC NP 24745 Biometric information protection 10.99	ongoing
		ISO/IEC AWI TR 22216 Introductory guidance on evaluation for IT security 20.00	ongoing
		ISO/IEC DIS 21878 Security guidelines for design and implementation of virtualized servers 40.20	ongoing
		ISO/IEC NP 20897 Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters 10.99	ongoing
		ISO/IEC DIS 20889 Privacy enhancing data de-identification techniques 40.20	ongoing
		ISO/IEC AWI 20547-4 Information technology -- Big data reference	ongoing

		architecture -- Part 4: Security and privacy fabric 20.00	
		ISO/IEC DIS 20543 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 40.00	ongoing
		ISO/IEC PRF TS 20540 Guidelines for testing cryptographic modules in their operational environment 50.00	ongoing
		ISO/IEC CD 20085-2 Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -- Part 2: Test calibration methods and apparatus 30.20	ongoing
		ISO/IEC CD 20085-1 Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -- Part 1: Test tools and techniques 30.20	ongoing
		ISO/IEC AWI TR 22216 Introductory guidance on evaluation for IT security 20.00	ongoing
		ISO/IEC DIS 21878 Security guidelines for design and implementation of virtualized servers 40.20	ongoing
		ISO/IEC NP 20897 Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters 10.99	ongoing
		ISO/IEC DIS 20889 Privacy enhancing data de-identification techniques 40.20	ongoing
		ISO/IEC AWI 20547-4 Information technology -- Big data reference architecture -- Part 4: Security and privacy fabric 20.00	ongoing
		ISO/IEC DIS 20543 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 40.00	ongoing
		ISO/IEC PRF TS 20540 Guidelines for testing cryptographic modules in their operational environment 50.00	ongoing
		ISO/IEC CD 20085-2 Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -- Part 2: Test	ongoing

		calibration methods and apparatus 30.20	
		ISO/IEC CD 20085-1 Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -- Part 1: Test tools and techniques 30.20	ongoing
		ISO/IEC CD 20009-3 Anonymous entity authentication -- Part 3: Mechanisms based on blind signatures concepts 30.60	ongoing
		ISO/IEC NP 20008-2 Anonymous digital signatures -- Part 2: Mechanisms using a group public key 10.99	ongoing
		ISO/IEC NP 19989-3 Criteria and methodology for security evaluation of biometric systems -- Part 3: Presentation attack detection 10.99	ongoing
		ISO/IEC NP 19989-2 Criteria and methodology for security evaluation of biometric systems -- Part 2: Biometric recognition performance 10.99	ongoing
		ISO/IEC NP 19989-1 Criteria and methodology for security evaluation of biometric systems -- Part 1: Framework 10.99	ongoing
		ISO/IEC NP 19989 Criteria and methodology for security evaluation of biometric systems 10.99	ongoing
		ISO/IEC DIS 19896-3 Competence requirements for information security testers and evaluators -- Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators 40.20	ongoing
		ISO/IEC DIS 19896-2 Competence requirements for information security testers and evaluators -- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers 40.60	ongoing
		ISO/IEC 19896-1 IT security techniques -- Competence requirements for information security testers and evaluators -- Part 1: Introduction, concepts and general requirements 60.00	ongoing
		ISO/IEC PDTS 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	ongoing

		30.00	
		ISO/IEC DIS 19086-4 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy 40.20	ongoing
		ISO/IEC AWI 18045 Methodology for IT security evaluation 20.00	ongoing
		ISO/IEC DIS 18033-6 Information technology security techniques -- Encryption algorithms -- Part 6: Homomorphic encryption 40.20	ongoing
		ISO/IEC 18033-3:2010/PDAM 2 30.60	ongoing
		ISO/IEC 18033-3:2010/DAmd 1 Kuznyechik 40.00	ongoing
		ISO/IEC CD 18032 Prime number generation 30.60	ongoing
		ISO/IEC AWI 15408-5 Evaluation criteria for IT security -- Part 5: Pre-defined packages of security requirements 20.00	ongoing
		ISO/IEC AWI 15408-4 Evaluation criteria for IT security -- Part 4: Framework for the specification of evaluation methods and activities 20.00	ongoing
		ISO/IEC AWI 15408-3 Evaluation criteria for IT security -- Part 3: Security assurance components 20.00	ongoing
		ISO/IEC AWI 15408-2 Evaluation criteria for IT security -- Part 2: Security functional components 20.00	ongoing
		ISO/IEC AWI 15408-1 Evaluation criteria for IT security -- Part 1: Introduction and general model 20.00	ongoing
		ISO/IEC 14888-3:2016/DAmd 1 SM2 digital signature mechanism 40.60	ongoing
		ISO/IEC NP 11770-5 Key management -- Part 5: Group key management 10.99	ongoing
		ISO/IEC 11770-4:2017/NP Amd 1 10.99	ongoing
		ISO/IEC 11770-3:2015/NP Amd 2 10.99	ongoing
		ISO/IEC DIS 11770-2 Key management -- Part 2: Mechanisms using symmetric techniques 40.20	ongoing
		ISO/IEC FDIS 10118-3 Hash-functions -- Part 3: Dedicated hash-functions 50.92	ongoing
		ISO/IEC CD 9798-5 Entity authentication -- Part 5: Mechanisms using zero-	ongoing

		knowledge techniques 30.20	
		ISO/IEC DIS 9798-3 Entity authentication -- Part 3: Mechanisms using digital signature techniques 40.60	ongoing
		ISO/IEC DIS 9798-2 Entity authentication -- Part 2: Mechanisms using authenticated encryption 40.20	ongoing
		ISO/IEC NP 9797-2 Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function 10.99	ongoing
ETSI	CYBER	Mobile/wireless systems, NFV	ongoing
OASIS			
ITU-T			
W3C			
IEEE			
IETF			
3GPP	SA3 5G Security	Studies on 5G security challenges, e.g. URLLC, Cellular IoT security, a.o.	ongoing

Internet of Things

ETSI	SMART M2M	WGs for IoT and large-scale pilots (LSPs) STFs ETSI (SSOs)	ongoing
	Multi-access Edge Computing	MEC ISG	ongoing
	Cross-sector Context Information Management for smart cities applications and beyond.	CIM ISG	ongoing
IEEE	Standard for an Architectural Framework for the Internet of Things	P2413	ongoing
	Standard for Harmonization of Internet of Things (IoT) Devices and Systems	P1451-99	ongoing
GSM Association			
ISO/IEC	ISO/IEC JTC 1/SC 41	Internet of Things and related	ongoing

International Organization for Standardization/ International Electrical Commission		technologies	
	ISO/IEC JTC 1/WG 11	Smart cities	ongoing
CEN			
IETF			
ITU			
3GPP			
OIC			
W3C			
OGC			
AIOTI Alliance for Internet of Things Innovation			

Cloud Computing

The reference for Cloud Computing are the results of the CSC1 activities (organised by ETSI) [3] and three reports resulting from ETSI's CSC2 activities [4][5][6].

IEEE Institute for Electrical and Electronics Engineers	Intercloud interoperability	P2302 Standard for Intercloud Interoperability and Federation (SIIF)	ongoing
ISO/IEC International Organization for Standardization/ International Electrical Commission	Information Security	27017 Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	Draft
		27036-4 Information security for supplier relationships — Part 4: Guidelines for security of cloud services	Draft
	Cloud Service Level Agreements	19086-2 Cloud computing – SLA framework and technology – Part 2: Metrics	Draft
		19086-4 Cloud computing – SLA framework and technology – Part 4: Security and Privacy	ongoing
	Data	23186 Framework of trust for processing of multi-sourced data	ongoing
	Cloud Fundamentals	TR 23188 Edge Computing Landscape	ongoing
		TR 23187 Interacting with Cloud service	ongoing

		partners (CSNs)	
ITU-T ITU Telecommunica-tion Standardi-zation Sector	Cloud Service Model	Y.DaaS-arch Functional architecture of Desktop as a Service	Draft
		Y.CCNaaS-arch Functional architecture of Network as a Service	Draft
	Intercloud	Y.CCIC-arch Functional architecture of inter-cloud computing	Draft
	Management	Y.oe2ecm Overview of e2eCloud Computing Management	Draft
		Y.e2ecslm-Req End-to-end cloud service lifecycle management	Draft
		M.rcsm Requirements for Cloud Service Management	Draft
NIST National Institute of Standards and Technology	Security	SP 500-299 NIST Cloud Computing Security Reference Architecture	Draft
	Cloud Service Level Agreements	SP 500-307 Cloud Computing Service Metrics Description	Draft
	Intercloud	NIST PWG Federated Cloud conceptual Model Sub Group	ongoing
		NIST PWG Federated Cloud Vocabulary Sub Group	ongoing
OGF Open Grid Forum	Service Level Agreement	GFD.192 WS-Agreement	Full Recom-mendation
		GFD.193 WS-Agreement Negotiation	Proposed Recom-mendation
	Cloud Interface Description and APIs	GFD.221 OCCI 1.2 - Open Cloud Computing Interface – Core	Proposed Recom-mendation
		GFD.222 OCCI 1.2 - Open Cloud Computing Interface – Templates Profile	Proposed Recom-mendation
		GFD.223 OCCI 1.2 - Open Cloud Computing Interface – HTTP Protocol	Proposed Recom-mendation
		GFD.224 OCCI 1.2 - Open Cloud Computing Interface – Infrastructure	Proposed Recom-mendation
		GFD.226 OCCI 1.2 Open Cloud Computing Interface – JSON Rendering	Proposed Recom-mendation
		GFD.227	Proposed

		OCCI 1.2 Open Cloud Computing Interface – Platform	Recom-mendation
		GFD.228 OCCI 1.2 Open Cloud Computing Interface – Service Level Agreements	Proposed Recom-mendation
		GFD.229 OCCI 1.2 Open Cloud Computing Interface – Text Rendering	Proposed Recom-mendation
		OCCI 2.0	ongoing
	Data Description	DFDL Data Format Description Language	Proposed Recom-mendation
	Scheduling	DRMAA 2.2	Proposed Recom-mendation
OMG			
IETF			
OASIS			

(Big) data technologies

ISO/IEC International Organization for Standardization/ International Electrical Commission		ISO/IEC JTC 1/WG 9 Big Data	ongoing
		ISO 14721:2012	Primarily geared towards data *archival* but can be repurposed for data curation
ITU-T			
W3C		DCAT-AP	
IEEE			
OASIS			
OGC			

5 Potential gaps

The following sections present gaps in standardisation identified for the 5 priority areas. The report is not aiming to provide a comprehensive list of gaps but to indicate major topics where gaps might be blocking future developments and should be addressed with higher priority.

5G communications

The ITU-T document *FG IMT-2020: Report on Standards Gap Analysis* published in 2016 [16] provides a comprehensive analysis of gaps in standardisation along with links to groups and activities of different SDOs, SSOs, projects and communities that already started working closing the gaps.

The gaps are clustered in the following groups

- High-level Architecture
- Network Softwarization
- End-to-end QoS
- Mobile front haul and back haul
- Emerging Network Technologies

The High-level Architecture group includes 19 gaps where most of them are addressed by different organisations, e.g., ITU-T groups, 3GPP, ISO/IEC JTC1 SC27, IETF.
2 gaps are not linked to related work yet: **Signalling to reduce end-to-end complexity**, **OAM protocols**.

The Network Softwarization group includes 21 gaps where most of them are already addressed by different organisations, e.g., ITU-T groups, 3GPP, ETSI, IEEE, TMF, OpenStack, OpenDayLight, CloudDtack, IETF, IRTF.
3 gaps are not linked to related work yet: **End-to-end reference model for scalable operation**, **Coordinated APIs**, **Energy management aspects of network softwarization**.

The end-to-end QoS group includes 9 gaps which are all addressed by different organisations, e.g., ITU-T groups, 3GPP.

The Mobile front haul and back haul group includes 21 gaps which are all addressed by different organisations, e.g., ITU-T groups, IEEE.

The Emerging Network Technologies group includes 15 gaps where all but one are addressed by different organisations, e.g., ITU-R, ITU-T, IETF, IRTF, 3GPP, Openflow.
1 gap is not not linked to related work yet: **Security (encryption)**.

The IETF document *Gap Analysis for Network Slicing* published in 2017 [18] describes requirements regarding network slicing and ongoing related activities in IETF working on standards addressing these requirements. The document concludes with the list of still open gaps for the 6 requirements (see Table 1 for details). There is no significant overlap with the gaps identified in the ITU-T analysis.

Table 1: **Network slicing gaps**

Requirements	**Gaps**
Network Slicing Resource Specification	1) A detailed specification of NSRS; 2) A companion YANG data model for NSRS; 3) Mechanisms/protocols for capability exposure; 4) Mechanism/protocols for NS state monitoring;
Cross-Network Segment and Cross-Domain	5) Mechanisms for secure cross-network segment and cross-

Negotiation	domain negotiation/inter-operation; 6) Information model for network slicing related message exchange; 7) Mechanisms/protocols for E2E NS composition/decomposition;
Guaranteed Slice Performance and Isolation	8) Mechanisms for on-demand, isolated, elastic and efficient network slice instantiation and resource association;
Network Slicing-Domain Abstraction	9) Common representation mechanism for network slices across multi-domain; 10) Mechanisms for customized network slices;
Slice Identification	11) Mechanisms and framework for network slice identification; 12) Mechanisms for dynamic discovery of instantiated network slices; 13) Mechanisms for network slicing E2E repository;
OAM Operation with Customised Granularity	14) Mechanisms for dynamic discovery of service with function instances and their capabilities; 15) Mechanisms for customised network slices OAM when overlay techniques are not in use.

The document of the 5G PPP [17] *Euro-5g – Supporting the European 5G Initiative* is a report from the standardisation activities associated with the 5G PPP phase 1 projects. It identifies relevant standardisation and regulatory bodies and describes the associated submissions and impact from the 5G PPP projects. The report describes work of these bodies related to many of the gaps identified in the two reports discussed above.

Moreover, the 5G-IA Pre-Standardization WG is working with phase 2 and phase 3 projects of the 5G PPP along with 3GPP specialists to identify gaps for 3GPP Release 17. Much of this work is aligned with EU priority topics, with EC representatives also actively involved in the WG. Trust-IT works closely with both groups. Moreover, the 5G-IA is part of an upcoming Task Force with 3GPP TSG Chairs and vertical industry associations to also pinpoint standardization priorities.

Gaps identified so far include:

- Adding new features incrementally with New Radio (NR) covering all relevant use cases that are commercially viable, e.g. drones and public safety.
- Enhanced NR unlicensed: essential features, with integrated access and backhauling.
- Massive Multiple Input Multiple output (MIMO): increase efficiency in real operations.
- Industrial Internet of Things (IIoT) and URLLC: build on Releases 15 and 16, with IEEE integration and adding missing features (e.g. massive machine type communications, mMTC for terminal energy efficiency).
- NB-IoT and LTE-M: sensor networks and public safety (sidelink, broadcasting, drones, mobile IAB nodes.
- Achieving very low latency and QoS for industrial applications, such as audio-visual media (there are 2 types of broadcast considered; one for media content and one for public safety), critical medical applications.
- Sidelink: network-controlled devices, gaming, media, logistics.

- Current Study Item on relays: indoors, important for blindspots; higher bit rates, lower latency, factories and interconnected devices.
- Continued advancement of non-terrestrial networks, with many 3GPP inputs coming from 5G PPP phase 2 project, SAT5G.

The peer 5G PPP CSA, Global5G.org (Coordinator: Trust-IT) is currently working on an updated 5G standardisation report (May 2019). A restricted report has also been produced by the above-mentioned Task Force on the outcomes of the Vertical User Workshop organised by EU-based market representation partners of 3GPP (February 2019).

Cyber Security

Cyber Security plays a crucial role in many domains, i.e. it is often handled as part of security concepts and realisations inside a specific domain. For example, aspects of and approaches to Cyber Security can be found in the other four priority domains IoT, Cloud Computing, Big Data, and 5G. Some of the standardisation gaps identified for these domains as presented in this section are related to Cyber Security. However, standards organisations have dedicated committees and groups that address specifically Cyber Security, e.g., the ESO ETSI TC Cyber and ISO/IEC JTC1 SC27. Moreover, ENISA (European Union Agency for Network and Information Security) [19] is a dedicated centre of expertise for cyber security in Europe. ENISA has published two reports which comprise the most recent standards gaps analysis in two relevant areas of Cyber Security: *Gaps in NIS standardisation* published 2016 [20] focussing on Network Information Security, and *Guidance and gaps analysis for European standardisation* published 2018 [21] focussing on Privacy standards in the information security context.

The report *Gaps in NIS standardisation* providing a high-level analysis of consequences for standardisation of network information security (NIS) taking into account *The Directive on security of network and information systems (NIS Directive)* entered into force in August 2016 [22]. The gaps identified are rather on a policy level or on the level of required activities of the member states than on the level of concrete standards or suggestions in which standardisation activity to engage. The report provides a rather comprehensive list of bodies and their corresponding groups and activities involved in global cyber security standards (see Table 2). With respect to the feasibility of determining standardisation gaps the report states “An immediate consequence of the diversity of the current standardisation ecosystem, and because of the extremely rapid pace of change, is that it is increasingly difficult to authoritatively determine if gaps in standardization or in capability exist.”.

Table 2: **Significant Cyber Security Standards fora [20]**

3GPP	CCRA	ETSI ISI	IIC	OAA	Plattform Industrie 4.0
3GPP SA2	CEN	ETSI LI	Influx DB	OASIS	RIOT
3GPP SA3	CENELEC	ETSI MTS-SIG	IO-Link	OASIS CTI	ROS
3GPP SA5	CEPOL	ETSI NFV	IoT Security Foundation	ODVA	SAE International
3GPP CT	CERT-EU	ETSI NTECH	IoTivity	OGC	SensiNact
ACDC	CIA	ETSI SAGE	IPEN	OIC-CERT	SGIP
ACEA	CIIAII	FIDO Alliance	IPSO	OM2M	Sofia2
AEF	CIS	FIRST	ISA	OMA	TCG

AIOTI	CLEPA	Fi-ware	ISF	OMG	The KNX Association
AllJoyn	Contiki	GlobalPlatform	ISO	OneM2M	The Open Group
Allseen Alliance	Continua: Health Alliance	GSMA	ISO JTC1/SC27	ONOS	The ULE Alliance
Apache Spark	CSA	GSMA FASG	ISO JTC1/SC6	OPC Foundation	The ZigBee Alliance
APCERT	CSC	H2020	ISO JTC1/SC7	Open Connectivity Forum	ThingSpeak
Arduino	CSCG	HGI	ITU ITU-D	OpenDaylight	Thread group
ASHRAE	DICOM	HL7 International	ITU ITU-R	openHAB	TMForum
Automation ML	easyway	HYPER/CAT	ITU ITU-T	OpenIoT	UDG Alliance
AVNU	eCl@ss	ICANN	ITU	OpenRemote	UniverSaal
BEREC	EclipseIoT	IEC	LinuxIoTDM	OpenStack	UPnP
Bluetooth	ECRG	IEEE	LoRa Alliance	OpenWSN	W3C
Broadband Forum	ENISA	IEEE 802 LAN/MAN Standards Committee	MITRE	OPFNV	Weightless
C2C-CC	EnOcean Alliance	IEEE P2413	Mosquitto	OSCE	Wi-Fi Alliance
CA/B Forum	ERTICO - ITS Europe	IETF	NATO	OSGi Alliance	WWRF
Cable Labs	ETSI	IETF IRTF	NATO CCDCOE	OWASP	
Calypso	ETSI CYBER	IETF MILE	NATO LIBGUIDE	Paho	
CCC	ETSI E2NA	IETF SACM	NIST	Particle	
CC-Link	ETSI ESI	IHE	Node-RED	PI International	

It should be noted that Table 2 above both includes entries on an organisational level, e.g., ETSI, CEN or OpenStack, and entries on a (technical) committee or working group level, e.g., ETSI MTS-SIG, OASIS CTI or ISO JTC1/SC27. A more complete list of bodies with brief descriptions is maintained by ETSI in *ETSI TR 103 306 Cyber; Global Cyber Security Ecosystem* [25]. The most recent version was published in 2017.

The report *Guidance and gaps analysis for European standardisation* provides a gap analysis and mapping of standards to the ISO/IEC 29100 Privacy Principles. The analysis is structured along the following 11 principles and focuses on international standards activities in ISO/IEC and European

standardisation activities in ESOs only. No gap without any standardisation activity was identified where European experts could start a new activity, working group or study group. However, a large number of ongoing activities in ISO/IEC or the ESOs would allow contributions from European experts.

- Principle #1: **Consent and choice**
- Principle #2: **Purpose legitimacy & specification**
- Principle #3: **Collection limitation**
- Principle #4: **Data minimisation**
- Principle #5: **Use, retention, and disclosure limitation**
- Principle #6: Accuracy & quality
- Principle #7: **Openness, transparency & notice**
- Principle #8: **Individual participation & access**
- Principle #9: **Accountability**
- Principle #10: **Information security**
- Principle #11: **Privacy compliance**

The principles with ongoing activities or standards in draft versions are typeset in bold.

Internet of Things

The ad hoc group 3 (AHG3) of ISO/IEC JTC 1/SWG 5 in 2014 undertook the task of identifying gaps in the area of IoT. The approach was trying to collect information about existing standards based on a template distributed to request information from as many standards groups as possible. In this process they collected over 400 standards. However, “AHG3’s feeling that this data was incomplete, a means to identify the gaps in the standards world was problematic.” [12]. Similar to Cloud Computing many standards used in the IoT domain have not been explicitly developed for IoT but for other domains, like Networking or Distributed Computing.

There are two recent reports on standardisation gaps in the IoT area: one from AIOTI (Alliance for Internet of Things Innovation) and one from ENISA.

The most recent report focused on gaps regarding IoT security standards has been produced and published by ENISA in 2018 [13]. The AIOTI report from 2018 in covers standardisation gaps of more aspects of IoT than security [14].

The ENISA report maps requirements to the standards development activities of SDOs and concludes “there is a gap in standards only insofar as it is unclear what combination of standards, when applied to a product, service or system, will result in a recognizably secure IoT. The proposal presented below [in the report] is to develop a process that alongside some certification marking on IoT products and services, that gives assurance to the market that the IoT product is as secure as can be reasonably expected.”.

The AIOTI report identifies 49 gaps, roughly half of them in the areas **Security and privacy**, **Connectivity**, **Data interoperability**, **Service platform**, **Devices and sensors**, and **Interoperable processing rules**. Additional topics considreded relevant are **(System) Safety** and **Health of Edge Computers**.
From the total number of gaps those that have been considered critical are sorted according to the domain they belong to and listed below:

Table 3: **Critical gaps per domain**

Domain	Gaps

IoT Architecture	• Multiplicity of IoT High Level Architectures (HLAs), platforms and discovery mechanisms
Service and Application	• Data interoperability: lack of easy translation mechanisms between different specific models. Need of a global and neutral data model. Seamless inter-working between data systems • Interoperable processing rules: lack of definition for advanced analysis and processing of sensor events and data to interpret the sensor data in an identical manner across heterogeneous platforms • Specific solutions at Service Layer to enable communications between the platforms (e.g., plugins to oneM2M platform)
Applications Management	• Usability (Societal gap)
Deployment	• Safety
Business	• Lack of a reference for business cases and value chain model to guide choices for deployment • Lack of knowledge about potentialities of IoT among decision makers, users

Additionally, the report presents the assessment of the CREATE-IoT project on Large-Scale Pilots perceived major gaps. The following table shows the gaps identified with criticality high:

Table 4: **Critical gaps (Large-Scale Pilots)**

Nature of the gap	Type	Criticality
Standards to interpret the sensor data in an identical manner across heterogeneous platforms	Technical	High
Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms	Technical	High
Easy accessibility and usage to a large non-technical public	Societal	High

Cloud Computing

The CSC2 project of ETSI has identified a number of standardisation gaps in its report *Cloud Computing Standards Maturity Assessment* [4] published end of 2015. Most of these gaps are still open. The list below contains those considered most relevant to be addressed.

During the acquisition phase **Risk Assessment** is critical for both the customer and the provider to make a well-grounded decision. Also, there is no standard for **Requirements specification** which would make it easier for the customer to compare providers based on their offers. And there is no standard for **Negotiation for multiple providers** which would support users creating multi cloud environments.

During the operation of Cloud services a number of critical gaps have been identified: there is no Cloud specific standard for **Administration of users, identities and authorizations**, there is no standard for **Responding to SLA infringements,** standards for **Monitoring Availability** (including performance monitoring for the different properties of a system, like, storage, processing, networking) are missing, both in terms of providing/retrieving the information and format/structure of the monitoring information, a standard for Cloud Computing specific **Monitoring Incident management** is missing, and there is no standard for **Preventative response to SLA infringement**. All of these standards are of increased importance in user driven multi cloud environments or federation resources of multiple clouds initiated by a provider.

Finally, in the phase of termination of a Cloud service a standard for **Providing an evaluation report** is missing. Filling this gap is – as for many of the previously mentioned gaps – essential to automate the Cloud provisioning process and the corresponding Cloud negotiation and usage.

(Big) data technologies

For an analysis of standardisation gaps in the area of Big Data two reports are considered: The report of ISO/IEC JTC1 *Big data - Preliminary Report 2014* [23] published in 2015 and the report of ITU-T *Y.3600 – Big data standardization roadmap* published in 2016.

The ISO/IEC JTC1 report provides a survey of the existing ICT landscape for key technologies and relevant standards/models/studies/use cases and scenarios for Big Data from JTC 1, ISO, IEC and other standard setting organizations, like ITU-T, W3C, OASIS, TM-Forum. The report also assesses the current status of Big Data standardization and identifies standards gaps, and proposes standardization priorities to serve as a basis for future JTC 1 work. One outcome of the report was the creation of WG9 for Big Data related standardisation activities. WG9 has been discontinued and its activities are continued in ISO/IEC JTC1 SC42 Artificial Intelligence.

The report describes both broad areas and specific areas of potential gaps in Big Data standardisation and maps the latter onto existing JTC1 SCs.

The broad areas are

1) Big Data use cases, definitions, vocabulary and reference architectures (e.g. system, data, platforms, online/offline, etc.);
2) Specifications and standardization of metadata including data provenance;
3) Application models (e.g. batch, streaming, etc.);
4) Query languages including non-relational queries to support diverse data types (XML, RDF, JSON, multimedia, etc.) and Big Data operations (e.g. matrix operations);
5) Domain-specific languages;
6) Semantics of eventual consistency;
7) General and domain specific ontologies and taxonomies for describing data semantics including interoperation between ontologies;
8) Big Data security and privacy access controls;
9) Remote, distributed, and federated analytics (taking the analytics to the data) including data and processing resource discovery and data mining;
10) Data sharing and exchange;
11) Data storage, e.g. memory storage system, distributed file system, data warehouse, etc.;
12) Human consumption of the results of big data analysis (e.g. visualization);
13) Energy measurement for Big Data;
14) Interface between relational (SQL) and non-relational (NoSQL) data stores;
15) Big Data Quality and Veracity description and management;

Area 1) related standardisation activities are performed ISO/IEC and ITU-T (see Table 6). In ITU-T most standards are under development. In ISO/IEC SC42, three standards have already been published, two more are under development: TR 20547-1 Big data reference architecture -- Part 1: Framework and application process, 20547-3 Big data reference architecture -- Part 3: Reference architecture. Areas 2) and 4) are not addressed by ISO/IEC activities but several standards have been developed by W3C and OASIS (see Table 6). Other areas are not yet addressed by Big Data standardisation activities or addressed in other existing JTC1 SCs (see Table 5).

The more specific areas which – at the time of the report – were expected to be handled by JTC1 are

1) Definition and vocabulary of Big Data
2) Big Data Reference Architecture

Both areas are now addressed with corresponding activities in SC42 WG2 after initial work started in JTC1 WG9.

The report also provides a mapping between standard gaps identified in this report and existing JTC 1 SCs as shown in Table 5.

Table 5: **Mapping between standard gaps identified and existing JTC1 SCs**

SC No	The title of SCs	Current scope and activities relevant to Big Data	Suggestions for future lines of investigation
SC6	Telecommunication and information exchange between systems	Networking technologies	• Standards and protocols for efficient transfer of Big Data
SC22	Programming Languages	Potential new language for Big Data applications	• Domain-specific languages
SC24	Computer graphics, imaging processing, and environmental data representation	Potential new methods of presenting data	• Visualization in Big Data analytics
SC27	IT Security techniques	Big Data creates a large number of Security and privacy issues	• Metadata and provenance standards
SC32	Data management and interchange	Database languages and systems related to Big Data	• Definition of standard interfaces (e.g. language, API) to support non-relational datastores • Definition of SQL extension to support exchange and integration between SQL and non-SQL datastores • Metadata and provenance standards • SQL and NoSQL standards for data mining • Support for large complex data structures in SQL and/or SQL/MM • Support for operations on complex data structures and defined

			operations on such structures (e.g. add, multiply union) • Standards for eventual consistency and acceptable consistency • Support for massive parallelism • Definition and registration of application and processing models • Representation of Big Data Veracity and Quality description and management attributes
SC34	Document description and processing languages	A large number of the descriptions and processing languages supported by SC 34 are leveraged in Big Data systems and architectures	• Scalability of these languages and implementations • General and domain specific ontologies. Taxonomies for describing data semantics including ontology interoperation
SC38	Distributed application platforms and services (DAPS)	SOA, Web Services, Cloud Computing	• Standards for horizontal scalability • Security, privacy and access controls for distributed file systems • Standards for data replication and distribution • Standards for identification and access to distributed object stores; APIs to access data and attributes
SC39	Sustainability for and by Information	Resource efficient data centre and green	• Measurement for energy cost of Big

	Technology	ICT	Data

The ITU-T Report *Y.3600 – Big data standardization roadmap* provides the standardisation roadmap for big data in the telecommunication sector. It describes the landscape and conceptual ecosystem of big data from an ITU-T perspective, related technical areas, activities in standards development organizations (SDOs) and gap analysis. The Big Data activities of SDOs largely overlap with the similar description in the JTC1 report, thus the standardisation environment has been stable from the period of the two reports until the analysis of Big Data standardisation activities StandICT.eu (see Section 4 in this deliverable. The report presents a matrix of Big Data standardization with two axes. The horizontal axis describes document categories which cover the subject of applications as follows:

- **General, definition**: the standard which provides general descriptions or terms and definitions of the technology;
- **Common requirements, use cases**: the standard which provides use cases and derived general/functional requirements;
- **Architecture**: the standard which provides reference architecture;
- **API, interface, profile**: the standard which provides common interface, API and/or its profile;
- **Data model, format, schema**: the standard which provides data model or protocol including scheme and/or its encoding format;
- **Others** e.g., guidelines, technical reports.

The vertical axis describes the related technologies for supporting big data as follows:

- **Fundamental**: concept of big data and its applications;
- **Data exchange**: for supporting big data publishing, sharing, transaction, etc.;
- **Data integration**: with heterogeneous data sources;
- **Analysis/visualization**: for mining model description, etc.;
- **Data provenance/metadata**: for data quality, history tracking, data management, etc.;
- **Security/privacy**: for big data, especially personal identification information;
- **Other**: big data related technologies which are not described above.

Table 6: **Standardization matrix of Big Data**

	General, definition	Common requirements, use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental	**ITU-T Y.3600** ISO/IEC 20546 **ISO/IEC 20547-1**	**ITU-T Y.3600**	**ITU-T Y.BDaaS-arch** **ISO/IEC 20547-3**			
Data exchange	**ITU-T Y.BigDataEX-reqts**	**ITU-T Y.BigDataEX-reqts**			OASIS AMQP 1.0 OASIS MQTT 3.1.1	
Data					W3C DCAT	

integration					W3C JSON-LD 1.0 **W3C JSON-LD 1.1** W3C LDP 1.0 W3C RDF 1.1 W3C OO	
Analysis/ visualization					DMG PMML 4.3	TMF BDAG R16.5.1
Data provenance/ metadata	**ITU-T Y.bdp-reats**	**ITU-T Y.bdp-reats**			W3C MVTD W3C MTDMW	
Security/ privacy	ITU-T X.1601 ISO/IEC 27000 IEO/IEC 29100	**ISO/IEC 20547-4**			ISO/IEC 27002 ISO/IEC 27018	**ITU-T X.CSC DataSec** ISO/IEC 27001
Other	**ITU-T Y.bDPI-Mec** **ITU-T Y.bDDN-fr**	**ITU-T Y.IoT-BigData-reqts** **ITU-T Y.dsf-reqts** **ITU-T Y.bDDN- req** ISO/IEC 20547-2	**ITU-T Y.SDN-ARCH**			ISO/IEC 19944 ISO/IEC 20547-5

Empty cells indicate potential gaps and standards typeset in bold depict work in progress.

6 EU priorities

The following sections provide suggestions for EU priorities derived from identification of potential gaps in Section 5. The priorities defined in EC documents including the Rolling Plan for ICT standardisation have been presented in Section 2. Suggestions could be useful, e.g., for existing projects like StandICT.eu or the ELITE-S project [15], or for similar follow-up projects.

5G communications

The 5G standardisation domain is as broad and diverse as the technology itself. On a European level contribution to the ESO ETSI's 5G-related TCs and ISGs on NFV, MEC and OS MANO (whose activities are kind of international at the same time through its participants) is considered beneficial. Moreover, on a European level we see a major role of 5G PPP and its various working groups contributing to filling the gaps in standardisation and through the on-going work of Global5G.org and synchronisation with the 5G-IA, industrial associations, 3GPP and ETSI. On an international level we consider 3GPP as a major player with standardisation in constant evolution, alongside the participation of 5G PPP projects and EU-based market partners, such as 5G Automotive Association; EMEA Satellite Operations Association (ESOA), 5G Alliance for Connected Industries and Automation

(5G-ACIA) and Public Safety Communications Europe (PSCE). The upcoming Task Force bringing together these key players is expected to further boost EU contributions to the 5G standards landscape,

Other key players ITU-T, IETF and IEEE as the dominant players where 5G standardisation is developed. ITU-T and IETF both delivered a standards gap analysis and have identified existing or established new working groups to close some of the standardisation gaps. IETF has the most open approach for contributors, followed by IEEE. ITU-T has the highest barrier in terms of fees. However, individuals from organisations that are already ITU-T members could easily contribute in, e.g., study groups or focus groups, as expert funded by StandICT.eu or by the ELITE-S project [15].

The upcoming report from Global5G.org[3] will capture EU contributions to 5G standardisation with a focus on vertical industries and partnerships. Interaction with industry and public safety associations will also help pinpoint priority regulatory issues and new approaches to the procurement of Public Protection and Disaster Relief (PPDR), as fostered by H2020 Project, Broadway, which is aimed at enabling a pan-EU broadband mobile system for public safety and is also part of PSCE[4],

Cyber Security

On the one hand, as stated in the corresponding sub-section of Potential gaps in Section 5, the Cyber Security standardisation landscape is wide and heterogeneous, which makes it rather difficult to identify individual activities beneficial from a European perspective. On the other hand, a number of EC communications and finally the *Directive on security of network and information systems (NIS Directive)* can be considered as foundational and high-level definition of the framework for standardisation requirements. Moreover, the ENISA report *Guidance and gaps analysis for European standardisation* provides concrete opportunities in which standardisation activities of ISO/IEC and the ESOs European experts could engage. While many security standards are not specific for regions or countries privacy and data protection still is. European experts should contribute defining privacy and data protection standards that implement the relevant European privacy and data protection legislation.

Internet of Things

The AIOTI report [14] suggest a number of domains, where standards are lacking. An important field for putting more European effort seems to be the domain of IoT Architecture, where globally still a multiplicity of IoT HLSs, platforms and discovery mechanisms exist. One approach could be to port the M2M developments of ETSI to standardisation activities of an international SDO. Moreover, Data interoperability (which partly overlap with activities in the (Big) Data domain) needs to be addressed on an international level. In contrast, standards for Usability could be prepared on a European level first (as many IoT applications have a certain locality) and brought forward to international standardisation in a second phase. As the AIOTI report states, Safety standards are already available for a long time in different, non-IoT fields. A study group established in an international SDO, e.g. in ISO/IEC JTC1 SC41 could investigate existing approaches and put forward a new working group that exploits the outcome of the study group to define international standards around Safety of IoT.

Cloud Computing

Cloud Service Level Agreements are still considered as essential for improving customer experience. Although, in ISO/IEC JTC1 SC38 WP3 four standards already have been published

- 19086-1 Service level agreement (SLA) framework -- Part 1: Overview and concepts.
- 19086-2 Service level agreement (SLA) framework -- Part 2: Metric model.
- 19086-3 Service level agreement (SLA) framework -- Part 3: Core conformance requirements.

[3] https://www.global5g.org/
[4] https://www.broadway-info.eu/.

- 19086-4 Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII.

there are still gaps to be addressed regarding SLA infringement and – more important – SLA metrics. Both high-level metrics suitable for the end-users' to express their demands, and low-level metrics to map the high-level metrics to requirements the service provider has to fulfil to satisfy the users' demands. Another report is under development: *ISO/IEC NP TR 23951 Cloud computing -- Best practices for cloud SLA metrics*, but its focus will be too narrow to be the base for one or multiple standards for the kind of SLA metrics mentioned before.

Standards for accessing monitoring data and standards for format and contents of these data is of equal importance, e.g. to allow the customer to evaluate its SLA while Cloud resources are used.

Cloud-specific standards for Administration of users, identities and authorizations would help closing the gap between stable and generally used developments from the domain of distributed computing, e.g. Grid Computing.

Considering the published and ongoing Cloud Computing-related standardisation work and the still existing gaps there is plenty of opportunities for European experts to create new study and working groups addressing these gaps.

(Big) data technologies

Big Data has been addressed in several standards bodies for years already, with a number of standards (including such of ISO/IEC) already published. With the increasing importance and ubiquity of a new generation of Artificial Intelligence requiring and using huge amounts of data for training, Big Data standardisation has gained momentum also. As described in the subsection for Big Data and potential gaps in Section 5 above there is a large number of standardisation activities. However, the activities are not scattered across many standardisation bodies but concentrated on less than 10 bodies, both SDOs and SSOs.

As can be seen from the list of broad areas (from the JTC1 report), the mapping of gaps to existing SCs for potentially addressing these gaps (as presented in Table 5) and the ongoing standardisation work and gaps presented in Table 6, there are many opportunities for contributions of European experts.

Since there are no standardisation activities regarding **API, interface, profile** experts should focus on these to increase usability and interoperability. This work should be done in SSOs or Open Source Software (OSS) Communities which have lower barriers for contribution and especially OSS Communities usually have faster development cycles. Once mature standards are available these could be contributed for publishing as an international standard if considered beneficial.

Despite its importance for Data interoperable data sharing and usage **Data integration** also has limited activities and should be addressed by experts with higher priority.

7 Prioritised list for the 1st call

For the prioritised list of topics for the first call StandICT.eu used two major sources: the outcome of the face-to-face meeting of the EAG and the 2018 version of the Rolling Plan for ICT standardisation [8]. While the EAG was focussing on the 5 priority domains as outlined in the EC's Communication: ICT Standardisation Priorities for the Digital Single Market [2] the Rolling Plan takes a broader approach along the four themes Key Enablers and Security, Societal Challenges, Innovation for the Digital Single Market, and Sustainable Growth with the 5 priority domains included in Key Enablers and Security.

The StandICT's Expert Advisory Group (EAG) had its initial face-to-face meeting February 28 organised to discuss and prioritise the list of SDOs and standards which was a result of Task 2.1 – Global ICT standardisation watch (the complete list as of March 7, 2018 has been presented in Section 4 above).

The prioritised list presented in the Annex (13) includes elements from all five areas. However, as explained below, it does not pick elements from the working document presented in Section 4, where Task 2.1 tries to cover all relevant SDOs and their ongoing standards activities.

During this meeting EAG and partners of the project discussed the different options for experts to contribute to standardisation in the five areas. The participants agreed not to narrow the call to individual standards that are currently under development (as described for the five areas above) but to launch the calls with broader scope. Several reasons have been identified for this approach:

For many standards, e.g. in the 5G area, companies are involved in the development with a large number of employees and a contribution from a single expert supported by StandICT.eu would presumably have limited impact.

Many standards of the initial list above are developed in SDOs that either require contributors to (i) pay a membership fee or to (ii) come from an organisation that has a liaison agreement with the SDO. (iii) exceeds the budget StandICT.eu has for experts and (iv) turned out to be difficult to achieve for a 2-years project when the project approached SDOs with the intention to create a liaison.

The project partners and the EAG decided not to structure the prioritised list along SDOs and standards (as done for the full list that will be the base for the StandICT.eu standardisation watch) as this would be too fine grained and put too much constraints on applicants.

The project partners and the EAG further agreed that the less specific the call is (referring to individual ongoing standardisation activities) the more applicants the project will have in response to the call.

Furthermore, the list should be prepared in a way that allows the applicant to propose new activities with impact.

The calls should not prescribe SDOs for standardisation activities but leave it to the applicants to select the right committee for their contributions.

The initial full list of relevant SDOs and standards includes a number of gaps, which are not yet addressed by standardisation activities. These are included in the prioritised list as emerging technologies.

In particular, Blockchain has been identified as emerging technology is now included in the list of topics from the actual Rolling Plan as prepared by the Multi Stakeholder Platform. Besides the overlapping topics in Key Enablers and Security the list includes a number of verticals and application areas relevant for the DSM.

Key Enablers and Security

1. 5G
2. Cloud computing
3. Public sector information, open data and big data
4. Internet of Things
5. Cybersecurity / Network and Information Security
6. Electronic identification and trust services including e-signatures
7. e-Privacy
8. E-infrastructures for research data and computing-intensive science
9. Broadband Infrastructure Mapping
10. Accessibility of ICT products and services

Societal Challenges

11. eHealth, healthy living and ageing
12. e-Skills and e-Learning
13. Emergency communications
14. eGovernment
15. eCall

Innovation for the Digital Single Market

16. e-Procurement — Pre and Post award

17. e-Invoicing
18. Card, internet and mobile payments
19. Preservation of digital cinema
20. Fintech and Regtech Standardisation
21. Blockchain and Distributed Digital Ledger Technologies

Sustainable Growth

22. Smart grids and smart metering
23. Smart cities / technologies and services for smart and efficient energy use
24. ICT environmental impact
25. European Electronic Toll Service (EETS)
26. Intelligent transport systems (ITS)
27. Advanced manufacturing
28. Robotics and autonomous systems
29. Construction — building information modelling
30. Common Information Sharing Environment (CISE) for the EU maritime domain

The first call was open for all 30 topics identified by the MSP. For the subsequent calls StandICT.eu will analyse the outcome of the first call together with the EAG to prepare topic lists that aim at achieving a broad coverage of the MSP's topics. The approach is described in the following section.

8 Call priorities

Given the rapidly-evolving nature of the standardisation landscape in the 5 ICT priority domains, the increasing number of SDOs and SSOs and the diversity of technical committees involved in the standards setting landscape that the project is targeting, StandICT.eu commits to put in place a continuous Open Call process, dynamic and inclusive, covering diverse activities and potential types of contributions. The Open Call is launched in Month 3 of the project with publication of the first call objectives and will close in Month 23, with publication of the last batch of funded proposals. A total of 10 cycles of proposal funding will be completed as part of the StandICT.eu Open Call. For every of the 10 cycles, the 7-step process of Figure 3 will be applied. Each cycle after the 1st one will start immediately after completion of the previous 60-day call for proposal, in parallel with starting the evaluation phase of the current cycle. In this way, a compact series of 10 cycles will be possible.

For the first call, all areas will be covered evenly as the topics addressed in the call follow the prioritised list of the 2018 Rolling Plan presented in Section 5 above.

Priorities and content of the subsequent calls that will be launched every two months will be defined according to

- Applications for grants resulting from the previous call(s), e.g., coverage of the areas, KPIs of the project related to the calls
- Results of the proposals granted (as available at a later point in time depending on the nature of the proposal)
- New fields for standardisation emerging, e.g., by SDOs, (OSS) communities, policy makers, etc.
- The 2019 version of the Rolling Plan for ICT Standardisation
- Contributions from the StandICT.eu EAG and synergies with key stakeholders (SDOs, SSOs, PPPs, relevant R&D projects etc.)

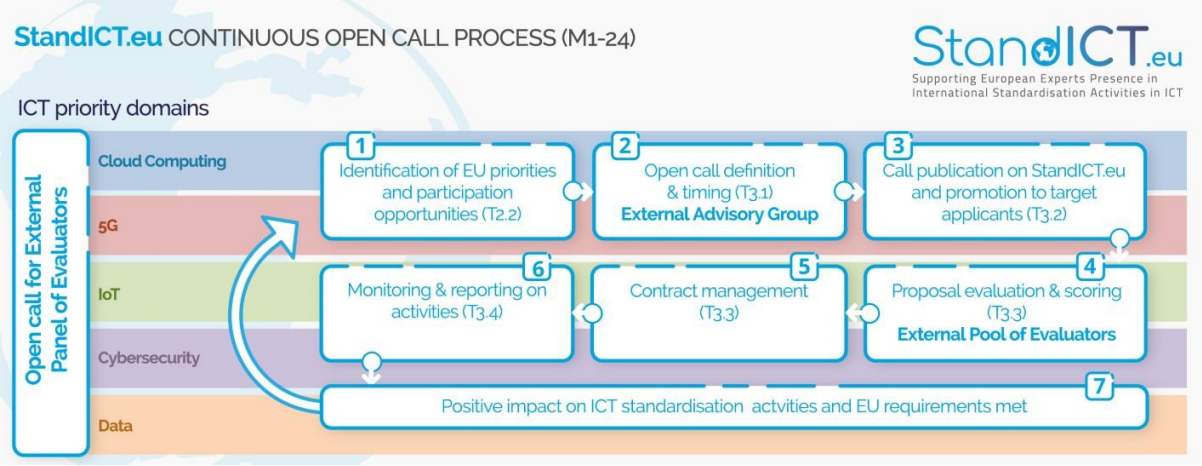


Figure 3: **Continuous Open Call process**

•

9 Role of communities and Open Source Software

Communities organised around specific aspects of the five priority areas play an important role for the development of specifications, software frameworks, reference implementations, complementing or accompanying standards developments or supporting standards-like developments. A large amount of these communities' outcomes is in the domain of Open Source Software (OSS) and as such much easier to get access to and use it than, e.g. standards from a Standards Setting Organisation like ISO where many are only available for purchase. The most benefit for potential users of standards arises when OSS communities and SDO start cooperating.

One example in the 5G area is the Open Source Open Platform for NFV (OPNFV) initiative, led by the Linux Foundation, which was launched on the 30th September 2014 with the participation of several IT and telecom vendors and telecommunications service providers. The objective of OPNFV is to provide a reference infrastructure platform for Network Functions Virtualization (NFV). Therefore, large parts of the OPNFV architecture are directly related to the architecture outlined in the documents provided by ETSI ISG NFV. To start with, OPNFV addresses an integrated solution for NFVI and VIM components of the ETSI NFV architecture that together build the infrastructure layer of the NFV framework.

Open Source MANO (OSM) is a collaborative open source project hosted by ETSI to develop an NFV Management and Orchestration stack aligned with ETSI NFV Information Models and APIs[5]. This complements the work of ETSI NFV and vice versa. This collaboration provides an opportunity to capitalise on the synergy between standardization and open source approaches and enables a bi-directional feedback loop while maximizing innovation and efficiency. Ten 5G PPP phase 2 projects contribute to OSM Releases and implement features relevant to their specific needs. The upcoming Global5G.org report (May 2019) will cover contributions and benefits to date.

One important outcome of StandICT.eu is contributing to the improvement of the relation between open source and standards. The EAG and the project partners agree that this can be done by explicitly addressing APIs in the open calls as APIs are in the focus of OSS and standardisation.

[5] https://osm.etsi.org/.

The relevance of APIs is different in the five areas as is the degree of impact open source has in the five areas, e.g. less in Cyber Security than in Cloud. With the experience of the first calls the project will fine-tune later calls regarding OSS and APIs.

10 Relation to StandICT.eu Standardisation Watch

The project partners have longstanding experience in standardisation and a good pre-existing network of contacts to SDOs and SSOs. The project has built on these assets for creating the initial list of relevant SDOs and their standardisation activities in the 5 priority areas and will further refine this list with experts identified inside Fraunhofer, experts from completed and active projects in the priority areas and experts from industry. Through Trust-IT's participation in 5G PPP, STANDICT.eu has direct access to updates and priority areas for 5G standardisation. Rational and factors for prioritisation, ordering of the list, and selection criteria have been described before in section 1.3.2.

Based on this list a continuous monitoring of SDOs, and their ongoing standardisation efforts will be implemented during the lifetime of the project. The project's web site will provide public access to regularly produced online reports covering the outcome of its monitoring activities and the assessments of the EAG.

In order to establish relevant and engaging topics for the continuous open call, StandICT.eu will implement and maintain a global ICT Standardisation Watch to monitor objectives and activities of SDO and SSO Working or Research Groups across the five priority areas. This will be further leveraged with the identification and presentation of potential gaps as (presented in Section 5) and of priority areas for EU participation (as presented in Section 6 derived from the gaps identified) in corresponding standardisation activities through the definition of StandICT.eu Open Call topics. With the overall output of this activity StandICT.eu is aiming to provide a single point to access all information relevant for standardisation in the priority areas defined through a sustainable platform after project completion,

11 Conclusions

The StandICT.eu project delivers through this document **D2.1 – Report on relevant ICT standardisation, potential gaps and EU priorities** the initial global overview on SDOs and their evolving standards in the five priority areas 5G, Cyber Security, IoT, Cloud Computing and Data. This deliverable provides an initial non-exhaustive overview. As the research yielded the level of ongoing standardisation is different for the five areas. For example, while for IoT there is a significant number of standardisation activities across different SDOs, Cloud Computing can be considered rather mature with many standards already in place and only relatively few still ongoing in a small number of SDOs. In contrast, the for the data area broader standardisation efforts have evolved only more recently but can use or re-use a number of already mature standards that have been developed for traditional IT infrastructures in the last decades. Finally, Cyber Security is a cross-cutting theme with both strong standardisation activities across all areas and dedicated standardisation activities, like the ISO 27000 series, and a broad legacy resulting from standardisation during the last decades.

StandICT.eu is focused on establishing itself as the European hub where SDOs and standardisation across the five priority areas will be monitored and published through the StandICT.eu Standardisation Watch, which will become publicly accessible through the StandICT.eu web portal in the next months

Through the additional two sections added to this report (Section 5 which covers the **Potential Gaps** in 5G communications, Cyber Security, Internet of Things, Cloud Computing, Big Data technologies; Section 6 that covers the **EU priorities** in the areas of 5G communications, Cyber Security, Internet of Things, Cloud Computing, Big Data technologies), the consortium wishes to capitalise on the content

to serve to feed into the monitoring reports for the funded applicants as well as into the Standards watch.

This additional information will serve to introduce the gap analysis into the Standards Watch and will also be reflected in the monthly monitoring report that the funded applicants need to complete, with a drop-down menu to facilitate compilation for the applicant and for the consortium which analyses and monitors the content for impact.

.

12 References

[1] GROW/F3 - Rolling Plan for ICT Standardisation 2017:
https://ec.europa.eu/docsroom/documents/24846/attachments/1/translations/en/renditions/native

[2] Communication: ICT Standardisation Priorities for the Digital Single Market
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265

[3] Cloud Standards Coordination Final Report (phase 1):
http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf

[4] Cloud Standards Coordination phase 2: Cloud Computing Standards Maturity Assessment
csc.etsi.org/resources/WP4-Report/STF_486_WP4_Report-v2.0.0.pdf

[5] Cloud Standards Coordination phase 2: Interoperability and Security in Cloud Computing
http://csc.etsi.org/resources/WP3-Report/STF_486_WP3_Report-v2.0.0.pdf

[6] Cloud Standards Coordination phase 2: Cloud Computing Standards and Open Source
http://csc.etsi.org/resources/WP2-Report/STF_486_WP2_Report-v2.0.0.pdf

[7] StandICT.eu web portal: http://www.standict.eu/

[8] GROW/F3 - Rolling Plan for ICT Standardisation 2018:
https://ec.europa.eu/docsroom/documents/28501/attachments/1/translations/en/renditions/native

[9] Cybersecurity Strategy of the European Union
https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[11] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[12] Internet of Things, Preliminary report
https://www.iso.org/iso/internet_of_things_report-jtc1.pdf

[13] IoT Security Standards Gap Analysis
https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis/at_download/fullReport

[14] High Priority IoT Standardisation Gaps and Relevant SDOs
https://aioti.eu/wp-content/uploads/2018/05/AIOTI-WG3_High_Priority_Gaps_v1.0_final.pdf.

[15] Future Leadership in ICT Standards in Europe "ELITE-S", Home Page
http://elite-fellowship.eu/

[16] ITU-T FG IMT-2020: Report on Standards Gap Analysis
https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Documents/T13-SG13-151130-TD-PLEN-0208!!MSW-E.docx

[17] 5G-PPP Euro-5g – Supporting the European 5G Initiative
https://5g-ppp.eu/wp-content/uploads/2017/10/Euro-5G-D5.3_5G-standardisation-requirements.pdf.

[18] IETF Gap Analysis for Network Slicing
https://tools.ietf.org/html/draft-qiang-netslices-gap-analysis-00

[19] European Union Agency for Network and Information Security, Home Page
https://www.enisa.europa.eu/

[20] Gaps in NIS standardisation. Recommendations for improving NIS in EU standardisation policy
https://www.enisa.europa.eu/publications/gaps-eu-standardisation

[21] Guidance and gaps analysis for European standardisation. Privacy standards in the information security context
https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation/at_download/fullReport

[22] The Directive on security of network and information systems (NIS Directive)
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[23] JTC1 Big data, Preliminary Report 2014
https://www.iso.org/iso/big_data_report-jtc1.pdf

[24] ITU-T Y.3600 – Big data standardization roadmap
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.Sup40-201607-I!!PDF-E&type=items

[25] ETSI TR 103 306: CYBER; Global Cyber Security Ecosystem
https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf.

13 Annex

The following topics have been identified by the EAG as relevant for the first call

Table 7: **5G communications**

NFV
(M)EC
Ontologies
APIs
Emerging technologies:
AI for 5G (and future networks
Blockchain

Table 8: **Cyber Security**

Cybersecurity risk management in the context of the NIS Directive
Security by design
Data Security and Privacy
Emerging technologies:
Blockchain
AI

Table 9: **Internet of Things**

Standardized ontologies including sector specific
Edge computing for IoT
Sector specific IoT security & privacy (e.g. Industrial, Healthcare, Agricultural)
Emerging technologies e.g.
Blockchain

AI

Table 10: **Cloud Computing**

Standardized APIs including OSS projects
Sector specific Cloud security & privacy (e.g. Manufacturing, Healthcare, Agricultural)
Emerging technologies e.g.
Blockchain
AI

Table 11: **Data**

Full cycle data handling
Open Data Standards
Emerging technologies:
AI
Blockchain