Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D8.1
Cybersecurity Standardization Engagement Plan

Document Identification	
Due date	31st July 2019
Submission date	5th August 2019
Revision	v2

Related WP	WP 8	Dissemination Level	PU
Lead Participant	CPT	Lead Author	CPT
Contributing Beneficiaries	GUF, CYBER, AIT, POLITO, UPRC, VTT	Related Deliverables	D8.3

Executive Summary

The aim of this document is to provide an initial description of the project's partners current engagement within the existing cybersecurity related standardization/certification activities, both international or national. By doing this we demonstrate Cybersec4Europe's potential to actively contribute to the further development of cybersecurity standardization/certification areas.

This deliverable is intended to be a full snapshot picture of the activities that our CyberSec4Europe partners are undertaking in the realm of Standardisation and Certification preparation. And it is important to note that these are only summaries of the activities as many partners go to a very significant depth in their extensive involvement. While some partners are clearly driving the efforts with Standards Development Organisations and their committees, others are active participants in contributing content and feedback. A deliverable much later in the project lifecycle will then summarise all of the results and efforts undertaken by our CyberSec4Europe partners and it is our positive hope that this will reflect our highly effective and significant contribution to Cybersecurity Standardisation and Certification.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Document information

Contributors

Name	Partner
Mark Miller / Victoria Menezes Miller	CPT
Liina Kamm	CYBER
Kai Rannenberg	GUF
Javier Lopez	UMA
Lea Hemetsberger	OASC
Juan Carlos Perez Baun	ATOS
Luca Durante	CNR
Liliana Pasquale/ Dr. Silvana Mac Mahon	UCD
Antonio Lioy	POLITO
Mariusz Nowostawski / Christoph Busch / Gkioulos Vasileios	NTNU
Kimmo Halunen	VTT
Antonia Skarmeta / Juan Antonio Martinez Navarro / Dan García Carrillo	UMU
Stephan Krenn	AIT
Borja Larrumbide Martinez	BBVA
Marco Crabu	ABI
Pasquale Annicchino	ARCH

Reviewers

Name	Partner
Liina Kamm	CYBER
Jozef Vyskoc	VaF

History

0.01	2019-03-28	M. Miller / V. Menezes Miller	1st Draft
0.02	2019-07-04	Following feedback from UMU, CNR	2nd Draft
0.03	2019-07-09	Descriptions of SDOs added	3rd Draft
0.04	2019-07-17	Feedback from WP8 partners (CYBER, POLITO)	4th Draft
0.05	2019-07-22	Further feedback from CYBER and UMU	5th Draft
0.06	2019-07-24	Feedback from ABI	6th Draft
0.07	2019-07-25	Additional comments ABI, BBVA, VaF	7th Draft
0.08	2019-07-30	Additional comments VaF	8th Draft
0.09	2019-07-31	Additional comments GUF, CPT	9th Draft
v1	2019-07-31	Final revision 1	Final v1
v1.1	2019-08-01	Additional comments GUF and UMA, reviewers' table	Final v1.1
v2	2019-08-02	Additional comments - last detailed review of GUF	Final v2
v3	2019-08-05	Clarification Section	Final v3

List of Contents

List of Figures

List of Tables

1 Introduction

This Cybersecurity Stakeholder Engagement Plan provides a snapshot of engagement of the Consortium of 43 partners in standardization activities, their collaboration and relationships with standardization bodies.

Table 1 below provides a brief summary of the content of this deliverable. While it is mainly a stocktaking exercise it contains a few first comments on the strategic opportunities and challenges for Europe.

Chapter	Title
Chapter 2	Describes the involvement of Consortium partners in standardization activities and related and pre-curson activities
Chapter 3	Next steps
Chapter 4	List of Acronymns

Table 1: Brief summary of deliverable chapters

2 Landscape of Consortium Standardization Activities

Between March and June 2019, information was collected from all partners concerning their involvement in standardization activities, specifically, the standards groups they participed in, their area of interest, the ongoing activity and the focal point in each case.
Of 43 partners in the consortium,

- 22 participate in standardization groups
- 13 do not participate
- 7 did not respond (C3P, DAWEX, GEN, I-BP, JAMK, KAU, TLEX)
- 11 standardization organsiations were identified

2.1 STANDARDIZATION ORGANIZATIONS

This section contains information on the main standardization organizations and activities that our partners have indicated they participate in. A list of the working group(s)/committee(s) in which a partner of the consortium is a member is provided, together with a brief explanation of the specific standard or area in which a partner of the consortium is involved and the current status in that activity.

Figure 1 contains a snapshot of the standards bodies and/or related organizations in which partners are involved.

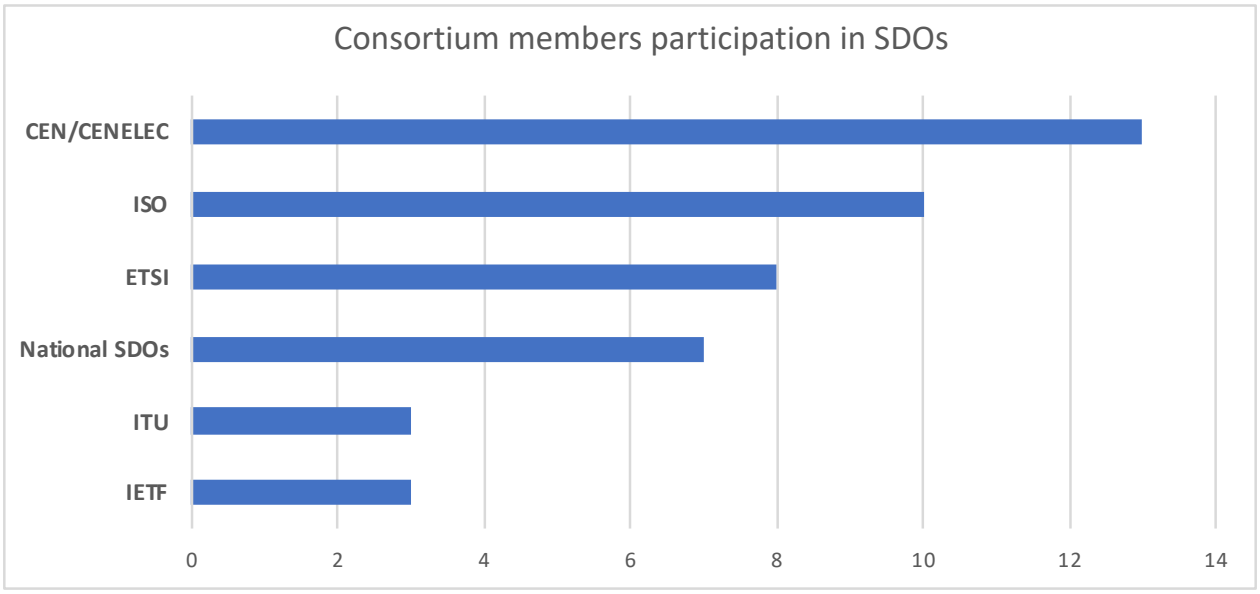

Figure 1: Consortium members participating in SDOs

2.1.1 CEN/CENELEC

> *"The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) are two distinct private international non-profit organizations based in Brussels.*
>
> *By setting common standards that are applied across the whole of the European single market, CEN and CENELEC ensure the protection of consumers, facilitate cross-border trade, ensure the interoperability of products, encourage innovation and technological development, include environmental protection and enable businesses to grow. Products and services that meet these European Standards (ENs) can be offered and sold in all of the participating countries.*
>
> *CEN and CENELEC bring together the national standards agencies of 34 countries."*
>
> (Extract from CEN/CENELEC web site.)
>
> Web site: www.cencenelec.eu/Pages/default.aspx

The Committee and Focus Group of CEN/CENELEC in which partners of the Consortium are involved are:

- **CEN/CLC/JTC 13** "Cybersecurity and Data Protection" which has six WGs
- **CEN-CENELEC Focus Group** on Blockchain and DLT which advises on EU technical requirements relating to blockchain and Distributed Ledger Technologies (DLT). The Focus Group does not develop standards.

Committee	Title	Partners
CEN/CLC/JTC 13	Cybersecurity and Data Protection	GUF
Focus Group	CEN-CENELEC Focus Group on Blockchain and DLT	NTNU

Table 2: CEN/CENELEC and partners' involvement

The following describes the participation of each partner in the above-mentioned Committee and Focus Group.

2.1.1.1 CPT

CONCEPTIVITY has been a participant in the joint activity between CEN/CENELEC and ECSO Working Group 1 with respect to cooperation discussions and joint efforts. Specifically there has been a joint workshop where CONCEPTIVITY took an active role.

2.1.1.2 GUF

CEN/CLC/JTC 13

The Johann Wolfgang Goethe-Universitat Frankfurt am Main (GUF) participates in CEN/CLC/JTC 13 "Cybersecurity and Data Protection". In general, the group mirrors the work of ISO/IEC JTC 1/SC 27, but is recently starting its own initiatves also, either to discuss guidelines to ISO/IEC standards or to start specific projects.

Current status:

Several SC 27 projects are in the process of being adopted, about 8 have already been adopted by the JTC (including 27001 and 29134 (originally handled by the previous JTC 8)) and are waiting for CEN and CENELEC Board decision.

2.1.1.3 NTNU

Norges Teknisk-Naturvitenskapelige Universitet's (NTNU) participation is mainly in the CEN-CENELEC Focus Group on Blockchain and DLT. This is a European Union based, focus group, to conduct the preliminary investigations on Blockchain and DLT technology in the context of European deployments and standardization. The life of this group is limited to the end of this year, and the members have been migrated to ISO/TC 307. It has been decided to follow the international standardization initiatives with ISO, and on national levels, and if there is a need for a European committee, it will be established later.

Current status:

The current work was focused on a publication of the official Blockchain and DLT whitepaper that summarizes the current state-of-the-art as well as the standardization needs, risks, future directions, and current problems and solutions in this space.

2.1.2 EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)

The European Telecommunications Standards Institute (ETSI) is a European Standards Organization (ESO). ETSI is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services with more than 850 member organizations drawn from over 60 countries and five continents.

Web site: https://www.etsi.org/

Partners are involved in the following groups:

Study Group	Title	Partner involvement
STF 561	Smart cities and communities: standardisation to meet citizen and consumer requirements	OASC
TC CYBER	Technical Committee on Cyber Security	AIT
ISG CIM	Industry Specification Group Context Information Management	UMU
ISG NFV	Industry Specification Group for Network Functions Virtualization	POLITO

Table 3: ETSI and partners' involvement

The following describes the participation of each partner in the above-mentioned Committees and Groups:

2.1.2.1 AIT

The Austrian Institute of Technology GGMBH (AIT) participates in TC CYBER, which is the most security-focused technical committee within ETSI. The committee works with stakeholders to increase privacy and security for citizens and organizations in Europe and beyond. TC CYBER covers aspects like cyber security ecosystems, IoT security, critical infrastructures, or personal data protection and cryptography.

Current Status:

Within TC CYBER, there are currently no ongoing work items with active AIT contribution.

2.1.2.2 BBVA

2.1.2.2. Banco Bilbao Vizcaya Argentaria SA (BBVA) has been in contact with ETSI to explore future collaborations and they have also invited ETSI to participate in a cloud stakeholder plenary session for them to present ETSI and to explain the challenges and solutions they see with certifications in Europe, but BBVA is currently not a member of ETSI.

2.1.2.3 OASC

Open & Agile Smart Cities (OASC) participates in ETSI STF 561: “Smart cities and communities: standardisation to meet citizen and consumer requirements”. In this STF 561, OASC has the role of Advisory Group Member.

The objective of the STF 561 is to deliver a document as an ETSI Technical Report, that will

1. take a first overview of what the needs of citizens in smart communities are;

2. relate those needs to standardisation activities, ongoing or foreseen, and assess if they are being met;
3. if not, make recommendations as to how to rectify this; and
4. lay down some basic principles as to how citizen needs should be addressed

The work of STF 561 started on 2 November 2018 and will be finished by 31 July 2020. The main milestones of the project are listed in the table below:[1]

Milestone	Description	Target Achievement Date
A	Completion of setting-up phase Progress report to be approved by TC HF by RC	15 Jan 2019
B	Early draft available (Table of contents and scope) Webpages creation Progress report to be approved by TC HF by RC	30 Apr 2019
C	Completion of web meetings Stable draft TR available Progress report to be approved by TC HF#80	15 Oct 2019
D	Delivery Interim report to EC/EFTA	30 Nov 2019
E	Holding Open meeting Start of consultation Progress report to be approved by TC HF#81	Feb 2020
F	Resolution of comments, Final draft TR and STF Final report approved by TC HF#82	Jun 2020
G	Final Report to EC/ EFTA Completion of project	31 Jul 2020

Table 4: STF 561 milestones

Current Status:

The STF 561 has sofar drawn up the work programme and as a first step created a stakeholder survey (https://standards4citizens.etsi.org/Survey/) to gather relevant input from the main stakeholders. More information about the next steps are available here: https://standards4citizens.etsi.org/

[1] From ETSI ST561 web page https://portal.etsi.org/STF/STFs/STFHomePages/STF561

2.1.2.4 UMU

Universidad de Murcia (UMU) is working in the ETSI Industry Specification Group for cross-cutting Context Information Management (ISG CIM). This group has released the NGSI-LD API, an extension of the Next Generation Services Interface (NGSI) provided by Open Mobile Alliance (OMA) which has been extended to support linked data (LD). Our main activity in this work is related to security and privacy. The goal of this activity is to introduce these considerations from the point of view of the information itself. Currently, Juan A. Martinez, is rapporteur for the WI-007-SEC of this group.
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53370.

Current status:

Regarding the work on the ISG-CIM, UMU has been involved in Work Item 00-7. We have released a first early draft and we are currently developing a second release of it where different security and privacy mechanisms such as authentication, authorisation and confidentiality has been considered. Additionally, UMU is working on using the current NGSI-LD vocabulary as a means to represent security properties that can be associated to entities represented using NGSI-LD.

2.1.2.5 POLITO

Politecnico di Torino (POLITO) is working to the security aspects of network functions within the ETSI Industry Specification Group for Network Functions Virtualization. More specifically, the emphasis of POLITO's work is in trust and integrity verification of software-defined infrastructures. As POLITO is not a full member of ETSI, it works in cooperation with Telefonica and Hewlett-Packard and parcticipates in meetings upon their invitation.

2.1.3 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

The International Organization for Standardization (ISO) is based in Geneva, Switzerland, and is an independent, non-governmental international organization with a membership of 164 national standards bodies. and 783 technical committees and subcommittees to take care of standards development.

Together with IEC, it is operating the Joint Technical Committee (JTC) 1 "Information Technology", which in turn has several subcommittees, eg. SC 27 and SC 37.

The scope of ISO/IEC JTC 1/SC 27 is 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, cryptographic and other security mechanisms, security aspects of identity management, biometrics and privacy, conformance assessment, accreditation and auditing requirements in the area of information security management systems, security evaluation criteria and methodology.

The scope of ISO/IEC JTC 1/SC 37 is the Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include for instance Biometric application programming interfaces, Biometric data interchange formats,

- Application of evaluation criteria to biometric technologies.
- The mission of ISO/IEC JTC 1/SC 37 is to ensure a comprehensive and high priority, worldwide approach for the development and approval of international biometric standards

Web site: www.iso.org

Partners of the Consortium are involved in the following committees:

- **ISO/IEC JTC 1/SC 27** "Information Security, cybersecurity and privacy protection" and **ISO/IEC JTC 1/SC 37** "Biometrics" which are subcommittees of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO)

and the International Electrotechnical Commission (IEC). SC 27 aims at developing standards for the protection of information and ICT.

- **SC 27** currently has published 182 ISO/IEC standards (includes updates), 68 ISO/IEC standards are under development (includes updates); there are 49 participating members and 29 observing members from all over the world. [2]
- **SC 37** currently has published 122 ISO/IEC standards (includes updates), 33 ISO/IEC standards are under development (includes updates); there are 28 participating members and 20 observing members.[3]

- **ISO/PC 317** "Consumer protection: privacy by design for consumer goods and services" currently with 14 participating members and 21 observing members. There is one ISO standard under development.[4]
- **ISO/TC 307** "Blockchain and distributed leger technologies" currently with 42 participating members and 12 observing members. There are 11 ISO standards under development (includes updates).[5]
- **ISO/TC 215** "Health informatics" currently has published 188 ISO standards (includes updates), has published 59 ISO standards (includes updates); there are 30 participating members and 31 observing members.[6]

Table 5 below provides a breakdown of the Committees, Working Groups and involvement of each partner, including related H2020 projects.

Technical Committee/ Sub-Committee/Committee/Study Group	Title of Committee/ Identification Number and title of standard	Partners involved	Related H2020 and earlier EU Projects
ISO/IEC JTC 1/SC 27	Information Security, cybersecurity and privacy protection		
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems	ATOS	CYBERWISER
	ISO/IEC 27005:2018 Information security risk managemenet	ATOS	CYBERWISER
	ISO/IEC 27010:2015 Information security management for	ATOS	CONCORDIA

[2] Statistics of May 2019 from ISO web site SC 27 https://www.iso.org/committee/45306.html
[3] Statistics of May 2019 from ISO web site SC 37 https://www.iso.org/committee/313770.html
[4] Statistics of May 2019 from ISO web site ISO/PC 317 https://www.iso.org/committee/6935430.html
[5] Statistics of May 2019 from ISO web site ISO/TC 307 https://www.iso.org/committee/6266604.html
[6] Statistics of May 2019 from ISO web site ISO/TC 215 https://www.iso.org/committee/54960.html

Technical Committee/ Sub-Committee/Committee/Study Group	Title of Committee/ Identification Number and title of standard	Partners involved	Related H2020 and earlier EU Projects
	inter-sector and inter-organizational communications		
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	AIT, CYBER	
	ISO/IEC 19592-1:2016 Secret sharing, Part 1: General	CYBER	
	ISO/IEC 19592-2:2017 Secret sharing – Part 2: Fundamental Mechanisms	AIT, CYBER	
	ISO/IEC CD 23264-1 Redaction of Authentic Data – Part 1: General	CYBER	Initiated by PRISMACLOUD and CREDENTIAL
	ISO/IEC WD 23264-2 Redaction of Authentic Data – Part 2: Schemes based on asymmetric mechanisms	AIT	Initiated by PRISMACLOUD and CREDENTIAL
	ISO/IEC WD 20009-3: Anonymous entity authentication – Part 3: Mechanisms based on blind signatures	AIT	
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification	NTNU, CYBER, GUF	
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services	GUF	
	ISO/IEC CD 20547-4 Big data reference architecture – Part 4: Security and Privacy	GUF	
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies	AIT, ATOS, CYBER, GUF, NTNU	
	ISO/IEC 17922:2017 Telebiometric authentication framework using biometric hardware security module	GUF	
	ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques	GUF	
	ISO/IEC 24745:2011 Biometric information protection	GUF	
	ISO/IEC 24760-1:2011, 2019	GUF	FIDIS, PrimeLife

Technical Committee/ Sub-Committee/Committee/Study Group	Title of Committee/ Identification Number and title of standard	Partners involved	Related H2020 and earlier EU Projects
	A framework for identity management – Part 1: Terminology and concepts		
	ISO/IEC 24760-2:2015 A framework for identity management – Part 2: Reference architecture and requirements	GUF	FIDIS, PrimeLife, ABC4Trust
	ISO/IEC 24760-3:2016 A framework for identity management – Part 3: Practice	GUF	FIDIS, PrimeLife, ABC4Trust
	ISO/IEC PRF TR 27550: Privacy engineering for system life cycle processes	GUF	
	ISO/IEC WD 27551 Requirements for attribute-based unlinkable entity authentication	AIT, GUF	CyberSec4Europe cf. tasks T3.2 and T5.3.
	ISO/IEC 27701:2019 (was 27552) Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines	GUF	
	ISO/IEC WD 27553 Security requirements for authentication using biometrics on mobile devices	GUF	
	ISO/IEC WD 27554 Application of ISO 31000 for assessment of identity management-related risk	GUF	
	ISO/IEC WD 27555 Establishing a PII deletion concept in organizations	GUF	
	ISO/IEC WD 27556 User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	GUF	
	ISO/IEC PDTS 27570 Privacy guidelines for Smart Cities	GUF	
	ISO/IEC TS 29003:2018 Identity proofing	ATOS, GUF	ARIES
	ISO/IEC 29134:2017 Privacy impact assessment –	GUF	

Technical Committee/ Sub-Committee/Committee/Study Group	Title of Committee/ Identification Number and title of standard	Partners involved	Related H2020 and earlier EU Projects
	methodology		
	ISO/IEC 29100:2011 Privacy framework	GUF	FIDIS, PrimeLife
	ISO/IEC 29101:2013, 2018 Privacy architecture framework	CYBER GUF	FIDIS, PrimeLife
	ISO/IEC TS 29115:2013 Entity authentication assurance framework	ATOS, AIT, GUF	ARIES, CyberSec4Europe's cf. tasks T3.2 and T5.3.
	ISO/IEC 29134:2017 Privacy impact assessment – methodology		
	ISO/IEC 29146:2016 A framework for access management	GUF	
	ISO/IEC 29151:2017 Code of practice for PII protection	GUF	
	ISO/IEC 29190:2015 Privacy capability assessment model	GUF	
	ISO/IEC 29191:2012 Requirements for partially anonymous, partially unlinkable authentication	GUF	
	ISO/IEC DIS 29184 Online privacy notice and consent	GUF	
ISO/IEC JTC 1/SC 37	Biometrics		
ISO/IEC JTC 1/SC 37/WG 1	Harmonized Biometric Vocabulary		
ISO/IEC JTC 1/SC 37/WG 2	Biometric Technical Interfaces		
ISO/IEC JTC 1/SC 37/WG 3	Biometric Data Interchange Formats	NTNU	
ISO/IEC JTC 1/SC 37/WG 4	Technical Implementation of Biometric Systems[10]		
ISO/IEC JTC 1/SC 37/WG 5	Biometric Testing and Reporting		
ISO/IEC JTC 1/SC 37/WG 6	Cross-Jurisdictional and Societal Aspects of Biometrics		
ISO/PC 317	Consumer protection: privacy by design for consumer goods and services	GUF	
ISO/TC 307	Blockchain and distributed leger technologies	NTNU	

Technical Committee/ Sub-Committee/Committee/Study Group	Title of Committee/ Identification Number and title of standard	Partners involved	Related H2020 and earlier EU Projects
ISO/TC 307/WG 1	Foundations	NTNU	
ISO/TC 307/WG 2	Security, privacy and identity	NTNU	
ISO/TC 307/WG 3	Smart contracts and their applications	NTNU	
ISO/TC 307/WG 5	Governance	NTNU	
ISO/TC 307/SG 2	Use cases	NTNU	
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems	NTNU	
ISO/TC 215	Health Informatics		
ISO/TC 215 IEC/SC 62A/JWG 7	Safe, effective and secure health software and health IT systems, including those incorporating medical devices	UCD	
IEC 80001-1:2010	Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities	UCD	
ISO TR 80001-2-7:2015	Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1	UCD	
ISO/IEC Study Group	Societal and Human Factors in IoT Based Services	ARCH	

Table 5: ISO and partners' involvement

2.1.3.1 AIT

ISO/IEC JTC 1/SC 27:

Austrian Institute Of Technology (AIT) participates in WG 2 which is dedicated to "Cryptography and security mechanisms", and WG 5 which is focusing on "Identity management and privacy technologies".

Current Status:

Within ISO/IEC JTC 1/SC 27, there are currently multiple ongoing projects with direct relation to CyberSec4Europe. Early stage projects in WG 2 include ISO/IEC 23264 "Redaction of Authentic Data, Part 1: General and Part 2: Schemes based on asymmetric mechanisms" while more mature projects include ISO/IEC 20009-3 "Anonymous entity authentication - Part 3:

Mechanisms based on blind signatures" (all (co-)edited by AIT, and the former having been initiated by the two H2020 projects PRISMACLOUD and CREDENTIAL).

In WG 5, projects include ISO/IEC 29115 "Entity authentication assurance framework" or ISO/IEC 27551 "Requirements for attribute-based unlinkable entity authentication". All these projects are closely related to CyberSec4Europe's ambition of privacy-preserving identity management, cf. tasks T3.2 and T5.3. WG-internal work items of general interest in particular include the development of necessary criteria for submitting cryptographic algorithms as potential candidates for inclusion into an ISO/IEC or ISO standard. The goal of this task is to increase the quality and trustworthiness of International Standards.

2.1.3.2 ARCH

Archimede Solutions (ARCH), through its leadership in Activity Group 05 for the Large Scale Pilots (LSPs), has been invited to contribute to the ISO/IEC Study Group on Societal and Human Factors in IoT Based Services which will also devote particular attention to the issue of privacy in IoT. The discussions are still at an early stage.

2.1.3.3 ATOS

ISO/IEC JTC 1/SC 27/WG 5 :

ATOS' involvement in WG 5 is to follow and contribute to ISO/IEC 29003, 29115 (related to ARIES project), and also 27005 and 27010 (related to Cyberwiser and Concordia projects respectively). ATOS is also involved in WG 1, although contributions are sent through national body (UNE). The most recent input was on the 3rd Working Draft of ISO/IEC 27002 (revision of 2nd edition 2013-10) –Information security controls.

Current Status:

- ISO/IEC TS 29003: April 2019 Technical Specification (TS): Published Notice of publication of ISO/IEC TS 29003:2018-03 (1st edition) — Information technology — Security techniques — Security techniques — Identity proofing;
- ISO/IEC 29003 Use cases for identity assurance: in April 2019 study period extended for 6 months;
- ISO/IEC 29115: Early revision (current version from 2013);
- ISO/IEC 27005: 4th revision (last revision in 2011);
- ISO/IEC 27010:2015-11-15 (2nd ed.) — Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications has been published in 2015
- Privacy Engineering Service based on ISO/IEC 27550: Study period. Currently is in draft technical report.

2.1.3.4 CYBER

ISO/IEC JTC 1/SC 27/WG 2 and WG 5:

Cybernetica AS (CYBER) represented Estonia in ISO/IEC JTC 1/SC 27/WG 2 and WG 5 for many years. Currently Estonia is no longer a voting member in SC 27 and CYBER has not participated in meetings in the recent years. Dan Bogdanov, PhD, currently a department head in CYBER was the editor of the following standards: ISO/IEC 29101:2013 Privacy Architecture Framework (WG 5, published 10/2013), ISO/IEC standard ISO/IEC 19592-1:2016 Secret sharing, Part 1: General (WG 2, published 11/2016), ISO/IEC standard ISO/IEC 19592-2:2017 Secret sharing, Part 2: Fundamental Mechanisms (WG 2, published 10/2017).

CYBER will also propose to the Estonian Centre for Standardisation that we actively continue our efforts in ISO/IEC.

2.1.3.5 GUF

ISO/IEC JTC 1/SC 27/WG 5:

After completion of foundational frameworks (especially ISO/IEC 24760 A framework for identity management and ISO/IEC 29100 Privacy framework) priorities for Working Group 5 are to develop related standards and Standing Documents on supporting technologies, models, and methodologies. WG 5 has completed 17 projects towards International Standards (IS) and one towards a Technical Specification (TS). It is currently active in ten further projects with more being expected. These projects can be grouped into three areas:

1. Frameworks and architectures
2. Protection concepts
3. Guidance on context and assessment

Kai Rannenberg (GUF) is the Convenor of WG 5.

Current status:

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2011, 2019, IS:2015, IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011; Amendment 1:2018)
- Privacy architecture framework (ISO/IEC 29101, IS:2013, 2018)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013, Revision WD)
- A framework for access management (ISO/IEC 29146, IS:2016)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, IS:2017) (formerly X.bhsm)

- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC CD 20547-4, CD) (together with WG 4)
- User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC 27556, WD)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011, Revision WD)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889, IS:2018)
- Online privacy notice and consent (ISO/IEC 29184, DIS)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551, CD)
- Security requirements for authentication using biometrics on mobile devices (ISO/IEC 27553, WD)
- Establishing a PII deletion concept in organizations (ISO/IEC 27555, WD)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision FDIS)
- Privacy capability assessment model (ISO/IEC 29190, IS:2015)
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018, IS:2014, 2019)
- Identity proofing (ISO/IEC 29003, TS:2018)
- Privacy impact assessment – methodology (ISO/IEC 29134, IS:2017)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151, IS:2017) (formerly X.gpim)
- Privacy engineering for system life cycle processes (ISO/IEC TR 27550, under publication)
- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines (ISO/IEC 27701, IS:2019 (was 27552)
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570, PDTS)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, WD)

ISO/PC 317:

- Consumer protection: privacy by design for consumer goods and services
- Standardization in the field of consumer protection: privacy by design for consumer goods and services.
- Currently in WD status.

2.1.3.6 NTNU

ISO/TC 307:

This is the international committee for standarization in the blockchain and DLT space. The work goes on in multiple study and working groups:

- ISO/TC 307/WG 1 Foundations
- ISO/TC 307/WG 2 Security, privacy and identity
- ISO/TC 307/WG 3 Smart contracts and their applications
- ISO/TC 307/WG 5 Governance
- ISO/TC 307/SG 2 Use cases
- ISO/TC 307/SG 7 Interoperability of blockchain and distributed ledger technology systems

ISO/IEC JTC 1/SC 27:

NTNU staff participates in the Working Group 3 (Security evaluation, testing and specification) on presentation attack detection standards for Biometrics. Further representation of NTNU is following Working Group 5 (Identity management and privacy technologies) with regards to the framework for biometric information protection.

ISO/IEC JTC 1/SC 37:

Christoph-Busch (NTNU) is chairing the Working Group 3 (Biometric Data Interchange Formats). WG 3 with NTNU are currently defining the Extensible Data Interchange Formats, which will be introduced by ICAO in 2020 as new standard for the biometric passport. Moreover we develop standards for biometric sample quality assessment, which is essential to accept or reject a biometric sample at the enrolment station. More details at: https://www.christoph-busch.de/standards-sc37wg3.html

2.1.3.7 UCD

Dr. Silvana Mac Mahon has been nominated Irish expert to ISO/TC 215 IEC/SC 62A/JWG 7 and has acted as international project leader, author and editor of *ISO/TR 80001-2-7:2015 - Application of risk management for IT-networks incorporating medical devices -- Application guidance -- Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*. This technical report contains an assessment method, process reference model and process assessment model that can be used by healthcare delivery organisations to assess the capability of their risk management processes against the requirements of IEC 80001-1. *IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities* focuses on ensuring the safety, effectiveness and security of medical IT networks.

Based on her work on ISO TR 80001-2-7, Dr. MacMahon was invited by the co convenors of JWG 7 to propose an approach to the revision of IEC 80001 and she is leading the process aspects of the revision. The revised standard has a broader scope than the original standard and is focused on risk management of health information technology systems. She drafted the CD1 draft of the standard and led the discussion of comments on the CD1 draft. Dr. MacMahon has also been an invited speaker at NHS Patient Safety Conference, EURAS Conference and NSAI standards forum. She is part of the JWG 7 leadership team and attends fortnightly meetings of the working group. Participation in this meeting allows her to keep up with developments of other standards within JWG 7 such as IEC 81001 and IEC 62304 though her main focus is on IEC 80001-1 and it's aligned technical reports. Dr. MacMahon has published papers both on the development of the TR and on the revision of IEC 80001-1.

Current Status:

The work on the revision of the standard is ongoing and was discussed at a recent meeting of JWG 7 in Gothenburg. The CD2 Draft was circulated and comments were received. Project Team meetings (which Dr. MacMahon would attend) were scheduled for 24th and 25th of June 2019 in London to discuss and resolve the comments received and agree upon the final draft of the standard. In addition, work is being undertaken to ensure that the terms and definitions in the revised version of IEC 80001-1 are consistent with those in the new standard under development ISO 81001-1 Health software and health IT systems safety, effectiveness and security -- Part 1: Foundational principles, concepts, and terms. All text from existing technical reports in the IEC 80001-1 standard are also currently being reviewed for potential inclusion in the revised IEC 80001-1 standard. Both the revised IEC 80001-1 standard and ISO 81001 are scheduled for registration as DIS later in 2019 with a view to being published in early 2020.

2.1.4 INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

The International Telecommunications Union (ITU) is based in Geneva, Switzerland. ITU embodies principles of public-private parternship, with its current membership of 193 countries and over 800 private-sector-entites and academic institutions. The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of information and communications technologies (ICTs).

Web site: www.itu.int

Partners are involved in the following ITU Focus Group:

- The **ITU Focus Group on Data Processing and Management (FG-DPM)** to support IoT and Smart Cities & Communities. The Focus Group was established by ITU-T Study Group 20 at its meeting in Dubai, 13-23 March 2017.

The accelerating population density in urban areas is increasing the pressure on the existing infrastructures to meet the needs of inhabitants. Accordingly, there is an increasing demand for connected cities with pervasive embedded devices, to improve quality of IoT and SC&C services. Taking into account the data interoperability, classification, format and security issues that affect various stakeholders, this Focus Group plays a role in providing a platform to share views, to develop a series of deliverables, and showcasing initiatives, projects, and standards activities linked to data processing and management and establishment of IoT ecosystem solutions for data focused cities.

Study Group	Title	Partner involvement
SG20	Internet of things (IoT) and smart cities and communities (SC&C)	
	WG1 - Use Cases, Requirements and Applications/Services	OASC
	WG2 - DPM Framework, Architectures and Core Components	ARCH

Table 6: ITU and partners' involvement

2.1.4.1 ABI

ABI Lab, in the role of Facilitator in ITU, is involved in the ITU cybersecurity programme which offers valuable tools, critical insights, assessment and technical assistance to support ITU membership – particularly developing countries – in increasing their cybersecurity capabilities and building trust and confidence in the use of ICTs.

2.1.4.2 ARCH

Archimede Solutions (ARCH) is involved in the context of the ITU and of the Focus Group on Data Processing and Management to Support IoT and Smart Cities and Communities and with other partners is leading the drafting of a Technical Report on "*Framework of Security and Privacy in DPM*". The technical report defines a framework for security and privacy in data processing management for data driven IoT and smart cities and communities. It first provides a description of the current framework in terms of data processing management. It then provides a rationale for a higher level ecosystem viewpoint for data security and privacy management in smart cities. It also explains the framework and provides guidance use.

Current status:

It is now in its final stage and a further discussion on the text will take place in July.

2.1.4.3 OASC

Open & Agile Smart Cities (OASC) is leading WG1 - Use Cases, Requirements and Applications/Services. The goal of this WG is to provide a technical specification "Use case analysis and general requirements for DPM".

Current Status:

Currently, a draft technical specification "Use case analysis and general requirements for DPM" is being prepared by WG1 of the FG-DPM. The next meeting took place mid-July in Geneva, all relevant information can be accessed here: https://www.itu.int/en/ITU-T/focusgroups/dpm/Pages/default.aspx

2.1.5 INTERNET ENGINEERING TASK FORCE (IETF)

IETF is an Internet standards body developing open standards through open processes in an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and its operation.

Web site: https://www.ietf.org/about/

Partners are involved in the following groups:

Study Group	Title	Partner involvement
I2NSF	Interface to Network Security Functions	POLITO
T2TRG	Things-to-things Research Group	UMU
RADEXT WG	RADIUS Extensions Working Group	UMU

Table 7: IETF and partners' involvement

The following describes the participation of each partner in the above-mentioned Groups.

2.1.5.1 UMU

UMU is working with the IETF Working Group and the Research Group. In particular, UMU is mostly focusing on the following groups in which its work has the the most potential to go through: T2TRG, RADEXT and ACE.

The Thing-to-Thing Research Group (T2T RG) is investigating open research issues in turning a true "Internet of Things" into reality, an Internet where low-resource nodes also known as "things" or "constrained nodes" can communicate among themselves and with the wider Internet, in order to take part in permission-less innovation. T2TRG focuses on issues that are related to opportunities for standardization in the IETF, i.e., it will start at the adaptation layer connecting devices to IP, and end at the application layer with architectures and APIs for communicating and making data and management functions (including security functions) available. T2TRG pursues objectives such as: definition of "benchmark" or "reference" environments, enabling regular **plug-tests** as a basis for repeatable, comparable research; describing practical, real world, cross-domain applications of connected "things"; dealing with taxonomy, technology

survey, and best practice documents. The RADIUS Extensions Working Group (RADEXT WG) focuses on extensions to the RADIUS protocol and clarifies its usage and definition. Also, it ensures backward compatibility with existing RADIUS implementations, as well as compatibility between RADIUS and Diameter.

Current status:

With T2TRG, UMU is providing a survey on the current bootstrapping technologies as part of the objectives of the research group. In this work, UMU is elaborating the current methods that are used in bootstrapping and making a differentiation amongst techniques that are used to do so. The aim of this work is to provide comprehensive information about the state of bootstrapping in IoT. This work is active and waiting for the decision of the RG chairs to go through as an RG item.

The work on RADEXT was an extension of the of the Long Range Wide Area Network (LoRaWAN) authentication mechanism to support Authentication, Authorization and Accounting (AAA) infrastructures. In this sense, UMU proposed a way of extending the LoRaWAN Joining Procedure to be used with RADIUS (and also in DIAMETER in a similar document). This effort is similar to the one being carried out by the LoRa Alliance, with the difference that UMU proposes the use of current standards to do so. This work is currently not active, waiting for the LPWAN working group to recharter and start considering security and extensions for current LPWAN technologies.

2.1.5.2 POLITO

Within IETF, POLITO is active in the I2NSF group where it is providing knowledge about modelling network security functions for various purposes (e.g. creation of standard APIs, automatic deployment of security policy). A draft-RFC has already been created and progress is expected in the coming years

2.2 NATIONAL STANDARDIZATION BODIES

2.2.1 ESTONIAN CENTRE FOR STANDARDISATION

"Established on 30 November 1999 by order of the Government of the Republic, the Estonian Centre for Standardisation (Eesti Standardikeskus, EVS) is a non-profit association that launched operations on 1 April 2000 under the Technical Regulations and Standards Act (Tehnilise normi ja standardi seadus).

Prior to then, standardisation had been overseen by the Estonian Standards Board. Established in 1991 as a state institution under the jurisdiction of the Ministry of Finance, the Standards Board aimed to steer and coordinate activities in the areas of standardisation, metrology and accreditation in Estonia. In January 1997, the Standards Board was transferred under the jurisdiction of the Ministry of Economic Affairs and Communications."

(Extract from EVS web site.)

Web site: https://www.evs.ee/

2.2.1.1 CYBER

Cybernetica (CYBER) is part of the expert group in the Estonian Centre for Standardisation Technical Committee 4 (Information Technology), EVS TK4 (TC4). This expert group decides which standards to translate into Estonian, gives feedback on and approves of the translations. With a country as small as Estonia, the choices have to be made carefully, because proper translation is expensive as there are very few translators who can understand the context as well as the language. Also it entails the creation of new Estonian language terms.

The technical committee also decides which international standardisation bodies to mirror and finds the standards that are most relevant to Estonia.

2.2.2 FINNISH STANDARDS ASSOCIATION

"The Finnish Standards Association SFS is the central standardization organization that controls and co-ordinates national standardization work in Finland.

SFS develops, approves and publishes national SFS standards. It also sells standards and communicates information about the standards and standardization to the public.

In addition, SFS operates the national WTO Enquiry Point.

SFS is a member of the International Organization for Standardization (ISO) *and the European Committee for Standardization* (CEN)*."*

(Extract from SFS web site.)

Web site: https://www.sfs.fi/en

2.2.2.1 VTT

In Finland, Teknologian Tukimuskeskus VTT Oy (VTT) has strong presence in the Finnish Mirror Group of ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection). Currently the group is working on the following (quite long) list of topics:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems; Security evaluation criteria and methodology.

Reijo Savola from VTT is the chairman of the Finnish Mirror Group of ISO/IEC JTC 1/SC 27.

Current status:

Work continues along normal lines.

2.2.3 GERMAN STANDARDIZATION BODY FOR INFORMATION TECHNOLOGIES (DIN)

DIN is the German standardization body for mirroring ISO, CEN and most of ISO/IEC and CEN/CLC standardization and for its own activities in the same areas. It creates technical standards for specific German requirements and translates/maps international standards to local habits and needs.

Web site: https://www.din.de/en

2.2.3.1 GUF

GUF hosts members of several DIN committees for their scientific merits and takes part in the activities of various groups (e.g. cybersecurity and privacy). Most of these groups are structured along the same lines as the corresponding European or international committees. In addition, some national strategy groups exist, e.g. for cybersecurity and privacy.

2.2.4 ITALIAN STANDARDIZATION BODY FOR INFORMATION TECHNOLOGIES (UNINFO)

UNINFO is the Italian standardization body for ICT technologies. It creates technical standards for specific Italian requirements and translates/maps international standards to local habits and needs.

2.2.4.1 POLITO

POLITO is an honorary member of UNINFO for its scientific merits and takes part in the activities of various groups (e.g. digital signature, electronic documents, electronic identity, intelligent transportation systems).

2.2.5 STANDARDS NORWAY

"Standards Norway (SN) is a private and independent member organisation, and is one out of three standardisation bodies in Norway. Standards Norway is responsible for standardisation activities in all areas except the electrotechnical field and the telecommunications field.

The organisation was established the 24 June 2003 with roots dating back to 1923. Standards Norway has approx. 75 employees and is located at Lysaker in the western part of Oslo.

Standards Norway is the national member of the International Organization for Standardization (ISO) and the European Committee for Standardization (CEN). Standards Norway holds a seat on the boards of these organisations.

Each year, Standards Norway publishes about 1 200 new Norwegian Standards (NS). Norwegian Standards are established on the basis of national draft standards as well as

on the basis of European and International Standards. Currently, more than 15 000 valid NS exist."

(Extract from Standards Norway web site.)

Web site: https://www.standard.no/en/

2.2.5.1 NTNU

Fintech, Banking, Blockchain/DLT Standards Norge SN/K 250 – SN/K 250 Bank og finansielle tjenester is the Norwegian equivalent of international ISO/TC 68. The Norwegian committee works on Fintech and banking standards, and for the last few years it has been also working on Blockchain and DLT technologies. There is a new initiative to separate the two groups, and form a new group, that would be the equivalent to ISO/TC 307.

The work includes standardization of protocols, currency codes, banking codes across Europe and in Norway. One of the active projects is the country-independent bank codes standard. ISO/TC 307 (and in the future the SN/K equivalent).

2.2.6 SPANISH ASSOCIATION FOR STANDARDIZATION (UNE)

"UNE is the only Standardisation Body in Spain, and it has been appointed so by the Ministry of the Economy, Industry and Competitiveness before the European Commission.

In this sense, UNE is the Spanish representative in the international and European organisations ISO/IEC and CEN/CENELEC, respectively, as well as in the national standardisation organisation ETSI."

(Extract from UNE web site)

Web site: https://www.en.une.org/

2.2.6.1 UMA

The University of Malaga (UMA) is a member of Spanish Normalization Technical Committee 320 (CTN320) on Cybersecurity and Personal Data Protection.

The field of activity of CTN320 is the normalization of methods, techniques and policies in the scope of Cybersecurity, information security, and ICT, that includes the following areas:

- methodologies for capture of requirements;
- security techniques and mechanisms, including the procedures for registration of security components;
- management of cybersecurity, information security, and ICT;
- documentation of support to management, including norms related to terminology, and security evaluation criteria;
- requirements and guidelines for protection of personal data y individuals privacy, including management aspects and privacy-by-design and by-default requirements.

Current status:

It must be pointed out that CTN320 is organized into subcommittees that mirror the WG structure of ISO/IEC/JTC 1/SC 27, so all the activity of CTN320 directly follows the activities of SC 27 on information security, cybersecurity and privacy protection.

2.2.6.2 BBVA

Banco Bilbao Vizcaya Argentaria's (BBVA) participation is mainly to ensure compliance with new or existing regulations. BBVA is not yet actively involved in the different WGs; however, they follow activities taking place in the CTN 320 Working group which revolves around Cybersecurity and Data protection. BBVA has been involved in providing feedback to standards such as the open consultation of the ISO/IEC 27002 during 2019.

2.2.7 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) – USA

"The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks."

(Extract from NIST web site)

Web site: https://www.nist.gov/

2.2.7.1 CYBER

CYBER is developing novel cryptographic technologies and offers them internationally. Often, this means that the organisation should work with the standards bodies of certain countries. Given the size of the market, the United States of America and their National Institute of Standardization (NIST) has been of interest. Notably, NIST standards are also used in technical work around the world. Therefore, working with NIST also makes sense with an international market.

In 2014, an international group of companies and researchers including CYBER, suggested that NIST standardizes threshold cryptography operations. Threshold cryptography covers multiple primitives, including threshold ciphers, secret sharing and more - basically all structures where an operation is conducted by multiple parties together. If a certain threshold of participants is reached, the operation is completed successfully. This can have confidentiality, integrity or reliability guarantees, depending on how the primitives are used.

Threshold cryptography has various applications, in protecting cryptographic keys and data, but also blockchain applications (e.g., custody and more).

NIST started the process by preparing a report (comparable to the study period process in ISO/IEC). A draft report was published with a public request for comments. CYBER responded to the questions posed and was, thus, involved in the process. Based on the comments, NIST put together the final report. Thus, the process is similar to other organisations. The difference is in the involvement of parties during drafting - NIST handles that internally, publishing the resolution of comments and the document differences, but no more involvement from the community is provided.

This report was published as NISTIR8214:
https://csrc.nist.gov/publications/detail/nistir/8214/final.

The comments and resolutions, including CYBER's contributions, are available here:
https://csrc.nist.gov/CSRC/media/Publications/nistir/8214/final/documents/nistir-8214-diff-comments-received.pdf

2.3 OTHER BODIES

It is well known that many other organisations contribute to the development of standards, including their precursors, policy aspects and especially pre-organisation and support during the standardisation process. Within this deliverable we have compiled the activities of our consortium partners that they believe and recognise as contributing to the standardisation process. We are by no means labelling these additional other organisations as SDOs, however, most often standardisation is stimulated by need originating outside of the SDOs and as such there are many many organisations who contribute to the process. Also, we do not expect to cover the comprehensive list of organisations addressing and supporting standardisation, but instead D8.1 represents our view of how our CyberSec4Europe partners are participating and contributing to these myriad standardisation activities.

2.3.1 CSP CERT - EUROPEAN CLOUD SERVICE PROVIDER CERTIFICATION WORKING GROUP

"The European Cloud Service Provider Certification Working Group is a private and public stakeholder group to explore and provide a recommendation to ENISA, European Commission and member states."

(Extract from CSP CERT web site)

Web site: www.cspcert.eu

2.3.1.1 BBVA

Certifications WG initiative is co-chaired by BBVA, which is leading a proposal to the European Commission and ENISA on a harmonized European Cloud Certification based on the Cybersecurity Act and led by a private-public partnership of different stakeholders.

2.3.2 CRIMINAL USE OF INFORMATION HIDING (CUIng) INITIATIVE

*"**Criminal Use of Information Hiding (CUIng) Initative** has been officially launched in June 2016 with the support by Europol's European Cybercrime Centre (EC3) to tackle the problem of criminal exploitation of information hiding techniques by working jointly and combining experiences of experts from academia, industry, law enforcement agencies and institutions.*

The main objectives of CUIng are to:

- ***Raise Awareness****: inform about the threat that information hiding techniques can pose. Increase sensitivity to cybercriminals' information hiding potential exploitation e.g. in companies. Emphasize e.g. how forensic investigations could be impacted and how significantly harder they are when such techniques are utilized.*

- ***Track Progress****: monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and spies.*

- ***Share Strategic Threat Intelligence****: bring together security professionals from institutions, academics and industry to distribute information and share experience from different angles (security professionals, academics, law enforcements, companies, institutions etc.).*

- ***Work Jointly****: cooperate and benefit from joint potentials to develop effective countermeasures and integrate it on a global scale (or at least EU level).*

- ***Educate & Train****: make law enforcement agencies, companies, institutions, individuals etc. ready and fully prepared to react to potential cybercriminals' information hiding exploitation."*

(Extract from CUIng web site)

Web site: https://cuing.org/

2.3.2.1 CNR

The Criminal Use of Information Hiding (CUIng) Initiative has been officially launched in June 2016 with the support by Europol's European Cybercrime Centre (EC3).

The main scope of CUIng is to investigate and quantify all the issues arising from the criminal exploitation of information hiding techniques. This initiative embraces different stakeholders and combine researchers, developers and experts from academia, industry, law enforcement agencies and institutions.

At this stage, the work performed by CUIng is mainly in the field of scientific publications and ad-hoc communications. Besides, members of CUIng regularly conduct talks, organize workshop in the most important International Conference and perform research in the field published in high-ranked journals and highly recognized magazines. Current activities aim at the following:

1. Raise Awareness: inform about the risks arising from the use of information hiding techniques.

2. Keep Track of Attacks and Countermeasures: monitor the increasing sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and spies.
3. Share Strategic Threat Intelligence: bring together security professionals from institutions, academics and industry to distribute information and share experience from different angles (security professionals, academics, law enforcements, companies, institutions etc.)
4. Encourage the Cooperation: try to promote cooperation to develop effective countermeasures and integrate it on a global scale.
5. Educate and Train: make law enforcement agencies, companies, institutions, and individuals prepared to react to potential information hiding malware and attacks.

Current status

Currently, Consiglio Nazionale Delle Ricerche (CNR) is devoted to start the works within the Project SIMARGL – Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware, funded within the H2020-SU-ICT-2018 call. Within the SIMARGL framework, which also includes CUIng, will perform research on novel and scalable detection techniques for covert channels / hidden communications nested within network flows by using machine learning approaches. Besides, along with other international partners and colleagues, we are preparing a CUIng event - The Third International Workshop on Criminal Use of Information Hiding (CUING 2019) to be held in conjunction with the 14th International Conference on Availability, Reliability and Security (ARES 2019 – http://www.ares-conference.eu).

2.3.3 ESTONIAN INFORMATION SECURITY AUTHORITY

Currently all Estonian government institutions have to follow the Estonian IT security standard (ISKE) which is based on the IT-Grundschutz by the Federal Office for Information Security of Germany (BSI). It has been compulsory in government institutions since 2008.

2.3.3.1 CYBER

CYBER has been involved in the development and updating of this standard and its application guides. As the BSI IT-Grundschutz has significantly evolved since it was used as a basis for ISKE, significant modifications have to be made to ISKE to keep it up to date.

2.3.4 EUROPEAN BANKING FEDERATION (EBF)

> *"The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 3,500 banks – large and small, wholesale and retail, local and international – employing about 2 million people."*

(Extract from EBF web site.)

Web site. https://www.ebf.eu/

2.3.4.1 ABI

- ABI Lab [Italian Banking Association – Lab] is one of the EBF National Banking Association member and represents the Italian banking community in the activities related to Research and Innovation in the banking industry. ABI Lab participates in the EBF Cybersecurity Working Group where Cybersecurity experts share their views on threats trends, awareness activities, and implementation of regulations.
- ABI Lab is also member of the EBF Ad Hoc Task Force EU Regulatory Framework of Experimentation.

2.3.4.2 BBVA

Web site: https://www.ebf.eu/spain/

In the context of the Spanish Bank Association, BBVA is involved in the following activities:

- open consultations on future regulations to harmonize/standardize them,
- harmonization of awareness campaigns with Europol in the EU,
- a proposal to harmonize different existing regulations such as incident reporting os multiple regulations which use different thresholds, templates and taxonomies,
- engagement with regulators and supervisors to explain challenges and try to harmonize future regulations.

2.3.5 EUROPEAN CYBER SECURITY ORGANIZATION (ECSO)

"The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries."

The Working Groups of ECSO are:

- *WG1: Standardisation, certification, labelling and supply chain management*
- *WG2: Market deployment, investments and international collaboration*
- *WG3: Sectoral demand*
- *WG4: Support to SMEs , coordination with countries and regions*
- *WG5: Education, awareness, training, cyber ranges*
- *WG6: SRIA and Cyber Security Technologies*

(Extract from ECSO web site)

Web site: https://ecs-org.eu/

2.3.5.1 ABI

ABI Lab is Member of the WG3, WG4 and WG5.

2.3.5.2 BBVA

BBVA is co-charing the WG3.3 Financial WG to explain challenges, propose solutions. BBVA has also participated in the user committee WG as a founder member to promote information sharing and other challenges between users in different sectors.

Furthermore, BBVA also participates in WG1 for the harmonization of security certifications in the financial sector.

2.3.5.3 CNR

CNR has been among the 5 facilitators for the creation of ECSO and serves in its Board. CNR is mainly involved in the WG6 SRIA and for defining the research and innovation priorities. CNR co-edited the first ECSO SRIA in 2016 as well as the subsequent modification in 2017.

2.3.5.4 CPT

CPT participates in ECSO Working Group 1 (WG1: Standardisation, certification, labelling and supply chain management). CPT is also involved in sub-working group 1.3 (Base Layer) and has been involved in the contribution and review of the following published documents:

- 6/2017, WG1 MEMBERS - STATE OF THE ART SYLLABUS
- 12/2017, WG1 MEMBERS - STATE OF THE ART SYLLABUS updated
- 12/2017, WG1 MEMBERS - European Cyber Security Certification - A Meta-Scheme Approach
- 2/2019, ECSO - Working Group 1: Mission, Objectives, Activities, Achievements

2.3.5.5 CYBER

CYBER is involved in WG1 and WG6 of ECSO. Similarly to VTT, CYBER is trying to get the Estonian SMEs to be more actively involved in standardization and certification. CYBER believes that this can be done by making the whole process more approachable to SME-s both time-wise and financially.

2.3.5.6 GUF

GUF is involved in WG1 and WG6 of ECSO. WG1 is carrying out the important task of facilitating discussions among stakeholders on the processes and the targets of cybersecurity certification, which is an important context for standardisation, as one can expect, that the EU certification initiatives will relate to several standards, but recommendations are needed to choose the appropriate standards.

WG6 and its work on a strategic research roadmap is connected to standards and needs to consider standardisation and its relation to research results, hence GUF is active there. GUF is also an elected member of the ECSO Board of Directors.

2.3.5.7 UMA

UMA participates in WG1, WG5 and, mainly, WG6 within ECSO. More precisely, UMA is co-chairing sub-Working Group 6.4 on *Basic & Disruptive Technologies*, which aims to address the Disruptive Technologies (Artificial Intelligence, Quantum Computing, Blockchain, etc.) vision, also including the traditional basics as privacy and trust.

Apart from co-chairing SWG6.4, and as part of its involvement in WG6, UMA has actively contributed to technical papers on IoT and blockchain, as well as to the definition of priorities for Horizon Europe and the Digital Europe Programmes.

2.3.5.8 UMU

UMU is involved in ECSO participating in different WGs like WG1 and WG6. Additionally in collaboration with ECSO, UMU has also contributed to workshops such as the one with the pilots and also some panel discussion in IoT Week.

UMU continues its work in WG1 related to the definition of meta-framework schema for defining the alternatives approached for certification. Also UMU has contributed to the State-of-the-Art Syllabus document based on the analysis made in the context of the EU ARMOUR project related to the labelling options.

2.3.5.9 VTT

In ECSO, VTT participates in the WG1 as a member and engages in the standardization and certification community in a broad sense. The VTT perspective is to try to get also the Finnish infosec companies and other stakeholders' views on the WG1 discussions as there are very few Finnish members of ECSO that participate in WG1.

2.3.6 EUROPEAN PAYMENTS COUNCIL (EPC)

"The European Payments Council (EPC) is one voice for payment service providers (PSPs) on all European payment issues.

It is a unique organization that aims to make it possible for citizens and businesses in the Single Euro Payments Area (SEPA) to pay with a single payment account or card across Europe as easily and conveniently as they do in their home country.

The EPC's goal is to contribute to harmonized payments in SEPA – a goal which ultimately supports European competitiveness and innovation.

The EPC is an international not-for-profit association formed of 75 members who are PSPs (mostly banks) or associations of PSPs.

In constant dialogue with other stakeholders and regulators at European level, its role is to support and promote the integration and development of European payments. The EPC is not part of the European Union institutional framework."

(Extract from EPC web site.)
Web site: https://www.europeanpaymentscouncil.eu/about-us/introducing-epc

2.3.6.1 ABI

ABI participates in the Payment Security Support Group and Card Fraud Prevention of EPC [https://www.europeanpaymentscouncil.eu/about-us/introducing-epc]. This WG is an international WG participated by national Banking Associations from EEA countries. Cybersecurity experts share their views on threats trends, awareness activities, and implementation of regulations with a special focus on SEPA schemes.

2.3.6.2 BBVA

BBVA takes part in open consultation or feedback over different standards such as payment, ISO standards or new regulations such as PSD2 to harmonize and agree with other industry players on common standards, guidelines or codes of best practices.

2.3.7 EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

"ENISA is actively contributing to European cybersecurity policy, supporting Member States and European Union stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. This work also contributes to the proper functioning of the Digital Single Market.

The Agency works closely together with Member States and private sector to deliver advice and solutions as well as improving their capabilities. This support includes inter alia:

- *the pan-European Cybersecurity Exercises,*
- *the development and evaluation of National Cybersecurity Strategies,*
- *CSIRTs cooperation and capacity building,*
- *studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others.*

ENISA also supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

Since 2019, following the bringing into force of the Cybersecurity Act (Regulation 2019/881), ENISA has been tasked to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of products, processes and services that support the delivery of the Digital Single Market.

The European Cybersecurity Act introduces processes that support the cybersecurity certification of ICT products, processes and services. In particular, it establishes EU wide rules and European schemes for cybersecurity certification of such ICT products, processes and services."

(Extract from ENISA web site)

Web site: https://www.enisa.europa.eu/

2.3.7.1 BBVA

BBVA has been involved in the financial expert Working Group for almost 4 years to provide feedback to ENISA on the challenges the financial industry has on cybersecurity, as well as to provide possible solutions. BBVA has been advocating for a more real-time and trusted information sharing, as well as to overcome the fragmentation challenges of incident reporting to different regulators and supervisors, using different taxonomies, templates and thresholds.

2.3.7.2 CPT

CPT has participated and contributed to the discussions and interactions during more than 7 ENISA events over the last one year, including presenting Cyberwatching efforts and ECSO cooperation opportunities.

2.3.7.3 GUF

GUF has participated and contributed to the discussions and interactions in ENISA since the beginning in 2004, mostly as the Academia Stakeholder Representative till 2013 and in the Permanent Stakeholder Group since 2013. GUF has also encoraged the liaison to ISO/IEC JTC 1/SC 27 (including the support for hosting meetings) and the collaboration with CEN/CLC JTC 13.

2.3.8 EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

"Europol is the European Union's enforcement agency. Headquartered in The Hague, the Netherlands, we support the 28 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations.

Large-scale criminal and terrorist networks pose a significant threat to the internal security of the EU and to the safety and livelihood of its people. The biggest security threats come from:

- *terrorism;*
- *International drug trafficking and money laundering;*
- *organised fraud;*
- *the counterfeiting of euros;*
- *trafficking in human beings.*

The networks behind the crimes in each of these areas are quick to seize new opportunities, and they are resilient in the face of traditional law enforcement measures."

(Extract from web site.)

Web site: https://www.europol.europa.eu/about-europol

2.3.8.1 ABI

ABI Lab is a Board Member of Europol. The working table discusses, periodically, new events and new trends related to cyber-crime.

2.3.8.2 BBVA

BBVA is involved with EUROPOL via their CERT (which is in direct contact with EUROPOL). BBVA has also participated jointly with EUROPOL to define awareness fraud campaigns such as last year's campaign during the month of October which is the European cyberseucirty month. BBVA has, in addition, helped in defining use cases, as well the translation into Spanish of all the content.

2.3.9 FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS-ISAC)

"The Financial Services Information Sharing and Analysis Center is an industry consortium dedicated to reducing cyber-risk in the global financial system. Servicing financial institutions around the globe and in turn their customers, the organization leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyberthreats."

(Extract from FI-ISAC website.)
Web site: https://www.fsisac.com/

2.3.9.1 ABI

ABI Lab participates in FI-ISAC, which is the Financial Institutions Information Sharing and Analysis Centre promoted by ENISA. FI-ISAC is an international WG with participation from LEAs, CERTs and Banking associations.

2.3.9.2 BBVA

BBVA is an active member of FS-ISAC and during several years BBVA has been actively participating in the Board of the European chapter.

2.3.10 G7 CYBER EXPERT GROUP

The G7 set up the **Cyber Expert Group (CEG),** a group of cyber security experts that meets regularly to facilitate progress on major international debates and that reports to G7 ministers and governors. This group is chaired by the United Kingdom and the United States.

Established in November 2015, the objectives of the CEG are (a) to identify the main cyber security risks in the financial sector and (b) to propose actions to be taken in this area. The publication of the "G7 Fundamental Elements of Cybersecurity for the Financial Sector" in October 2016 and the "G7 Fundamental Elements for Effective Assessment of Cybersecurity" in October 2017 constituted major advances in this area.

Within the CEG, coordination work is carried out on various topics such as the identification of vulnerabilities, penetration testing, the risks of contagion resulting from relations with third parties, and cooperation between the public and private sectors.

2.3.10.1 ABI

ABI Lab is a National Representative for the financial sector. G7 Cyber Expert Group aims to identify and face new vulnerabilities for EU Financial Ecosystem.

2.3.10.2 BBVA

2.3.10.2 Although BBVA is not a member of this WG, their participation with G7 and G20 is effective but indirectly via the International Institute of Finance (IIF), which almost two years ago created a Cybersecurity Working Group in which BBVA is an active member. Via this WG, BBVA provides feedback to G7 and G20 countries. IIF meetings usually concurred during G20 ones. Most of the advice is related to the current challenges encountered but also to possible solutions such as incident reporting, information sharing, creating a common cybersecurity lexicon, improving operational resilience and collaboration with different public and private stakeholders (governments, regulators, supervisors, law enforcement, cross sector industry, this parties, etc).

2.3.11 INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA)

"As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the ***Information Systems Audit and Control Association****, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves."*

(Extract from web site.)

Web site: http://www.isaca.org/About-ISACA/Pages/default.aspx

2.3.11.1 BBVA

BBVA has several employees participating in different WGS in the ISACA Madrid Chapter. In addition, a large number of BBVA's cybersecurity employees are certified in different ISACA certifications.

2.3.12 INNOVATION AND NETWORKS INNOVATION AGENCY (INEA)

"The Innovation and Networks Executive Agency (INEA) is the successor of the Trans-European Transport Network Executive Agency (TEN-T EA), which was created by the European Commission in 2006 to manage the technical and financial implementation of its TEN-T programme.

INEA officially started its activities on 1 January 2014 in order to implement the following EU programmes:

- *Connecting Europe Facility (CEF)*
- *Parts of Horizon 2020 – Smart, green and integrated transport + Secure, clean and efficient energy*
- *Legacy programmes: TEN-T and Marco Polo 2007-2013*

INEA's main objective is to increase the efficiency of the technical and financial management of the programmes it manages."

(Extract from website)

Web site. https://ec.europa.eu/inea/en

The European Commission's Directorate General for Communications Networks, Content and Technology is responsible for the implementation of a cybersecurity strategy of the EU to ensure a safe, secure, trustworthy and resilient digital environment. The Connecting Europe Facility (CEF) is the EU's financing mechanism supporting the development of interconnected trans-European networks. The Digital Infrastructure stream of the CEF (CEF Digital) invests in the collective infrastructure needed for Digital Service Infrastructures (DSIs). Web site: https://ec.europa.eu/inea/en/connecting-europe-facility

2.3.12.1 ABI

ABI Lab is Member of the INEA CEF Cyber Governance Board. National Representatives from the EU CERT community, members of the CEF Telecom funded projects, EU Comm representatives, ENISA, EU CERT members meet to discuss the on-going projects and the evolution of any issue related to the cybersecurity topic. The main purpose of the CEF Cyber DSI Governance Board is to provide an overarching governance body for all CEF Cyber Security DSI projects

2.3.13 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

2.3.13.1 UMA

UMA is part of two Technical Committees (TCs) of the IEEE Systems, Man, and Cybernetics Society (SMC): the TC on Homeland Security (TCHS) and the TC on Enterprise Information Systems (TCEIS). The former aims to promote and guide information systems, algorithm, and database research of relevance to international and national security; whilst TCEIS deals with fostering research, development, technical innovation, and international collaboration in the area of EIS/ES (Enterprise System) through a discipline framework as Industrial Information Integration Engineering.

Through these two committees, UMA benefits in many research aspects and especially in the cooperation with other entities and experts in the sector. Namely, the idea behind these two committees is to find the way to interact with academy and professionals in the area, exchange research ideas and collaborate in possible joint research projects, participate in primary international conferences and workshops to further network across academic and industry lines

for future research opportunities, establish relationships with HS/EIS professionals from different regions of the world, and facilite training, education and outreach programs.

2.3.14 TRUSTED COMPUTING GROUP (TCG)

"The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM), Trusted Network Communications (TNC) and network security and self-encrypting drives. TCG also has work groups to extend core concepts of trust into cloud security, virtualization and other platforms and computing services from the enterprise to the Internet of Things."

(Extract from TCG web site)

Web site: https://trustedcomputinggroup.org/

2.3.14.1 POLITO

POLITO is working within TCG to standardize various solutions related to trust anchors in virtualized environments, based on either full Virtual Machines or lightweight ones (such as containers). This work is in its initial phase but very hot given the current emphasis on virtualized infrastructures for computation, storage, and networking.

3 CONCLUSIONS, RECOMMENDATIONS AND NEXT STEPS

This deliverable is purely the initial snapshot of where we currently stand as CyberSec4Europe in relation to our contributions and efforts in Cybersecurity Standardisation and Certification. By showing how comprehensively we have covered the different areas Cybersec4Europe's potential to contribute to the development of Cybersecurity Standardization and Certification is clearly demonstrated. The second deliverable in this series will come much later in the project and will expand on it by reflecting the results from the efforts undertaken.

Already now one can see a growing global interest in cybersecurity standardization. This offers opportunities and challenges alike, as can be seen from the following example:

European countries, of which many were founders of e.g. ISO/IEC JTC 1/SC 27 and of which one country (Germany) is operating the Secretariat, can be happy, that SC 27 is one of the committees with the largest coverage over the world, so they invested early into a successful endeavour. However at the same time the growing interest, participation and influence of other countries, especially from Asia, poses a challenge and a wake-up-call to appropriately cover all projects in order to make sure that the European voice is heard. Practically, it is even harder for European national standardisation organisations to host meetings for the growing group, while e.g. Asian countries do not seem to have this problem. European joint support, as once given by ENISA may be needed more in future.

At the same time, European Standardisation is important also for the Common Market, but it should not reduce paying attention to global standardization.

4 List of Acronyms

4.1 List of acronyms of Consortium Partners

Acronym	Name of Consortium Partner
ABI	ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA
AIT	AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
ARCH	ARCHIMEDE SOLUTIONS SARL
ATOS	ATOS SPAIN SA
BBVA	BANCO BILBAO VIZCAYA ARGENTARIA SA*
BRNO	MASARYKOVA UNIVERZITA
C3P	UNIVERSIDADE DO PORTO
CNR	CONSIGLIO NAZIONALE DELLE RICERCHE
CONCEPT	CONCEPTIVITY SARL
CTI	INSTITOUTO TECHNOLOGIAS YPOLOGISTONKAI EKDOSEON DIOFANTOS
CYBER	CYBERNETICA AS
DAWEX	DAWEX SYSTEMS
DTU	DANMARKS TEKNISKE UNIVERSITET
ENG	ENGINEERING - INGEGNERIA INFORMATICA SPA
FORTH	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
GEN	COMUNE DI GENOVA
GUF	JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN
I-BP	INFORMATIQUE BANQUES POPULAIRES
ICITA	INTERNATIONAL CYBER INVESTIGATION TRAINING ACADEMY SDRUZHENIE
ISGS	INTESA SANPAOLO SPA
JAMK	JYVASKYLAN AMMATTIKORKEAKOULU
KAU	KARLSTADS UNIVERSITET
KUL	KATHOLIEKE UNIVERSITEIT LEUVEN
NEC	NEC LABORATORIES EUROPE GMBH
NTNU	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU
OASC	OPEN & AGILE SMART CITIES
POLITO	POLITECNICO DI TORINO

Acronym	Name of Consortium Partner
SIE	SIEMENS AKTIENGESELLSCHAFT
SINTEF	SINTEF AS
TDL	TRUST IN DIGITAL LIFE
TLEX	TIME.LEX
TUD	TECHNISCHE UNIVERSITEIT DELFT
UCD	UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN
UCY	UNIVERSITY OF CYPRUS
UM	UNIVERZA V MARIBORU
UMA	UNIVERSIDAD DE MALAGA
UMU	UNIVERSIDAD DE MURCIA
UNILU	UNIVERSITE DU LUXEMBOURG
UNITN	UNIVERSITA DEGLI STUDI DI TRENTO
UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER
UPS-IRIT	UNIVERSITE PAUL SABATIER TOULOUSE III
VAF	VaF, S. R. O.
VTT	TEKNOLOGIAN TUKIMUSKESKUS VTT Oy

4.2 List of Acronyms (other than Consortium partners listed in Section 4.1)

Acronym	Name
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
CD	Committee Draft
CEF	Connecting Europe Facility
CEG	Cyber Expert Group
CIM	Context Information Management
DIS	Draft International Standard
DSI	Digital Service Infrastructure
DLT	Distributed Ledger Technologies
DPM	Data Processing and Managemen
EBF	European Banking Federation
ECSO	European Cyber Security Organization
ENISA	European Union Agency for Cybersecurity

Acronym	Name
EPC	European Payments Council
ETSI	European Telecommunications Standards Institute
EUROPOL	European Union Agency for Law Enforcement Cooperation
FDIS	Final Draft International Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIF	International Institute of Finance
INEA	Innovation and Networks Innovation Agency
IS	International Standard
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITU	International Telecommunications Union
JTC	Joint Technical Committee
JWG	Joint Working Group
LD	Linked Data
LoRaWAN	Long Range Wide Area Network
LSP	Large Scale Pilots
NGSI	Next Generation Services Interface
NIST	National Institute of Standards and Technology
OMA	Open Mobile Alliance
PDTR	Preliminary Draft Technical Report
PDTS	Preliminary Draft Technical Specification
SDO	Standards Developing Organizations
SEPA	Single Euro Payments Area
SG	Study Group
TCG	Trusted Computing Group
TNC	Trusted Network Communications
TPM	Trusted Platform Module
TR	Technical Report
TS	Technical Specification
WD	Working Draft
WG	Working Group