EUROPEAN GAPS & PRIORITIES IN THE CYBERSECURITY DOMAIN HOW STANDICT.EU SUCCESSFUL APPLICANTS ARE CONTRIBUTING TO FILL THE VOID AND TO DEVELOP CYBER-RELATED STANDARDS

Authored By

Trust-IT Services

Date: 24th June 2019

Project Partners of StandICT.eu
Trust-IT Services & FraunHofer SCAI

This report was produced by the StandICT.eu, a partner in the project (7804391) is a Coordination and Support Action (CSA) co-funded by the European Commission under the Research and Innovation Framework Programme, Framework Programme Horizon 2020 (H2020).

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Commission and may not be held responsible for the use which may be made of the information contained therein. Reproduction is authorised provided the source is acknowledged

Executive Summary

The StandICT.eu initiative covers key ICT Standardisation priority areas with further focus on specific vertical sectors. The Call topics follow predominantly the 5 main domains of the European Digital Single Market as well as the priority areas as outlined in the **2019 Rolling Plan for ICT Standardisation** and its future updates.

Cybersecurity is one of the pillars where a major focus will be steered in 2019 by StandICT.eu following the EC attempt to step up Cybersecurity within the whole European Union and efficiently tackle the raising concern coming from citizens and industry. The investment that the European Union is putting in place to ensure a reliable level of cyber-safety and to prevent cyber threats can rely on relevant numbers:

"Consumer representatives are now active in ETSI TC CYBER and ISO PC 317 'Consumer protection: privacy by design for consumer goods and services' thanks to the StandICT project. It is key to be able to count on such sources of funding. The recruitment of consumer experts in the ICT field is very challenging because of the technical aspect of the work."

- **+660** Centres of Cybersecurity expertise across EU
- **+60.000** Cybersecurity companies in EU
- Expected **+10%** annual market growth rate
- **€30 millions**: the overall Cybersecurity Market value in 2020

The EU continuously works on many fronts to strengthen cybersecurity and cyber resilience. It has an advanced **cybersecurity regulatory framework** in place (comprising the *EU Cybersecurity Act* and the *Network & Information Security Directive*).

So, how can StandICT.eu give its contribution with a view to build this solid defensive scheme?

StandICT.eu intends to effectively capitalise on the vast experience of its Cybersecurity experts. The scope of this document is to highlight the outcomes and activities of the 5 most successful applications in the field of Cybersecurity in order to clearly understand which are the main European Gaps & Priorities tackled and how these people are tangibly contributing to the development of determined Standards (or supporting the related Working Groups). The document is organised under the following main priority sections:

- Principal field of activity of the experts
- ICT Challenges addressed in the Standardisation Area
- Making a Difference
- Identifying Best Practices
- Future Actions of Further specifications work necessary

Table of Contents

Glossary

Acronym	Definition
CEN/CLC	CEN and CENELEC
IEEE	Institute of Electrical and Electronics Engineers
WG	Working Group
SDO	Standards Developing Organisation
JTC	Joint Technical Committee

Principal Fields of Activity

- Personal data protection and cybersecurity
- Blockchain and Distributed Ledger system, Cybersecurity/DLT/Blockchain
- Security evaluation, models, information security/ cybersecurity risk management & IT Security & Methodology for IT Security evaluation
- Cryptographic techniques and Blockchain standards & Development of a common framework for Cybersecurity & Blockchain Standards
- Security System and Video-Surveillance (ICT Challenges addressed in the Standardisation Arena & Privacy Management in Products & Services

Making a Difference

Setting new and effective standards on lightweight evaluation methodologies suitable to the IoT world security would be the European contribution to better cybersecurity as a whole. The potential benefits of the IoT and other digital services and systems can only be achieved only if products and services are designed with trust, privacy and security built in, so consumers feel they are secure and safe to use.

All applications or systems has to perform a standard security checklist to maximize their safety as much as possible. Internal policies and procedures have to be built in existing or new companies. All employees during the execution of their respective works have a big part of responsibility. It's a global task not only dedicated to IT staff in charge to maintain the network or code the application/system. The adoption of these **mutually agreed checklist and guidelines** will be a crucial step further for each company's cyber safety.

In the SD12 case (*ISO/IEC JTC 1/SC 27 Standing Document No. 12 on the Assessment of Cryptographic Techniques and Key Lengths*), the document has been updated from several years without any modification. This is helping not only people who is implementing standards or involved in certification process, but also delivering open and free knowledge to everybody who has a question related to crypto standards, think on utilities, manufacturers, service providers.

Recommendations

Work is still under way to help overcome difficulties to share basic information, especially in urban and dense environments, but a suggestion going forward would be to proceed in combining:

- The creation of a dedicated transverse CEN/CENELEC WG with this sole objective (the recently created CEN/CENELEC Sector Forum on Security could be one of the sponsors thereof) and
- Establishing a **cooperation with the Open Geospatial Consortium (OGC)** and/or ISO TC 211 Geographic Information/Geomatics in charge of geographic representation, which have started to work on this matter.

Identifying Best Practices

Candidates supported the approval of ETSI TS 103 645 "Cyber Security for Consumer Internet of Things". It is proposed to transpose TS 103 645 on consumer IoT security into an EN. It is essential that the standard respects the European rules on personal data protection and the security. It is possible that the standard will be used in the context of the European Cybersecurity Act

The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required. Devices and services have to be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it, when the consumer wishes to remove a service from the device and/or when the consumer wishes to dispose of the device.

- *Follow an onboarding / offboarding checklist* - This checklist should contain a list of all the steps everyone need to enforce when an employee, contractor, intern joins/leaves a company.
  https://about.gitlab.com/handbook/general-onboarding/
  https://about.gitlab.com/handbook/offboarding/
- *Gamify security and train employees on a regular basis*
- *Run Security tests on your code* - Static Application Security Testing (SAST) is an easy and fast way to find security vulnerabilities in every code.
- *Go hack yourself* - If a company does not have yet a structured security team, help create a multidisciplinary Red Team to strengthen the whole and infrastructure.

Few national cybersecurity schemes are using security evaluation methodologies which represents a simplified approach of the Common Criteria, for example:

- Dutch Baseline Security Product Assessment (BSPA)
- French Certification de Sécurité de Premier Niveau (CSPN)
- Spanish Certificación Nacional Esencial de Seguridad (LINCE)

These methodologies result in much faster and less expensive evaluations, however, with limited assurance. They are however much in line with the provisions of newly published EU Regulation on cybersecurity certification framework (the Cybersecurity Act).

ISO is the highest institution where national bodies representing each country participates on the development of new standards and comments. There are several point of view and initiatives. The commitment is to harmonize these visions in only one achieving high consensus.

Future Actions or Further Specifications work necessary

Development of a general standard procedure to be accurately defined at a later stage. Standardization is a powerful way for regulator as well to push the adoption.

Second call for contributions on "Lightweight cybersecurity evaluation methodologies" was issued by CEN/CLC/JTC13/WG3 (Security evaluation and assessment) with a deadline for submission on 05.07.2019. Inputs from expert will be considered at the JTC13/WG3 meeting on July 10th, with possible outcome in the shape of Draft European Standard.

SD5 and SD12 play an important role in this conservative world by allowing technology companies from diverse origins to transparently and securely transfer all control of their networks (including data access and data content) to their customers, allowing them to successfully overcome potential concerns regarding their origin.

Europe should take a leading paper on these standardization processes in order to protect their citizens and their market. We, as European experts, have to represent our countries' interests in WGs and Committees in order to ensure that cybersecurity is properly implemented and the security goals are achieved globally.

Over the last five years, the European Commission DG Home (as well as national authorities) has taken measures and launched research programs to improve the resilience of critical infrastructures to cyber-physical threats. Typically, as many hardware electronics subsystems have been replaced by small processor-based equivalents, intrusion in specialized IT systems may result in major incidents.

A good option today is to make sure that all the events detected (cyber or physical) are time-stamped at capture in UTC, to be able to combine a tree of possible causes with a strange occurrence of synchronized patterns to correlate events, eventually allowing to locate and neutralize the author of the attack.

Development of tools to help in such situations requires research (several relevant H2020 projects are already underway, but they may need to be alerted on the matter), before a dedicated standardization project is initiated in CEN/CLC JTC 13.

Recommendations

The ICT Standards should express security policies and procedures to help industrials to execute them internally. StandICT.eu (or similar projects) support will be critical to endure the participation of European experts in international standardisation.

Getting Engaged

How can you collaborate with StandICT.eu?

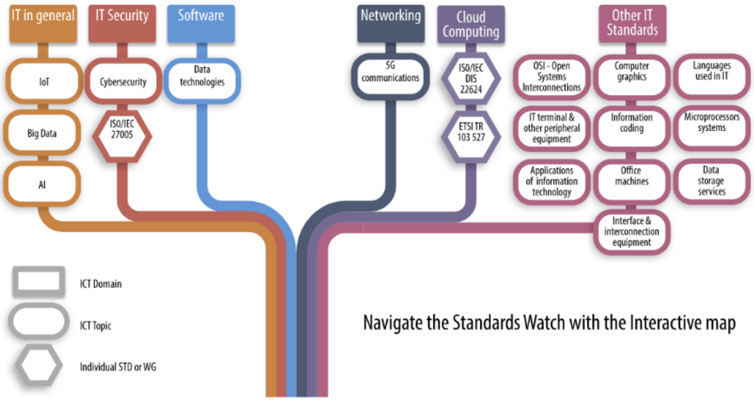
- Apply for a grant under the remaining **7th and 8th Open Call** to contribute to the development of Standards in the listed ICT priorities and to join the activities of WGs and Technical Committees of international SDOs.
  https://www.standict.eu/node/2076/

WORKING ON ICT STANDARDS?
Apply for funding through the 7th Open Call!
Deadline: 28 June 2019, 17:00 CEST
ROME
7
8
Open Calls

- Tell us what you are doing in ICT Standardisation!
  StandICT.eu boasts an "***ICT Standards Insights***" section to collect contributions

from experienced Standards Specialists in the priority areas as outlined in the 2019 ICT Rolling Plan on Standardisation.
Send us your insights to gain visibility through all main StandICT.eu channels.
https://www.standict.eu/ict-standards-insights

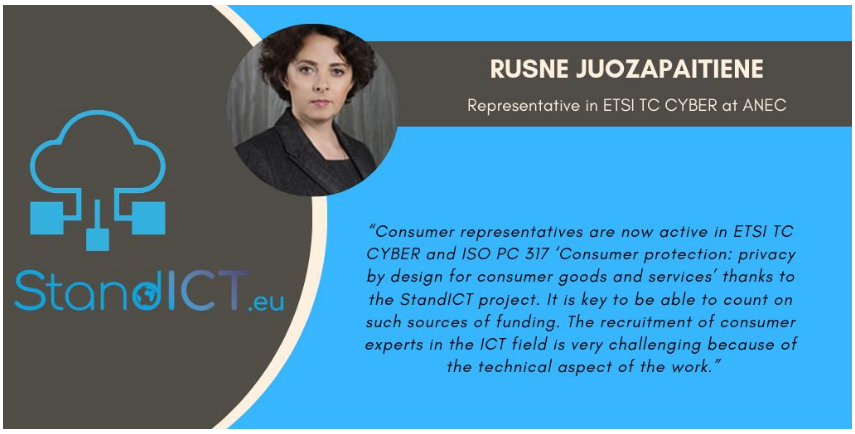
- **Standards Watch**
  The Standards Watch monitors the status of ICT standards
  at international level, mapping critical areas such as Cybersecurity, 5G, Cloud Computing, IoT, Big Data and Artificial Intelligence. Representatives may personally participate to the mapping of the Standards landscape through the "Wiki Watch" by leaving a message under the Standards related to their own field of experience. Throughout 2019 we are inviting all experts working on ICT Standardisation to actively contribute to the wiki watch to make the Standards Watch a truly useful tool for the Standards Community.
  https://www.standict.eu/standards-watch



Navigate the Standards Watch with the Interactive map

Annex 1 – List of ICT Standards Experts and SDOs involved in the content of the report

We would like to thank the following representatives who contributed to the following report with their insights

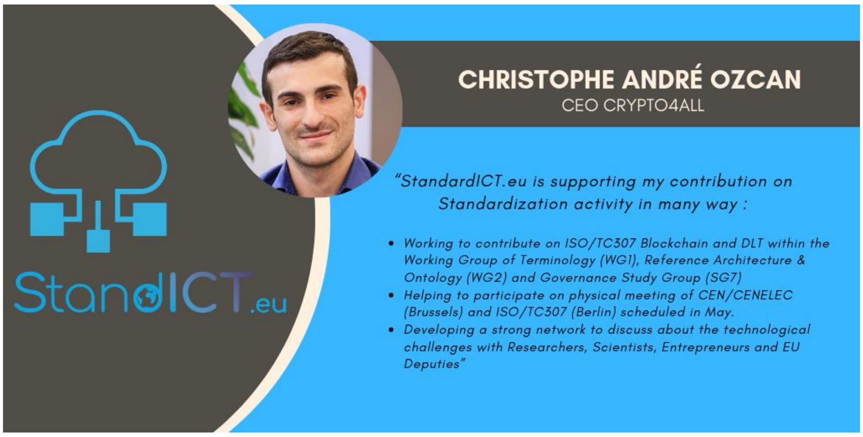


RUSNE JUOZAPAITIENE

Representative in ETSI TC CYBER at ANEC

"Consumer representatives are now active in ETSI TC CYBER and ISO PC 317 'Consumer protection: privacy by design for consumer goods and services' thanks to the StandICT project. It is key to be able to count on such sources of funding. The recruitment of consumer experts in the ICT field is very challenging because of the technical aspect of the work."

Rusne Huozapaitiene ETSI TC CYBER – ISO PC317



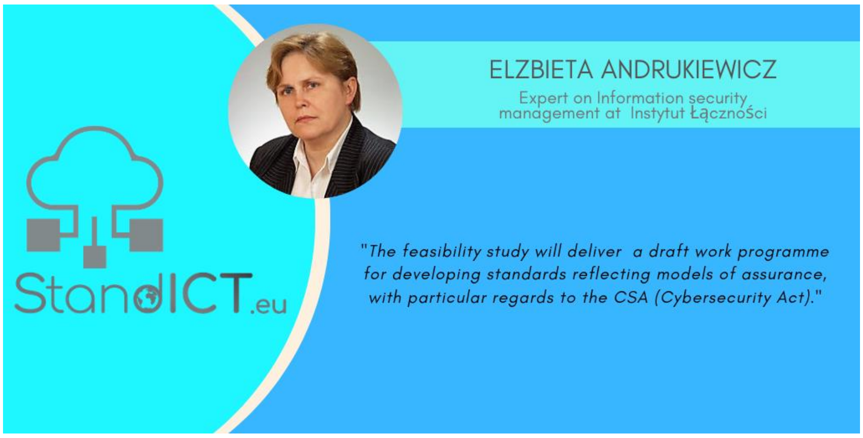
CHRISTOPHE ANDRÉ OZCAN

CEO CRYPTO4ALL

"StandardICT.eu is supporting my contribution on Standardization activity in many way :

- *Working to contribute on ISO/TC307 Blockchain and DLT within the Working Group of Terminology (WG1), Reference Architecture & Ontology (WG2) and Governance Study Group (SG7)*
- *Helping to participate on physical meeting of CEN/CENELEC (Brussels) and ISO/TC307 (Berlin) scheduled in May.*
- *Developing a strong network to discuss about the technological challenges with Researchers, Scientists, Entrepreneurs and EU Deputies"*

Christophe André Ozcan ISO/TC 307 - Blockchain and distributed ledger technologies



ELZBIETA ANDRUKIEWICZ

Expert on Information security management at Instytut Łączności

"The feasibility study will deliver a draft work programme for developing standards reflecting models of assurance, with particular regards to the CSA (Cybersecurity Act)."

Elzbieta Andrukiewicz CEN/CENELEC JTC 13 (Cybersecurity and data protection)

JEAN-FRANÇOIS SULZER

Independant consultant

"Standardizing the balance between CCTV-based security and Privacy-by-Design is the exciting citizen-centric challenge StandICT allows me to be part of! After 47 years in industry and being a 30-year veteran in standardization, it is a win-win situation where I can pass my experience to the younger skills."

Jean-Francois Sulzer

CEN/CLC/JTC Privacy management in products and services
IEC TC 79 Alarm and electronic security systems

Gerard Vidal - ***ISO/IEC SC27 WG2 (Cryptography and security mechanisms working group)***