European Standardization Organizations

Workshop ‘Interoperability of security'

We start at 10:00 CEST

21 April 2022

Your webinar moderator

Els Somers

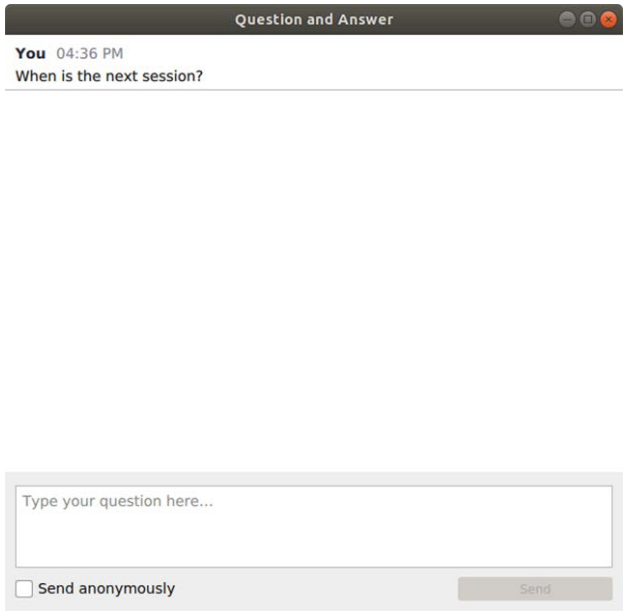
Project Manager

Policy & Partnerships

esomers@cencenelec.eu

Get the most out of the webinar today

- You are muted
- Use the Q&A panel to submit your questions



- Talk about us on Twitter #training4standards @Standards4EU

Agenda

- Introduction CEN and CENELEC
- What is interoperability of security?
- ENISA point of view
- Needs of DG Home – a concrete case
- View of DIN – CEN's German member
- Industry's point of view – Horizon 2020
- Wrap up
- Q&A

Your speakers today

Christina THORNGREEN
Project Manager ‘Energy & Living’
CEN-CENELEC
cthorngreen@cencenelec.eu

European Standardization Organizations

CEN - European Committee for Standardization

CENELEC - European Committee for Electrotechnical Standardization

ETSI - European Telecommunications Standards Institute

→ Recognized by European law (EU Regulation 1025/2012)

Standardization happens at different levels

- Aim: identical standards in Europe and worldwide

National

European

International

CEN and CENELEC deliverables

European Standards (EN)

Prime deliverable by excellence

Technical Specifications (TS)

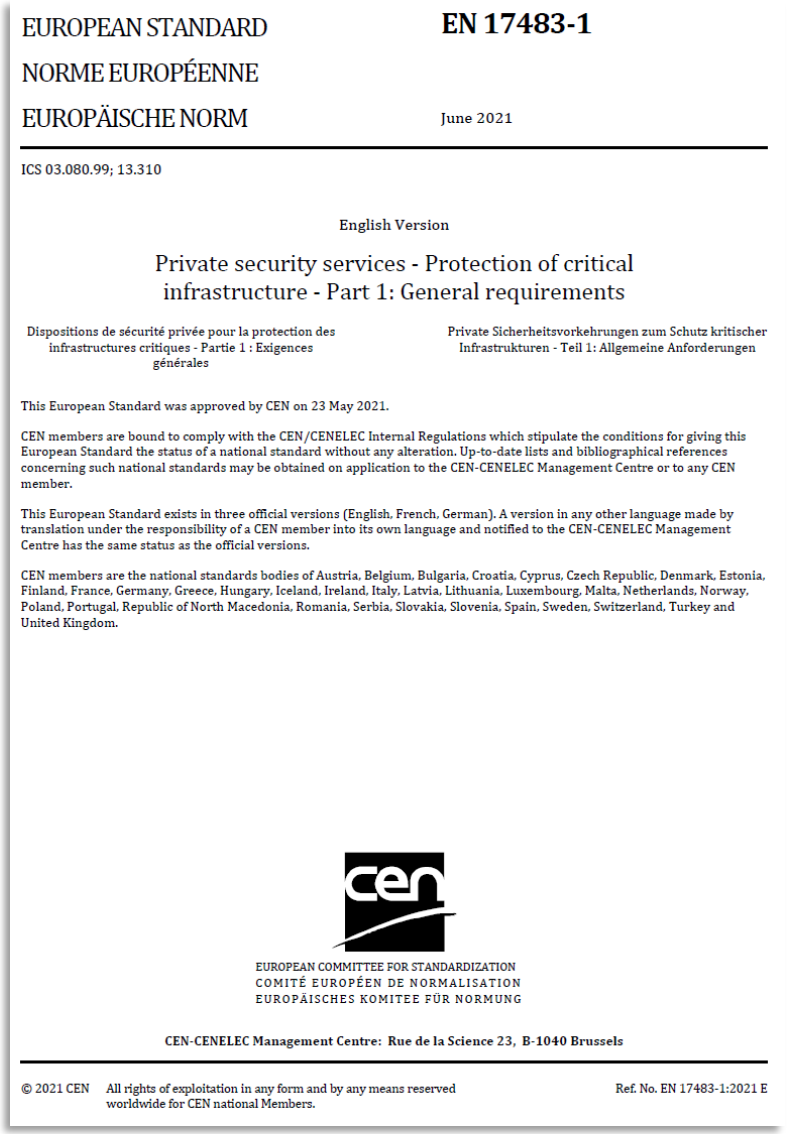
Pre-standard

Technical Reports (TR)

Informative document / Guide

Workshop Agreements (CWA)

Document, developed by a Workshop, which reflects an agreement between identified individuals and organizations responsible for its contents



EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 17483-1

June 2021

ICS 03.080.99; 13.310

English Version

Private security services - Protection of critical infrastructure - Part 1: General requirements

Dispositions de sécurité privée pour la protection des infrastructures critiques - Partie 1 : Exigences générales

Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen - Teil 1: Allgemeine Anforderungen

This European Standard was approved by CEN on 23 May 2021.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 17483-1:2021 E

CEN and CENELEC Sector Forum on Security

SECTOR FORUM ON SECURITY

- established in January 2019, SFS secretariat
- experts from different sectors of the security industry
- coordinates security-related standardization

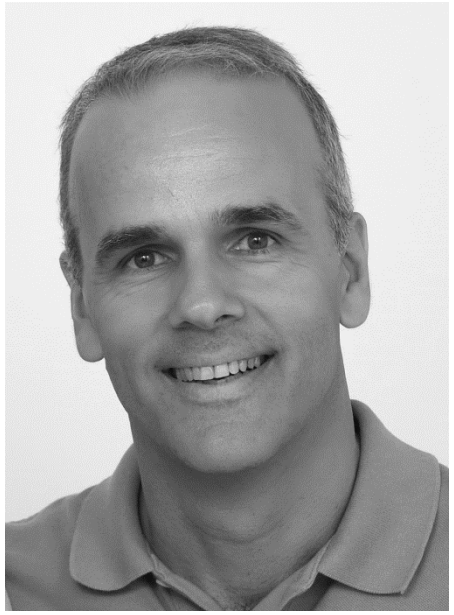
Your speakers today

Jean-Pierre QUÉMARD

CEO of KAT

a consulting company in digital and security technologies

Your speakers today



Dr. Andreas MITRAKAS

Head of Unit – Market, Certification & Standardisation

European Union Agency for Cybersecurity (ENISA)

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Interoperability in cybersecurity policy and standardisation

Dr. Andreas Mitrakas
Head of Unit, “Market, Certification & Standardisation”

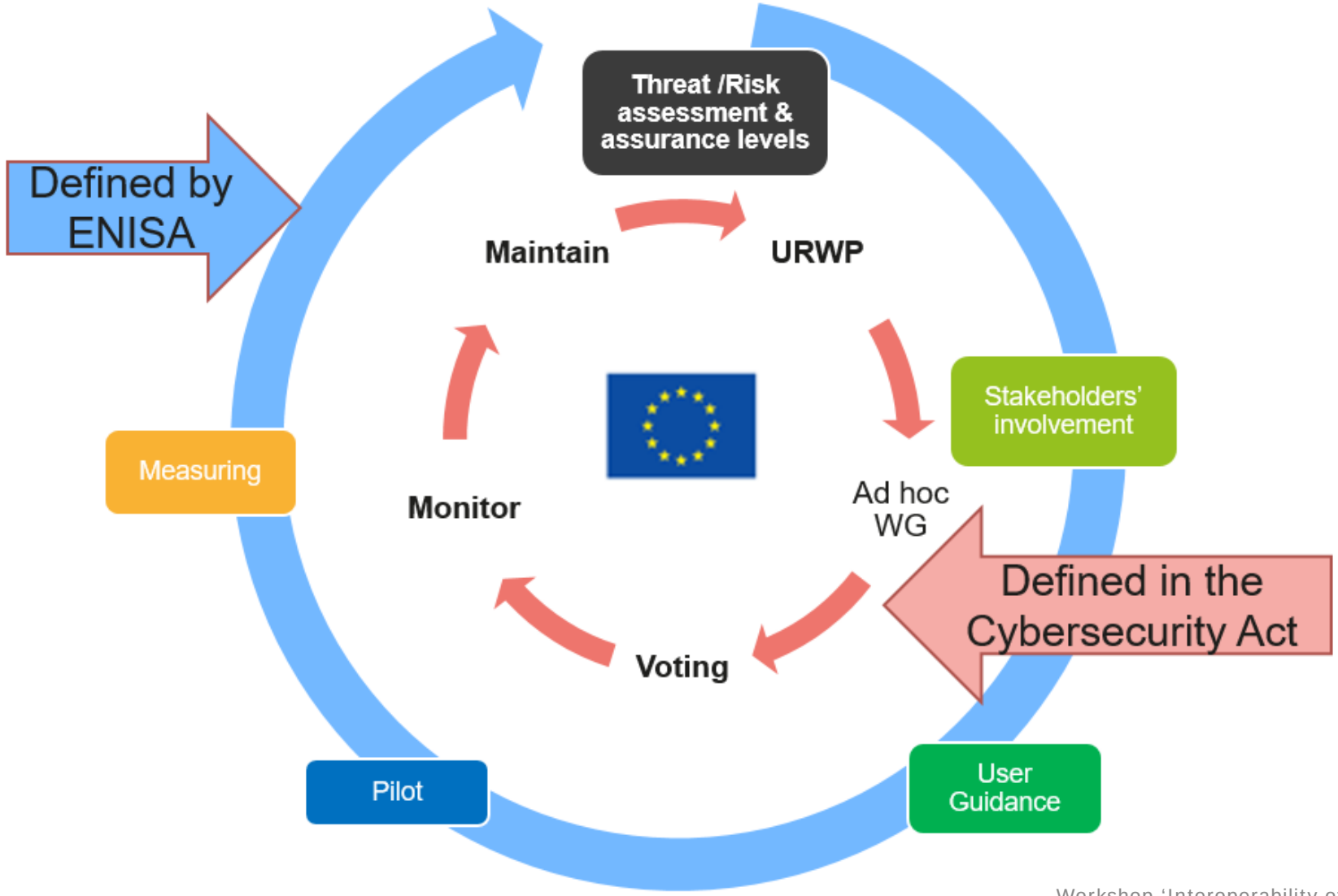
Interoperability and security
CEN CENELEC Security sector forum, Webinar

| 04 | 2021

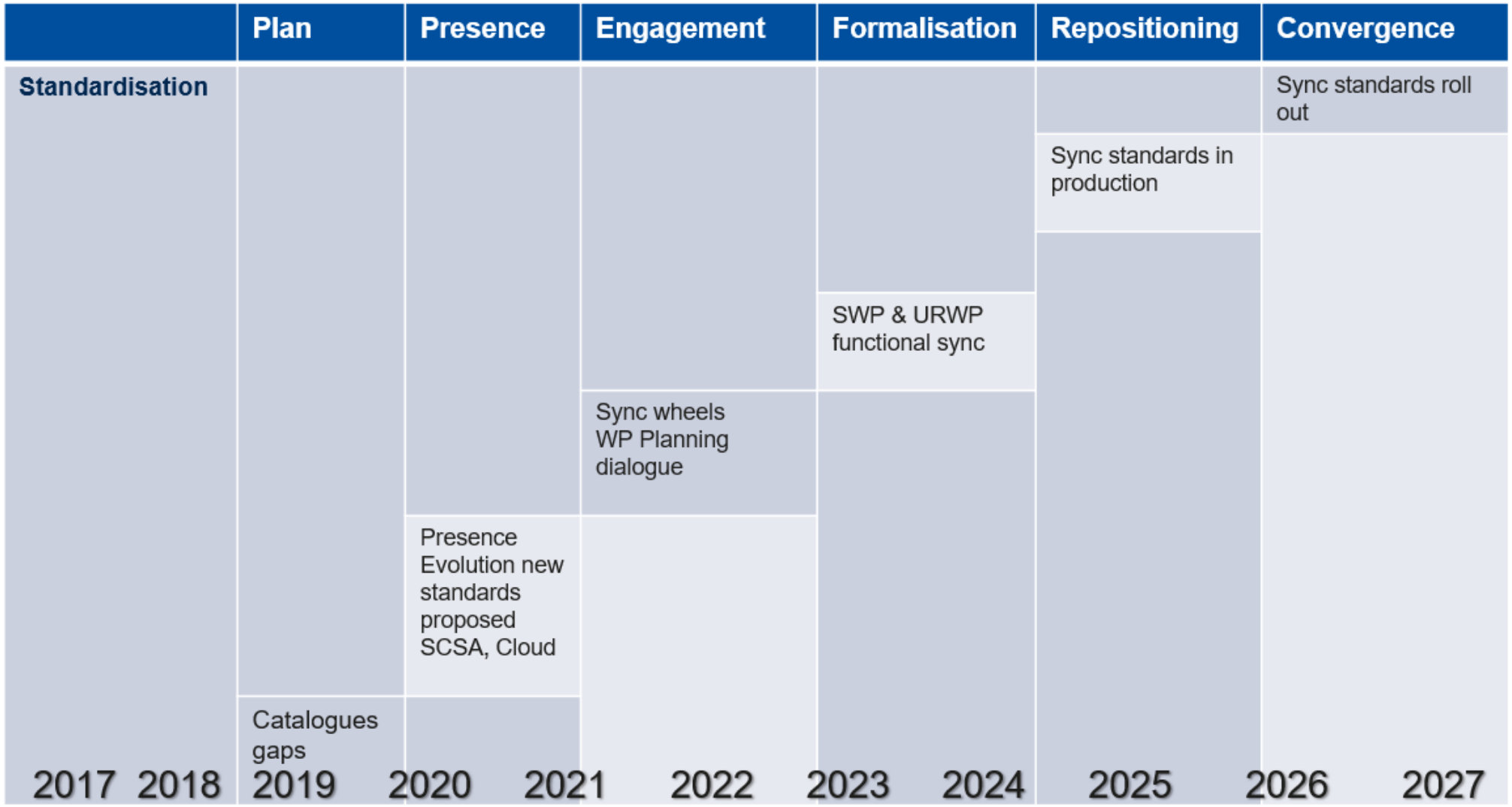
Agenda

- Certification scheme lifecycle
- Six stages of transformation: cohesive interoperability
- Cybersecurity standardisation

The circle of Trust: lifecycle of a scheme



Six stages of transformation



Dynamic approach to standardization

Influence stakeholders

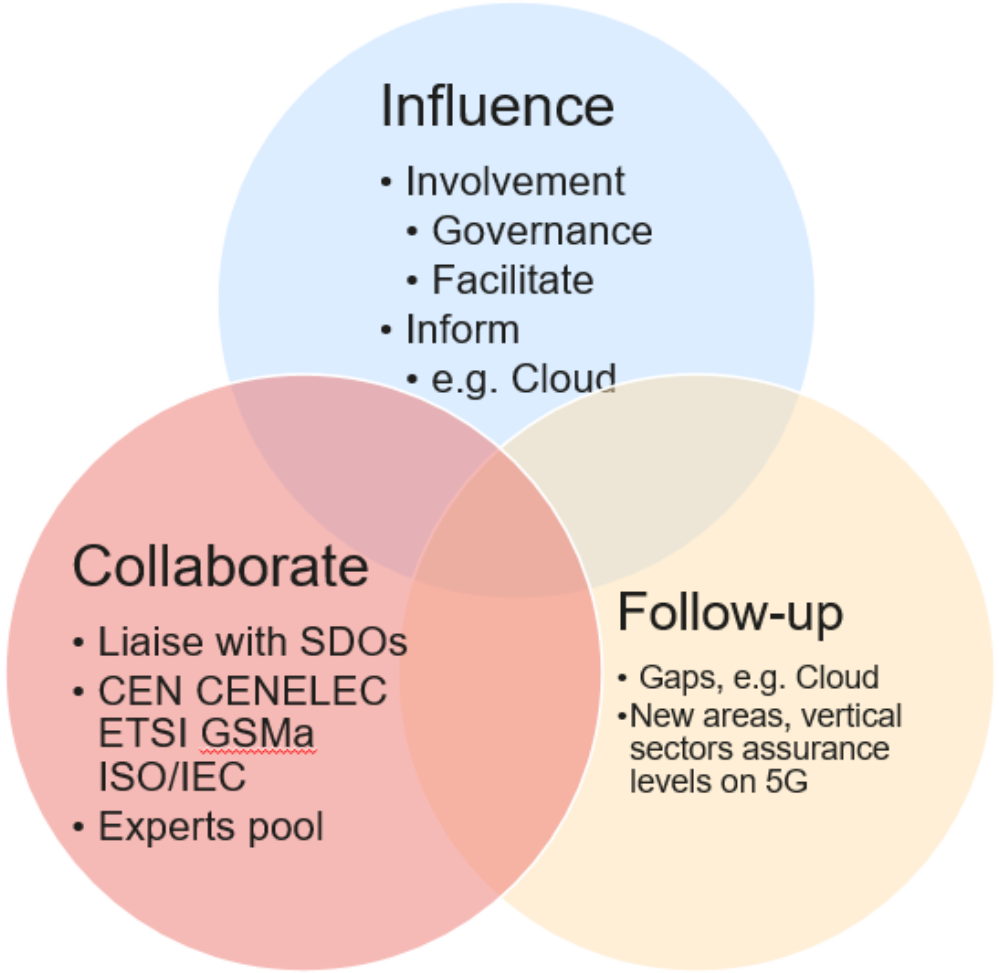
on key policy areas including cybersecurity certification

Collaborate with public interest and private stakeholders

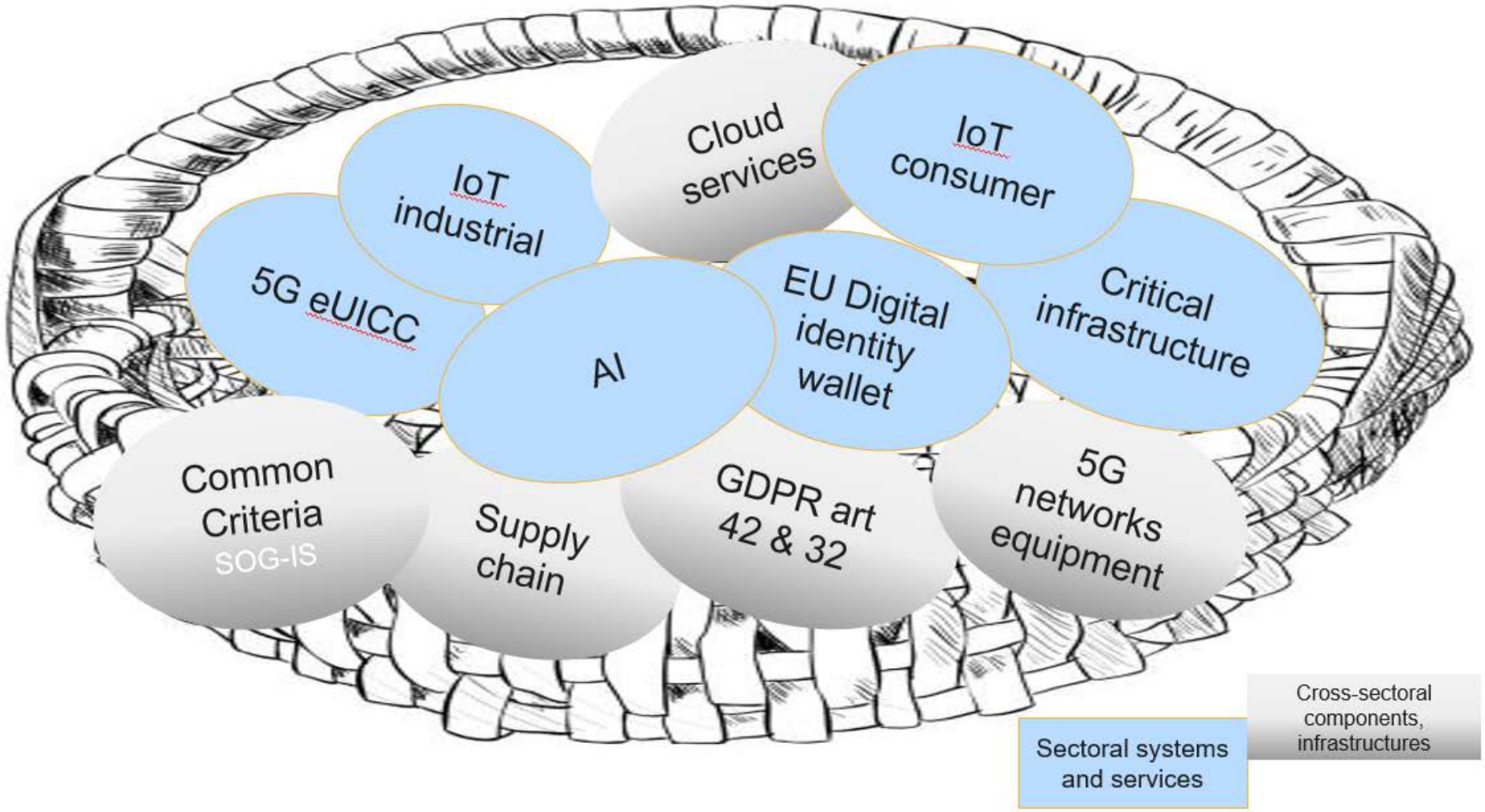
on the use and development of standards

Following up

On gaps and new content areas e.g. assurance level methodology



Eggs in a basket….



... and likely policy follow ups

Support the Commission at the EU cybersecurity standardisation policy level bringing in cross-policy cybersecurity insight

Develop relations with MS standardisation organisations

Collaborate on knowledge management and training on cybersecurity standardisation

Proactively pursue innovation goals with ECCC

Assist in translating legal requirements e.g. Rule of Law, to technical and organisational ones some for standardisation

THANK YOU FOR YOUR ATTENTION

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europe.eu

Your speakers today

Gilles ROBINE

DG Home

European Commission

Standardisation in support of the Security Union objectives

Gilles ROBINE
European Commission - DG HOME

Interoperability and security CEN CENELEC sector forum, Webinar

21 / 04 / 2022

Agenda

Standardization in support of EU Security Policy

Challenges ahead in the field of cyber investigation

A concrete case: lawful interception and lawful access to retained data

Standardisation in support of EU Security Policy

Standards are key to ensure **availability** and **adequacy** of the measures deployed to face emerging threats by:

- contributing to a strong EU security market,
- ensuring a uniform quality in the provision of security services throughout the EU territory,
- facilitating joint actions at and within the EU borders,
- enabling future proof and tech neutral EU legislations (e.g. RED directive, AI Act, etc..)

Challenges in the field of digital investigation

- More than **90% of investigations** require access to digital evidence
- Investigators need to **find, access, read** and **process** digital evidence,
- All these actions are heavily impacted by EU legislations:

  Find: Child Sexual Abuse online,

  Access & read: E-evidence, e-Privacy regulation, Digital Services Act, Data Act

  Process: AI Act

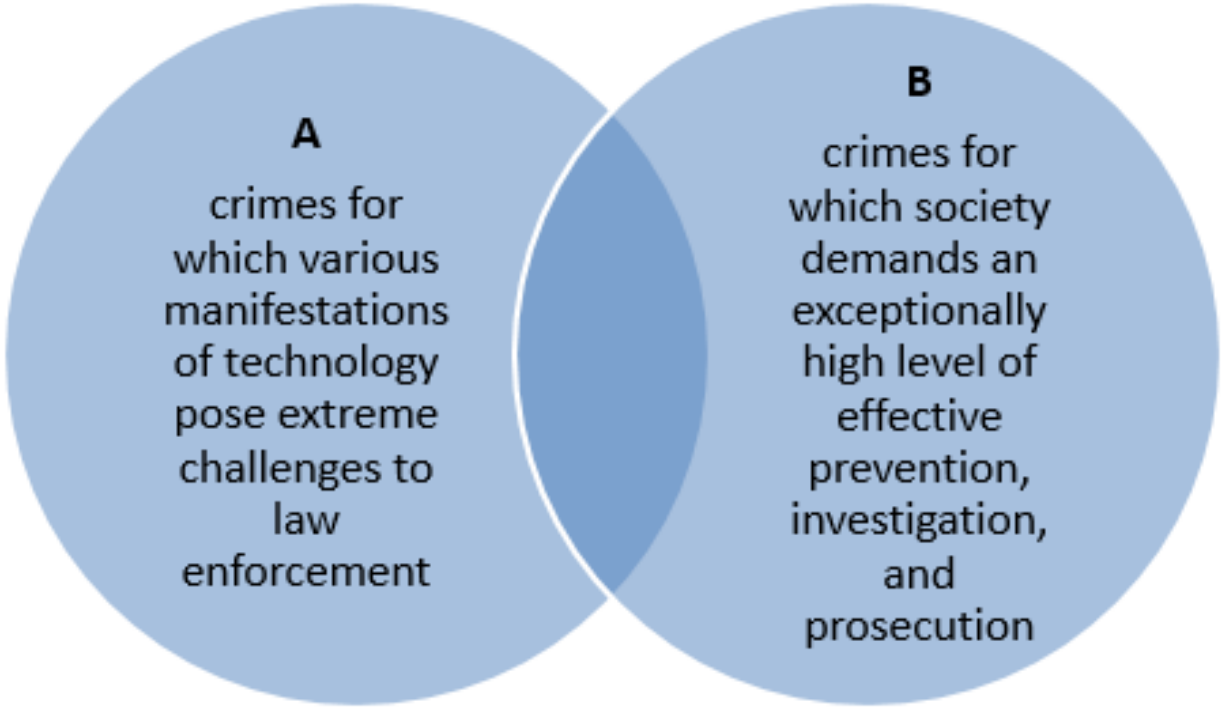
  All: cybersecurity related regulations

…that are (or should be !) supported by standards

More challenges related to technology

- Security through encryption, security despite encryption (see E2EE)
- Privacy by design, lawful access comes after (see 5G)
- Geolocation of data and territoriality issues
- IoTs including vehicule forensics,
- Vehicle to vehicule/infrastructure (V2X)
- Edge computing

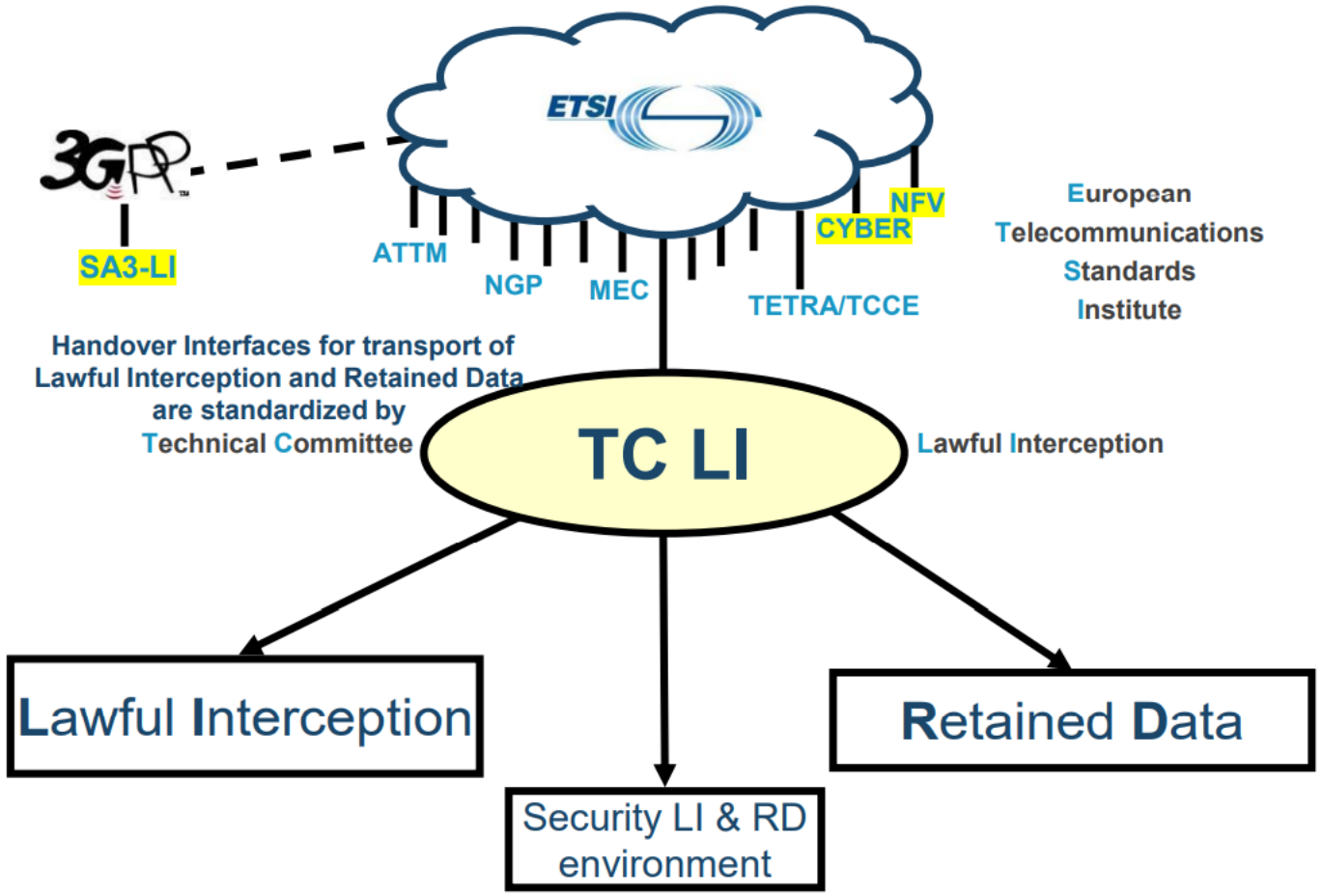
Operational challenges



The '**Going Dark**' Phenomenon

Focus on lawful interception and lawful access

LI in ETSI



C1 Public

Focus on lawful interception and lawful access

- Has to deal with enhanced security and privacy requirements (e.g. Subscriber Concealed Identifier),
- Has to deal with (possibly) encrypted VoIP (N9HR – Home Routing)
- Has to deal with E2EE application level communication providers

Thank you for your attention

gilles.robine@ec.europa.eu

Security in the Digital Age

DG HOME

European Commission

Your speakers today

Benjamin HELFRITZ

DIN, Deutsches Institut für Normung

CEN-CENELEC Security sector forum - Interoperability of Security

interoperability just will come through horizontal activities

reducing the fragmentation on several levels definitions / involvement / regulation

Benjamin Helfritz

Fragmented field – the issue security

- security is not only a digital issue (digital and physical aspects)
- security as a part of information technology / digitalisation is a sector overarching issue
- security is a issue of maximal increasing importance (high pressure)
- security is a issue of several interest groups (economically & governmental)
- security is not safety - but it is a protection goal of our time
- security experts are rare
- several security interest groups are not familiar with standardisation or typical ways of regulation (NLF)
- security is not only a question of security experts
- security is a holistic issue and partly extremely complex
- developing „system innovations“ is a extraordinary new challenge
- the digitalisation and security is a new field – the cake is still not distributed
- the regulation is late

Fragmented field – the issue security

- security is not only a digital issue (digital and physical aspects)
- security as a part of information technology / digitalisation is a sector overarching issue
- security is a
- security is a
- security is n
- security exp
- several secu
- security is n
- security is a
- developing „
- the digitalisa
- the regulation is late

▶THE RESULT

→ wide and high fragmented field of activities
→ high fragmentation of definitions and solution findings
→ critical fragmentation of expert- and stakeholder involvement
→ critical fragmentation of regulation

ineffective and inefficient handling of the topic

Fragmented field – the issue security

Regulation

- NIS
- GDPR
- Sector Directives (NLF)
- CSA
- Cyber Resilience Act
- …

Governm.

- DG Connect
- DG Grow
- DG Home
- …
- BMI
- BMWK
- BMDV
- …

Standardisation / Solution Activ.

- Classical Standardisation Bodies
- Additional Standardisation Organizations (W3C, IEEE, ...)
- Consortial Standardisation
- CSA Schemes

Economical

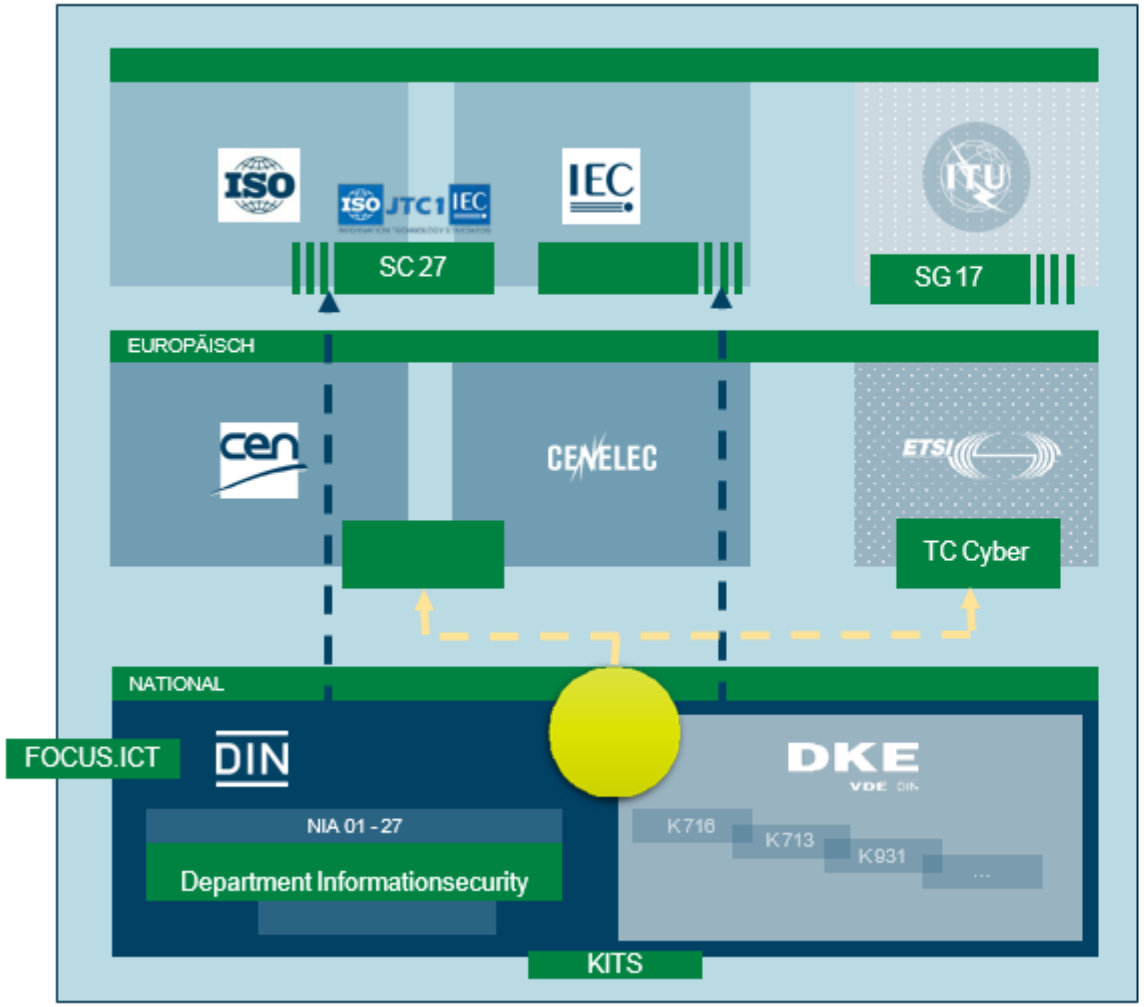
- Security experts
- Integrator
- Producers
- Users
- …

Fragmented field – the issue security

Reducing the fragmentation

→ shaping the organisational level

Shaping the organisational level



Standardisation

2005 → DE - Presidial Commitee FOCUS.ICT

2011 → DE - Coordination Office Cybersecurity

2018 → EU - JTC 13

2021 → DE on EU - DIN-DKE Panel

2022 → DE Department Informationsecurity

Shaping the organizational level

Standardisation

2005 → DE - Presidial Commitee FOCUS.ICT

2011 → DE - Coordination Office Cybersecurity

2018 → EU - JTC 13

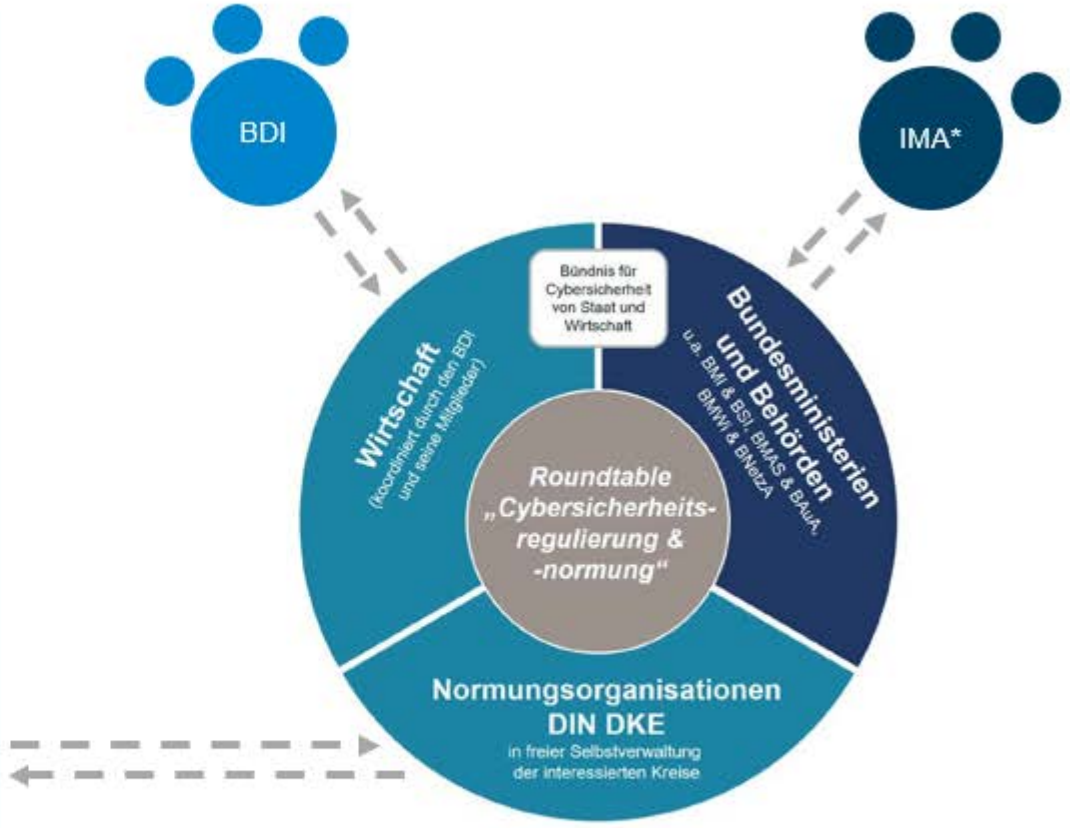
2021 → DE on EU - DIN-DKE Panel

2022 → DE Department Informationsecurity

Stakeholder

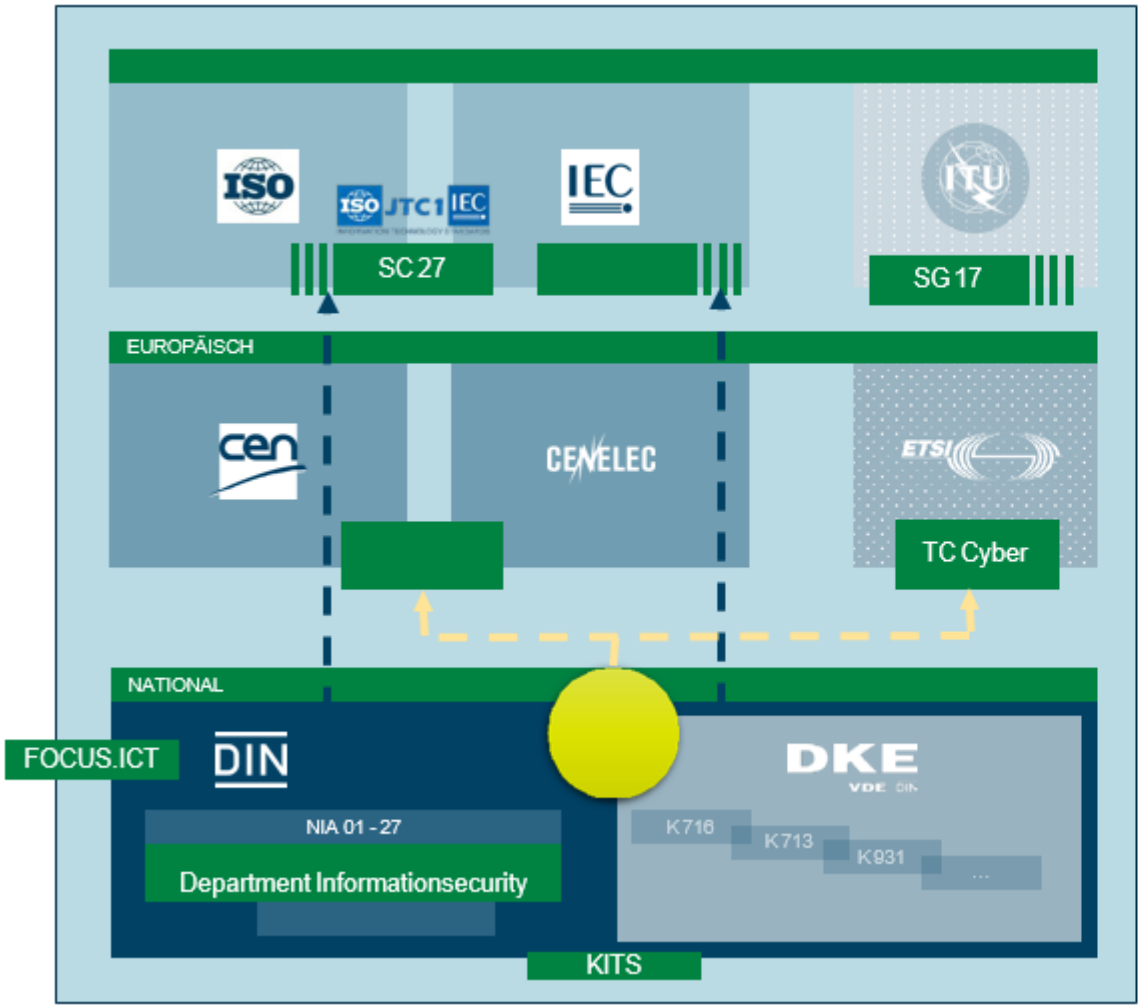
2021 → Interministerial Commitee

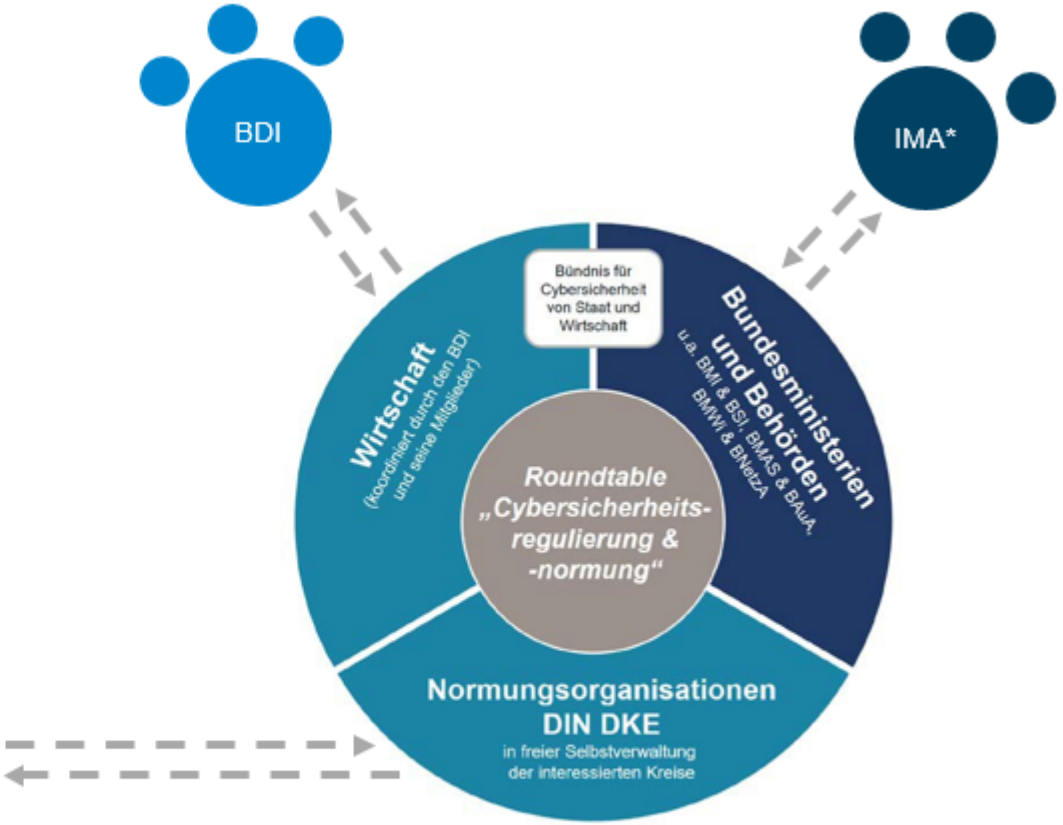
2022 → Stakeholder Dialouge



*IMA = Interministerieller Ausschuss IKT Standardisierung Fokus Cybersicherheit

Shaping the organizational level



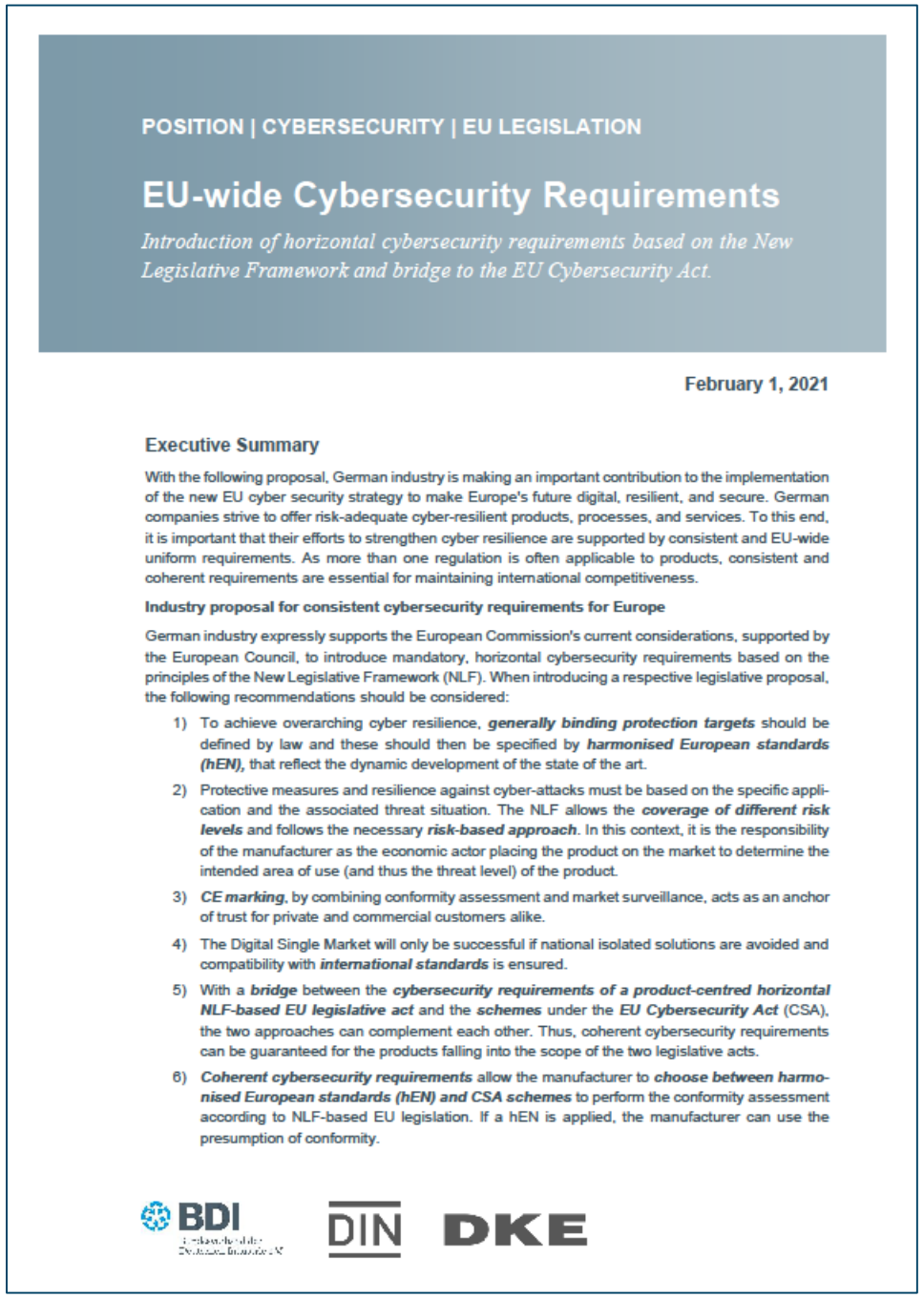


*IMA = Interministerieller Ausschuss IKT Standardisierung Fokus Cybersicherheit

Fragmented field – the issue security

Reducing the fragmentation

→ contributions on possible regulation



POSITION | CYBERSECURITY | EU LEGISLATION

EU-wide Cybersecurity Requirements

Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act.

February 1, 2021

Executive Summary

With the following proposal, German industry is making an important contribution to the implementation of the new EU cyber security strategy to make Europe's future digital, resilient, and secure. German companies strive to offer risk-adequate cyber-resilient products, processes, and services. To this end, it is important that their efforts to strengthen cyber resilience are supported by consistent and EU-wide uniform requirements. As more than one regulation is often applicable to products, consistent and coherent requirements are essential for maintaining international competitiveness.

Industry proposal for consistent cybersecurity requirements for Europe

German industry expressly supports the European Commission's current considerations, supported by the European Council, to introduce mandatory, horizontal cybersecurity requirements based on the principles of the New Legislative Framework (NLF). When introducing a respective legislative proposal, the following recommendations should be considered:

1) To achieve overarching cyber resilience, ***generally binding protection targets*** should be defined by law and these should then be specified by ***harmonised European standards (hEN),*** that reflect the dynamic development of the state of the art.
2) Protective measures and resilience against cyber-attacks must be based on the specific application and the associated threat situation. The NLF allows the ***coverage of different risk levels*** and follows the necessary ***risk-based approach***. In this context, it is the responsibility of the manufacturer as the economic actor placing the product on the market to determine the intended area of use (and thus the threat level) of the product.
3) ***CE marking***, by combining conformity assessment and market surveillance, acts as an anchor of trust for private and commercial customers alike.
4) The Digital Single Market will only be successful if national isolated solutions are avoided and compatibility with ***international standards*** is ensured.
5) With a ***bridge*** between the ***cybersecurity requirements of a product-centred horizontal NLF-based EU legislative act*** and the ***schemes*** under the ***EU Cybersecurity Act*** (CSA), the two approaches can complement each other. Thus, coherent cybersecurity requirements can be guaranteed for the products falling into the scope of the two legislative acts.
6) ***Coherent cybersecurity requirements*** allow the manufacturer to ***choose between harmonised European standards (hEN) and CSA schemes*** to perform the conformity assessment according to NLF-based EU legislation. If a hEN is applied, the manufacturer can use the presumption of conformity.

BDI DIN DKE

DIN

CEN CENELEC

FOCUS.ICT

EU-wide Cybersecurity Requirements

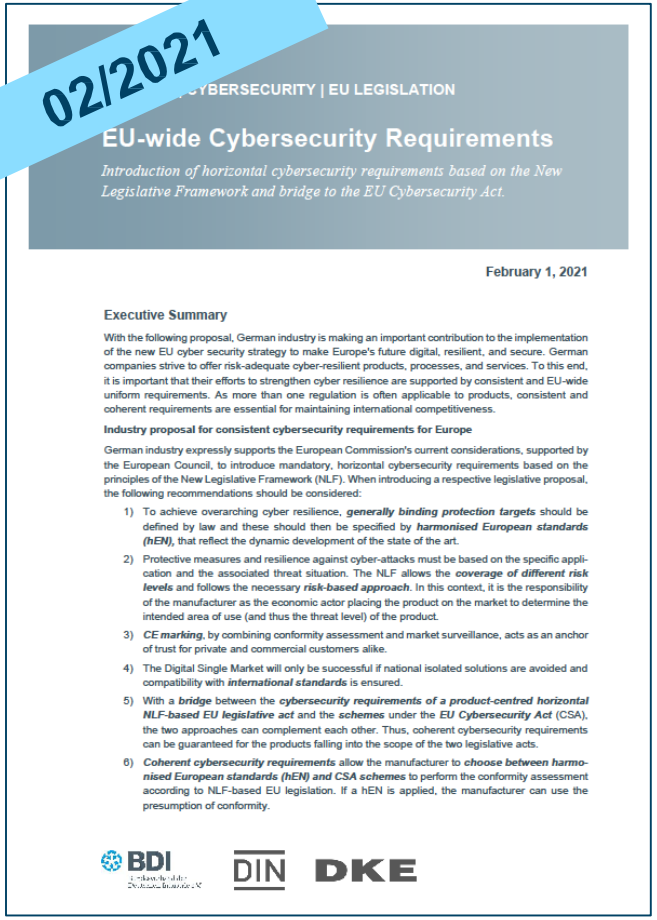
Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act.

(issued 2. February 2021)

http://www.din.de/go/eu-cybersecurity

Avoid fragmentation on the regulational level

02/2021



CYBERSECURITY | EU LEGISLATION

EU-wide Cybersecurity Requirements

Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act.

February 1, 2021

Executive Summary

With the following proposal, German industry is making an important contribution to the implementation of the new EU cyber security strategy to make Europe's future digital, resilient, and secure. German companies strive to offer risk-adequate cyber-resilient products, processes, and services. To this end, it is important that their efforts to strengthen cyber resilience are supported by consistent and EU-wide uniform requirements. As more than one regulation is often applicable to products, consistent and coherent requirements are essential for maintaining international competitiveness.

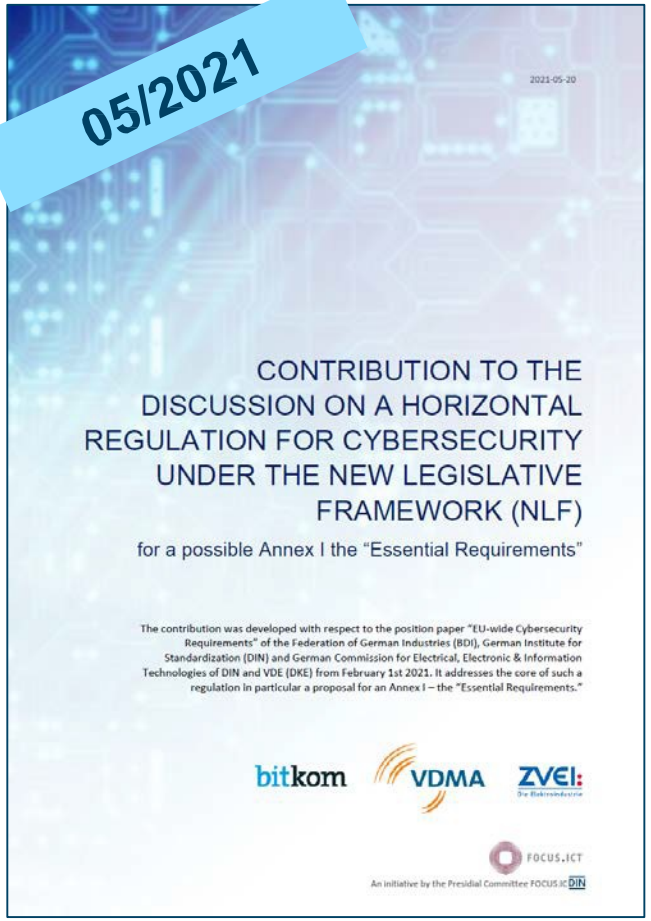
Industry proposal for consistent cybersecurity requirements for Europe

German industry expressly supports the European Commission's current considerations, supported by the European Council, to introduce mandatory, horizontal cybersecurity requirements based on the principles of the New Legislative Framework (NLF). When introducing a respective legislative proposal, the following recommendations should be considered:

1) To achieve overarching cyber resilience, ***generally binding protection targets*** should be defined by law and these should then be specified by ***harmonised European standards (hEN),*** that reflect the dynamic development of the state of the art.
2) Protective measures and resilience against cyber-attacks must be based on the specific application and the associated threat situation. The NLF allows the ***coverage of different risk levels*** and follows the necessary ***risk-based approach***. In this context, it is the responsibility of the manufacturer as the economic actor placing the product on the market to determine the intended area of use (and thus the threat level) of the product.
3) ***CE marking***, by combining conformity assessment and market surveillance, acts as an anchor of trust for private and commercial customers alike.
4) The Digital Single Market will only be successful if national isolated solutions are avoided and compatibility with ***international standards*** is ensured.
5) With a ***bridge*** between the ***cybersecurity requirements of a product-centred horizontal NLF-based EU legislative act*** and the ***schemes*** under the ***EU Cybersecurity Act*** (CSA), the two approaches can complement each other. Thus, coherent cybersecurity requirements can be guaranteed for the products falling into the scope of the two legislative acts.
6) ***Coherent cybersecurity requirements*** allow the manufacturer to ***choose between harmonised European standards (hEN) and CSA schemes*** to perform the conformity assessment according to NLF-based EU legislation. If a hEN is applied, the manufacturer can use the presumption of conformity.

BDI DIN DKE

05/2021



2021-05-20

CONTRIBUTION TO THE DISCUSSION ON A HORIZONTAL REGULATION FOR CYBERSECURITY UNDER THE NEW LEGISLATIVE FRAMEWORK (NLF)

for a possible Annex I the "Essential Requirements"

The contribution was developed with respect to the position paper "EU-wide Cybersecurity Requirements" of the Federation of German Industries (BDI), German Institute for Standardization (DIN) and German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (DKE) from February 1st 2021. It addresses the core of such a regulation in particular a proposal for an Annex I – the "Essential Requirements."

bitkom VDMA ZVEI

FOCUS.ICT

An initiative by the Presidial Committee FOCUS.ICT DIN

02/2022

2022-02-28

CONTRIBUTION TO THE DISCUSSION ON THE UPCOMING CYBER RESILIENCE ACT UNDER THE NEW LEGISLATIVE FRAMEWORK (NLF)

for a possible assignment of Conformity Assessment Procedures

The contribution was developed complementary to the Contribution to Essential Requirements in a Horizontal Regulation for Cybersecurity under the NLF - by BITKOM, VDMA, ZVEI from 20. May 2021.

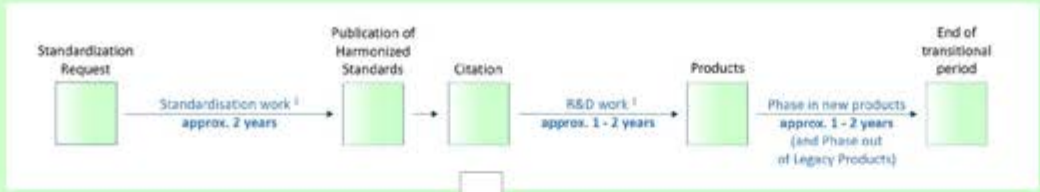
bitkom VDMA ZVEI

FOCUS.ICT

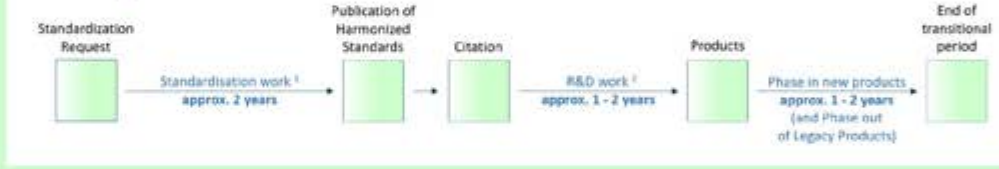
An initiative by the Presidial Committee FOCUS.ICT of DIN

Avoid fragmentation on the regulational level

NLF
RED
CS del. acts



NLF
Horizontal
CS regulation



CSA

NLF-CSA-Bridge

Fragmented field – the issue security

Reducing the fragmentation

→ A community mission

Benjamin Helfritz
Project Coordinator
External Relations
DIN
Deutsches Institut für Normung

benjamin.helfritz@din.de
+49 30 2601-2791

DIN
Deutsches Institut für Normung e. V.
Saatwinkler Damm 42/43
13627 Berlin

www.din.de

Your speakers today

Dr. Aikaterini POUSTOURLI

Strategy H2020 Project

STRATEGY
Interoperability for crisis management

CEN-CENELEC Security sector forum (SF-SEC)
3rd Webinar on Interoperability

Interoperability of Security
Industry View

STRATEGY Project

Dr. Aikaterini POUSTOURLI

(STRATEGY‘s and Satways Ltd. Liaison to CEN/TC 391 and ISO/TC 292 WG3)

Date: 21/04/2022

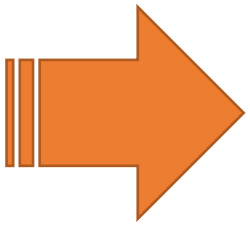
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 883520. This communication material reflects only the authors' view and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

WHO: Project Overview

- SU-DRS03-2019 topic: Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)
- Duration: September 2020 – August 2023
- Overall budget: €6.833.075.00
- EU contribution: €5.997.293,25
- Requested funding: *funded as requested*
- Consortium: **23 partners** across 14 European Countries
- *National Standardisation Bodies (5 entities – ASI/AT, SFS/FIN, UNE/ES, ASRO/RO, SIS/SWE)*
- *End-users (6 public bodies, including fire brigades, medical services, law enforcement, civil protection and command and control centres)*
- *SMEs (6) including the European Organisation for Security (EOS) and Industries*
- *RTOs (6)*
- Training, Testing and Validation Programme: At least 8 TTXs, 1 Full exercise, Interoperability events and standaridisation workshops.

WHAT: STRATEGY in a Nutshell

STRATEGY aims to contribute to the EU pre-standardization process through streamlining, testing and validating (in realistic environments) interoperability-related standardization items in systems and procedures addressing the operational needs of practitioners involved with Crisis Management.



8 Thematic Areas (Streams)

- Search and rescue
- Critical infrastructure protection
- Response planning
- Command and control
- Early warning and Rapid damage assessment
- Chemical, biological, radiological, nuclear and high-yield explosive (CBRN-E)
- Training
- Terminology/Symbology

WHAT: Interoperability

ISO 22300:2021(en) Security and resilience — Vocabulary,

interoperability (3.1.136) is the ability of diverse systems and organizations to work together

and from the single-entry point of view,

interoperability (3.1.137) is the ability of single-entry point to route queries for objects (3.1.161) carrying unique identifiers (UIDs) (3.2.44) to the responsible authoritative source (3.2.13) for trusted verification function (TVF) (3.2.43). Note 1 to entry: Interoperability includes the ability of multiple authentication systems to deliver similar responses to user groups.

To enhance better cross-border collaboration between different kinds of emergency services, attention should be given to interoperability and standardization.

European Commission's Joint Research Centre (JRC)-DRMKC - Disaster Risk Management Knowledge Centre-Science for Disaster Risk Management 2020:Acting Today, Protecting Tomorrow; The European Science and Technology Group (E-STAG); NATO Standardization Agreements (STANAGs); European Defence Standards Reference System (EDSTAR); Defense Standardization Program Office (DSPO)/U.S. Department of Defense (DoD); Institute of Electrical and Electronics Engineers (IEEE); ITU-T Study Groups; EOS, IFAFRI; UNDRR - Sendai Framework for Disaster Risk Reduction 2015-2030; Recommendations of UNECE, (United Nations Economic Commission for Europe); ….

WHAT: Interoperability

According to surveys and interviews conducted by several bodies, main barriers to data interoperability in Europe originate in the technical, economic and political domains, with prominent examples including lack of standardization, challenges in data disaggregation and restrictive data protection policies. Furthermore, data collected for specific purposes often lack the content, format or metadata needed for transfer and use in other contexts. Data interoperability affects all phases of the disaster risk management cycle from local to national and regional level.

European Commission's Joint Research Centre (JRC)-DRMKC - Disaster Risk Management Knowledge Centre-Science for Disaster Risk Management 2020:Acting Today, Protecting Tomorrow; The European Science and Technology Group (E-STAG); NATO Standardization Agreements (STANAGs); European Defence Standards Reference System (EDSTAR); Defense Standardization Program Office (DSPO)/U.S. Department of Defense (DoD); Institute of Electrical and Electronics Engineers (IEEE); ITU-T Study Groups; EOS, IFAFRI; UNDRR - Sendai Framework for Disaster Risk Reduction 2015-2030; Recommendations of UNECE, (United Nations Economic Commission for Europe); ….

WHY: Main Challenge

(Pre) Standardisation

Enhanced Interoperability

Effective and efficient crisis management

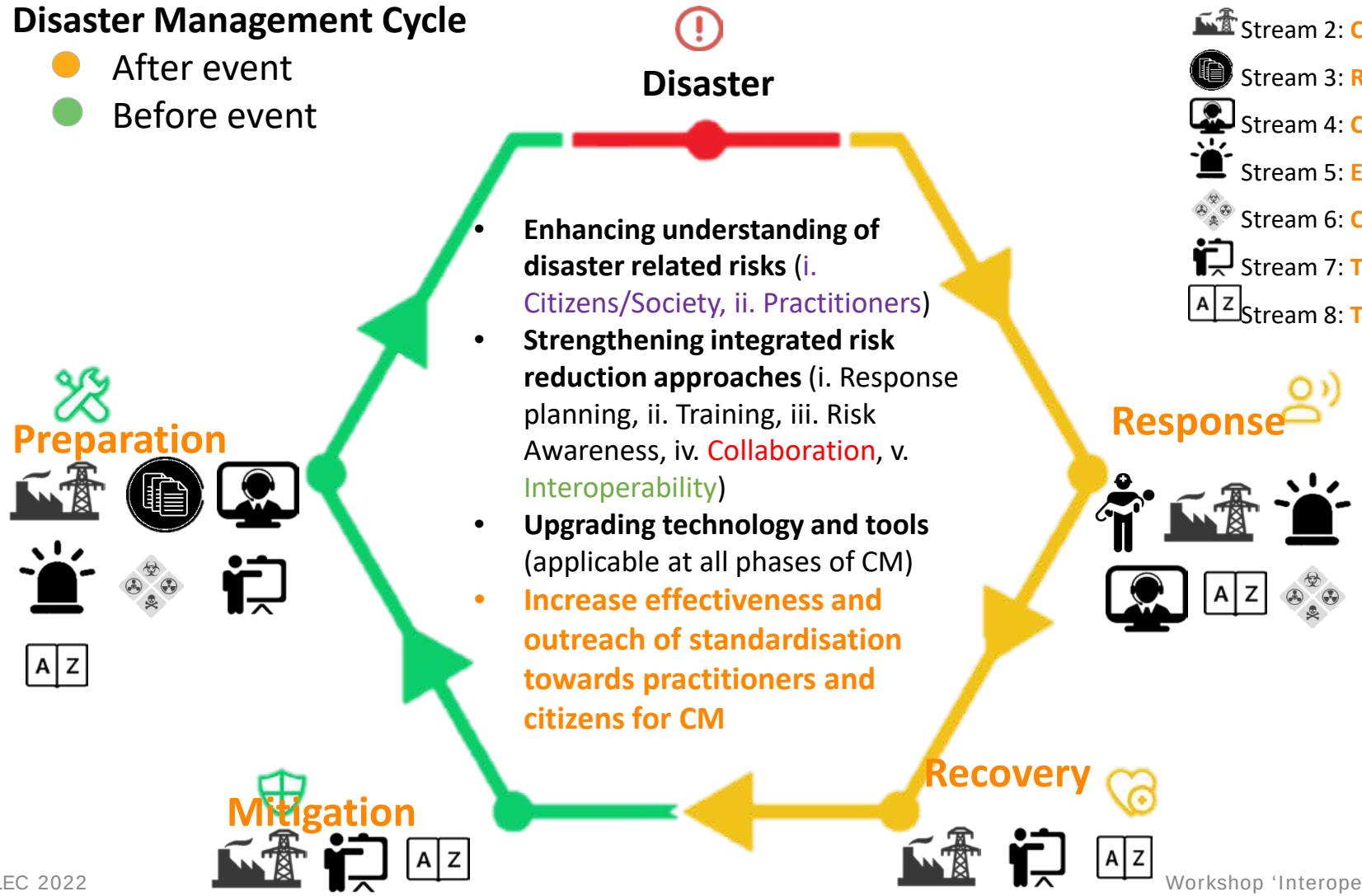
WHY: Some considerations

- **Interoperability,** as a **key feature** in **crisis management** systems and procedures, is still inefficient
- **Common standards** for emergency communication are missing
- **Lack** of **testing** and **validating standards in** organizational and technical **interoperability in realistic environments**
- **Crisis management systems** and their components **aren't standardized**
- **Familiarization** of operational communities **with** validated **pre-standardisation processes needs a persistent integration with NSBs and the Industry.**
- End users and small enterprises are **marginally involved** in the **standardization process**.
- **Long lasting pre-standardization processes** - **several work items under preparation** - **gaps in the standardisation funnel**
- National standardisation across the EU is progressing in different speeds
- **CEN Workshop Agreements** (CWAs) is a significant link between R&D and standardization. Their use needs to be maximized by all parties involved in the standardisation process.

What & where: main targets

Disaster Management Cycle

- After event
- Before event



Stream 1: **Search and rescue**

Stream 2: **Critical Infrastructures protection**

Stream 3: **Response planning**

Stream 4: **Command and control**

Stream 5: **Early warning and Rapid damage assessment**

Stream 6: **CBRN**

Stream 7: **Training**

Stream 8: **Terminology/Symbology**

How: Conceptual Methodology and WP Interaction

Investigate standardization universe across considered thematic streams

Identify standardization gaps within the considered thematic streams

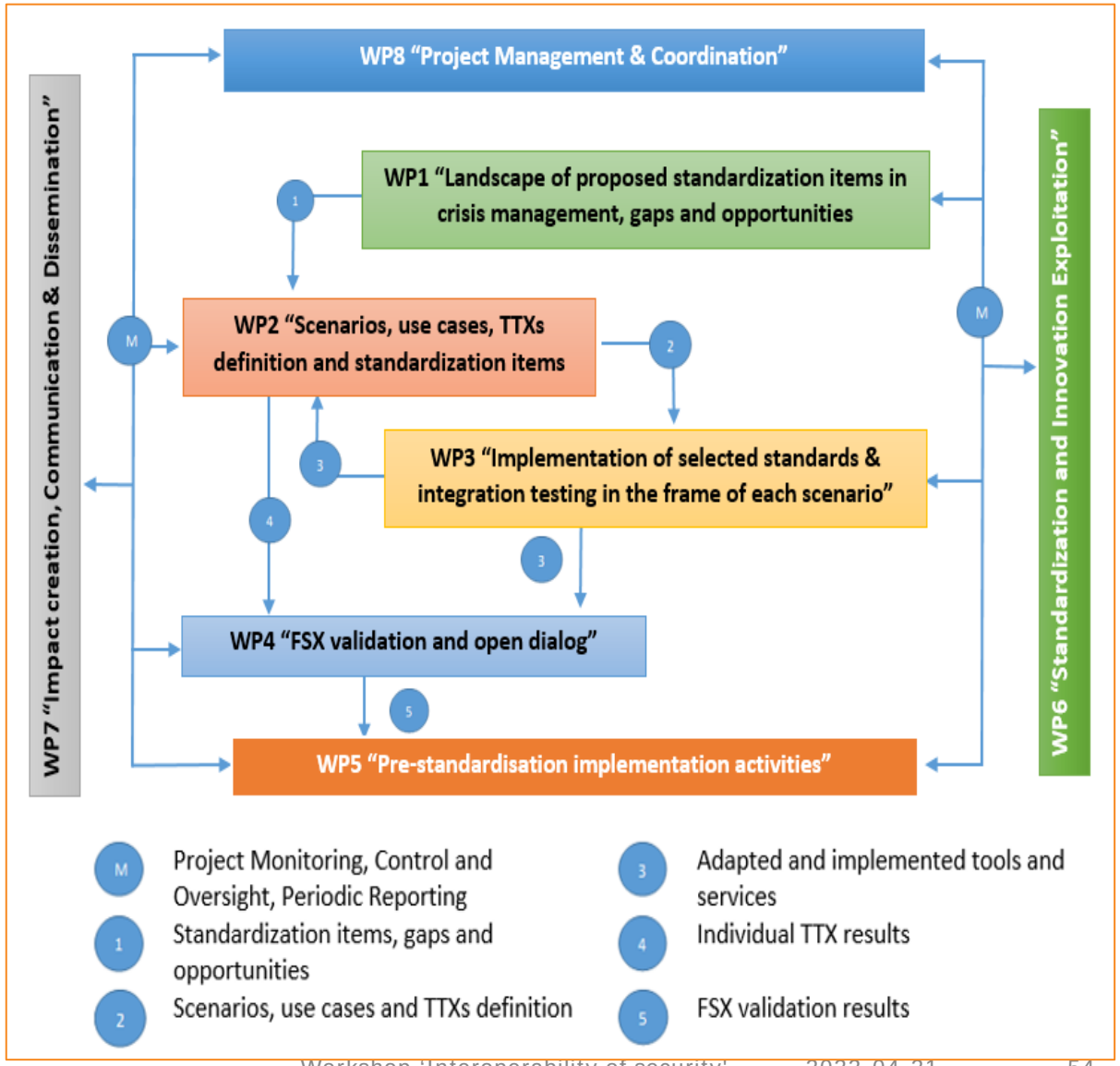
Prioritize standardization needs against identified gaps for each stream

Elaborate realistic use cases for each stream covering selected operational needs

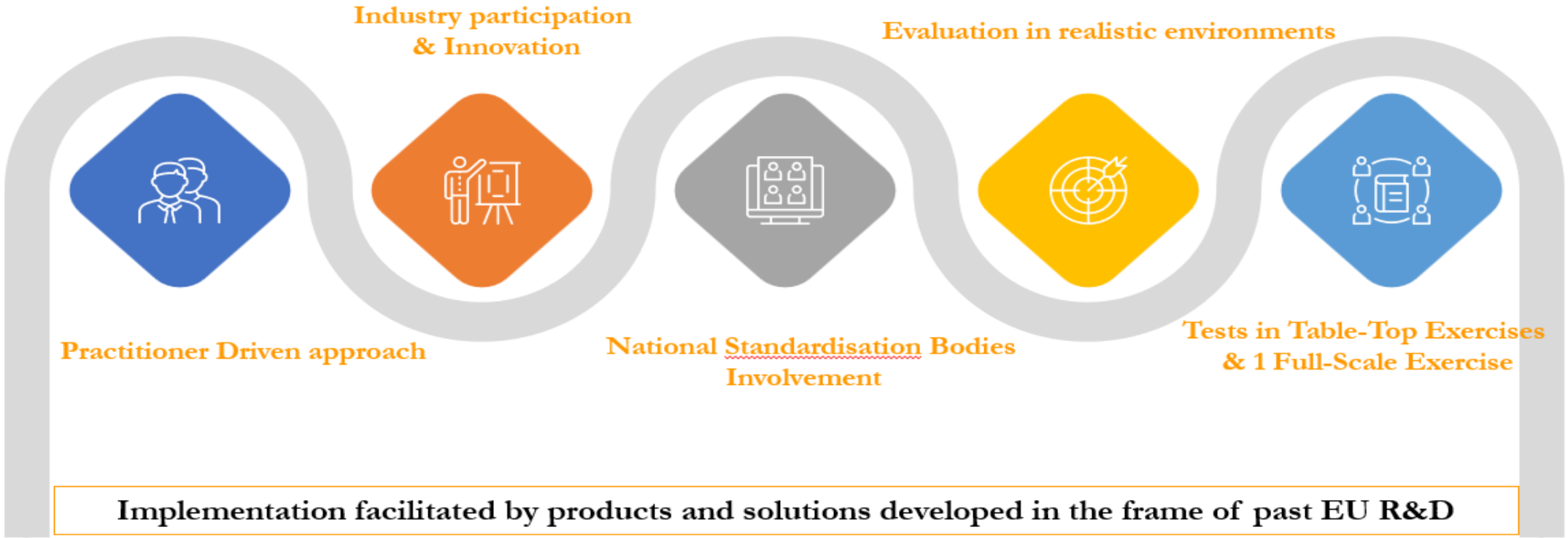
Implement (Pre) standardisation activities for each stream

Evaluate the (pre -)standardisation activities through TTXs and FSX

At least - 8 CWAs, 4 proposals for new items, draft one standard.



Why: Main Concepts … *behind methodology*



ISO/TC 292 WG3, Approved Liaison C (28-02-2022). Systematic Interaction-Provision of consolidated and compiled comments on the: ISO 22398 (ISO TC 292/WG 3 N 488) - Societal security — Guidelines for exercises ; ISO 22351 Message structure for exchange of information
CEN/TC 391, Liaison established (November 2021). Systematic Interaction-Provision of consolidated and compiled comments on the ISO 22324:2015 "Societal security — Emergency management — Guidelines for colour coded alerts"; prEN ISO 22361 "Security and resilience — Crisis management — Guidelines for a strategic capability".
STRATEGY is developing 11 CWAs and 2 TSs which falling within eight thematic areas (streams) of the crisis management cycle. The related proposals have been approved by the CEN/TC 391.

When: Summary of (Pre)Standardization Activity

11 CEN Workshops announced and / or in progress

Stream	CWA Title	Proposal Form Status	Project Plan Status	Kick off Meeting *	Planned TTX Date
5.1 Search & Rescue	Requirements for acquiring digital information from victims during Search and Rescue operations.	Approved	Submitted	14th March 2022 ☑	June 2022 (France)
5.2 Critical Infrastructures	Emergency management – Incident situational reporting for Critical Infrastructures.	Approved	Submitted	6th April 2022	7 June 2022 (Greece)
	Semantic layer definition and suitability of EDXL-CAP+EDXL-SitRep	Approved	Submitted	6th April 2022	7 June2022 (Greece)
5.3 Response Planning	Structuring the emergency response plans of public safety agencies focusing on incidents such as CBRN and waste disposal plants emergencies	Approved	Submitted	27th January 2022 ☑	8 June (Greece)
5.4 Command & Control	Collaborative Emergency Response – Communication and sharing of operational information among multiple public safety agencies	Approved	Submitted	18th February 2022 ☑	9 June (Greece)
	Management of forest fire incidents – SITAC-based symbology	Approved	Submitted	16th February 2022 ☑	9 June (Greece)
5.5 Early Warning	Guidelines for effective social media messages in crisis and disaster management	Approved	Submitted	21st March 2022 ☑	6 July (Netherlands)
	Emergency Management - Rapid damage assessment of buildings and alerting protocol	Approved	Submitted	22nd March 2022 ☑	7 July (Greece)
5.7 Training	Specifications for Digital Scenarios for Search and Rescue Exercises	Approved	Submitted	10th February 2022 ☑	May 2022 (France)
	Standardisation of Implementation Guidelines for evaluation and assessment reporting of exercises for crisis management	Approved	Submitted	8th February 2022 ☑	Along all TTXs
5.8 Terminology	Guidelines for the mapping of terminology and icons	Approved	Submitted	1st March 2022 ☑	TTX of 5.4, 5.5, 5.6

Technical Specification Documents (TS) –2 in progress

Stream	TS Title	First Draft Date	NWIP Form Date	Planned TTX Date
5.6 CBRN-E	Societal and citizen security — Electronic Chain of Custody for CBRNE events — Part 1: Overview and concepts	February 2022	March 2022	Oct2022
	Societal and citizen security — Electronic Chain of Custody for CBRNE events — Part 2: Data management and audit	February 2022	March 2022	Oct2022

** For further details on participation please visit the project site and/or the CEN-CENELEC portal*

When: Testing/Validation Tabletop Exercises (TTXs)

Aim

- Test the intermediate results of the CWA/TS elaboration process
- Receive feedback by end-users regarding applicability / benefits relevant to the operational exploitation of the elaborated (pre-) standardization items
- To identify areas for further improvement

Organisation

- Event(s) planned between May –October 2022
- Each stream item shall be tested in at least one TTX, in some case jointly with other streams
- Organization of TTXs is homogenously approached though XGM* methodology
- Preparations have been initiated
- To be attended by STRATEGY Partners and local / national / international stakeholders /experts

** based TGM methodology elaborated in DRIVER+ & adapted to the context of STRATEGY*

When: Testing/Validation Full Scale Exercises (FSX)

Aim

- To validate and provide a “proof of concept” regarding the (pre-) standards in realistic operational conditions and as much as possible with real assets.
- To showcase the interdependencies (where applicable) of different standardization streams and their applicability to multiple use cases and threat scenarios
- To collect feedback for supporting the evaluation and validation process of the crisis management standardization solutions and items.

Organisation

- Planned for later in spring 2023
- Will cover all steams based on a realistic operational CM scenario(s)
- Demonstrations will be performed – to the extend possible - with real physical systems and communications, operating on real data for the environmental conditions and realistic data (gathered from simulation and modelling tools) for the simulated disaster and its effects
- To be attended by STRATEGY Partners and local / national / international stakeholders and experts

Facilitating EU pre-standardization process through streamlining and validating interoperability in systems and procedures involved in the crisis management cycle

STRATEGY
Interoperability for crisis management

Get involved!

For more information visit

strategy-project.eu | @ strategy_eu | STRATEGY Project | info@strategy-project.eu

H2020-EU.3.7. - Secure societies - Protecting freedom and security of Europe and its citizens MAIN PROGRAMME
H2020-EU.3.7.5. - Increase Europe's resilience to crises and disasters
Topic(s), SU-DRS03-2018-2019-2020 - Pre-normative research and demonstration for disaster-resilient societies

Thank you for your attention

Any questions?

Presenter: Dr. Aikaterini POUSTOURLI

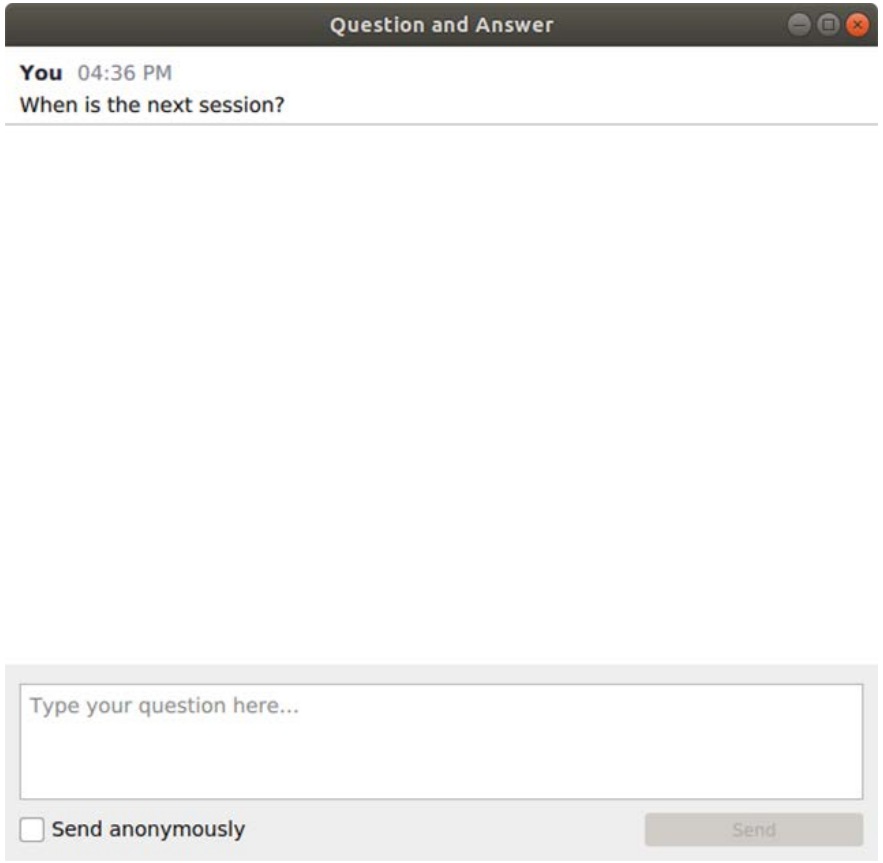
a.poustourli@satways.net

+30 210 6840036

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883520. This communication material reflects c
authors' view and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

Question time

- Use the Q&A panel to submit your questions



European Standardization Organizations

Thank you for your participation!

Next webinars

2022-05-23: Stakeholder Workshop ‘Standards For Climate: uptake of nature-based solutions in urban and rural areas’
2022-06-02: CEN-CENELEC Sector Forum PPE - Workshop "Smart PPE – standardization for design and use”

2022-06-08/09: Putting Science Into Standards workshop “Data quality requirements for inclusive, non-biased & trustworthy AI”