EUROSMART

The Voice of the Digital Security Industry

European Cybersecurity Competence Centres and its related Community

Proposal on primary missions

Eurosmart welcomes the European Commission proposal on creating a European Cybersecurity Competence center (ECCC) which would be backed by a dedicated network and a Community of accredited stakeholders. This initiative will enable the creation of a Community of expertise in Cybersecurity which will encompass the European industry, public authorities and research organisations. This initiative is more than necessary to consolidate the European Cybersecurity Digital Single Market and to develop the already well recognized European expertise and know-how in this area.

Even if the European Cybersecurity is globally recognized for its excellence, its attached ecosystem remains extremely weak compared to the 600 billion EUR global cybersecurity market. This situation put the European Digital Sovereignty at risks and for this reason, Eurosmart and its members expect from this initiative to help to increase the weight of this ecosystem both in qualitative and in quantitative terms. The European Union must be able to take advantage of its own digital assets and to make it (cyber)secure.

Eurosmart proposes the European Commission and the policy makers to take into consideration the following points as primary missions to be undertaken within the ECCC Community:

1. *On certification: Promote the benefits and encourage adoption of European Cybersecurity certifications amongst the Community members.*
2. *Disseminate the cybersecurity knowledge through dedicated formations to help the traditional European industry to take advantage of Cybersecurity innovations.*
3. *Nurture the SMEs’ expertise in the European Cybersecurity landscape.*
4. *Support the European standardisation strategy through the involvement of the Community and give a true consistency to the European Cybersecurity industrial policy.*

1. On the European Cybersecurity Certification approach

The European cybersecurity certification group contributes to the robustness of European cybersecurity products, services and processes. This certification framework coupled with the European Competence Center initiative constitute a real asset for the Union to make its cybersecurity products, services and processes at the forefront of the global market. This combined strategy will reverse the current tendency where, despite of its cybersecurity industrial capabilities, Europe largely depends on non-European providers.

Eurosmart expects from the policy maker to enhance the consistency between its qualitative certification approach as laid down in the Cybersecurity act and the expected increasing number of European actors who need to gain access to the cybersecurity certification process. Some initiatives are necessary to make the European Cybersecurity certification framework a real asset for the Cybersecurity industrial policy, Eurosmart recommend as follows:

1.1. Support the definition of Protection Profiles (PP) and high-level certification approaches

It is expected from the upcoming Cybersecurity Act and its related initiatives, to ensure a smooth transition of the current certification frameworks and more precisely of the SOG-IS to the new European one. The European Cybersecurity Competence Center and its Community could facilitate this transition and make the new SOG-IS 2.0 available to new actors. The ECCC could more specifically contribute to the definition of protection profiles for critical infrastructures which tackles domains as defined by the NIS Directive: energy, transport, banking, financial, health, water and digital infrastructures. These domains are the ones to be primarily concerned by the high-level certifications. The ECCC is the right place to host and support the definition of PPs by involving concerned stakeholders, expert from the industry, research and national security agencies.

The level “high” deserves a specific approach due to its sensitive nature. The ECCC could initiate a close and continuous cooperation amongst the Community Members involved in certification processes at level “high” (i.e. the EUCCG, PSG group, ENISA, EDPS, CERT-EU at EU level, the CERTs, the national authorities, industry and RTOs). The work undertaken by the Community shall pay attention to the way the CABs are accredited in order to ensure a homogeneous functioning of the certification process at this critical level.

1.2. Facilitate the definition of qualitative candidate schemes for the traditional European Industry at the level “Substantial”

To address the substantial level of cybersecurity certification, the ECCC community could design innovative certification approaches as a common ground for sectorial legislations such as electronic appliances, toys, cars and the current verticals currently which are usually covered by the Safety compliance, but which will be concerned by Cybersecurity issues. This strategy supported by the ECCC through relevant grants (Digital Europe, Horizon Europe programs) could bring together RTOs, Industry, experts. This community of various actors could take benefit from the innovative outcomes of the research in matter of certification, and thus, before the placing of new products and services on the European market. The supported and granted tasks could include:

- The definition of innovative candidate schemes according to the needs expressed by the Community with a sectorial approach;
- The definition of new evaluation methodologies by involving European CABs, industry and national agencies. This approach could help the Community members to take advantage of

the know-how on pentesting to increase the quality of the developed candidate schemes while tackling substantial level methodologies. The security level “substantial” should manly concern B2B context in Europe, which can address in the meantime critical infrastructures.

1.3.1.3 EU Cybersecurity level “basic”

The European Competence Center could be the right place to commonly define the basic requirement for the security level “basis”. This level will be an entry point for many market players which are not familiar with security requirements.

Some basic principles must be disseminated through the community to ensure that even the level “basic” provides a minimum of robustness for products, services and process.

In this field, Eurosmart advocates for including minimal cybersecurity features to prevent any unauthorised access, modification, or information disclosure. This basic assurance level should be usable as minimum requirements for all connected electronic devices, consumer electronics, or applications.

2. Dissemination of the European cybersecurity know-how to the traditional European industry and to the SMEs

Cybersecurity is everywhere and profoundly impact the way new products and services are designed. Currently, when developing a new product, traditional manufacturers are to deal with functional specifications, standards and conformity to demonstrate that products, services, or process comply with relevant EU safety legislations. With the increasing development of the IoT and IoTT (Internet of Thinking Things) market, cybersecurity is sometimes considered as an additional layer to the current question of safety and conformity.

The ECCC and the Cybersecurity funding programs could help the EU actors and especially the SMEs that lack of resources, to take the path of cybersecurity. The ECCC Community could create synergies through dedicated working groups and programs to better understanding cybersecurity issues when it comes to the development of new product and services. Eurosmart identified several missions that should be conferred to the ECCC:

2.1. Formation in Cybersecurity to companies

Concreate actions should be undertaken to train and inform all the EU market players about cybersecurity certifications when developing products and services. The goal is to span the gap between the safety and cybersecurity “mindsets”.

Within the companies, quality departments manage traditional safety issues (conformity against functional specifications) but they are not able to deal with cybersecurity certification approach. Europe is about to face an alike GDPR issue which required to create new DPO-positions and to train people within the organisations. Similarly, the deployment of cybersecurity certification schemes will require the training of departments and employees to understand and to manage security certification needs. The ECCC and the Community could help to develop such training sessions, identify good practices and develop guidelines and recommendations according to the specific sectorial needs.

2.2. Increase the number of experts, develop the skills of the community

The ECCC shall aim at facilitating the quick adoption of the European Cybersecurity Certification Framework, to succeed in this task it shall capture experts with IoT vertical knowledge and IT-security expertise. Several initiatives are expected to attract these profiles within the Community and to increase their number and disseminate their knowledge.

For instance, when it comes to hardware attacks penetration testing and certification approach, the whole European industry relies on a very small ecosystem which encompass about 600 peoples. These people are extremely rare resources and are necessary to enable high-quality cybersecurity certification processes. More specifically it is the role played by community of expects such as the JHAS group under the JIL and operated by Eurosmart and the ISCI WG-1. Certification in cybersecurity cannot overlook the pentesting approach and its community, cybersecurity is a matter of human intelligence when the safety approach is restricted to automated process.

The ECCC could support both the training of the next generations of pentesters and the dissemination of their work to support the increase in quality and efficiency of the European cybersecurity resilience.

3. Support the expertise and the sufficient representativeness of the European SMEs

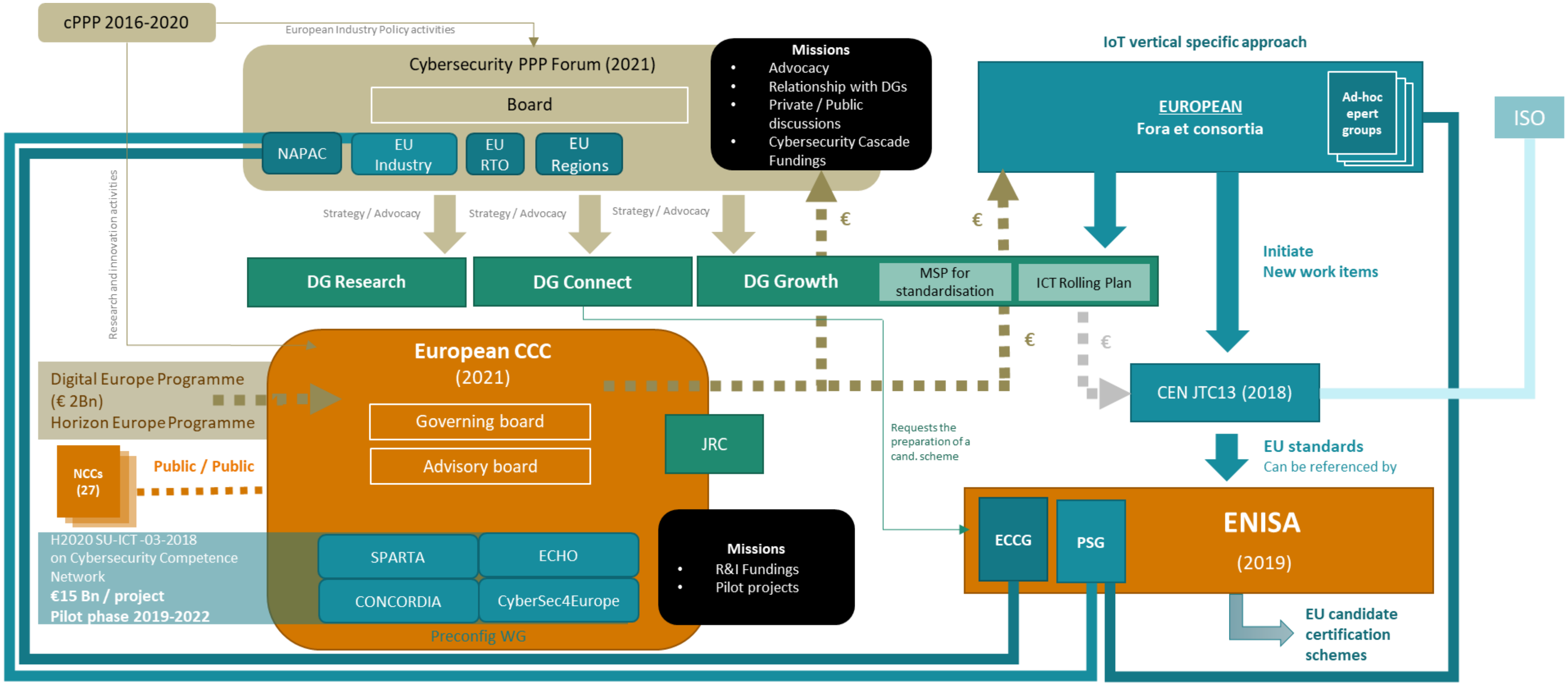
Similarly, mechanisms must be added to ensure a sufficient representativeness of SMEs, their involvement in the ecosystem is obviously needed as they are concentrated a significant part of the EU know-how in matter of cybersecurity. The whole European industry relies on this expertise as most of the current SOG-IS CABs being able to perform pentests are SMEs. The know-how developed in this companies must benefit to all the value-chain. Eurosmart recommend dedicate at least €100bn to European cascading funding to the benefit of the cybersecurity SMEs. This European cascading funding can be managed by the evolution of the current cPPP infrastructure.

4. Link the European Standardisation approach with the European Cybersecurity Certification Framework

The European standardisation harmonisation is supported by a well-defined regulatory approach where CEN and CENELEC are playing a key role. The newly created *CEN JTC13* shall be the converging point between safety and cybersecurity works on standardisation. It is nevertheless necessary to renew the current work of pre-standardisation that is undertaken by stakeholders. Eurosmart is convinced that Europe must take example on the good practices from the non-EU and US fora and consortia in terms of governance.

The accreditation of genuine "European" organisations within the ECCC Community is key. Incentives should be put forward to gather and/or transform European group of actors into identified fora and consortia. These European Fora and Consortia would reach the critical mass to be able to initiate new standardisation works items according their sectorial needs. This work could be backed by the ECCC in close collaboration with CEN/CENELEC, ENISA and the MSP for standardisation. Eurosmart put in this perspective the JRC mapping of more than 660 organisations from across the EU as cybersecurity centres of expertise. However, a clear legal definition is a much needed first step toward the consolidation and the identification of relevant EU stakeholders.

2021 European Cybersecurity landscape



cPPP 2016-2020

European Industry Policy activities

Research and innovation activities

Cybersecurity PPP Forum (2021)

Board

NAPAC

EU Industry

EU RTO

EU Regions

Missions

- Advocacy
- Relationship with DGs
- Private / Public discussions
- Cybersecurity Cascade Fundings

Strategy / Advocacy

Strategy / Advocacy

Strategy / Advocacy

DG Research

DG Connect

DG Growth

MSP for standardisation

ICT Rolling Plan

€

€

€

€

IoT vertical specific approach

EUROPEAN
Fora et consortia

Ad-hoc epert groups

ISO

Initiate
New work items

CEN JTC13 (2018)

EU standards
Can be referenced by

Digital Europe Programme
(€ 2Bn)
Horizon Europe Programme

NCCs (27)

Public / Public

H2020 SU-ICT -03-2018
on Cybersecurity Competence Network
€15 Bn / project
Pilot phase 2019-2022

European CCC
(2021)

Governing board

Advisory board

JRC

SPARTA

ECHO

CONCORDIA

CyberSec4Europe

Preconfig WG

Missions

- R&I Fundings
- Pilot projects

Requests the preparation of a cand. scheme

ECCG

PSG

ENISA
(2019)

EU candidate certification schemes

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Cabinet Louis Reynaud**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient Mobile Security**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**Bureau Veritas ,SGS**), laboratories (**Brightsight, , CEA-LETI**, **Keolabs**, **SERMA, Trust CB**), research organisations (**Fraunhofer AISEC, ISEN**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com