Cyber security Act – Certification part

1st of March 20018

EUROSMART

The Voice of the Digital Security Industry

European Cyber Security Definition from ECSO

European Cyber Security is our common science, knowledge, trustworthy processes, products, services and infrastructures to protect (in a sustainable way) our countries, industries / economies, citizens and institutions against damaging Cyber-attacks while respecting our European Values.

We are not alone !

Already 7 Cyber Acts in the world with their associated certification schemes

(more to come !)

Typical product or service pillars:

Functional specification	Conformity against functional specification	Privacy certification	Security certification
CEN /CENELEC/ETSI/ITU or proprietary	Assess conformity with the functional standard	GDPR/ePrivacy Ongoing definitions of Privacy certification schemes	Cybersecurity Act: certification schemes
Currently in used by all European industrial sectors		Ongoing / under definition	Today only SOG-IS or private schemes such as EMVCo are existing

Trying to understand the actors & process of the Proposed EU regulation – Article 8 & TITLE III

EUROSMART

The Voice of the Digital Security Industry

"Cybersecurity Act" :
Regulation proposal on creating the EU Cybersecurity Agency and defining the Information and Communication Technology cybersecurity certification

Part 1 & 2

Putting ENISA at the heart of the EU Cybersecurity operational activities

Part 3

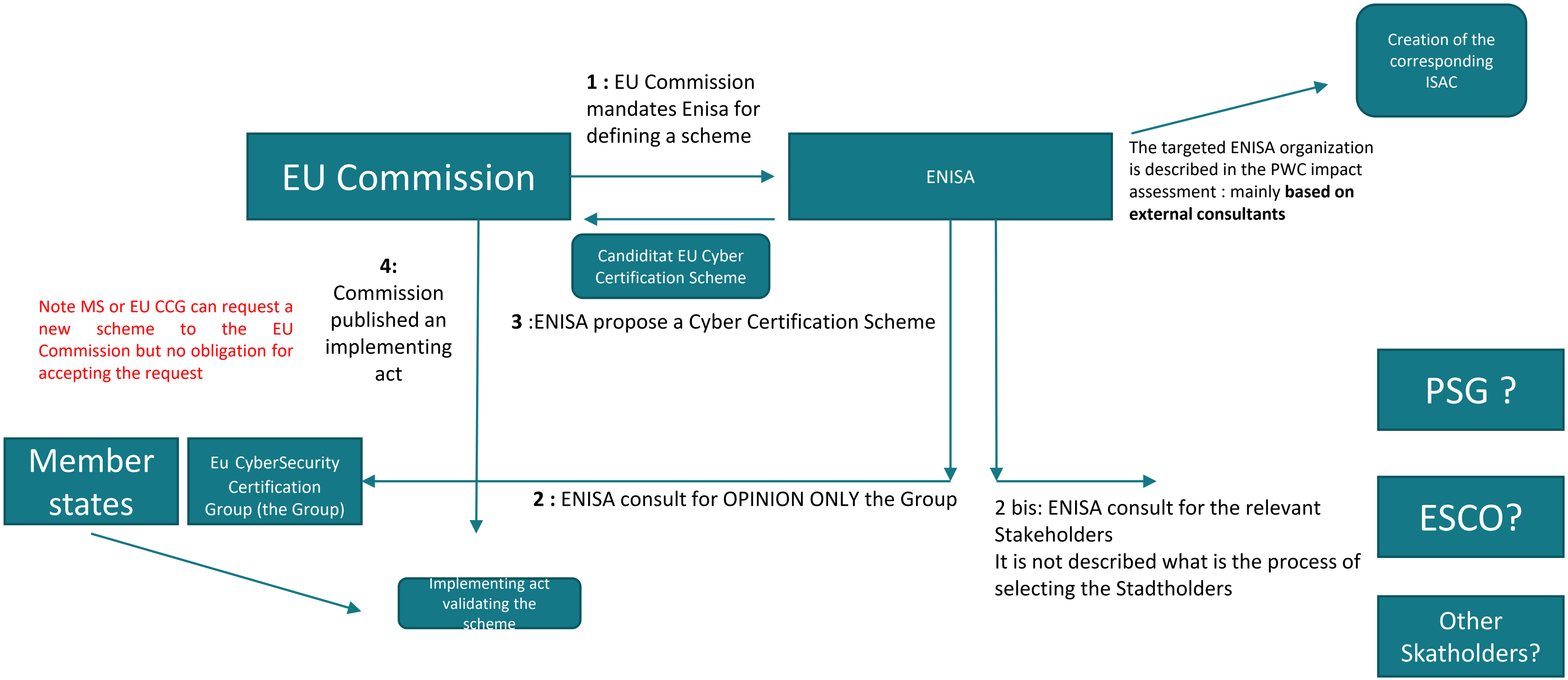
Defining the Eu Cybersecurity certification frame work

Step 1 : **Creation & Governance** of a new Certification Scheme at EU Level – Voluntary scheme for the industry but mandatory that member states put it into in place

Step 2 : **Enforcement** of the new Certification Scheme at the national level (e.g. Actors in France)

Step 3 : **Introduction of new Certification Schemes** (created in the Step 1) to make is mandatory for the industry : Using the sectorial regulation from the different DG (FIMA, Conect, Home, Move etc…)

Step 1: Creation & Governance of a new Certification Scheme at EU Level



EU Commission

ENISA

1 : EU Commission mandates Enisa for defining a scheme

Candiditat EU Cyber Certification Scheme

3 :ENISA propose a Cyber Certification Scheme

Creation of the corresponding ISAC

The targeted ENISA organization is described in the PWC impact assessment : mainly **based on external consultants**

Note MS or EU CCG can request a new scheme to the EU Commission but no obligation for accepting the request

4: Commission published an implementing act

Member states

Eu CyberSecurity Certification Group (the Group)

2 : ENISA consult for OPINION ONLY the Group

Implementing act validating the scheme

2 bis: ENISA consult for the relevant Stakeholders
It is not described what is the process of selecting the Stadtholders

PSG ?

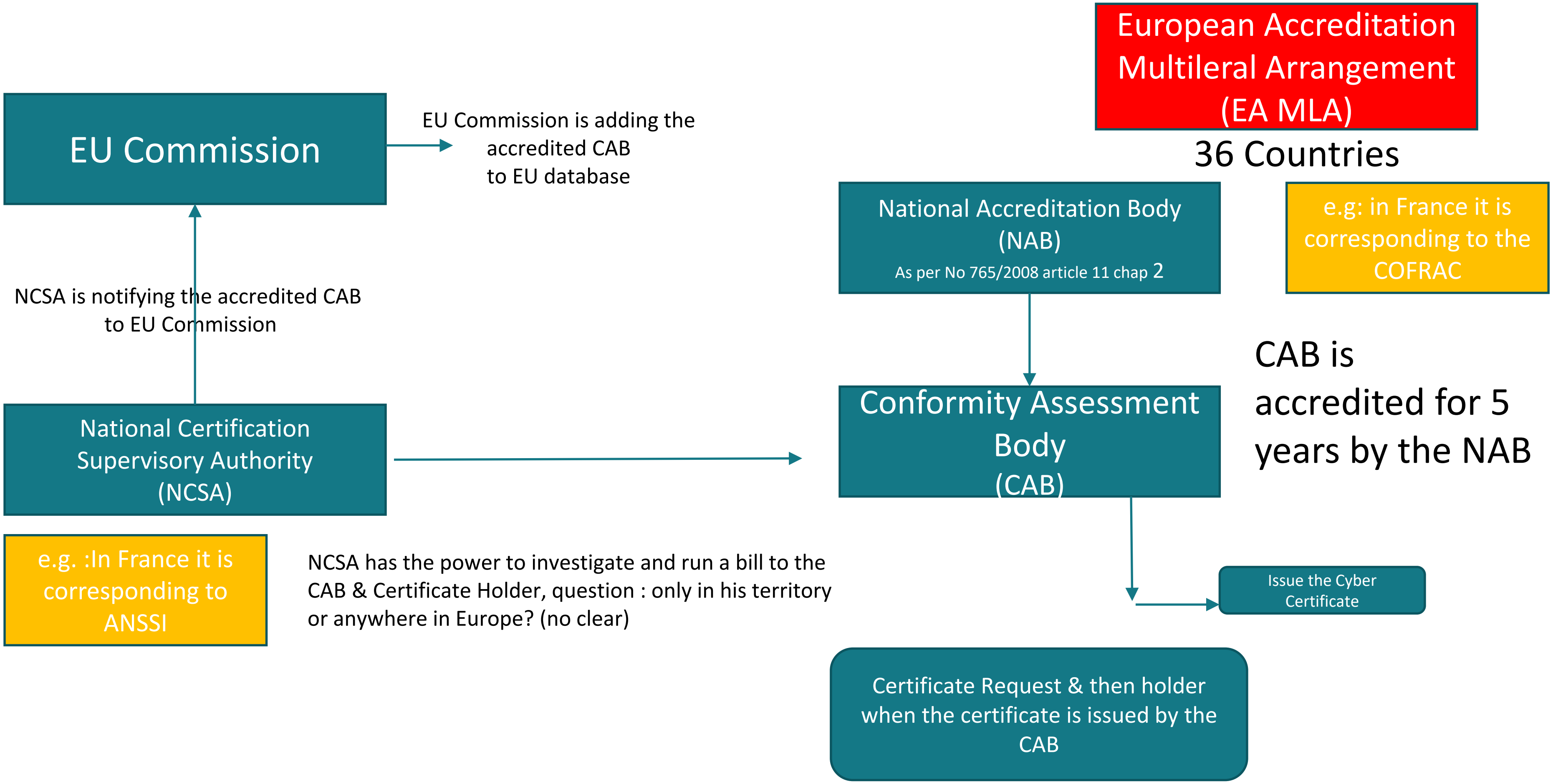
ESCO?

Other Skatholders?

Private security certification schemes be endorsed by ENISA as EU standards

EUROSMART
The Voice of the Digital Security Industry

Step 2: Enforcement of the new Certification Scheme at the national level (e.g. Actors in France)



European Accreditation Multileral Arrangement (EA MLA)

36 Countries

EU Commission

EU Commission is adding the accredited CAB to EU database

National Accreditation Body (NAB)

As per No 765/2008 article 11 chap 2

e.g: in France it is corresponding to the COFRAC

NCSA is notifying the accredited CAB to EU Commission

CAB is accredited for 5 years by the NAB

National Certification Supervisory Authority (NCSA)

Conformity Assessment Body (CAB)

e.g. :In France it is corresponding to ANSSI

NCSA has the power to investigate and run a bill to the CAB & Certificate Holder, question : only in his territory or anywhere in Europe? (no clear)

Issue the Cyber Certificate

Certificate Request & then holder when the certificate is issued by the CAB

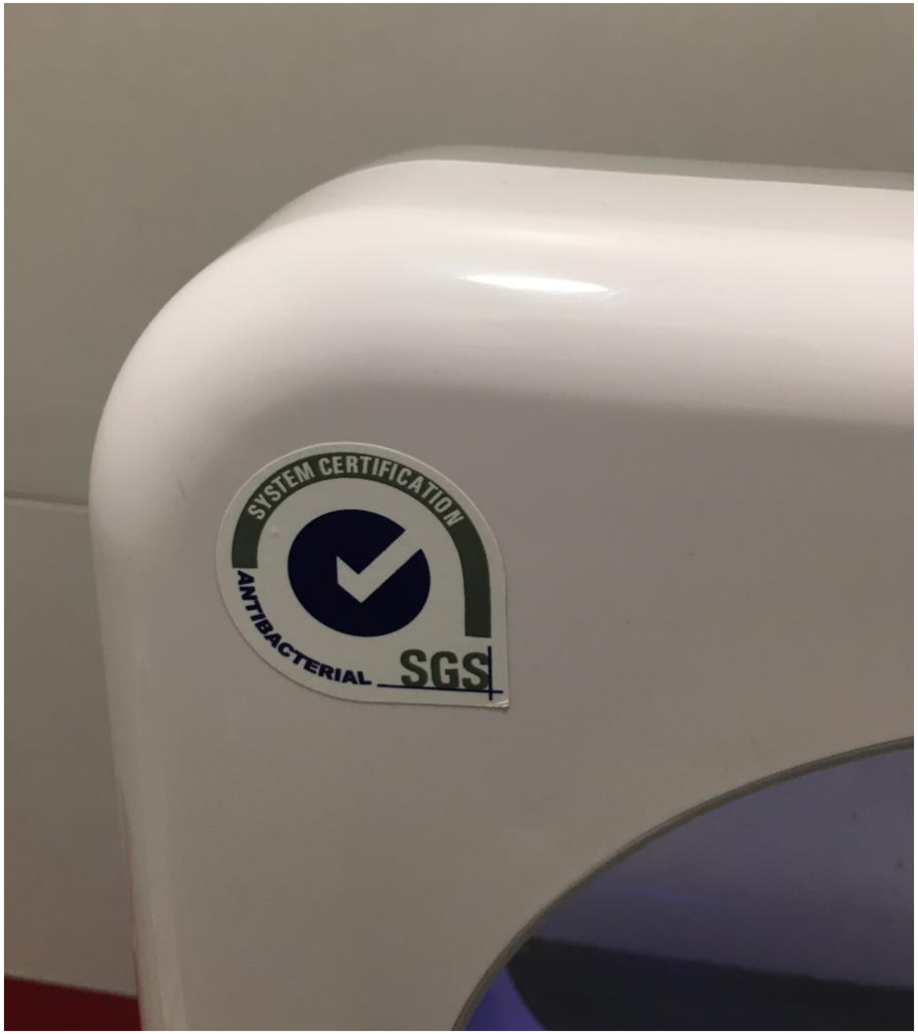
Step 3: Introduction of new Certification Schemes (created in the Step 1) to make them mandatory for the industry

- eg:
  - Radio Equipment Directive
  - WEEE directive
  - ITS?
  - eCall?
  - eIDAS for Server Signing and QSCD
  - PSDII?
  - Package Telecom?
  - Autorisation to sale a new car type in Europe?

Five outcome-based principles from the European digital industry

- *Clear legal definition of essential terms*
- *Fair and Open European governance during the preparation phase of the candidate European certification schemes*
- *Well-defined European Certification objectives: Mandatory ethical hacking during the security evaluation*
- *European standards must be the basis for preparation a new candidate European certification scheme*
- *ENISA's Intellectual Property Rights should be defined*

Certificat exemple as per the European Accreditation Multileral Arrangement (EA MLA)



EUROSMART
The Voice of the Digital Security Industry

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Stéfane MOUILLE
President
Stefane.mouille@eurosmart.com

Pierre-Jean VERRANDO
Director of operations
pierrejean.verrando@eurosmart.com

Eurosmart | Rue du Luxembourg 19-21 | 1000 Brussels | Belgium
Tél. +32 2 506 88 38