CYBER SECURITY COALITION.be

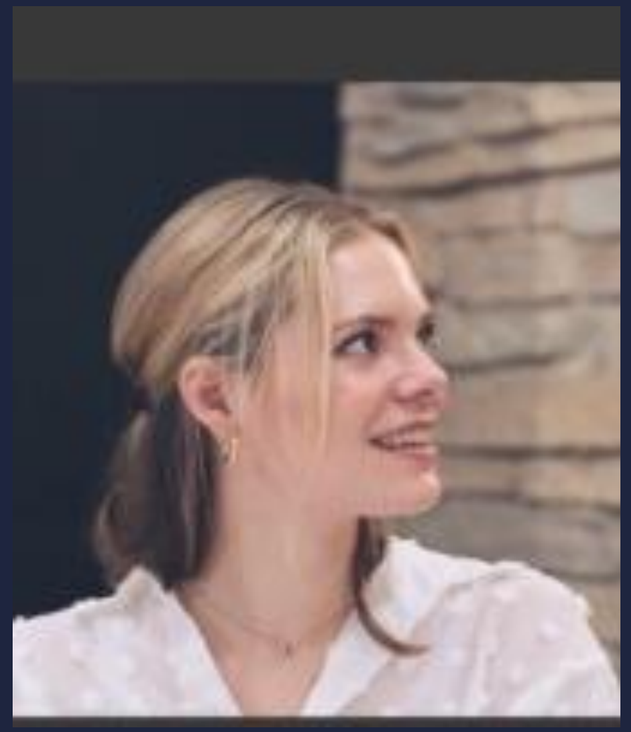
CENTRE FOR CYBER SECURITY BELGIUM

EU Cybersecurity Act: Moving forward

31 March 2021 (2:00 pm – 3:00 pm)

Our guest speaker: Morgane Truant

CENTRE FOR CYBER SECURITY BELGIUM



CENTRE FOR CYBER SECURITY BELGIUM

EU Cybersecurity Act (CSA)

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

30/03/2021

Content

1. EU Cybersecurity Act (CSA)
2. NCCA: Proposal for national implementation
3. Pipeline and Future schemes

1. EU Cybersecurity Act (2019/881)

(art. 46-68 CSA)

Union-wide voluntary certification framework that provides common cyber security rules and evaluation criteria for ICT products, processes and services.

Certificate valid in all Member States.

➡ National implementation 28 June 2021

EU Cybersecurity Certification Scheme

A comprehensive set of EU-level rules, technical requirements, standards and procedures applicable for the certification or conformity assessment of ICT products, services and processes.

Issuance of a EU certificate

Conformity self-assessment

Mutual recognition mechanism

- Improve and ensure trust in digital single market

  → Transparency cybersecurity assurance levels

- Harmonization cybersecurity practices

  → Address internal market fragmentation: conflicting or overlapping national certification schemes

- Drive the maturity in the market for security

Levels of certification assurance

The level of assurance corresponds to the risk associated with the intended use of the product, service or process.

Basic

- Minimize known basic risks of cyber incidents and cyber attacks
- Conformity self-assessment,

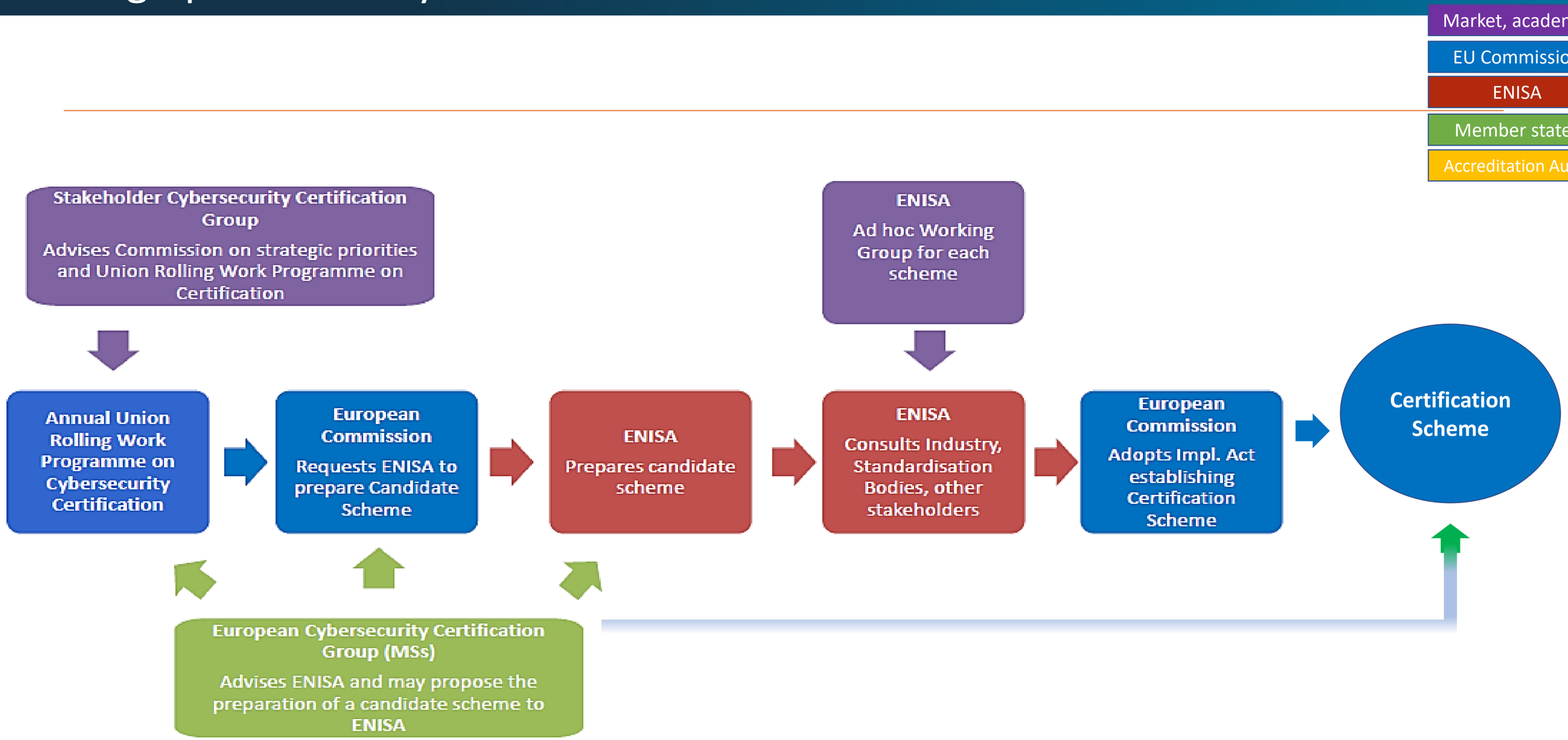
Substantial

- Minimize risks of cyber incidents and cyber attacks by actors with limited skills and resources
- Basic + conformity security features

High

- Minimize the risks of advanced cyber attacks by actors with significant skills and resources
- Substantial + efficiency testing

Setting up a voluntary certification scheme



2. Proposal for national implementation

CCB proposition to act as NCCA

1. Representation EU level

2. Issuance of certificates (high or deviating)

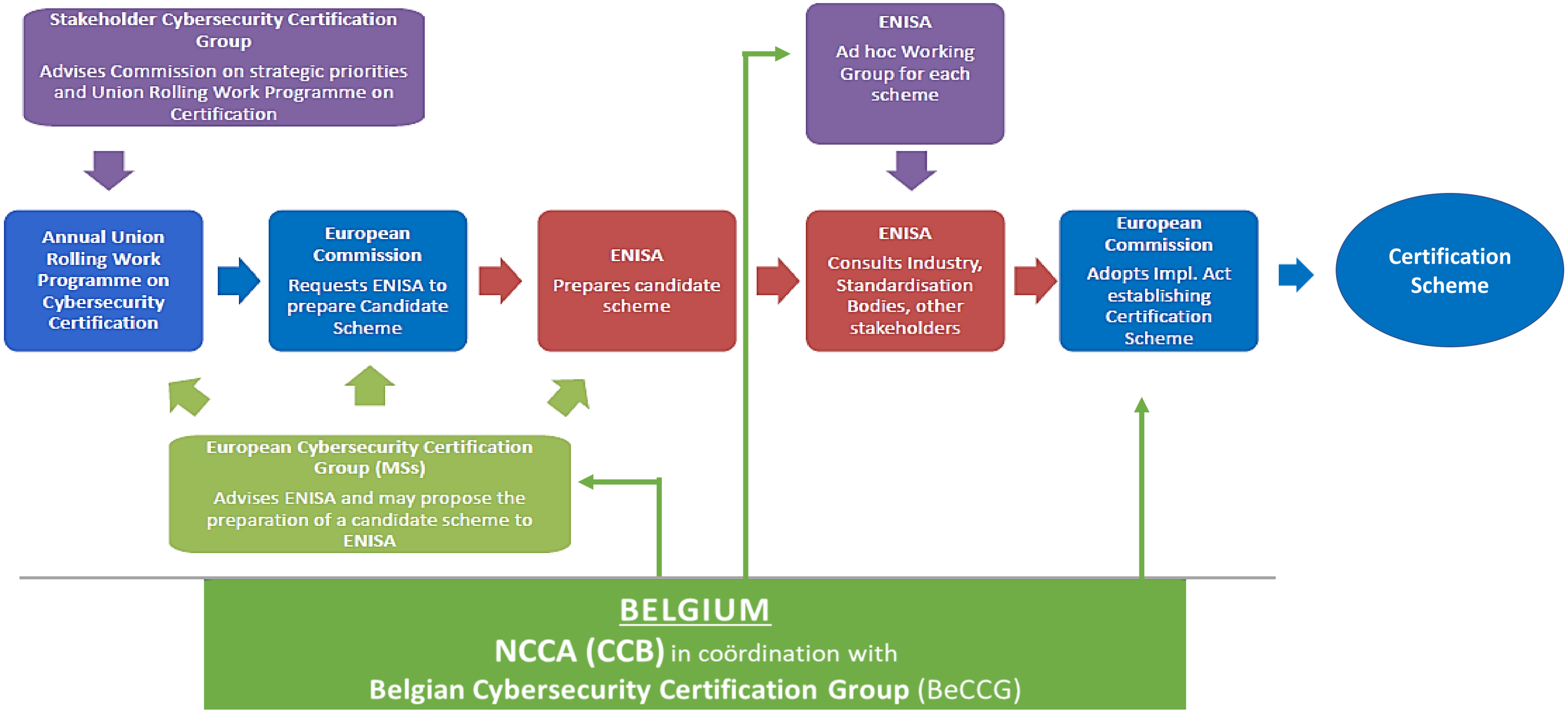
3. Supervision

Representation in the EU (I)

NCCA represents the Belgian cybersecurity certification position in the ECCG

(European cybersecurity certification group)

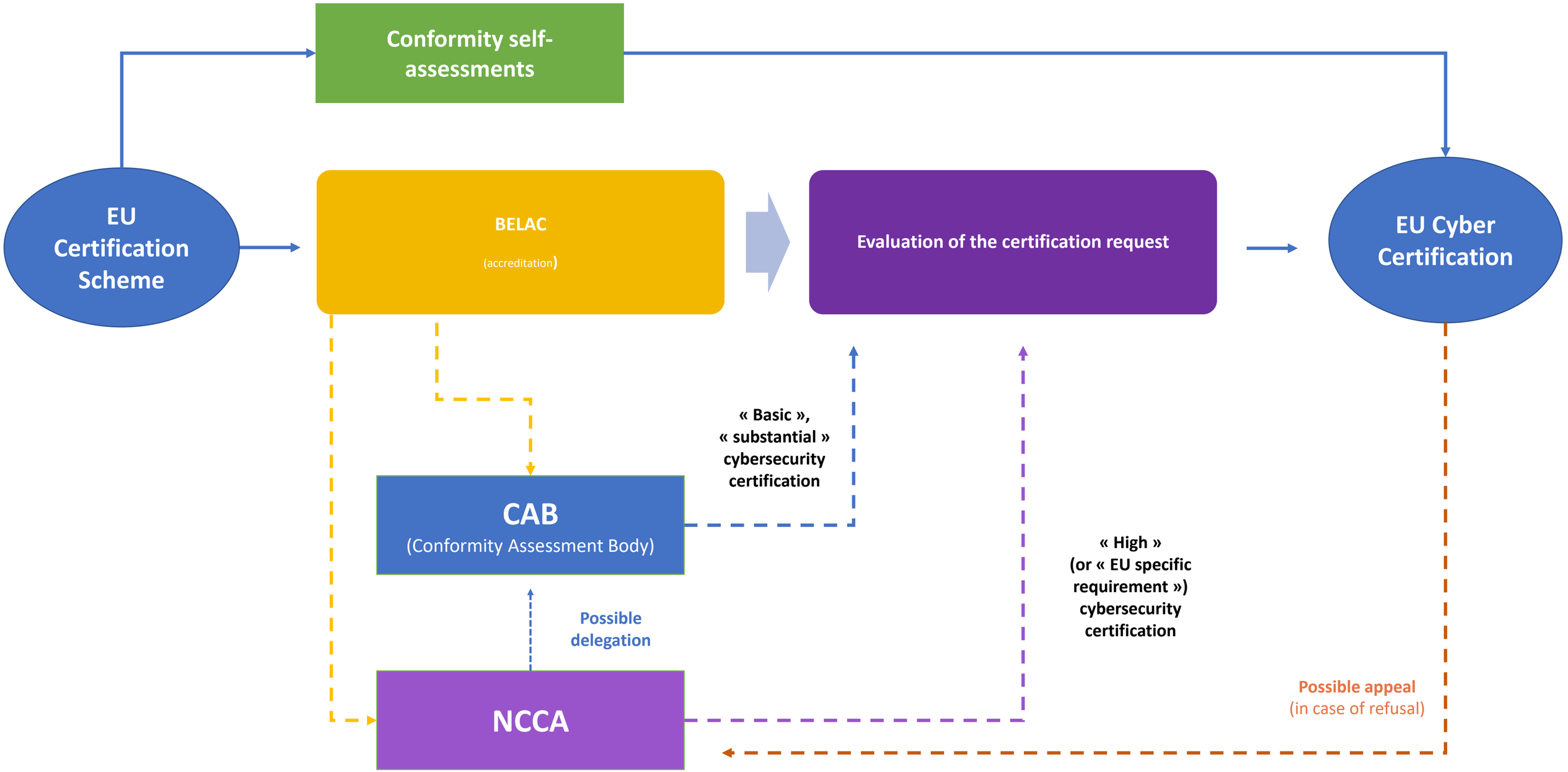
- Determine certifications priorities
- Draft European cybersecurity schemes
- Five-yearly international peer review


Stakeholder Cybersecurity Certification Group
Advises Commission on strategic priorities and Union Rolling Work Programme on Certification
ENISA
Ad hoc Working Group for each scheme
Annual Union Rolling Work Programme on Cybersecurity Certification
European Commission
Requests ENISA to prepare Candidate Scheme
ENISA
Prepares candidate scheme
ENISA
Consults Industry, Standardisation Bodies, other stakeholders
European Commission
Adopts Impl. Act establishing Certification Scheme
Certification Scheme
European Cybersecurity Certification Group (MSs)
Advises ENISA and may propose the preparation of a candidate scheme to ENISA
BELGIUM
NCCA (CCB) in coördination with
Belgian Cybersecurity Certification Group (BeCCG)

Issuance of certificates (II)

Assurance level **basic** and **substantial**	Assurance level **high**
• Issued by a CAB (accredited by BELAC)	• Issued by the NCCA
• Or by the NCCA or by a public CAB if required by the scheme (art. 56-5 CSA)	• Or by the CAB in case of delegation by NCCA (art. 56-6 CSA)

Issuance of certificates



| Supervision (III)

NCCA carries out the supervision tasks

- 1. Inspection of CAB’s, holders of certificates, manufacturers or providers performing conformity self-assessment
- 2. Sanctions (restriction, suspension or revocation, administrative fines)
- 3. Complaints, appeals

3. Pipeline and Future schemes

Announcement and Publication: https://www.enisa.europa.eu/

- Publication of schemes under CSA
- EU certificates and EU conformity declarations (no longer valid/withdrawn)
- Replacement of national schemes by EU schemes

Pipeline

- Common Criteria
- Cloud Services
- 5G

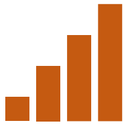
Common Criteria: EUCC

- First candidate-scheme under CSA
- Scope: Certification of ICT products at level substantial and high
- Foundation: SOG-IS CC scheme
- Final stages
- Implementation: no fixed date but « as soon as possible »

Cloud Services: EUCS

- Scope: certification of cloud services at level basic, substantial and high
- Foundation: Report of the CSP-CERT working group, C5 scheme, SecNumCloud scheme and others
- Draft version currently for external review – ENISA website

Request for 5G networks



- End of January: COM request for candidate certification scheme
- Phase 1: Build on existing schemes (NESAS)
- ECCG support but proposal for gap analysis
- Phase 2: availability of 5G scheme - depending on gap analysis (no fixed date)

Reflection on future schemes: URWP

- URWP not adopted by COM yet (so no publication yet)
- Update at least once every three years (more if needed)
- Move towards more sectorial requirements
- Near future: IoT, IACS
- Distant future: Secure Development Lifecycle, AI

CENTRE FOR
CYBER SECURITY
BELGIUM

- ✓ Proposal on table and broad outlines drawn up
- ✓ One scheme almost concrete
- ✓ Short term no impact
- ✓ No initiative yet for compulsory schemes
- ✓ Keep you up to date

CENTRE FOR
CYBER SECURITY
BELGIUM

morgane.truant@ccb.belgium.be

www.cybersecuritycoalition.be/webinars/

Subscribe to our Cyber Pulse newsletter

Join our mailing list to receive updates from the Cyber Security Coalition.

Email Address

First Name

Last Name

I agree to receive Cyber Pulse and know that I can easily unsubscribe at any time.

SUBSCRIBE NOW!

Thank you