CENTRE FOR CYBER SECURITY BELGIUM

Cybersecurity Coalition Focus Group New regulations and standardization

CCB as NCCA

EU CS Certification Scheme

The date here

CCB

1. **Created by Royal Decree 10/10/2014**

Contribute to build a safer and reliable internet

Create national policy and capabilities with existing actors

Under the authority of the Prime Minister

2. **NIS-law 7 April 2019 & Royal Decree 12 July 2019**

CCB is the national CSIRT and is the national authority
in charge of monitoring and coordinating
the implementation of the NIS

3. **Cybersecurity Certification-law 20 July 2022**

Designation of certification authority
In charge of coordination, certification and supervision
The implementation of the CSA

Legal mission CCB as national authority for Cyber Security

1. Implementation of the Belgian Cyber Security **Strategy** & Policy
2. Centralized management of Belgian Cyber Security **projects**
3. Ensuring public, private and academic **coordination**
4. Adapting the **regulatory framework**
5. Ensuring **crisis management**
6. Implementation of guidelines and **security standards for public institutions**
7. Belgian representation in **international** cybersecurity forums
8. Security evaluation and **certification**
9. Informing and raising **awareness**

CENTRE FOR
CYBER SECURITY
BELGIUM

CCB Certification

25/10/2021

Vision CCB Certification

- Promote certification as a tool to contribute to the realization of the CCB mission

  ‘making Belgium one of the least vulnerable countries in Europe in the cybersecurity domain’
- Guide and support Belgian companies in the EU cybersecurity certification process
- Achieve a certified and compliant Belgian market within an EU Market

Mission CCB Certification

Promote & Awareness

- Communicate & raise awareness to end-user, producers of ICT products, processes, services and Belgian CABs
- Point of Contact
- Guide Belgian companies in EU certification process

Control, Inform and Adjust

- Scheme development
- Certification
- CSA support BELAC
- Market surveillance ICT p, p, s
  - Complaint investigation
  - Cooperation with other NCCA's
  - Sanctioning
- Annual activities report
- Peer evaluation

Represent

- In private sector – with sectorial and technical organisations
- Representation of BeCCG in ECCG & ENISA
- Representation as CA in BELAC
- Comply legal obligations
- Follow-up cybersecurity certifications schemes
- Standardisation (ISO/IEC/JTC1/SC17 + 27 –CEN/CLC JTC13 - ISO/IEC JTC1/SC42 – CEN-CLC JTC21 – CONFAS)

Coordinate

- Lead and coordinate BeCCG
- Coordination cybercertification affairs in BE
- POC for administrations
- Support CCB projects

CENTRE FOR CYBER SECURITY BELGIUM

EU Cybersecurity Act (CSA) (2019/881)

26/04/2022

EU Cybersecurity Act

Unionwide voluntary certification framework providing common cyber security rules and evaluation criteria for ICT products, processes and services. An issued certificate is valid in **all Member States.**

- Harmonize cybersecurity practices (replacing national schemes with EU schemes)
- Boost the maturity of the cybersecurity market

EU Cybersecurity certification schemes

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

- Issuance of EU certification
- EU-conformity self assessment

Assurance levels (in schemes)

The assurance level is in line with the risk level associated with the intended use.

National Implementation Plan

Centre Cybersecurity Belgium as the NCCA

1. EU representation

2. Issuance of certificates (high and deviating)

3. Supervision

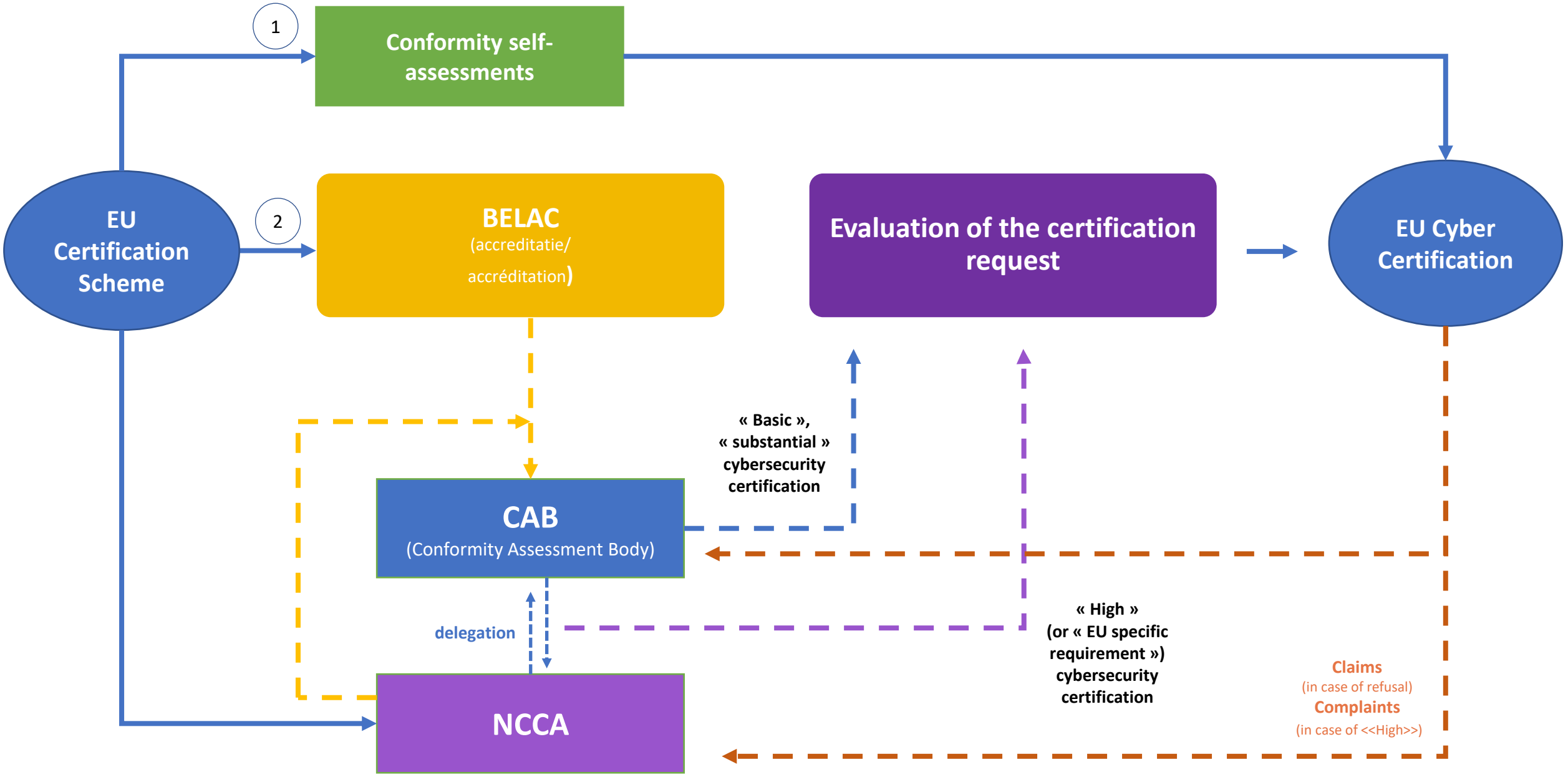
1 EU Representation

| NCCA (CCB) represents the Belgian cybersecurity certification position in the ECCG

- Certification Priorities
- Drafting of European cybersecurity certification schemes
- Five-yearly international peer review

→ **BeCCG;** consultation group for BE positioning (inc. market surveillance authorities)

Issuance of certificates



3 Supervision

→Rule: NCCA supervision

1. Inspection of certificate holders, "conformity self-assessors (+ CAB with NAB)

   →Exception to inspection: Unless otherwise assigned by Royal Decree

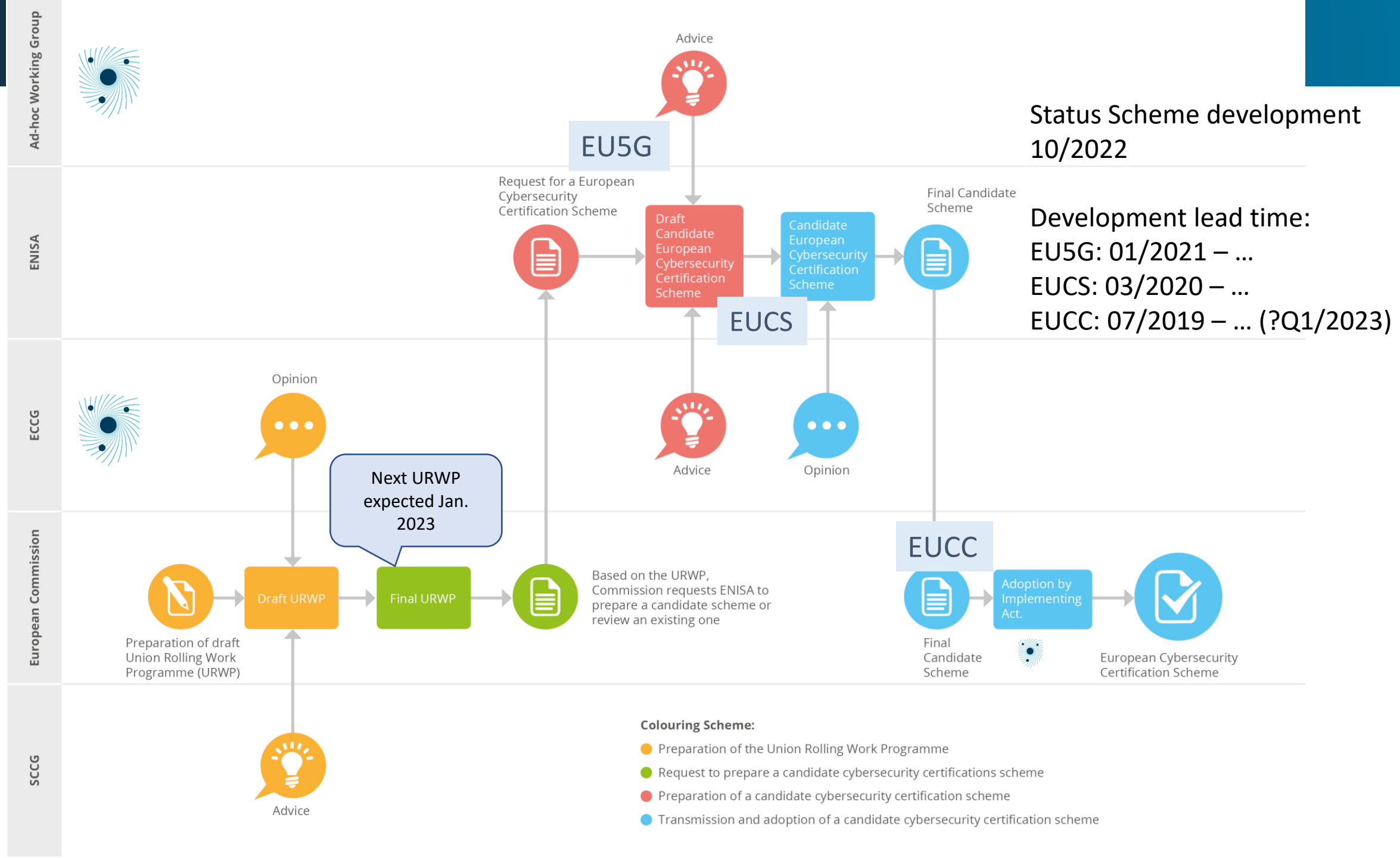
2. Sanction
3. Complaint / Appeal
4. Vulnerability handling

CENTRE FOR CYBER SECURITY BELGIUM

CSA Act – Status overview
Certification scheme development

DISCLAIMER:

All schemes are still under discussion and can be changed. The information in the following slides only provides an overview of the current discussions.



Status Scheme development 10/2022

Development lead time:
EU5G: 01/2021 – …
EUCS: 03/2020 – …
EUCC: 07/2019 – … (?Q1/2023)

CENTRE FOR CYBER SECURITY BELGIUM

EUCS – the candidate European cybersecurity certification scheme for cloud services

The date here

European cybersecurity certification scheme (EUCS)

- **Scope**: The certification of the cybersecurity of cloud services.
    - Must allow users to identify the cloud services guaranteeing the highest levels of security, data protection and immunity to extraterritorial laws.

- **Most important sources**:
    - BSI C5:2020 - National scheme Germany [C5]
    - ANSSI SecNumCloud - National scheme France [SecNumCloud]
    - ISO 27002:2022 (Information security, cybersecurity and privacy protection — Information security controls)
- **Based on:**
    - ISO 17065:2012 (Conformity assessment - Requirements for bodies certifying products, processes and services) ➔ *CABs performing certification*
    - ISO 17025: 2017 (General requirements for the competence of testing and calibration laboratories) ➔ *CABs performing vulnerability identification and penetration testing*

Key features of the EUCS candidate scheme

- Is a voluntary scheme;
- The scheme's certificates will be applicable across the EU Member States;
- Is applicable for all kinds of cloud services – from infrastructure to applications;
- Boosts trust in cloud services by defining a reference set of security requirements;
- Covers three assurance levels: 'Basic', 'Substantial' and 'High';
- Proposes a new approach inspired by existing national schemes and international standards;
- Defines a transition path from national schemes in the EU;
- Grants a three-year certification that can be renewed;
- Includes transparency requirements such as the location of data processing and storage.

Assurance levels

CS-Basic

Minimise the **known basic** risks of incidents and cyberattacks

- Limited assurance (self assessment)
- Review of CSP evidence
- Focusing on well-defined procedures and security mechanisms

CS-Substantial

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources**

- Reasonable assurance
- Design effectiveness
- Operating effectiveness

CS-High

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources**

- Reasonable assurance
- Stronger requirements, including automated monitoring
- Penetration testing

Source: enisa

Two assessment methods

Limited assurance

For the Basic level only:

- Mostly a review of evidence provided by the CSP
- In fact, a self-assessment reviewed by a 3rd party
- Fully integrated in the main scheme, certificate lifecycle, maintenance, *etc*.
- Mostly for vendors with no certification

Reasonable assurance

For the Substantial and High levels:

- "Normal" audit of a cloud service
- Focus on the ISMS and processes, but some interest in the "product" underlying the service
- Following a specific methodology, fully defined in the scheme
  - Compatible with both ISO17021-1 and ISAE3000/3402
- Vendors can keep their certification strategy

Source: enisa

To Do in the upcoming period

- CEN-CENELEC work – to be continued
  - Requirements for cloud services (WG2) ➔ Link to ISO 27001
  - Requirements for CABs (WG3) ➔ Link to ISAE - ISO 170x
- EUCS core ➔ till now focus on the requirements
- Blocking topic: European Digital Sovereignty ➔ no breakthrough yet
  - EUCS Annex J: Independence From Non-Eu Laws
- Work on Guidance – to be started
- Start to involve the accreditation community

Questions?

Johan Klykens
Head of CCB Certification Service
Centre for Cybersecurity Belgium (CCB)
certification@ccb.belgium.be

Dirk De Paepe
Cybersecurity Certification Expert
Centre for Cybersecurity Belgium (CCB)
certification@ccb.belgium.be