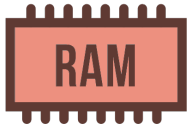
Where Certification meets CRA

Maika Föhrenbach

European Commission, DG CONNECT

Conformity assessment approach



Default category — self-assessment (90%)
(memory chips, mobile apps, smart speakers, computer games...)

Important products — application of standards/third-party assessment
(operating systems, browsers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)

Draft Commission guidelines – Section 6 ‘important and critical products’
(public consultation closed on 13 April)

European Commission

Conformity assessment venues under CRA

New Legislative Framework			EU Cybersecurity Act
Self-assessment (Module A)	**EU-Type examination (B+C)**	**Full quality assurance (H)**	**European cybersecurity certification schemes**
Manufacturer only	**Notified body + Manufacturer**	**Notified body + Manufacturer**	*To be specified* **-** European certification scheme based on Common Criteria (**EUCC**) **Q4,2026** INPUT: **ENISA study & pilot project**

European Commission

Conformity assessment bodies for the CRA

- Member States to notify competent authorities by **June 2026**
- By **December 2026**: Sufficient notified bodies in place
- Driving a consistent approach & level playing field:
  - ✓ Cooperation with Member States – informal group of notifying authorities, support by ENISA
  - ✓ Explore synergies with RED DA & EUCC
  - ✓ Engagement with European Accreditation
  - ✓ Engagement with private CABs
- Future working group of notified bodies

Towards an EU conformity assessment ecosystem

- **CRA:** Presumption of conformity (EUCC), possible mandatory certification, due diligence….
- **CRA**: Conformity assessment bodies leveraging EUCC
- **CSA 2.0**: Alignment & synergies with CRA (security objectives, CABs)
- **CSA 2.0**: ENISA to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem
- Cooperation between CRA market surveillance authorities / Notifying Authorities / NCCAs