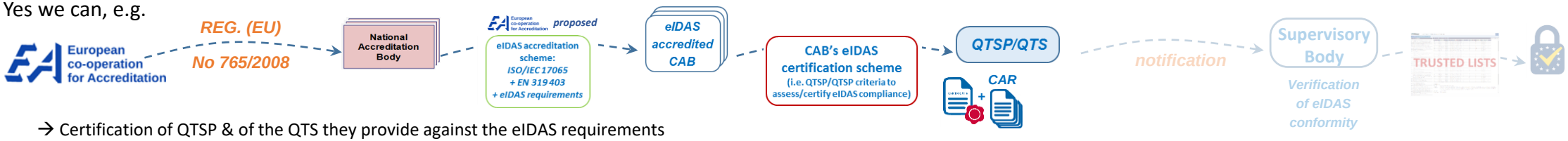
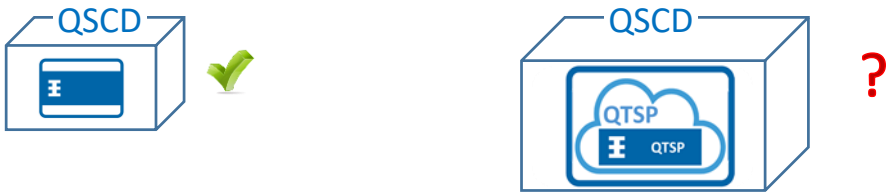
- Can we certify something else than QSCDs in the area covered by eIDAS? Which schemes should apply?
  - Yes we can, e.g.



→ Certification of QTSP & of the QTS they provide against the eIDAS requirements

- Particular points / problems with QSCD certification from your point of view



- Which concrete schemes should apply to QSCD certification – are the existing ones "good enough"?
  - Existing ones quite appropriate for devices like 
  - New ones or combination for dealing with  kind of device
- How do you perceive the effect of the new legislation (Cybersecurity Act) on all the "eIDAS framework"
  - Hope the wheel will not be reinvented …
  - Leveraging on the existing (e.g. less disruption) but improving it (e.g. fitting new "beasts")
- Can certification in the area of trust services/electronic ID be perceived as burden, or rather as competitive advantage?

  → Balance between
    - Raising the bar to an acceptable level (e.g. security/quality/trust), and
    - Costs / competitive disadvantage versus non-EU providers
- How, in practical way, the CABs verify the requirement of certification?
  - "Classic devices" … Common criteria, protection profile, evaluation, certification … quite well-oiled system
  - "QTSP/QTS" … as many "eIDAS certification scheme" as eIDAS accredited CABs