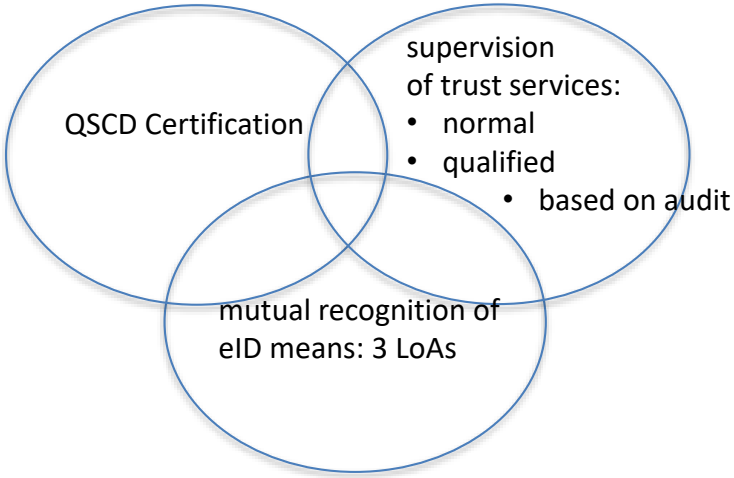
Not 1 but 3 assessements systems under eIDAS – services rely on 1, 2 or the 3 systems



E.g. of service relying on 3 systems;
qualified signature creation through eID Card

QSCD certification in eIDAS: a long & brand new experiences …

« old » - QSCD in the hand of signatory (e.g. smart-card)

eIDAS inherits from « long » history since the « old » signature Directive already ruled the certification of «S»SCD

Lesson learned: no framework for certification:
- rqs on designated body under CD not clear intl. framework, no list of SSCD,
- PPs existed, offering presumption of compliance (were not mandatory).

« new » QSCD remotely managed

… It took some time to have PPs for this case. They are … brand new.

QSCD certification in eIDAS: long & brand new experience …

eIDAS enhancements: article 30 & IA 2016/650 (framework for certification) – article 31 (list of QSCDs).

⇒ reuse of existing PPs (exist since begin 2000 years)

⇒ stronger confidence on the certification process => in equivalence of device.

Reverse side : outside Art 30 frame (where standards for the security assessment of information technology products limits PPs to a list, and limiting alternatives), other / new technical criteria for presumption of compliance (Article 29) have few chance to pop-up.

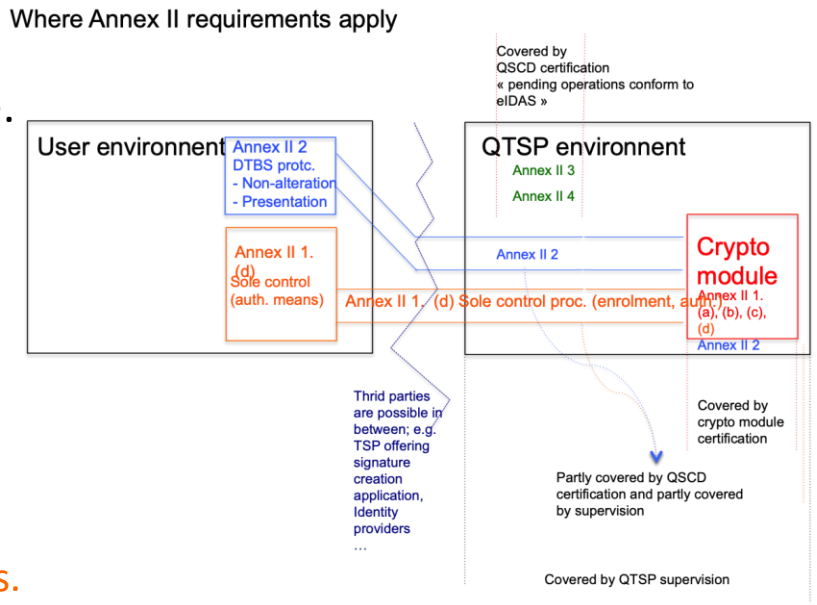
« new » QSCD remotely managed – in this case the device is managed by a TSP and offered as a service. Longer to put in place:

a) such QSCD falls under 2 eIDAS assessment systems: certification & supervision, as:

- Rqs on the device *and*
- Rqs on the procedures to implement it as a service.

PPs for such device puts assumptions on its environment that needs to be assessed outside the certification process. First type requirements assessed through the certification model, second type by the supervision model.

⇒ Need to fix the border – avoid gaps !



« new » QSCD remotely managed – longer to put in place

b) service “signature creation” closely linked to service “certificate issuance”
⇒ when the two TSPs are not the same, some crucial tasks from a security point of view needs to be coordinated (e.g. registration/enrolment).

c) lifecycle to create a PP is long …

If it’s not too difficult to certify that a device is “technically” a QSCD, it’s not obvious (but necessary to validate), to claim that a device is an “eIDAS” QSCD

Supervision of trust services

There is no imposed audit scheme (each CABs has its one), and no mandatory standard(s) as technical criteria.
A problem?

- some technical standards are broadly used by the accredited CABs in the different MS.
- … even NON-Q_TSP follow them as benchmark, or invests in devices that are QSCD_certified, even when not offering Signature services.
- International recognition ?

Experience: TSPs are very keen to have clear requirements.
Sentences not sufficiently precise open for interpretation cause of problem before / during audit.
Typical case; the “equivalence” to face to face for registering a user.