

Estonia's Certification Landscape



No domestic certification tradition

Small market size.

Cybersecurity certification has historically been leaned other countries' schemes — no need existed to build a national one.



Semi-mandatory national frameworks

ISKE / E-ITS binding only for vital service providers; recommendation/mandatory for the wider public sector.

International companies follow corporation set regulations. ISO 27000 family, PSD2, etc



Consequence: no NAB—CAB ecosystem

No established accreditation—certification chain and no national CAB for cybersecurity schemes.

Existing CISA (and other) certified auditors for assessing existing regulations.

EUDIW: New Obligation, Missing Structure



Legal obligation, no structure

EUDIW certification (CIR 2024/2981) requires a national scheme — but no body with the required competences existed.



Lukewarm private-CAB interest

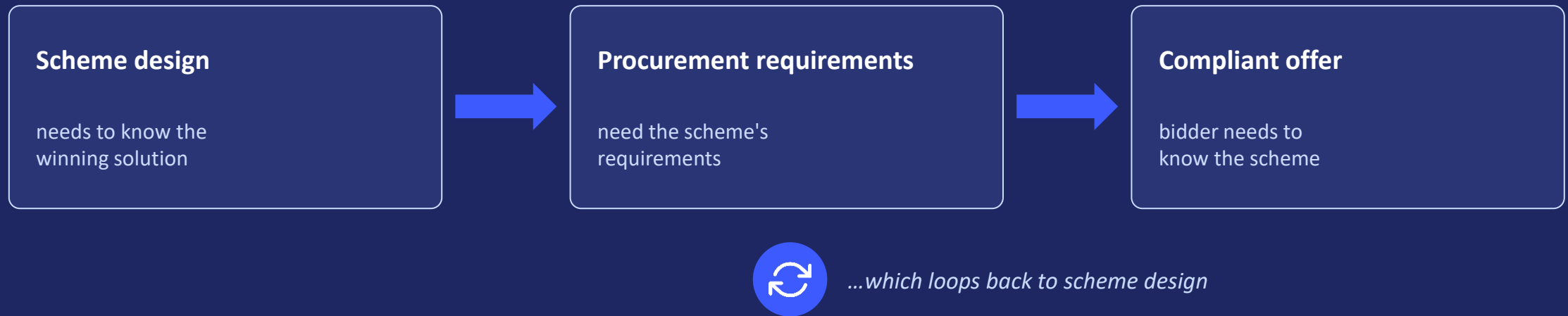
European private CABs hesitant: per-scheme accreditation makes a small market unattractive to enter.



Procurement adds complexity

Estonia procures the Wallet / PID Provider as a certified end-to-end service — certification and procurement intertwine.

The Chicken-and-Egg Problem — and a Pragmatic Way Forward



Way Forward: NOBCCS — Nordic-Baltic Cooperation on Certification

- Cooperative scheme developed with NOBID partners — pooling scarce certification competences across small member states
- NOBCCS as the default certification baseline for Estonia's Wallet / PID Provider procurement
- Negotiated procedure keeps flexibility: bidders may propose the scheme their product conforms to — and commit to finding a CAB willing to certify it