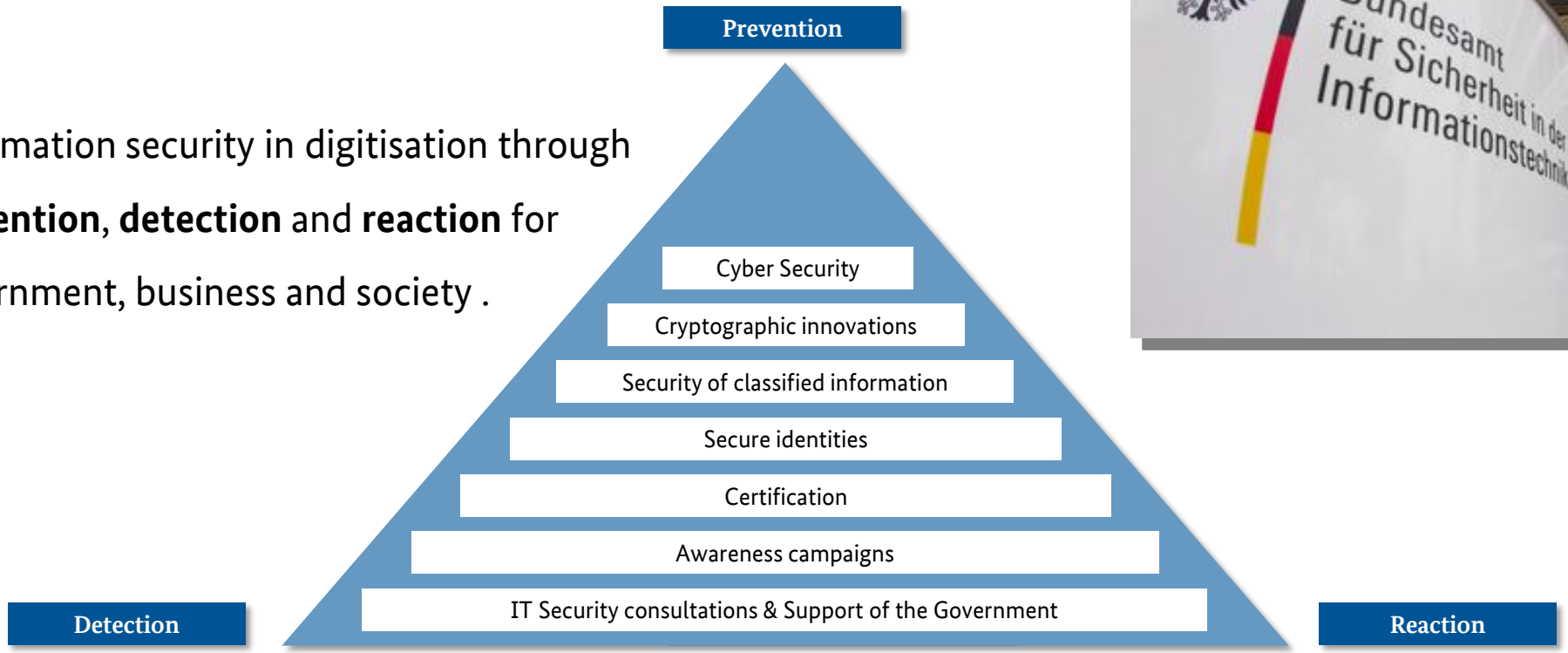
Federal Office
for Information Security

How Europe's Cybersecurity Act and CCRA can be Best Friends

Matthias Intemann

The mission of the Federal Office for Information Security (BSI)

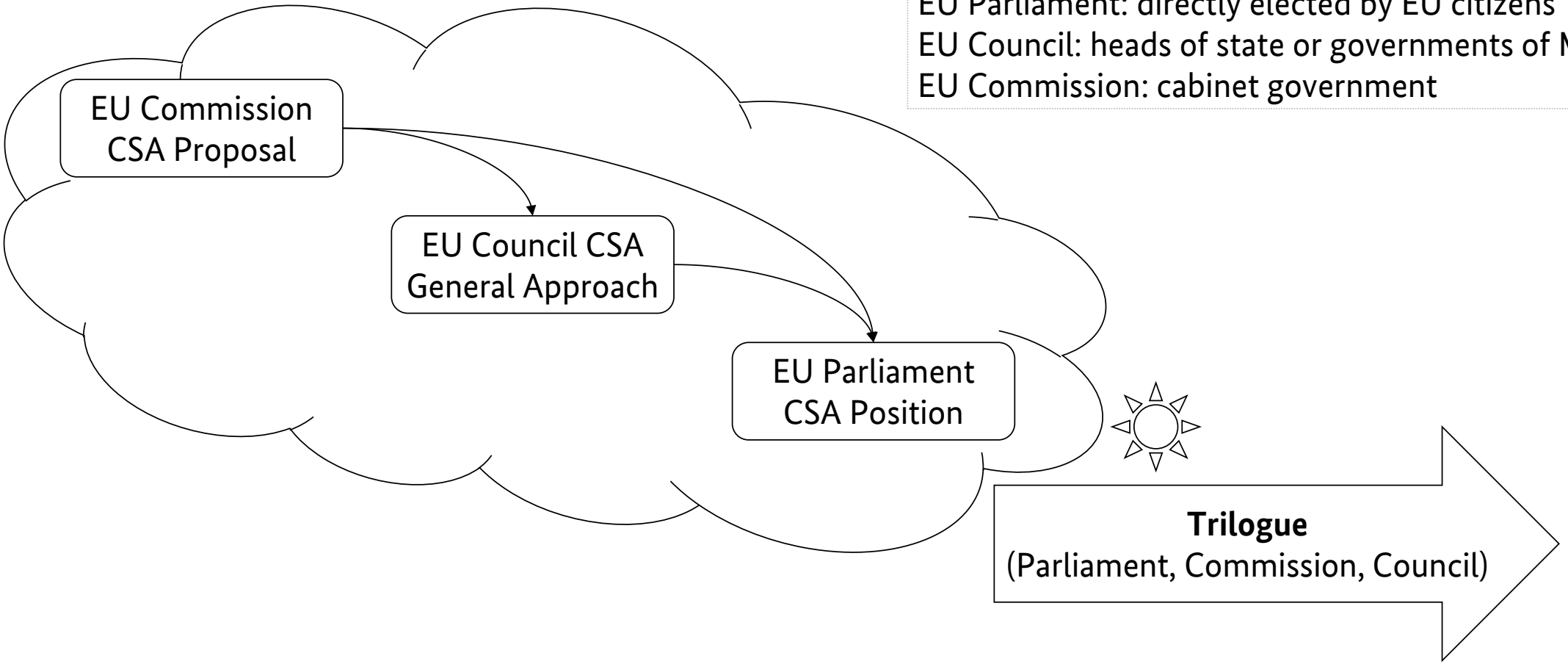
Information security in digitisation through **prevention**, **detection** and **reaction** for government, business and society .



Federal Office
for Information Security

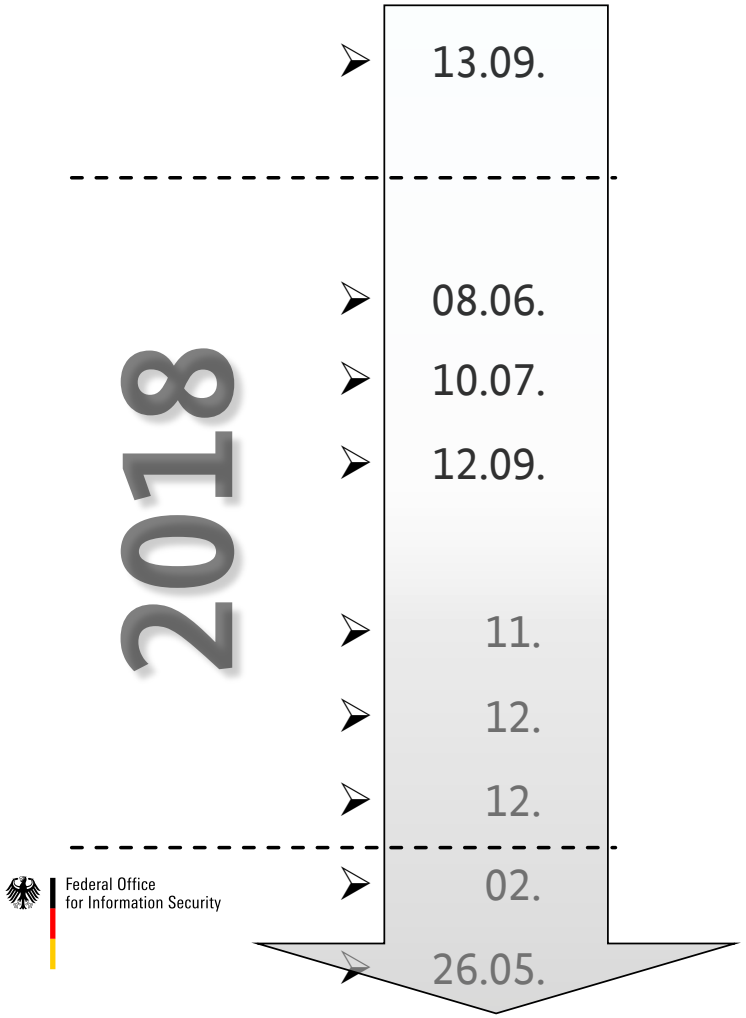
CSA legislative process until today

EU Parliament: directly elected by EU citizens
EU Council: heads of state or governments of MSs
EU Commission: cabinet government



Federal Office
for Information Security

Cyber Security Act
- Timeline -



Federal Office for Information Security

EU COM adopts Cybersecurity Package incl. CSA (DG CON)

EU Parliament (ITRE Committee) and EU Council (HWP Cyber) each discuss the proposal, involving stakeholders

EU Council General Approach on CSA

EU Parliament Resolution on CSA

Start of trilogue phase

Magic behind closed curtains

(envisioned) final trilogue session

(envisioned) adoption CSA by EU council during AT presidency

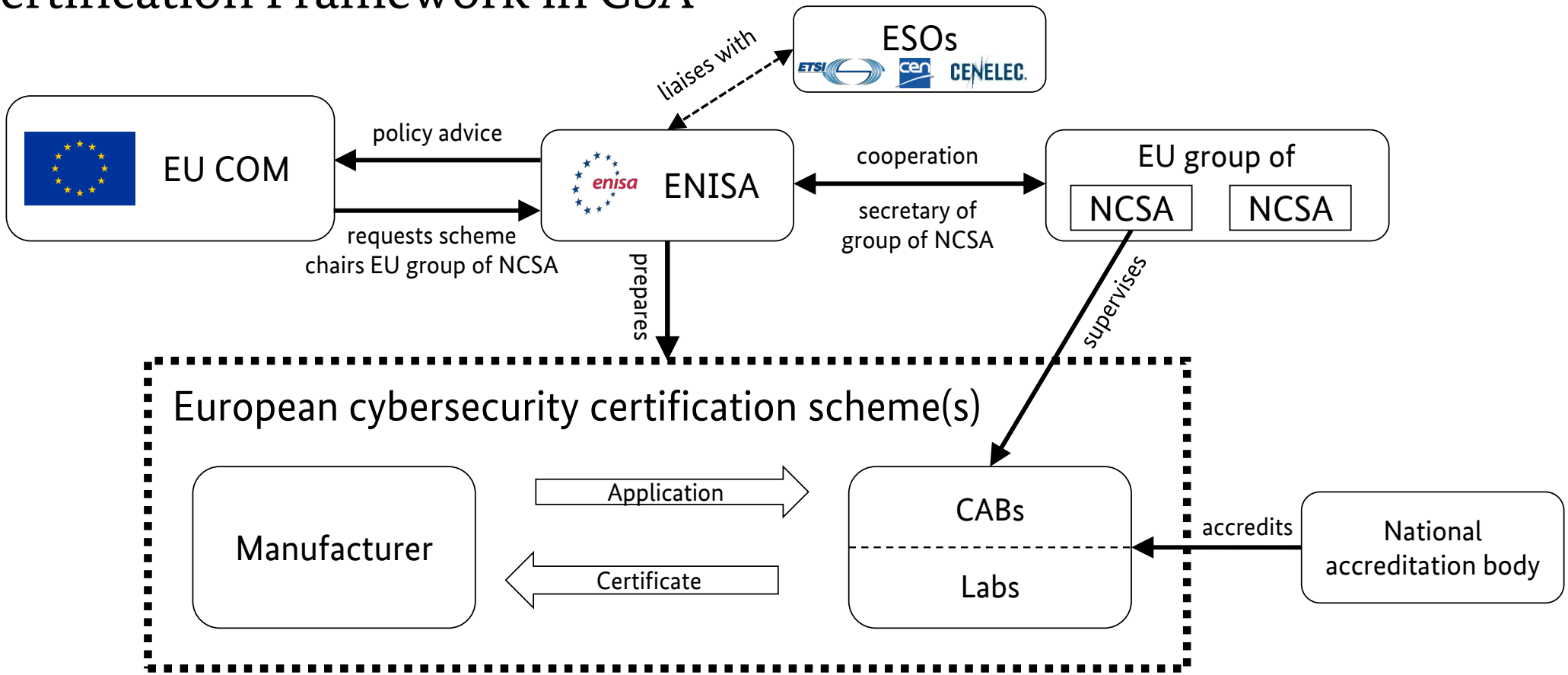
(envisioned) EU Parliament formal approval

implementation of CSA

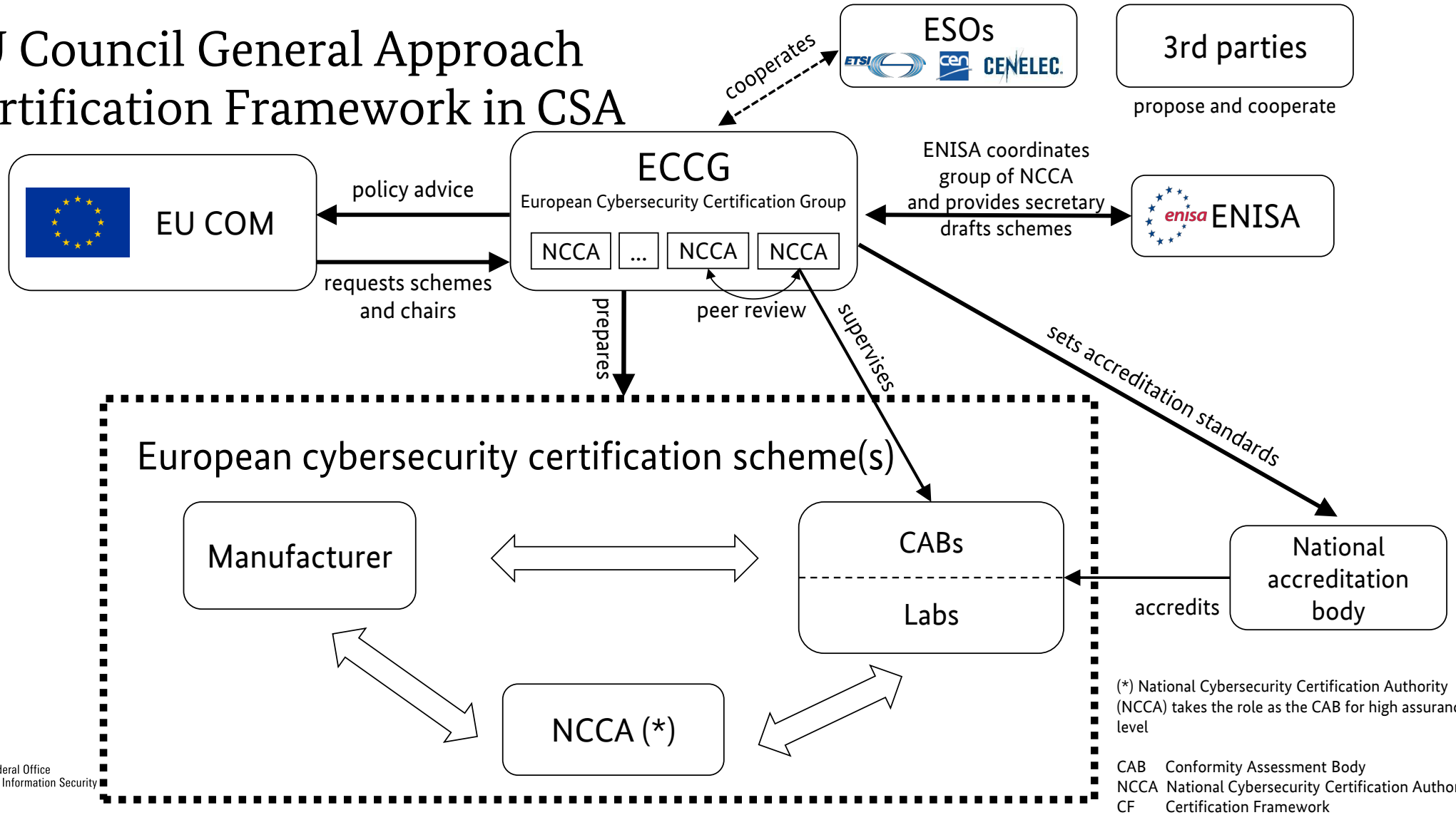
Election of EU Parliament

CSA Cyber Security Act
HWP Horizontal Working Party

EU Commission Proposal
Certification Framework in CSA



EU Council General Approach Certification Framework in CSA

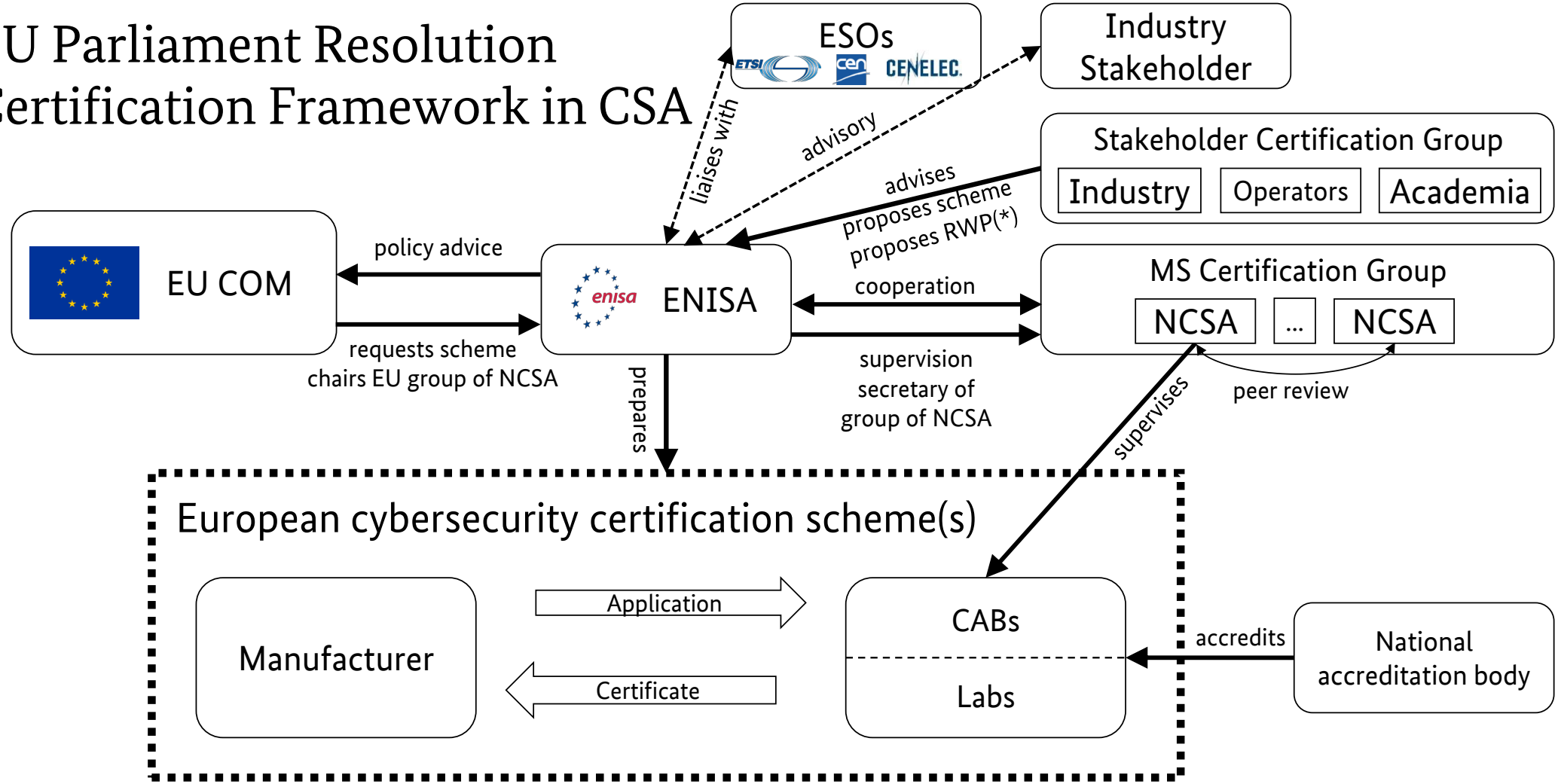


(*) National Cybersecurity Certification Authority (NCCA) takes the role as the CAB for high assurance level

CAB Conformity Assessment Body
NCCA National Cybersecurity Certification Authority
CF Certification Framework

Federal Office for Information Security

EU Parliament Resolution Certification Framework in CSA



Federal Office for Information Security

(*) Rolling Work Programme for creating Schemes

Cyber Security Act (Proposal EU Parliament)

Main differences to EU COM proposal and EU Council General Approach regarding Certification Framework:

- “ENISA Advisory Group” spin off: “Stakeholder Certification Group” with strong influence
- Binding: Rolling Work Programme on schemes
- Essential Service Operators **mandated** to use certification at level “high”
- No public CAB for high
- ECCG should be MSCG
- Delegated acts for schemes instead of implementing acts
- Different approach to peer review

European Cybersecurity Certification (Council GA)

- EU Cybersecurity Certification covers:
  - **Products**, Services, Processes
- Assurance Levels are:
  - **Basic** (certification by accredited CAB or conformity self-assessment)
  - **Substantial** (certification by accredited CAB or in duly justified cases by public body)
  - High (**certification by public body** or a private CAB to which this task has been delegated)
- Certificates **are recognised in all EU MS**
- National Cybersecurity Certification Schemes covered by a **EU Cybersecurity Certification Scheme** shall cease to produce effects
- Commission may recommend negotiation for mutual recognition agreements – **conditions should be provided by each scheme** on adoption
- Certification is **voluntary** unless mandated by (other) policy or regulation

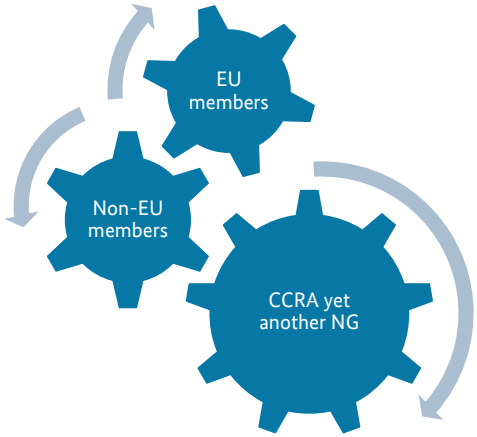
Possible Mismatches CCRA and CSA (Council GA)

CCRA	CSA	
Assurance Basic and Substantial by public body	Assurance Basic and Substantial by private body	Organisational
Assurance High not covered	Assurance High by public body	
Members are nations	EU negotiates MRA for schemes	
VPA among MS	Peer Review among MS (not third countries)	
All application off CC mutually recognised	Might be limited to certain areas of application through scheme definition	
No rules on disclosure of vulnerabilities	*Vulnerabilities need to be reported by vendor and appropriately shared with MS by NCCA, according to scheme policy*	Split Standards
Is open for ST or PP usage (-> national endorsement statement)	*Might set PP to be applied (-> others should not be used then)*	
Sets mandatory supporting documents (e.g. along cPP)	*Sets (other) mandatory supporting documents*	

Federal Office for Information Security

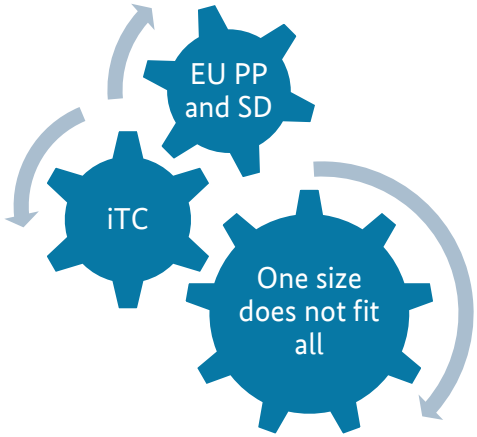
Possible Solution to Organisational Challenges

- Initially, no changes needed, as EU scheme using CC needs to be set up, first
- For a period, both can co-exist, EU MS will probably slowly withdraw from issuing CCRA certificates
- Change Arrangement:
  - Move mutual recognition with EU MS to meta level, recognising certificates between CCRA and EU, not between MS, new option in CCRA
  - Accept oversight of national bodies over private CABs and recognize according certificates
  - Accept Peer Reviews within EU and CCRA role as observer
  - Split CCRA into mutual recognition with EU and technical WG to continue involvement of EU



Possible Solution to Dissociation Challenges

- CCRA to anticipate rules on vulnerabilities in certified products including disclosure (CCRA is lacking this also without CSA)
- Mutual usage of standards to have option of closing upcoming gaps or at least use synergy effects when issuing more than one certificates
  - CCRA members should be open towards also issuing certificates according to European standards
  - EU scheme should be open towards issuing certificates based on CCRA PP and SD



Summary and Conclusions

- ✓ Member States strongly support General Approach
- ✓ CSA has potential to massively strengthen European cyber security
- ✓ CSA gives Europe a strong voice in standardisation of IT security
- ✓ 14 (15) of 28 (30) members of the CCRA are (kind of) members of EU
- ✓ CSA and CCRA can, when combining efforts, grow stronger
- ✓ If CCRA remains as is, involvement of EU members is likely to decrease
- ✓ If CSA scheme conflicts with CCRA, EU members cease to produce certificates for CCRA
- ✓ CCRA has potential of being partner for Europe to avoid conflicting application of CC, forming a stronger market and strengthening IT security

Thank you!

Contact

Matthias Intemann
Section D23 Certification of Software and COTS products

zertifizierung@bsi.bund.de
Tel. +49 (0) 228 99 9582-0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn

www.bsi.bund.de/EN/

Federal Office
for Information Security