KONFERENSEN
INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

17-18 SEPTEMBER 2019

The European Cybersecurity Certification Framework

Informationssäkerhetskonferensen
för offentlig sektor 2019

knowit

Richard Oehme

2019 – Sep – Senior Advisor Societal Security, Knowit Cybersecurity & Law

2018 - Aug 2019 – Director Cyber security and Critical infrastructure protection, PwC Sweden.

2018 – Chairman at the Swedish Security and Defense Industry Associations Cyberdefense group (SOFF)

2009-2017 Director Office of Cyber Security and Critical Infrastructure Protection, Swedish Civil Contingencies Agency.

2008-2009 Senior Adviser and Head of Analysis Section, Office of Crisis Management. Prime Minister's Office.

2005-2008 Deputy Director and Head of IT- and Protective Security, Government Office.

2001-2005 Special Adviser, Secretariat for Intelligence co-ordination, Ministry of Defence.

1989-2000, National Defence Radio Establishment (FRA), Analyst, Head of Section, Head Signals Collection Site, Chief of Staff, Director at FRA management board.

1981- Reserve officer

Certifiering av IT produkter ur att historiskt perspektiv

knowit

SOG-IS Mutual Recognition Agreement

- Etablerat som svar på en uppmaning till EU Medlemsstater från EU-rådet 1992.
- Signerat av 17 EU/EFTA länder
- Frivilligt och icke-bindande samarbete och överenskommelse för erkännande av certifikat.
- Avser certifieringar enligt standarden ISO/IEC 15408 ”Common Criteria”.
- Avser certifikat på assuransnivå EAL4, samt EAL7 för smarta kort och liknande produkter.

Common Criteria Recognition Arrangement

- Etablerat 1999
- Signerat av 31 länder inom och utom EU.
- Frivilligt och icke-bindande samarbete och överenskommelse för erkännande av certifikat.
- Avser certifieringar enligt standarden ISO/IEC 15408 ”Common Criteria”.
- Avser certifieringar på assuransnivå EAL2, samt EAL4 för produkter där specifika krav utvecklats.

Alla medlemmar i SOG-IS MRA är även medlemmar i CCRA

- Certifikat från sådana medlemmar kan ha båda CCRA och SOG-IS MRA märke.

Sverige är medlem i båda.

Motiv för införandet

knowit

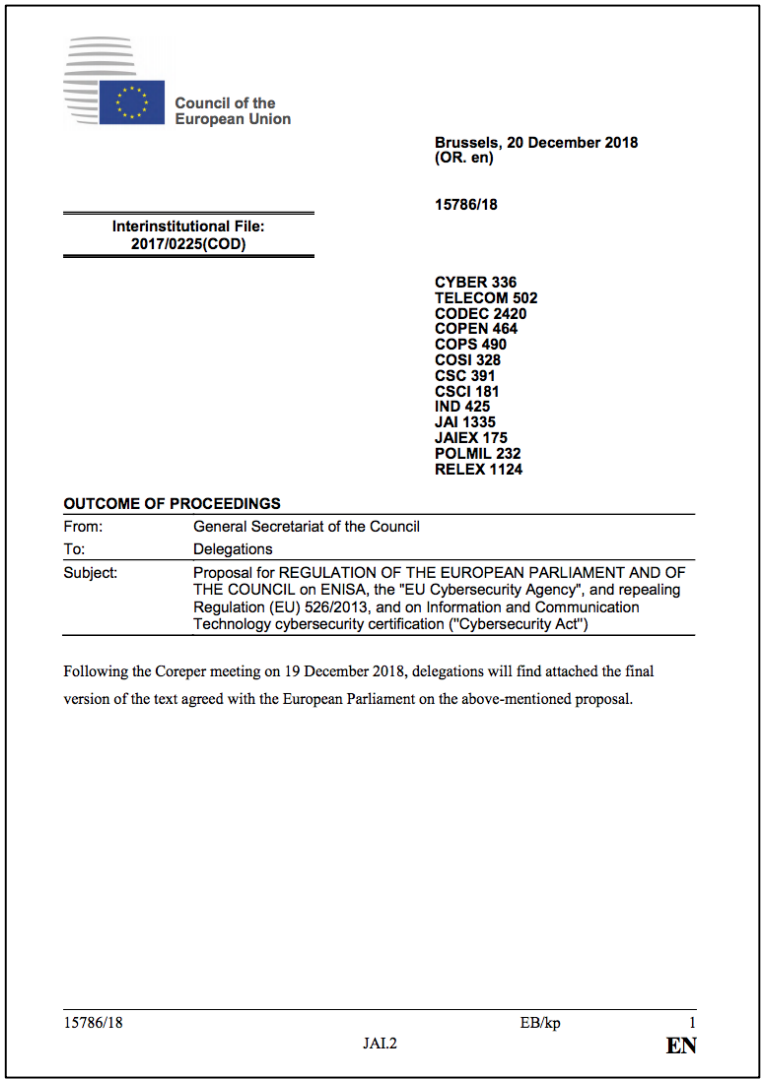
- Digitaliseringen av vårt samhälle leder till ett allt större behov av cybersäkra produkter och tjänster.
- Cybersäkerhetscertifiering spelar en viktig roll för att öka förtroendet för digitala produkter och tjänster.
- En gemensam europeisk strategi för cybersäkerhetscertifiering är en viktig del av den digitala inre marknaden.
- I cybersäkerhetsakten fastställs det europeiska ramverket för cybersäkerhetscertifiering (the **European cybersecurity certification framework**).
- Ramverket möjliggör skapandet av skräddarsydda, frivilliga europeiska cybersäkerhetscertifieringsscheman för IKT-produkter, tjänster och processer. Ett ramverk, många scheman.

knowit

Cyberakten

” Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')”

Förslaget presenterades av kommissionen 13 september 2017 och Parlamentet antog förslaget den 12 mars i år (2019) - Rådet har även formellt godkänt regelverket 9 april.
- Trädde ikraft i juli 2019



Council of the European Union

Brussels, 20 December 2018
(OR. en)

15786/18

Interinstitutional File:
2017/0225(COD)

CYBER 336
TELECOM 502
CODEC 2420
COPEN 464
COPS 490
COSI 328
CSC 391
CSCI 181
IND 425
JAI 1335
JAIEX 175
POLMIL 232
RELEX 1124

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Following the Coreper meeting on 19 December 2018, delegations will find attached the final version of the text agreed with the European Parliament on the above-mentioned proposal.

Beståndsdelar

knowit

Cyberakten består av två huvudsakliga komponenter:

- Ett utökat mandat och mer resurser för den Europeiska Nät och Informationssäkerhetsbyrån (ENISA). (*Från: 84 > 125 personer // €11 > €23 million*)
- Ett EU gemensamt certifieringsramverk med ett gemensamt regler bestående av tekniska krav och standars. ”The EU cybersecurity certification framework”.

I vilket kontext ska Cyberakten ses? - (Fokus certifieringsramverket)

”*In order to scale up EU’s response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single market.*”

- Digitaliseringens möjligheter kontrasteras nu med ett tydligt hoten mot samhällsviktiga funktioner. Inom ramen för detta är certifiering av IKT en fråga om både skydd av samhället men även skydda av egen industri. Bakom det sist nämnda ligger såväl genuina säkerhetsintressen som ren protektionism, skydd av eget företagande.

Övergripande om ramverket

knowit

Certifieringsramverket är ett grundläggande nytt steg i EU: s säkerhetsarbete, och den kommer att få en djupgående inverkan inte bara den offentliga sektorn utan även mer på företag inom och utanför unionen, och särskilt för kritiska infrastrukturproducenter och operatörer.

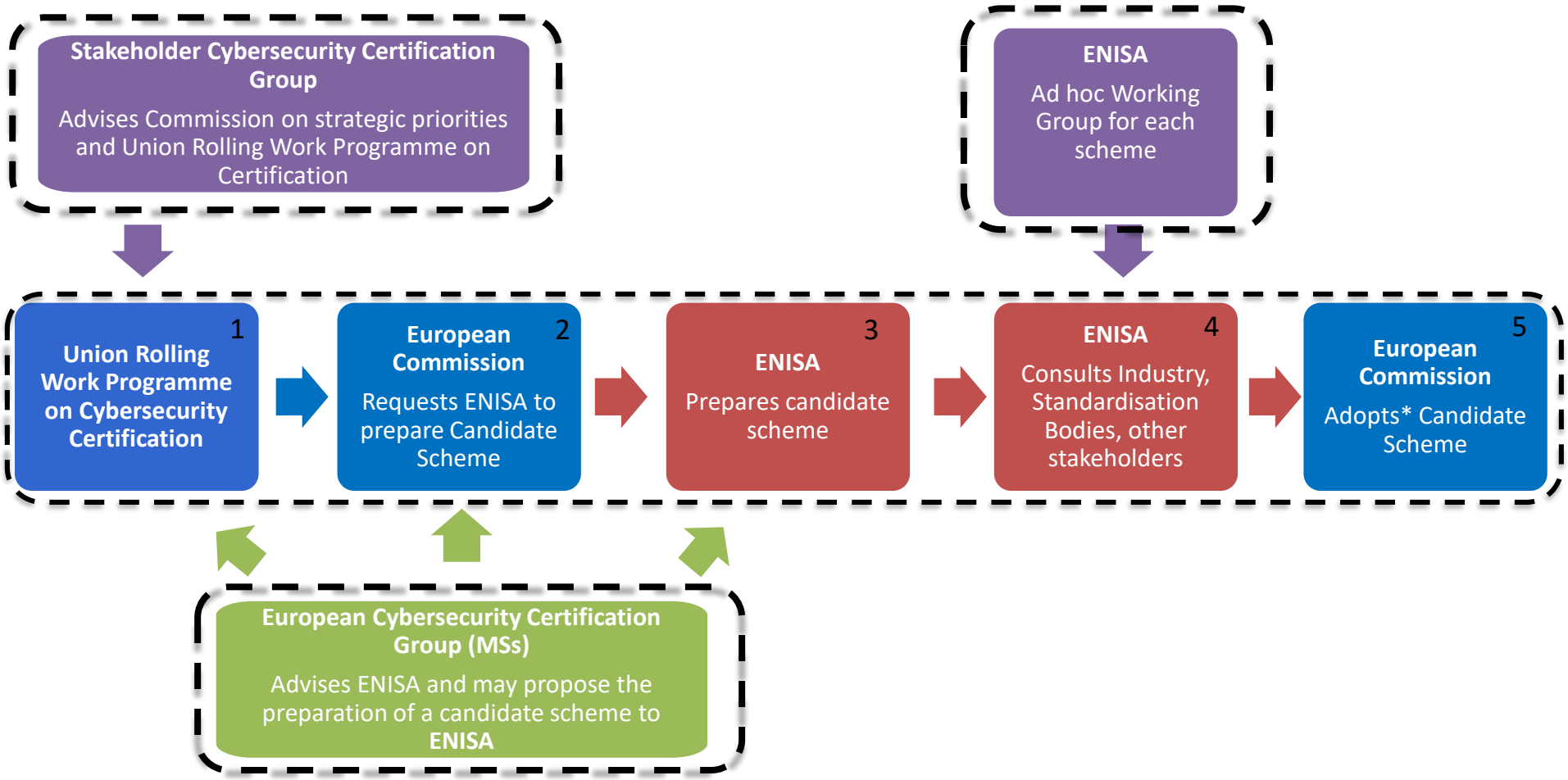
ENISA kommer få en betydande roll i hanteringen av certifieringsordningen.

Certifieringsramverket kommer att tillhandahålla ett EU-omfattande certifieringssystem omfattande en uppsättning regler, tekniska krav, standarder och förfaranden. Detta kommer att baseras på en överenskommelse på EU-nivå för utvärdering av säkerhetsegenskaperna för en specifik IKT-baserad produkt eller tjänst, t.ex. smarta kort.

Det producerade certifikatet kommer att erkännas i alla medlemsstater, vilket gör det lättare för företagen att handla över gränserna och för köpare att förstå säkerhetsfunktionerna för produkten eller tjänsten.

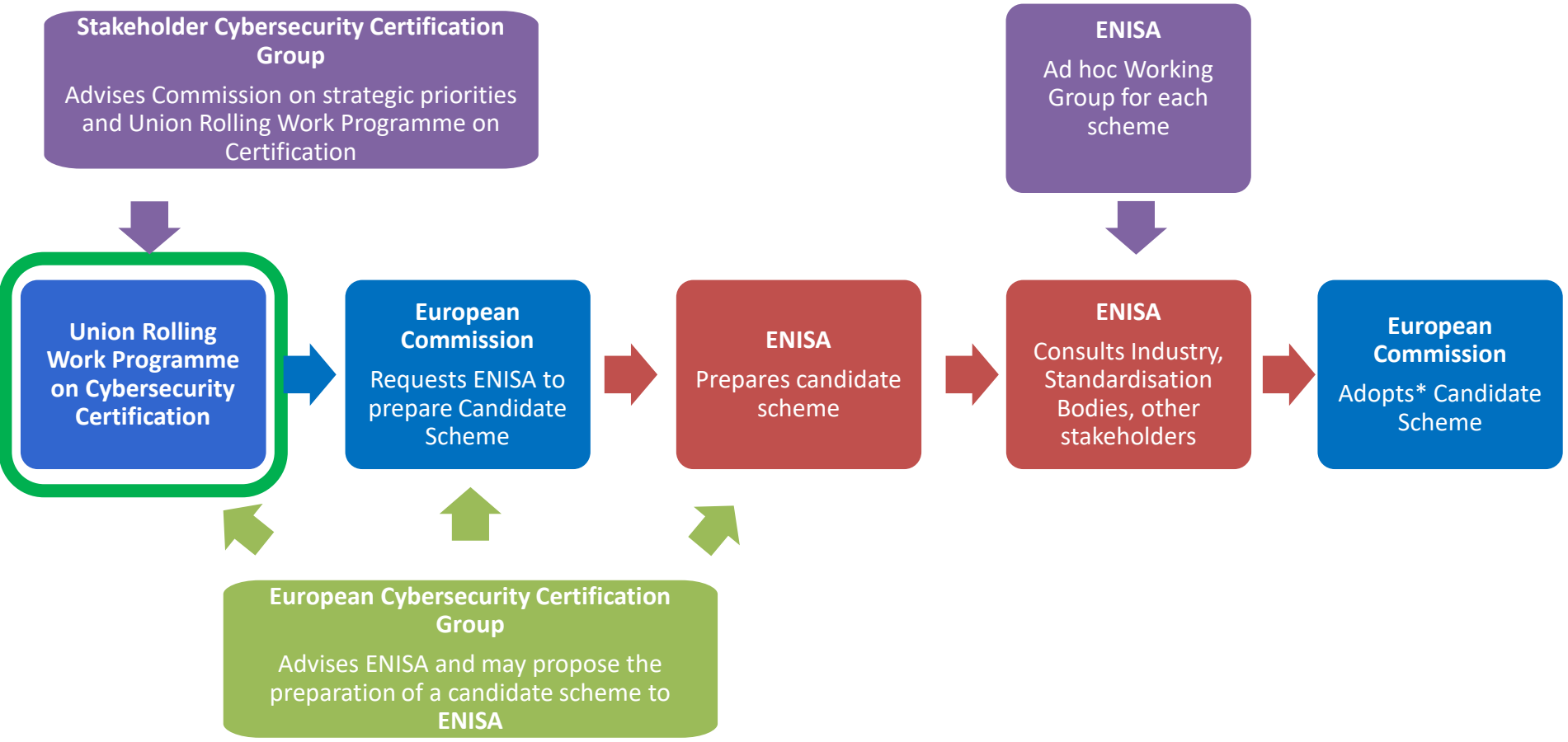
The EU Cybersecurity Certification Framework

The lifecycle of a European Cybersecurity Certification Scheme



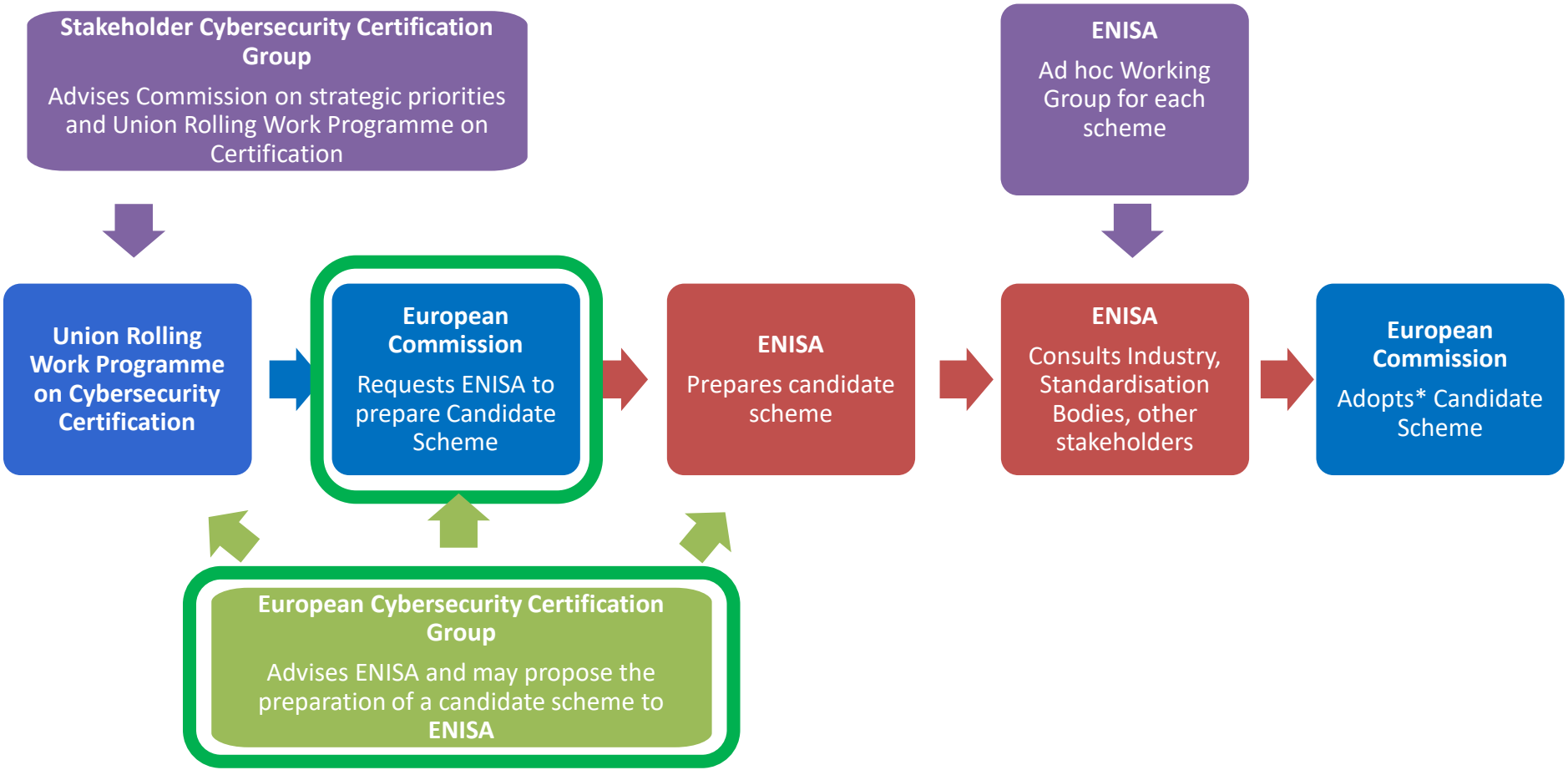
The EU Cybersecurity Certification Framework

Plan



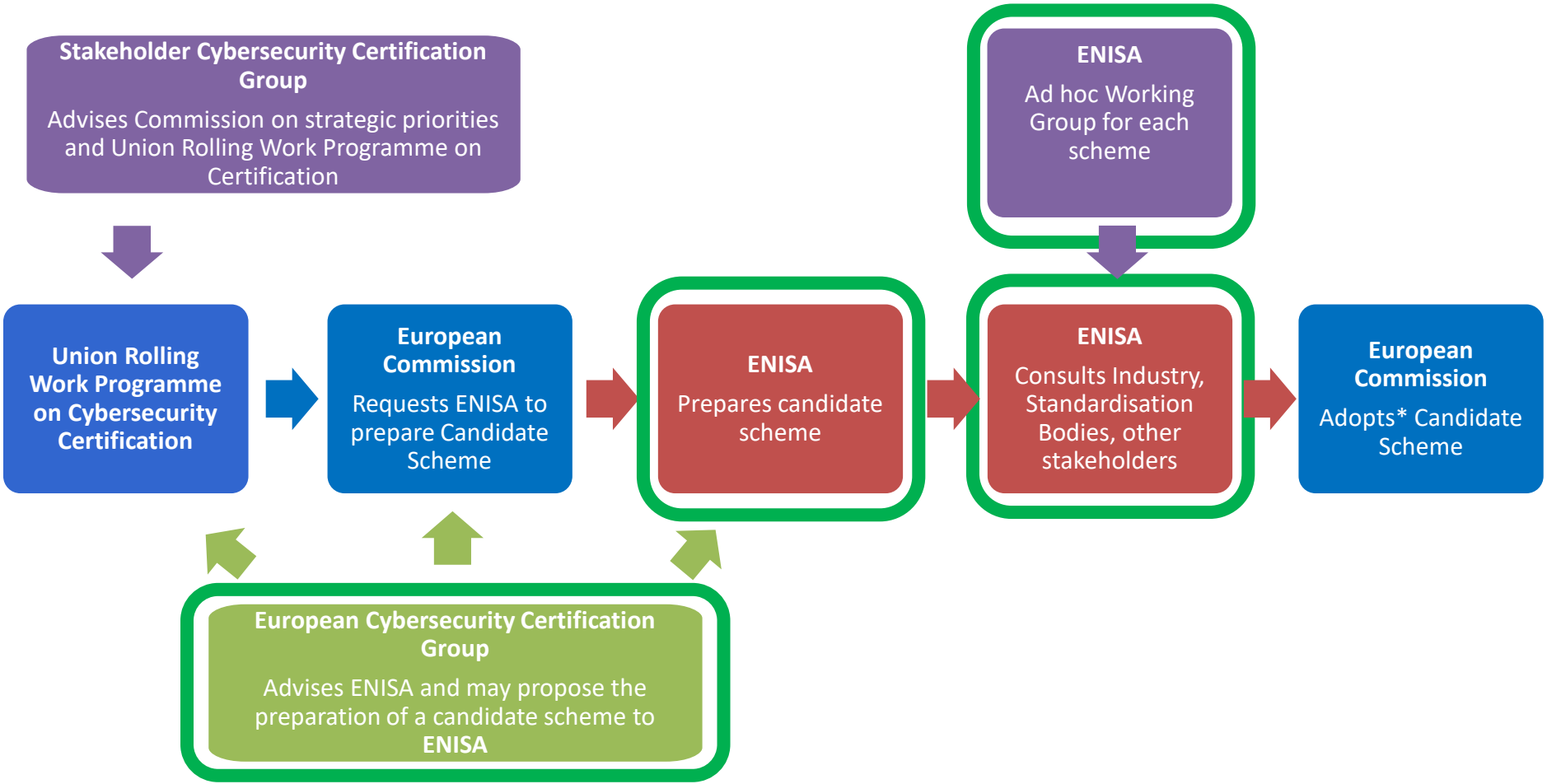
The EU Cybersecurity Certification Framework

Request



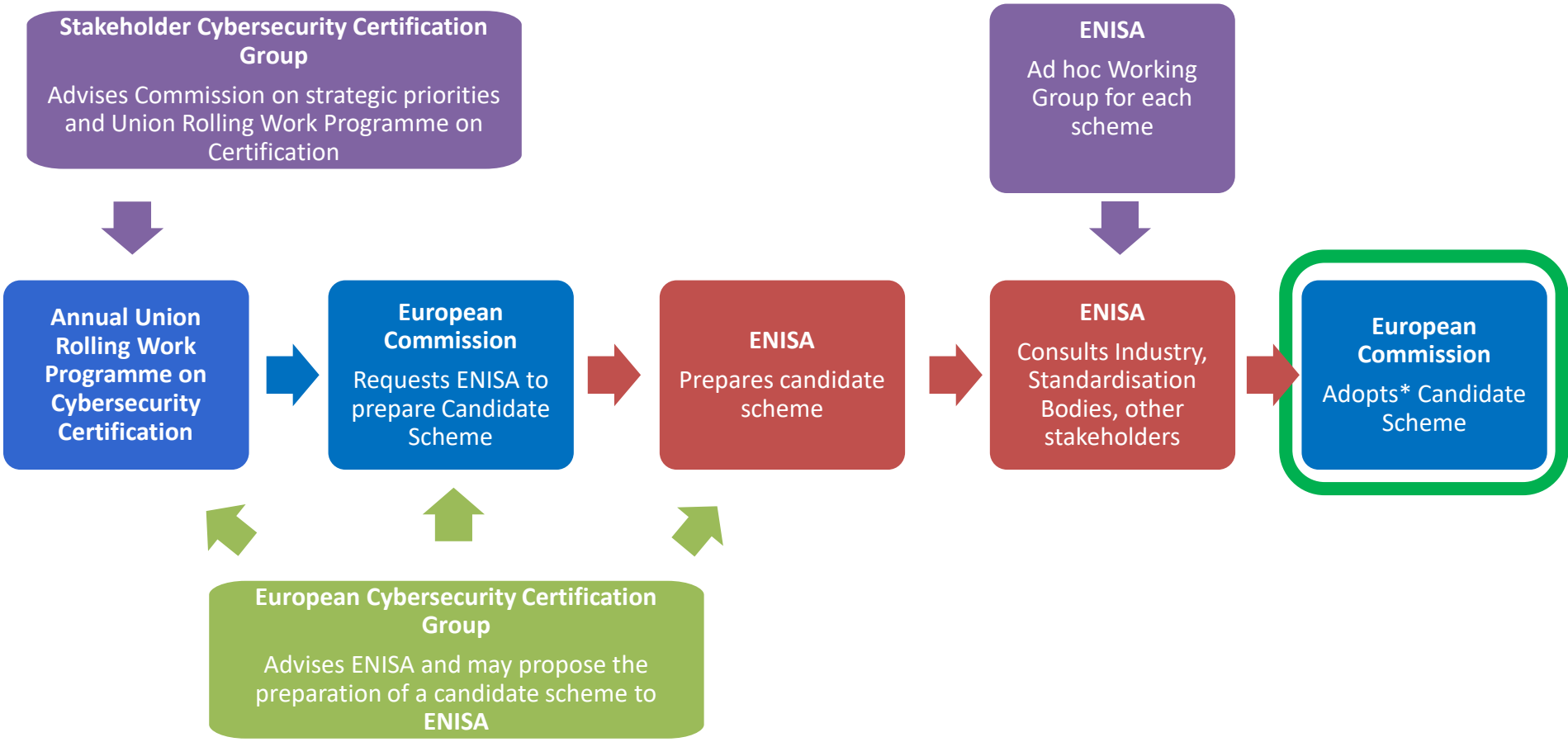
The EU Cybersecurity Certification Framework

Prepare



The EU Cybersecurity Certification Framework

Implement and Review



Vissa detaljer i ramverket

knowit

- Certifieringsordningen ska styras av tydliga säkerhetsmålsättningar
- Ramverket ska möjliggöra skapandet av skräddarsydda certifieringssystem för för cybersäkra IKT-produkter, tjänster och processer
- Ett ramverk, många scheman
- Certifieringen ska vara frivillig, om inte annat anges i EU-lag eller i lagstiftning i en medlemsstat
- Tre nivåer av certifiering: *Basic*, *Substantial*, *High*
- Ett europeiskt certifikat som utfärdats ska erkännas i alla medlemsstater
- Om ett europeiskt certifieringschemat kräver en "hög” assurance nivå, ska certifieringen enligt detta ramverk endast kunna utfärdas av ett nationell certifieringsorgan

Status i arbetet

knowit

2019-06-07

- CSA publicerad i EU Official Journal.

2019-06-27

- CSA träder i kraft, utom art 58, 60, 61, 63, 64 and 65.

2019-07-08

- Sr Hultqvist utser FMV/CSEC Dag Ströman till Sveriges representant i medlemsstaternas rådgivande grupp, ECCG.

2019-07-12

- Informellt möte för ECCG, Bryssel.

2019-07-23

- Kommissionen efterlyser kandidater till Näringslivets intressegrupp.
- OSA senast 2019-09-17

2019-08-06

- ENISA meddelar att de av Kommissionen ombetts att utveckla ett schema för Common Criteria, som ska ersätta SOG-IS MRA.
- ENISA efterlyser kandidater till expertgrupp som ska vara till stöd för ENISA, OSA 2019-09-19

2019-09-18

- Första formella ECCG-mötet i Bryssel

Vilka certifieringsordningar behövs?

knowit

- Kommissionen har redan bett ENISA att utveckla ett schema för IT-säkerhetsprodukter baserat på Common Criteria.
- Kommissionen förbereder även schemor för
  - Molntjänster (Cloud)
  - Industriautomation och kontrollsystem (IACS)
- Kommissionen inbjuder nu EU medlemsstater att föreslå andra prioriterade schemor.
- Vilka schemor behöver Sverige?

Några avslutande reflektioner kring certifiering

knowit

Det finns en spänning mellan vad EU kan göra och MS mandat
- Cybersäkerhet ligger i mitt i skärningspunkten mellan vad EU kan ”bestämma” - Handel och vad MS bestämmer - Nationell säkerhet.

EU-fokus eller globalt fokus?
- Det pågår en dragkamp inom EU mellan två viktiga principer:
a. Ska EU etablera regleringar, EU standarder och kontrollsystem som främjar EU-leverantörer (och därmed etablerar tekniska handelshinder) med åberopande säkerhetsargument (”fortress Europé”)?
b. Eller ska EU verka för globala standarder och kontrollsystem för att minska fragmentering och protektionism (”global cyber approach”)?

ENISA har fått en allt tydligare roll och det centrala styrmedlen för EU:s arbete med it-certifieringar blir ’The rolling work programme’.

Det är viktigt att framhålla att certifieriering av produkter inte ensamt är svaret på säkerhets-utmaningarna. Vi måste nu få till ett helt annat förhållningssätt när det gäller ICT utveckling - Mer **Security by designe** (bygga in säkerhet från början) och **Security by implementation** (Säker kod/Safe Code) - Detta måste reflekteras i vilka schemor som utvecklas och prioriteras.

TACK!

Richard Oehme
Senior Advisor Societal Security
Knowit, Cybersecurity & Law

T: +46 70 144 28 08 | E: richard.oehme@knowit.se
Knowit | Klarabergsgatan 60, 111 21 Stockholm | **knowit.se**

https://www.knowit.se
https://www.knowit.se/insight/facebook
https://www.knowit.se/linkedin
https://www.knowit.se/twitter
Twitter: @RichardOehme
LinkedIn: linkedin.com/in/richard-oehme-a17445153