THE EU CYBERSECURITY AGENCY

Cybersecurity certification

Eric Vetillard, Ph.D.
Lead Certification Expert
ENISA

03 | 02 | 2020

PROLOGUE

PRIVACY-RELATED ACTIVITIES AT ENISA

ACTIVITIES OVERVIEW

Guidelines/tools for data controllers

Tool — Risk assessment & security measures

Tool — Methodology for personal data breach assessment

Data protection by design and by default

Privacy Enhancing Technologies (PETs)

Data Protection Authorities
EDPB, EDPS, EC
Data controllers/industry
End users/ consumers

End users protection

Tool — PETs maturity assessment platform

Online privacy tools for the general public

Electronic Communications Privacy

Cookies

Tracking and Profiling

ACTIVITIES IN 2019

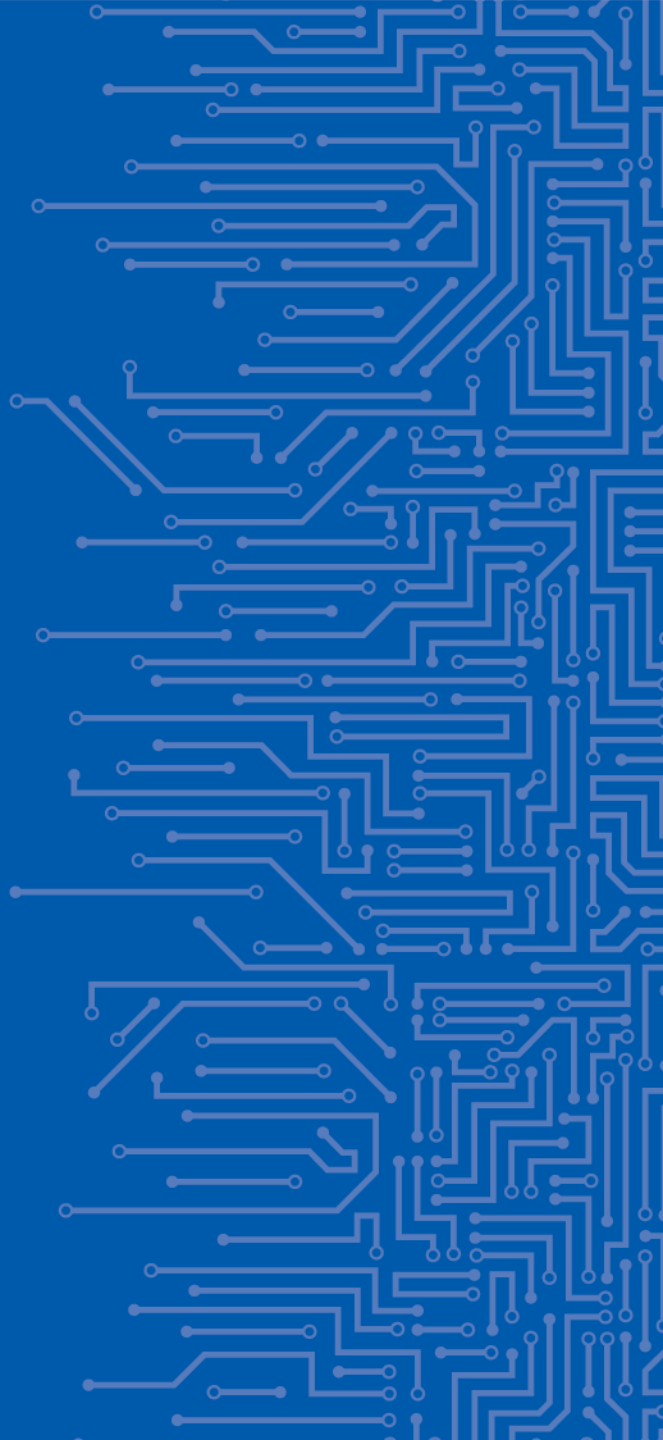
#1 Guidelines on data pseudonymisation

#2 Risk assessment tool for personal data security

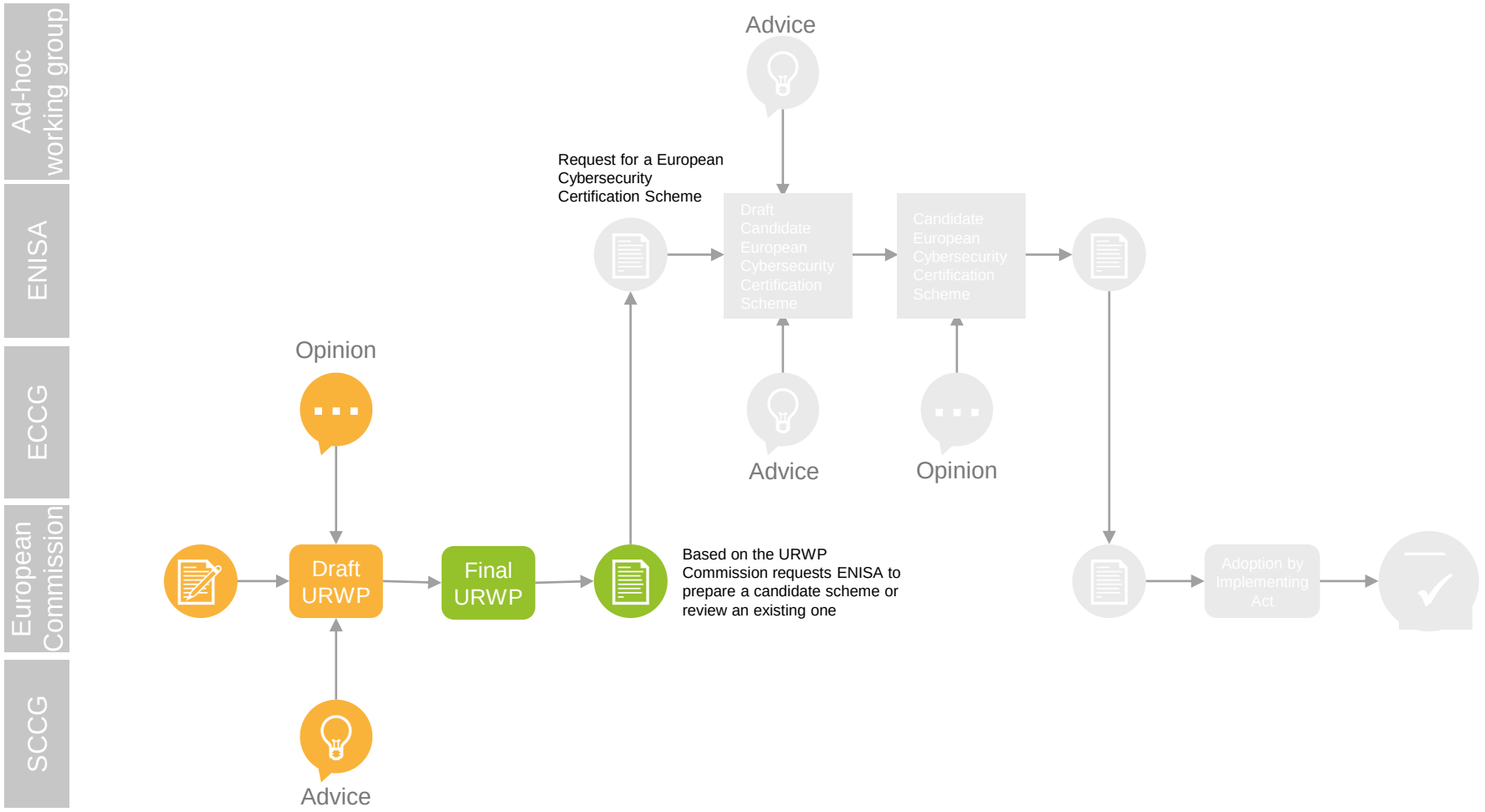
STAKEHOLDERS AND COMMUNITY BUILDING

CYBERSECURITY CERTIFICATION

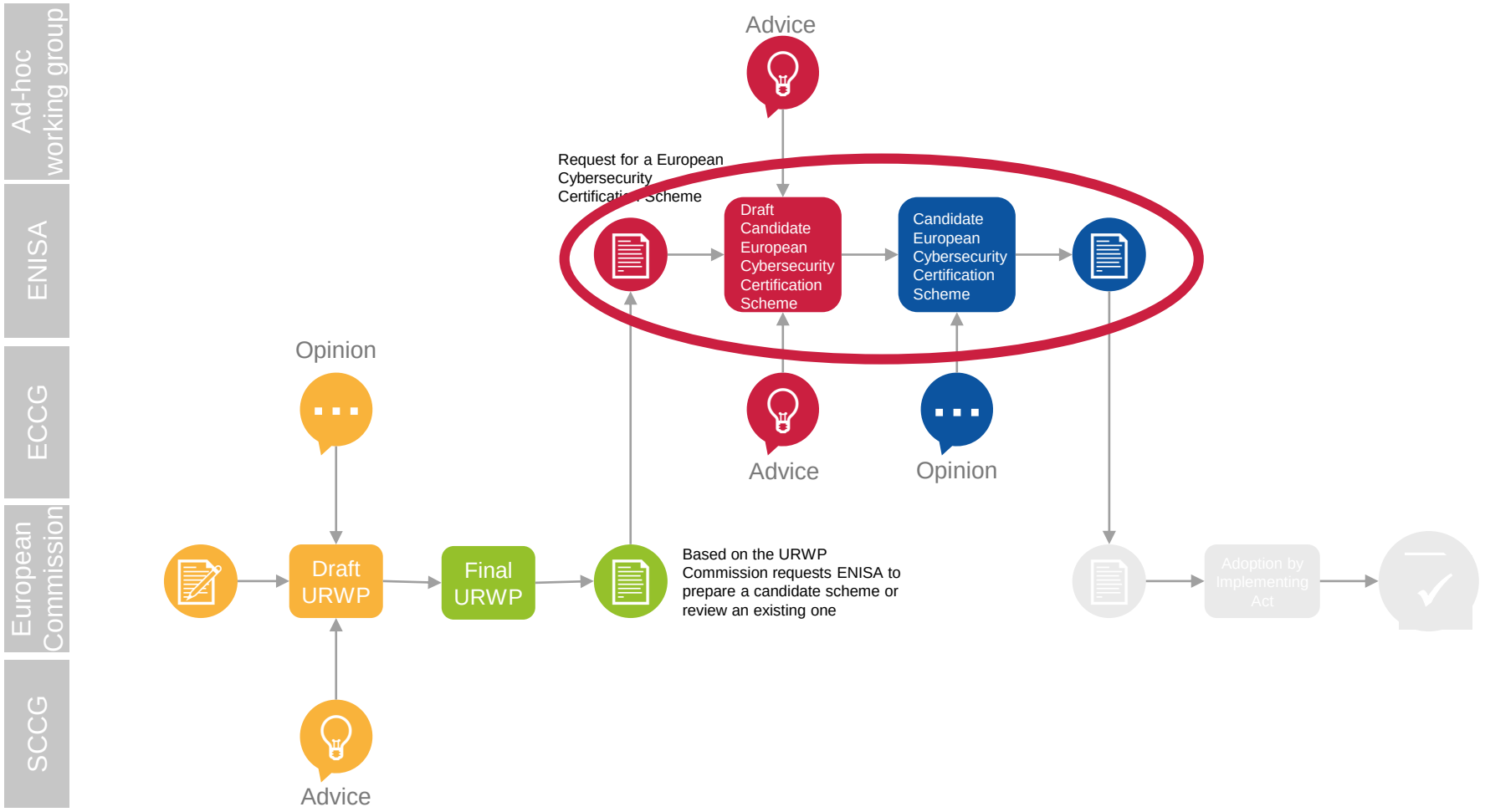
BUILDING A CERTIFICATION SCHEME



CERTIFICATION SCHEME PREPARATION PROCESS



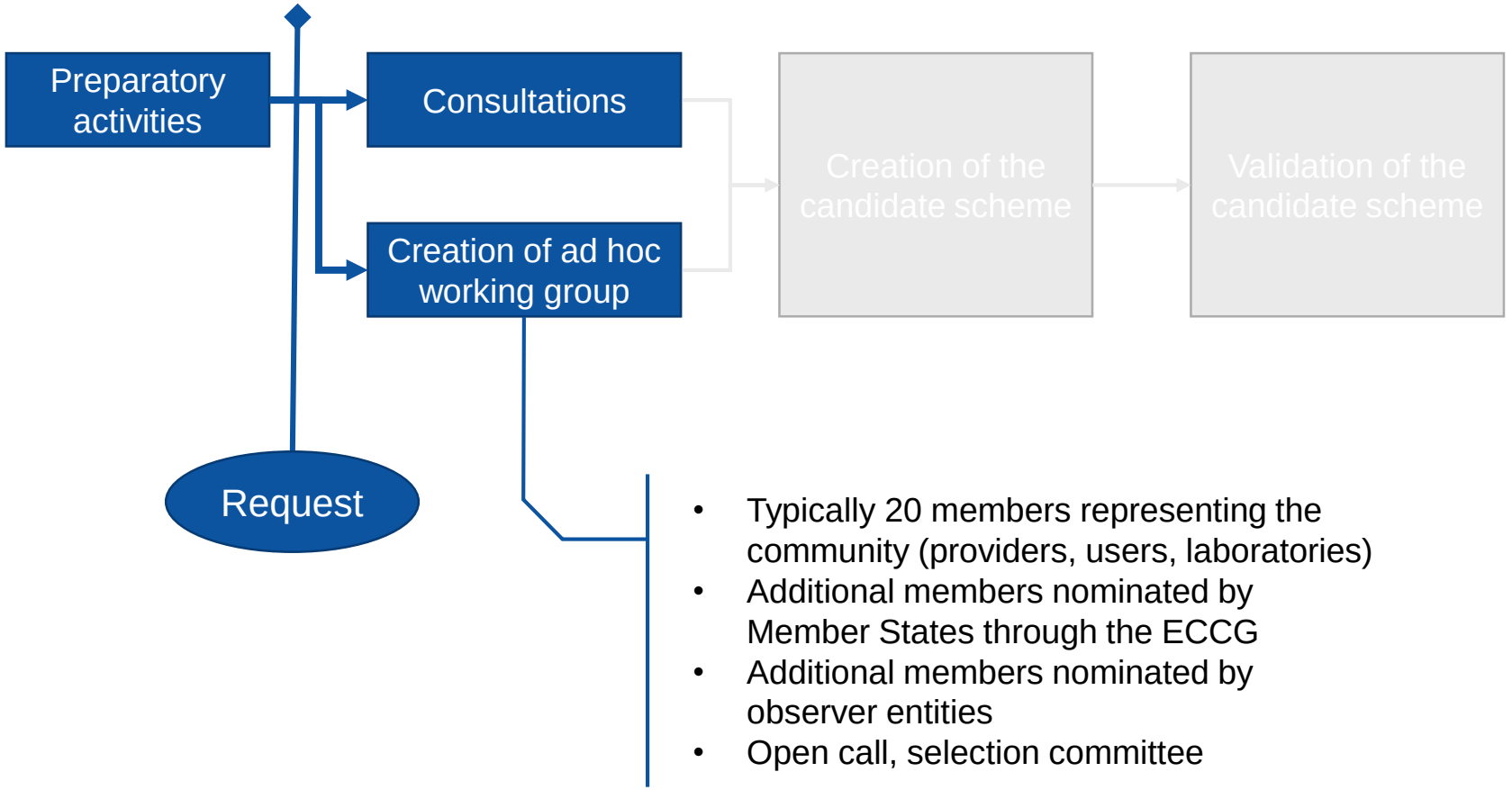
CERTIFICATION SCHEME PREPARATION PROCESS



WHAT IS IN A CYBERSECURITY CERTIFICATION SCHEME?

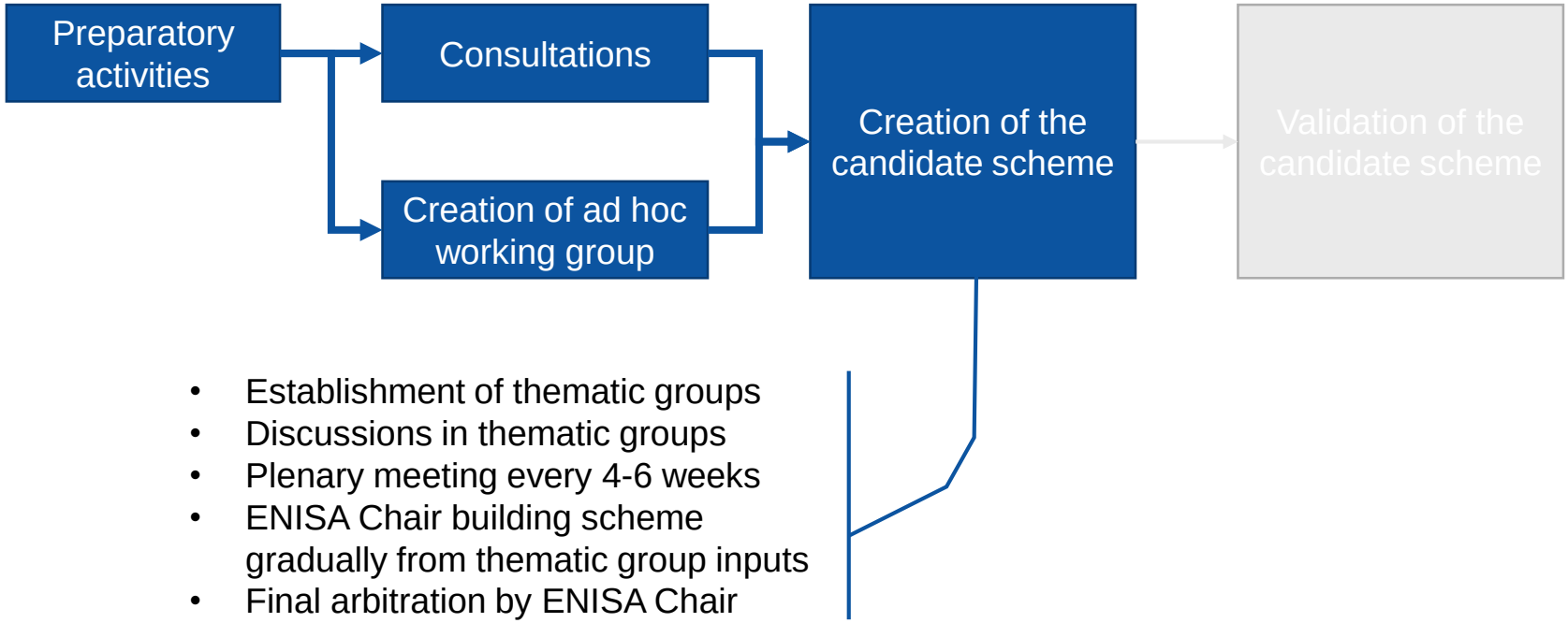
a. Subject matter and scope
b. Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
c. References to the international, European or national standards applied in the evaluation, and if not available to technical specifications
d. One or more assurance levels
e. An indication whether conformity self-assessment is authorized
f. Specific requirements for the CABs
g. Specific evaluation criteria and methods to be used
h. The information necessary for the evaluation or otherwise to be made available by the applicant
i. If applicable, the conditions of use of marks and labels
j. Rules for monitoring compliance of certified and self-assessed products
k. Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope
l. Rules concerning the consequences for products that have been certified or self-assessed and do not comply
m. Rules concerning how previously undetected vulnerabilities should be reported and handled
n. Rules concerning the retention of records by CABs
o. Identification of national and international schemes with the same scope
p. Content and format of the certificates and EU statements of conformity
q. The period of the availability of EU statements of conformity and related documentation
r. Maximum period of validity of certificates
s. Disclosure policy for certificate issuance, withdrawal, amendment
t. Conditions for mutual recognition with third countries
u. Where applicable, rules for peer assessment
v. Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

BUILDING A CERTIFICATION SCHEME
AD HOC WORKING GROUP

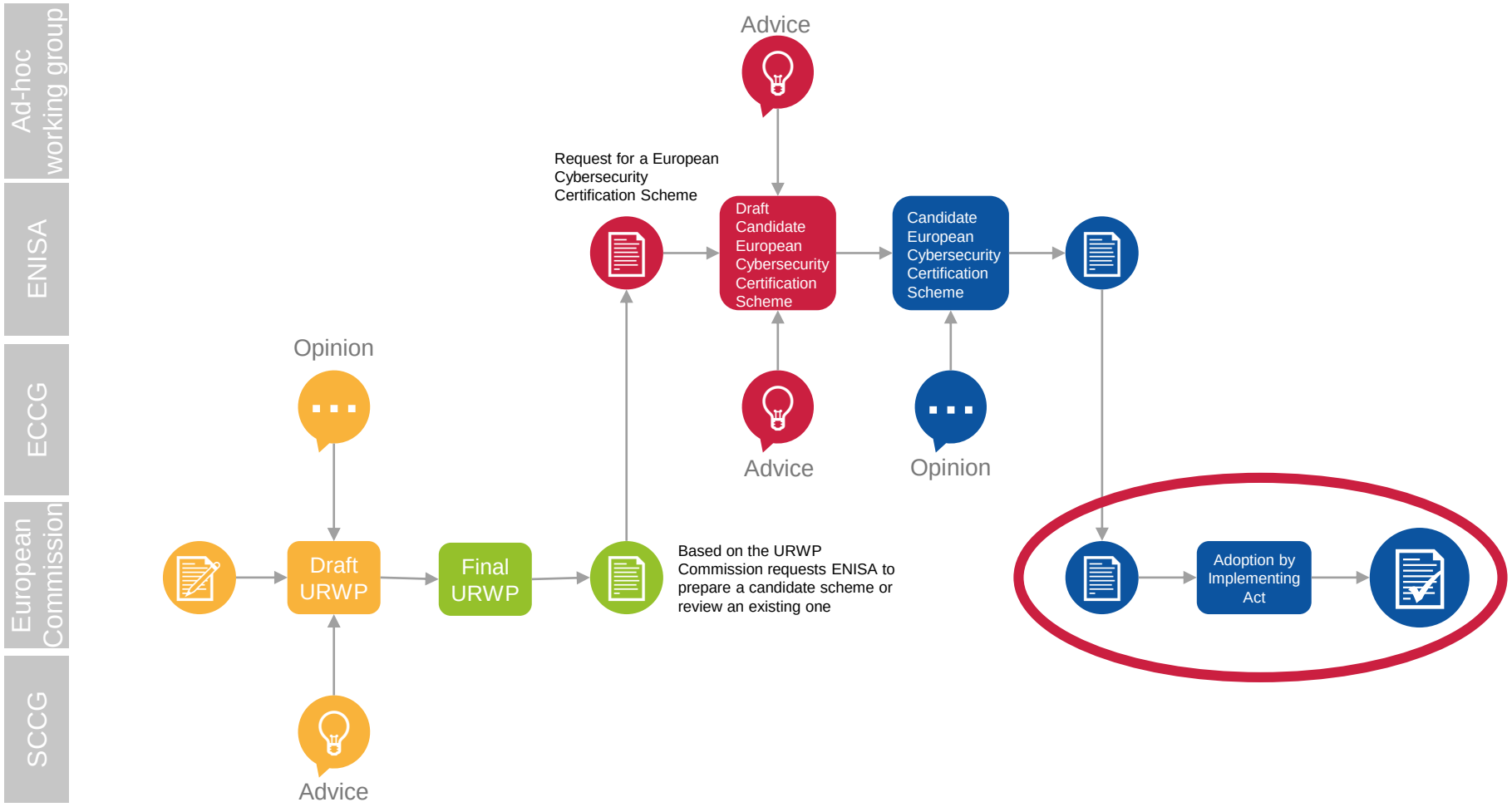


- Typically 20 members representing the community (providers, users, laboratories)
- Additional members nominated by Member States through the ECCG
- Additional members nominated by observer entities
- Open call, selection committee

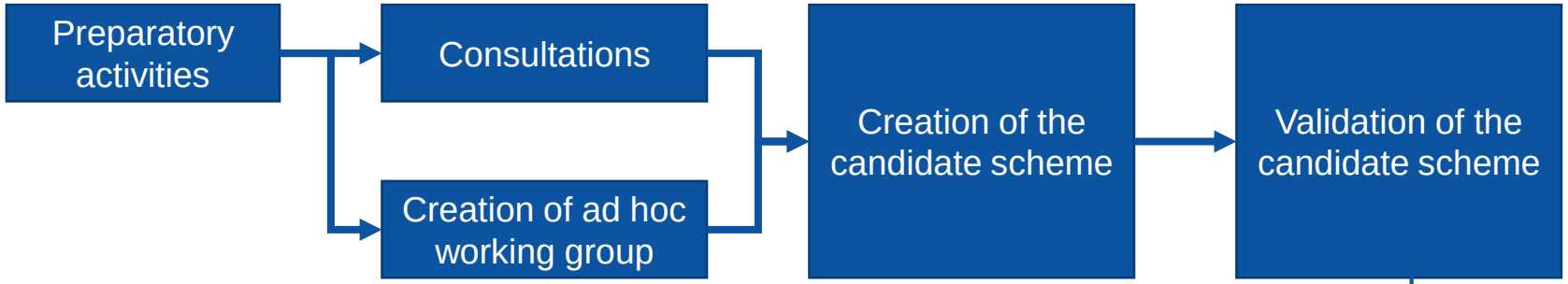
BUILDING A CERTIFICATION SCHEME *NEGOTIATION AND CREATION*



MAKING THE SCHEME INTO LAW



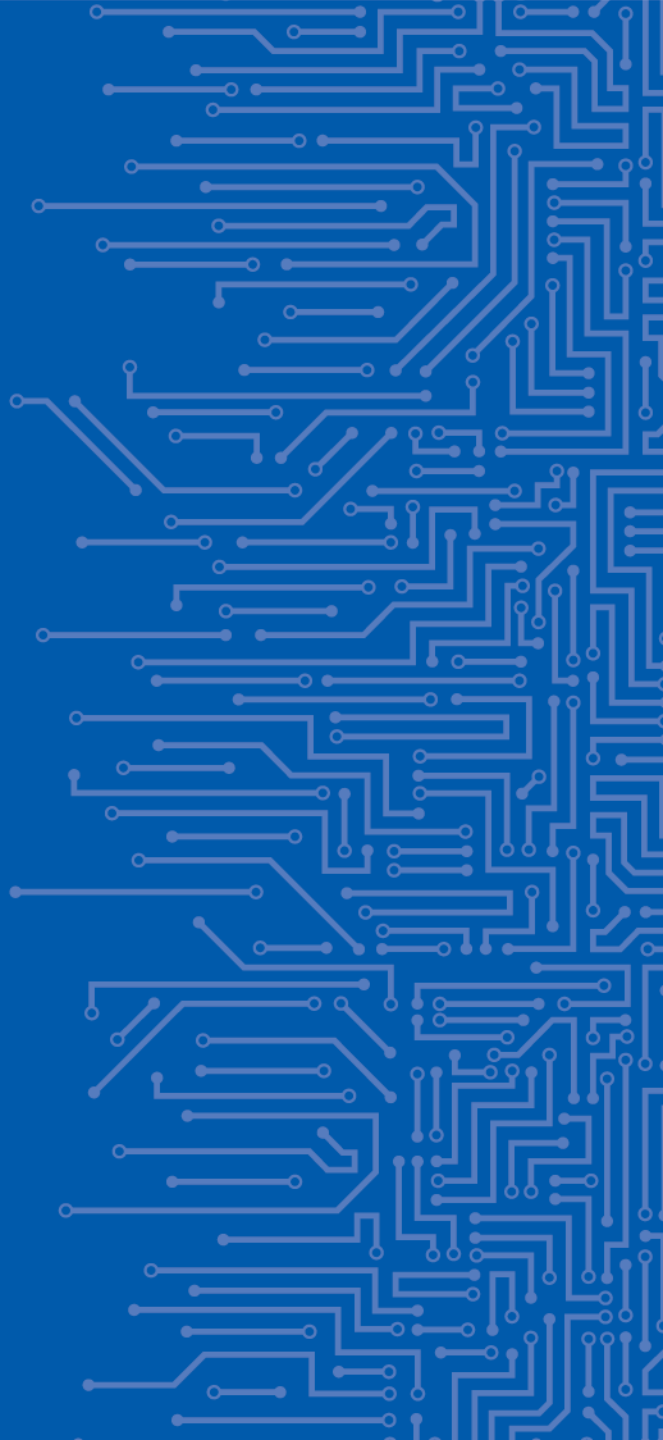
BUILDING A CERTIFICATION SCHEME *VALIDATION*



- Public and open validation phase
- Then, validation by the ECCG
- Continued validation during comitology
- The scheme may come back to the ad hoc Working Group at any time

CYBERSECURITY CERTIFICATION

A SCHEME FOR CLOUD SERVICES



CURRENT STATUS

Two requests received from the Commission, Union Rolling Work Programme in preparation.

The two schemes are under preparation:

- A continuation to the SOG-IS scheme
- A scheme for cloud services

A work programme is being prepared

- To be released at the end of June
- By the Commission, with input from member states (ECCG) and stakeholders (SCCG).

More scheme requests may be received before June

THE CLOUD SERVICES SCHEME

The cloud services scheme is the second request received from he commission, in November 2019.

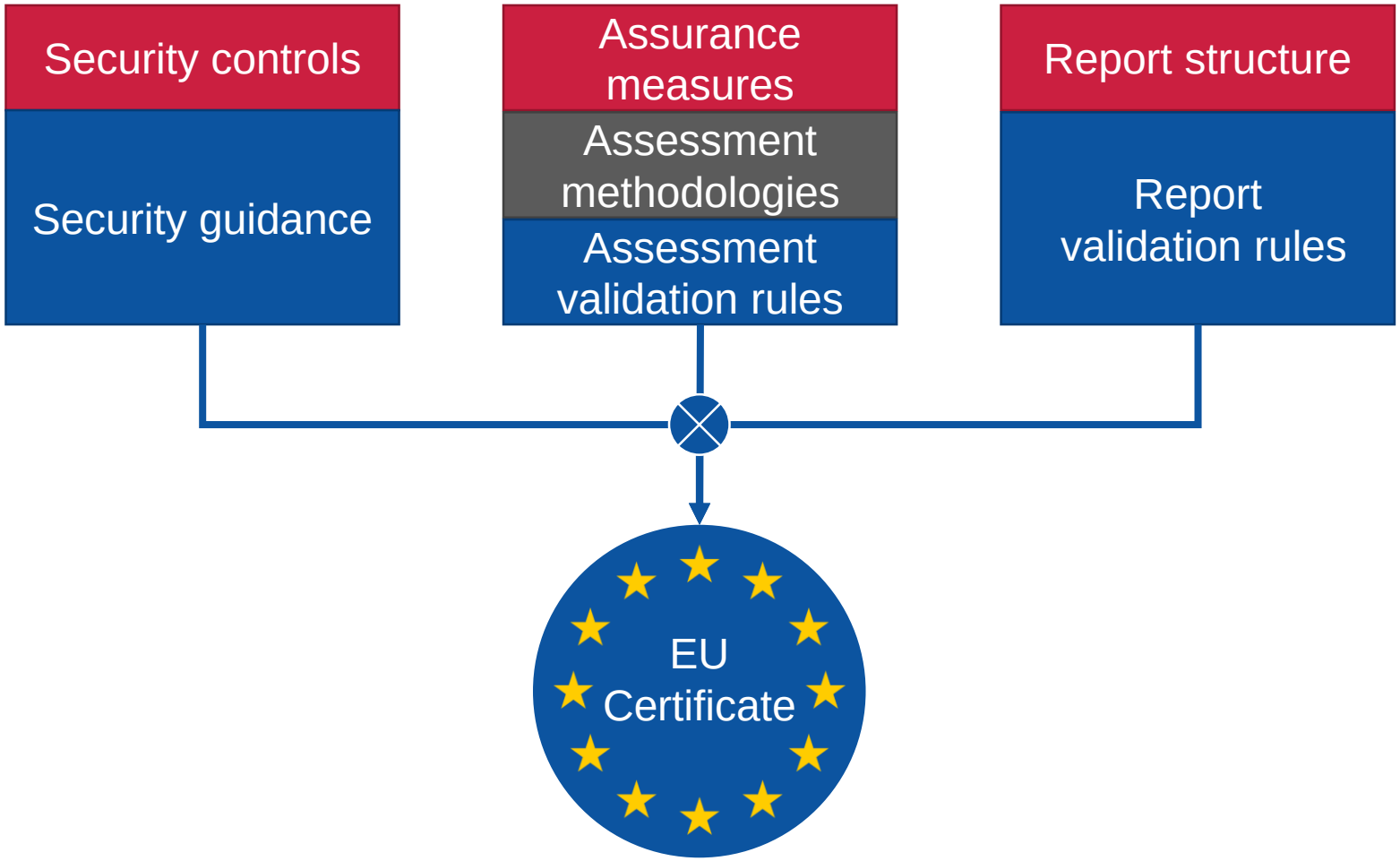
A horizontal scheme covering all cloud services

- From infrastructure (IaaS) to complete services (SaaS)
- Covering all suitable levels (Basic, Substantial, High)
- Need to support many different verticals

Many challenges ahead

- No basis like Common Criteria: A lot of content to create
- Several schemes from Member States and private bodies

SOME INITIAL DIRECTIONS



CLOUD CYBERSECURITY & PRIVACY

Security certification is a technical tool, and a prerequisite for privacy.

Security certification only addresses technical issues

- Don’t count on us to solve sovereignty issues
- Don’t count on us to verify privacy issues
- But you can count on us to support you on technical matters

Security controls to be verified for privacy

- Technical controls like encryption, authentication, *etc*.
- Organizational controls like requirements for risk analysis or strict management
- But, no privacy-specific measures like pseudonymisation

A SECURITY PROFILE FOR PRIVACY?

Could we complement the core scheme for privacy?

What possibilities are offered?

- Refining existing security controls
- Add new security controls
- No way to add assurance measures, only shift in levels

Could that be useful in the context of privacy?

- I don’t know, but may be you do

CONSUMER CLOUD SERVICES *PRIVACY & SECURITY COMPLIANCE*

The cybersecurity scheme for cloud services does not directly address consumers

For consumers, we need to add a few important things

- A specific risk analysis for the customer service
- Add new security controls
- A result that can be easily understood with marks and labels

Looking at ways to move ahead

- Is this another security scheme?
- Should we link security and privacy for consumer services?
- Both aspects are important yet hard for consumers

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europe.eu