Security Conference 2022

European Cybersecurity Certification Framework

Eric VETILLARD, ENISA

03/10/2022

AN EU SCHEME?

The EU Cybersecurity Act has defined the idea of a European Cybersecurity Certification Framework.

Certification is seen as a useful tool in the fight for cybersecurity

- An EU-wide framework can promote the use of certification in Europe, reducing market fragmentation
- Harmonization between EU countries is a positive development for vendors, reducing the costs of certifying the same product / service in several schemes and standards
- Certification can be a useful tool for procurement by EU companies and Member States

Certification remains voluntary in principle

- Latest draft regulations mention regulation as a way to be “presumed compliant” to requirements
- Yet, certification may eventually become mandatory in specific use cases with due justification

THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

The framework is defined by Regulation (EU) 2019/881, including some design principles for schemes.

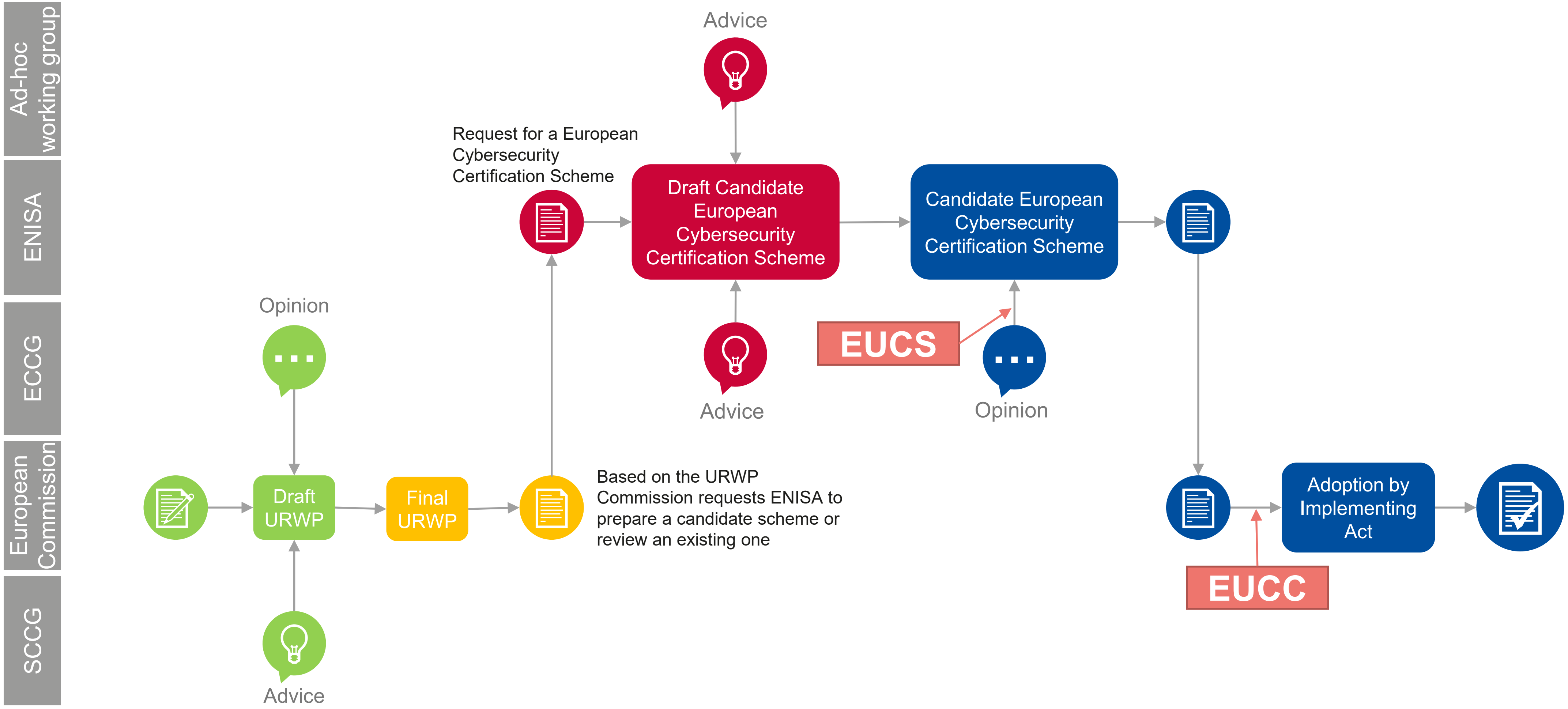
The framework defines concepts such as:

- Several assurance levels: ‘basic’, ‘substantial’ and ‘high’, for different uses, based on a risk assessment
- Mandatory disclosure of critical information from vendors, including security user documentation
- Continuous compliance monitoring beyond initial certification

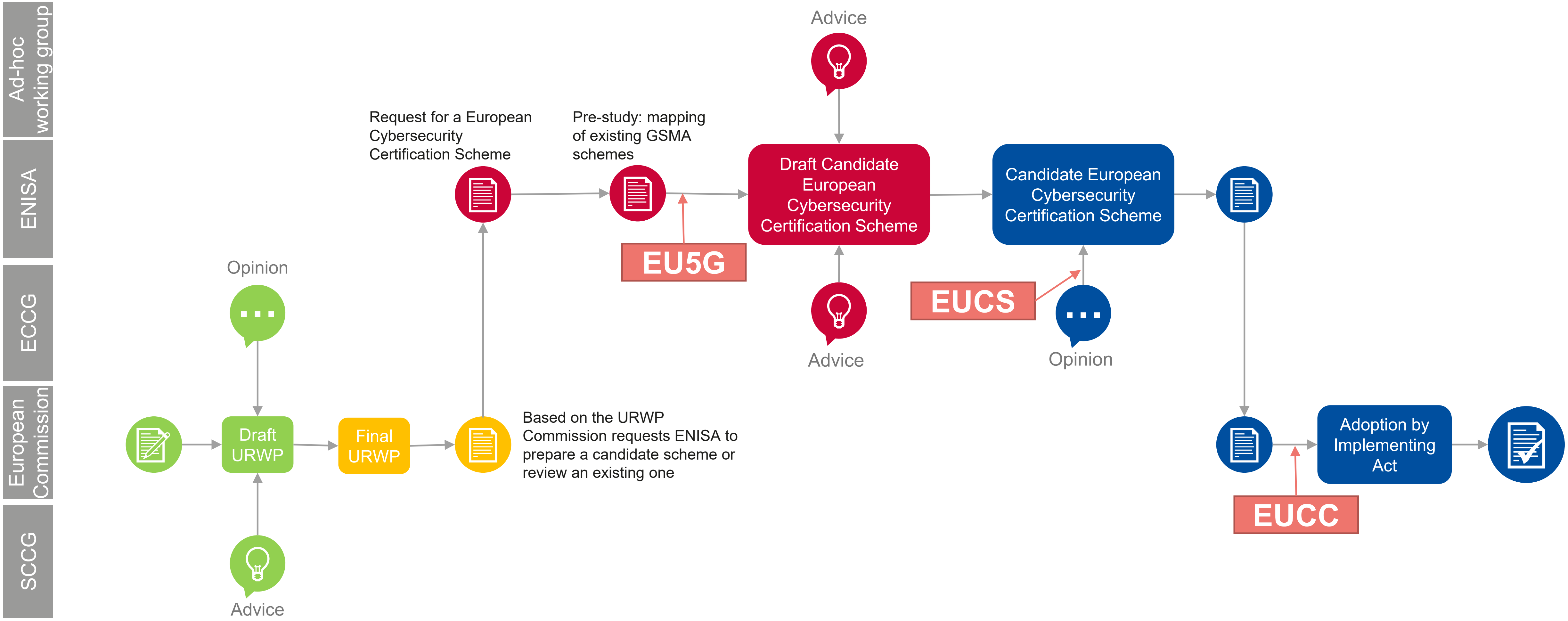
WHAT IS IN A CYBERSECURITY SCHEME?

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, 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

EUCS SCHEME PREPARATION PROCESS


Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Opinion
Draft URWP
Final URWP
Advice
Request for a European Cybersecurity Certification Scheme
Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one
Advice
Draft Candidate European Cybersecurity Certification Scheme
Advice
Candidate European Cybersecurity Certification Scheme
EUCS
Opinion
Adoption by Implementing Act
EUCC

EUCS SCHEME PREPARATION PROCESS


Ad-hoc working group
ENISA
ECCG
European Commission
SCCG
Opinion
Draft URWP
Final URWP
Advice
Request for a European Cybersecurity Certification Scheme
Pre-study: mapping of existing GSMA schemes
EU5G
Advice
Draft Candidate European Cybersecurity Certification Scheme
Advice
Candidate European Cybersecurity Certification Scheme
EUCS
Opinion
Adoption by Implementing Act
EUCC

Based on the URWP Commission requests ENISA to prepare a candidate scheme or review an existing one

MANY CHALLENGES, SOME UNFORESEEN

The development of schemes faces challenges, generic and specific, foreseen and unforeseen.

Among the generic challenges, some challenges were foreseen

- Each scheme is an Implementing Act, *i.e.*, a law: not practical for a new development
- A scheme is a live document, evolving with technology and current practice

Sone challenges were unforeseen

SPECIFIC CHALLENGES

EUCC, the pioneer

The first scheme in the ECCF

- Every process is new
- Every process takes more time than expected
- Some processes run into issues, like the drafting on the Implementing Act
- New regulations (CRA)

EUCS, the wild west

The first uncharted scheme

- No basis for requirements or for assessment
- Contributed the result to CEN/CENELEC for maintenance
- Bonus question on sovereignty

EU5G, public-private

Existing private schemes

- The requests mentions the schemes from GSMA
- An EU scheme has very different constraints
- Relationship is somehow new

LOOKING FORWARD: FEASIBILITY STUDIES

The next schemes will face some of the same issues, and some new ones. How to optimize the development process?

Learn from experience

- We are already doing it: EUCS reused many EUCC concepts, EU5G is reusing EUCS and EUCC ideas

Work at the framework level

- Some thematic groups, like on vulnerabilities, are shared between all schemes

Be prepared

- We will work on feasibility studies on the topics mentioned in the URWP
- Identifying stakeholders, regulatory and certification context, possible challenges
- First targets are expected to be AI and IoT, both coming with interesting challenges

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎ +30 28 14 40 9711

✉ certification@enisa.europa.eu

🌐 www.enisa.europa.eu