EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity certification in ENISA

Dr Andreas Mitrakas
Head of Unit “Data Security & Standardisation”

“The Future of Standards in Cybersecurity” PKN/NIT/ ISO/IEC JTC 1/SC 27 Conference, Warsaw

17 | 09 | 2020

ENISA mission in cybersecurity certification

To contribute to the emerging EU framework for the certification of products, services and processes

To draw up **certification schemes in line with the Cybersecurity Act** providing stakeholders with a sound service that adds value to the EU while supporting the framework

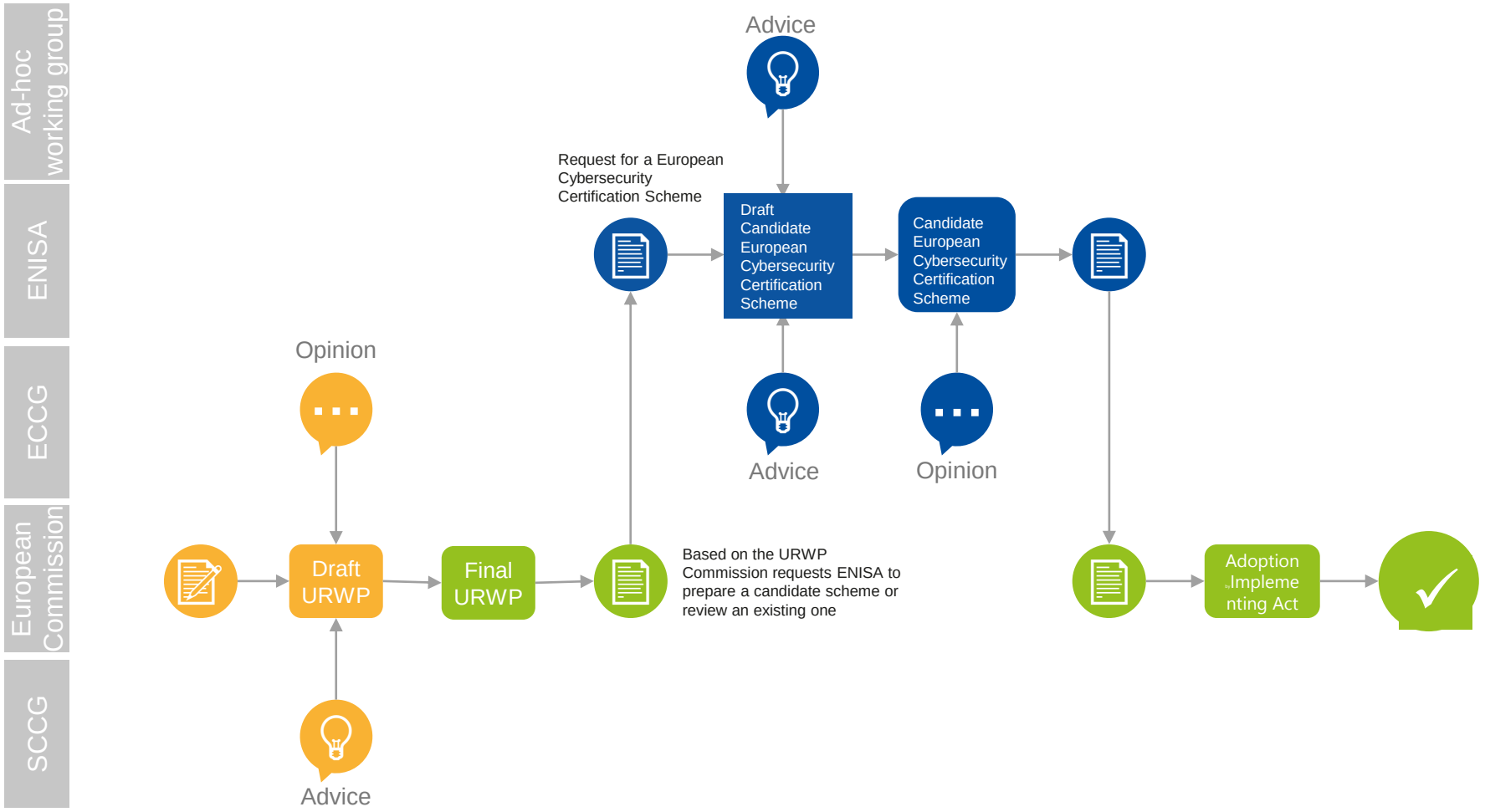
Key outputs

- Draft and finalised candidate certification schemes products, services and processes
- Secretariat support (SCCG) and Co-chair SCCG (w/ Commission)
- Support the Commission to Chair ECCG
- Support review of adopted certification schemes
- Implement and maintain a public website
- Support peer review of national cybersecurity certification authorities
- Advice on market aspects relevant to cybersecurity certification

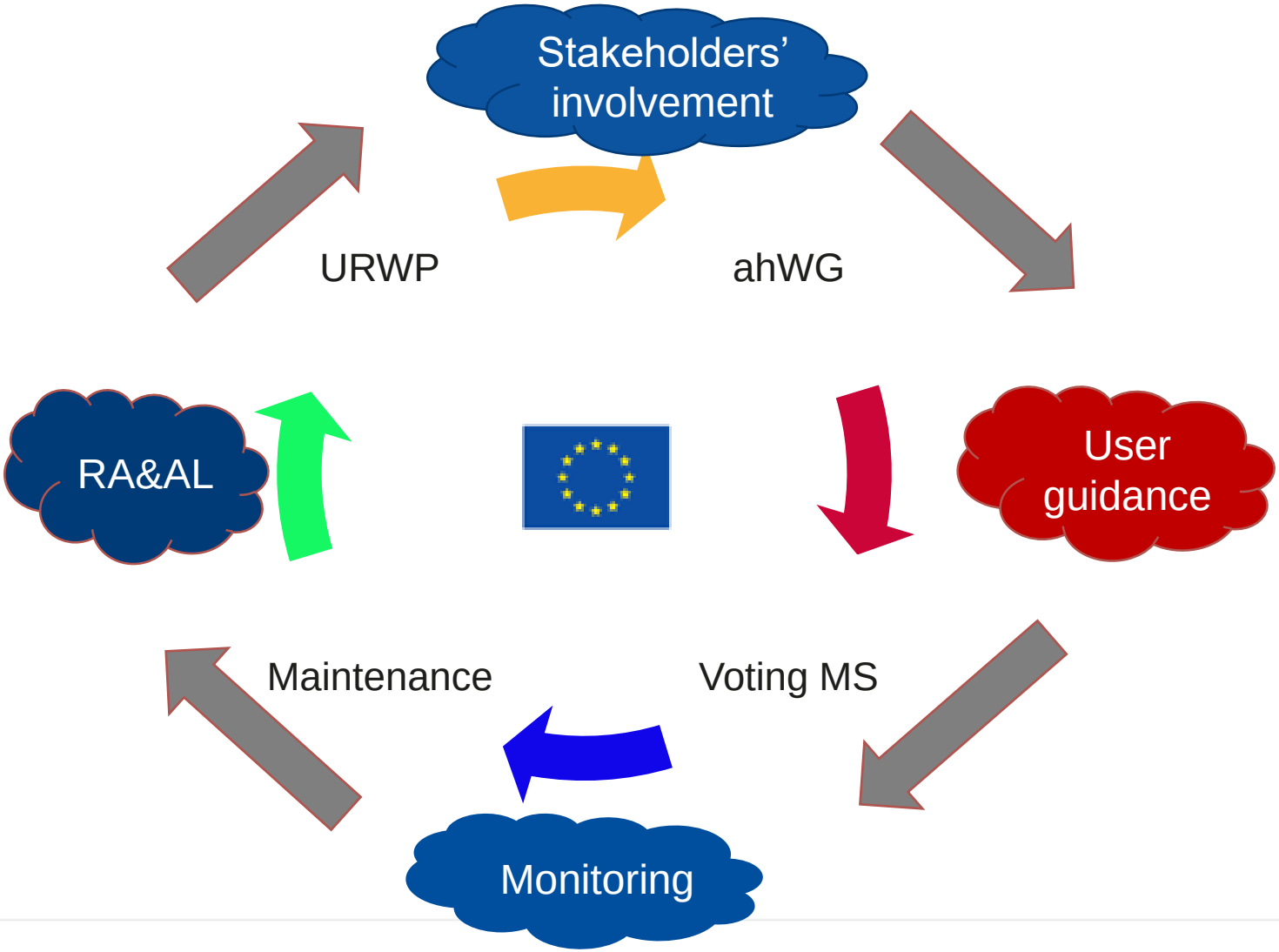
CERTIFICATION SCHEME
WHO'S WHO

Ad-hoc working group	• Representatives of the community, invited by ENISA ED • Advises ENISA while preparing a specific candidate scheme
ENISA	• In charge of writing candidate schemes • Leads the preparation work
ECCG	• European Cybersecurity Certification Group • Representatives of the Member States (National Authorities) • Member States are implementing the schemes
European Commission	• Coordinates the work on schemes through requests to ENISA • Writes implementing acts from candidate schemes • Manages comitology
SCCG	• Stakeholders Cybersecurity Certification Group • Representatives of the community, advises on work programme

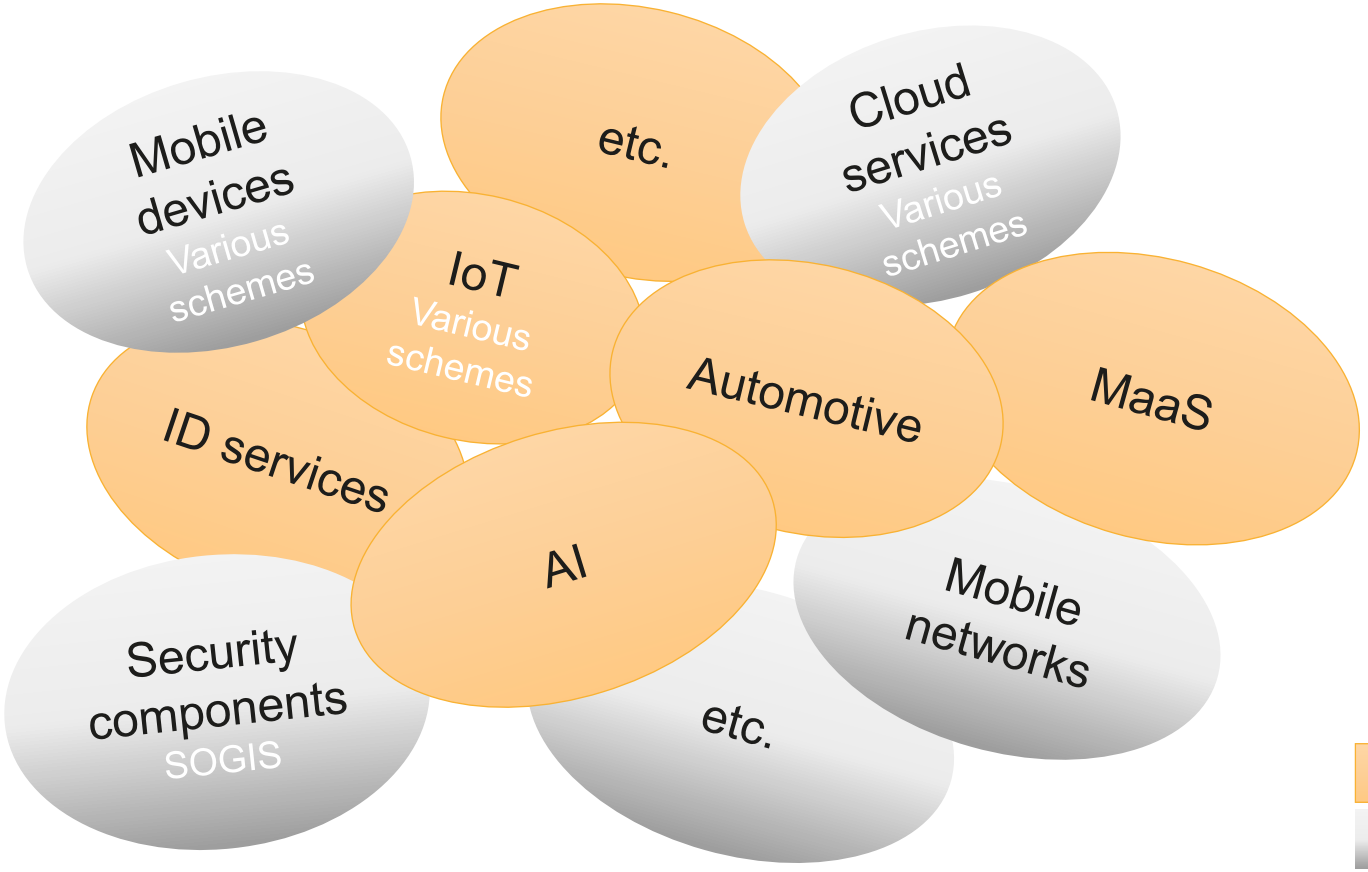
CERTIFICATION SCHEME *PREPARATION PROCESS*



Lifecycle reflections

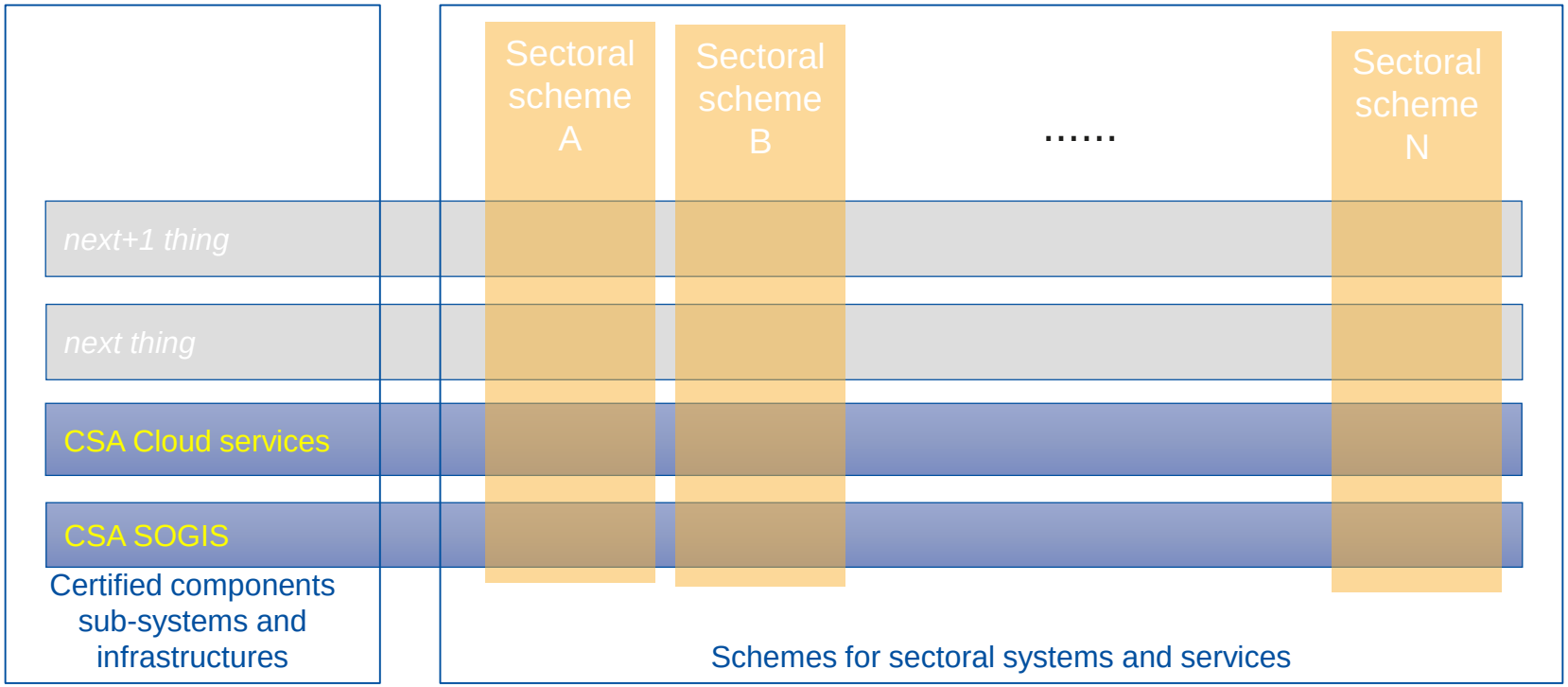


A MULTITUDE OF CANDIDATES



STRUCTURING AND PRIORITIZING

Sectoral schemes benefit from a broad availability of certified components and subsystems



BENEFITS AND BENEFICIARIES

Certification proves conformity to an implementation specification

- Security requirements to a component, system of service must be defined
- Appropriate security measures must be specified

Beneficiaries of cybersecurity certification

- **Customers (B to C and B to B) can rely on a defined assurance level of a service**
- **System owners can rely on the security level of supplied components or subsystems**
- **Service providers can rely on a defined assurance level of an infrastructure that they would like to use for their services or a business partner that they want to cooperate with.**

Benefits of cybersecurity certification:

- Enables an open marketplace / supply chain for security products and services
- Establishes trust between system operators and service providers without the need for a direct partnership → Enables establishing multi-stakeholder service ecosystems on a notional or multinational scale.

EXAMPLE

Example telecommunications

- **Global system**
- **Implementation state of certification**
  - **Evaluation and certification addresses all aspects of interoperability → implemented e.g. by the Global Certification Forum**
  - **Security certification implemented in some areas, more to come.**

RISK BASED REQUIREMENTS

CSA suggest

- **risk-based identification of security and certification requirements**
- **risk-based assignment of assurance levels**
- **security by design**

Proposal: Risk assessments (RA) for sectoral systems and services

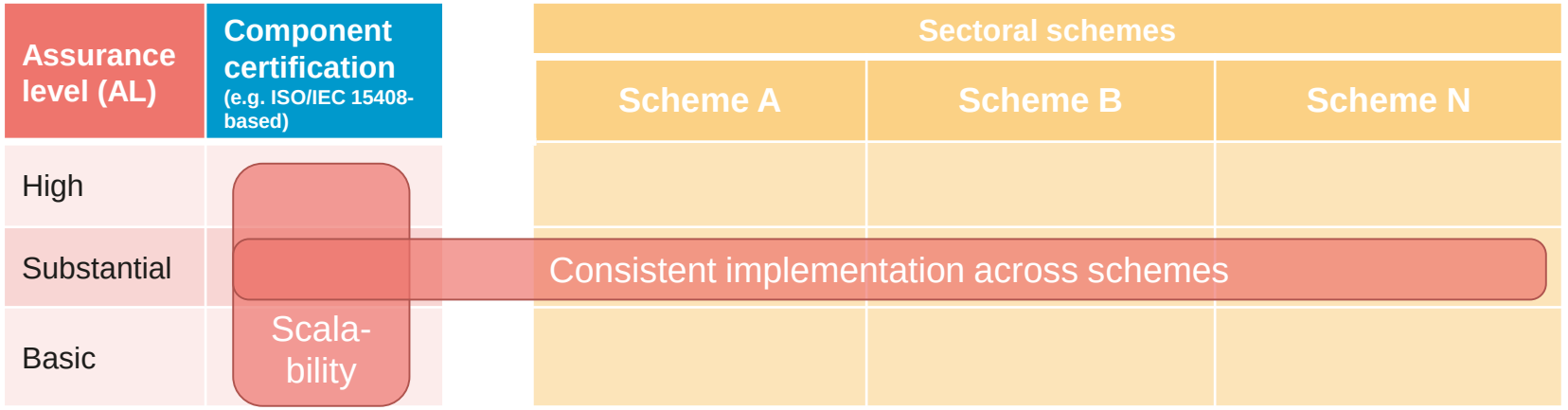
- **Stakeholder involvement for definition of assets / scenarios**
- **Transparent process for identification of risks**
- **Risk based definition of security / certification requirements and assurance levels**
- **Risk-based input for security by design**
- **Inputs for architecture optimization concerning efficient, cost-effective certification**

Objective: Stakeholder acceptance by hitting the balance between relevant risk and cost for security & security certification

COHERENCE

SUPPORTING RE-USE, AVOIDING FRAGMENTATION

Consistency and scalability are key for market acceptance



Scalability: Schemes should minimize effort for upgrades of certified products/subsystems to higher AL

Consistent implementation of AL across schemes:

- Supports seamless integration of certified products or subsystems in other schemes
- Optimizes vendor's market reach and minimizes cost of certification per product/subsystem

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