EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity Certification in the EU: Breaking New Ground

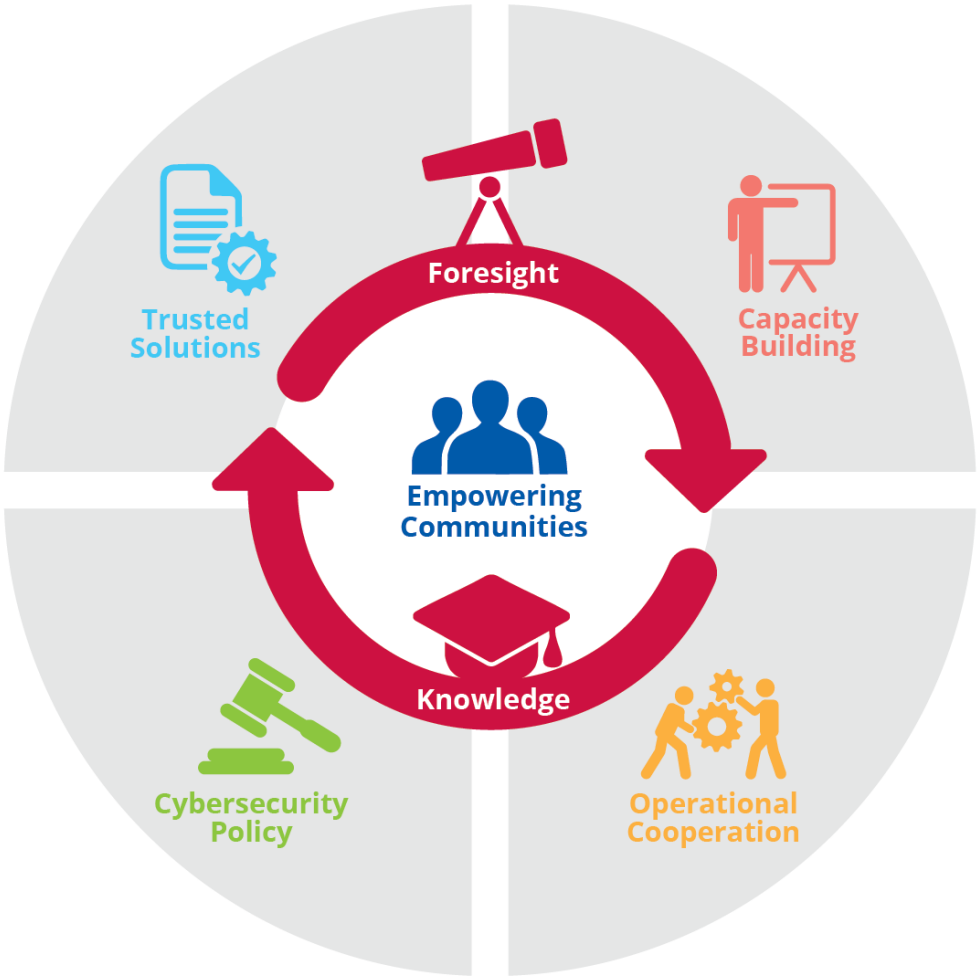
Dr Andreas Mitrakas, Head of Unit “Market, Certification & Standardisation”, ENISA

Omnisecure 2023
Berlin
22 | 05 | 2023

Agenda

Setting the stage → Policy objectives → Sample provisions

ENISA: What we do

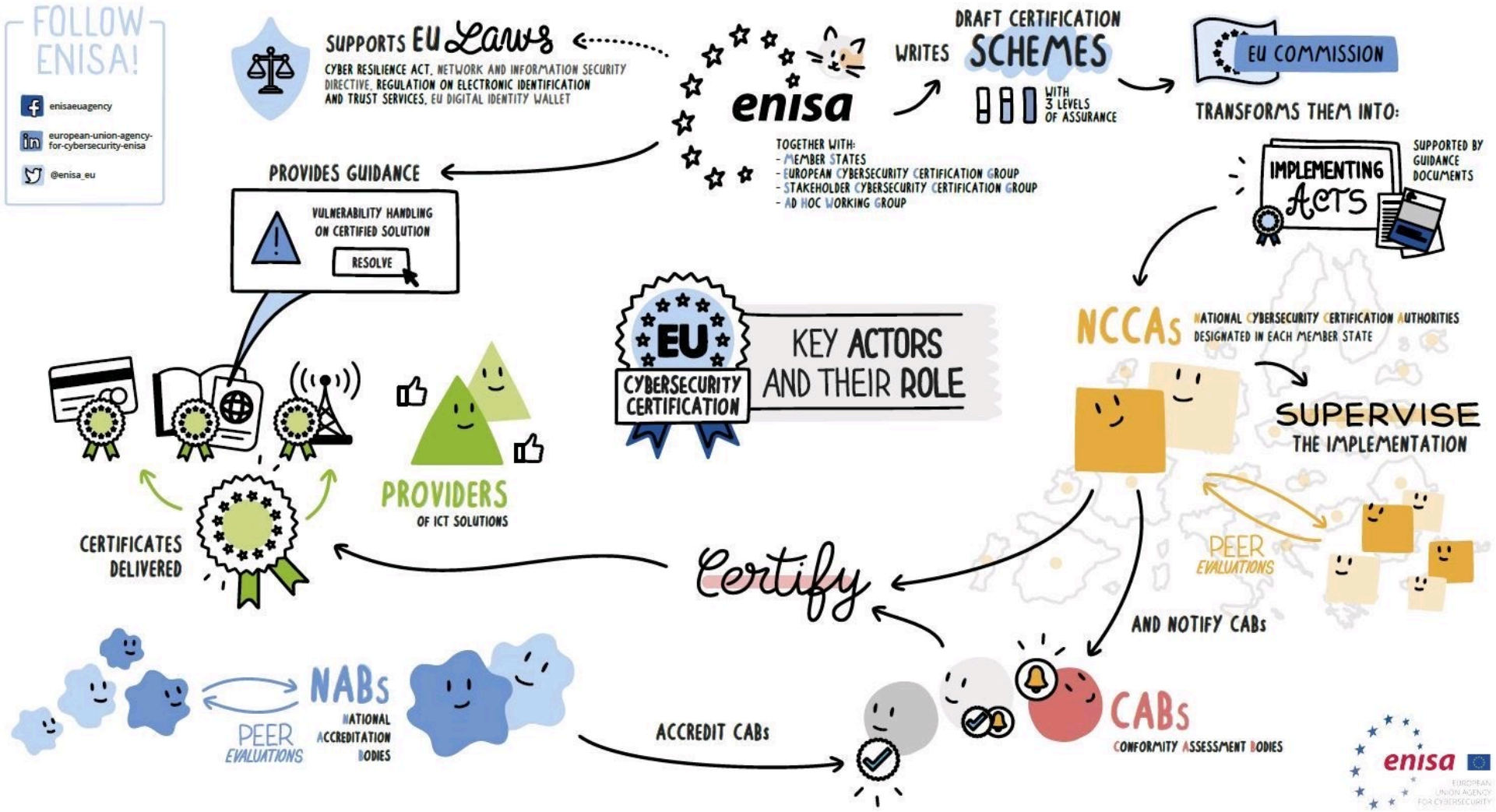


Legal basis

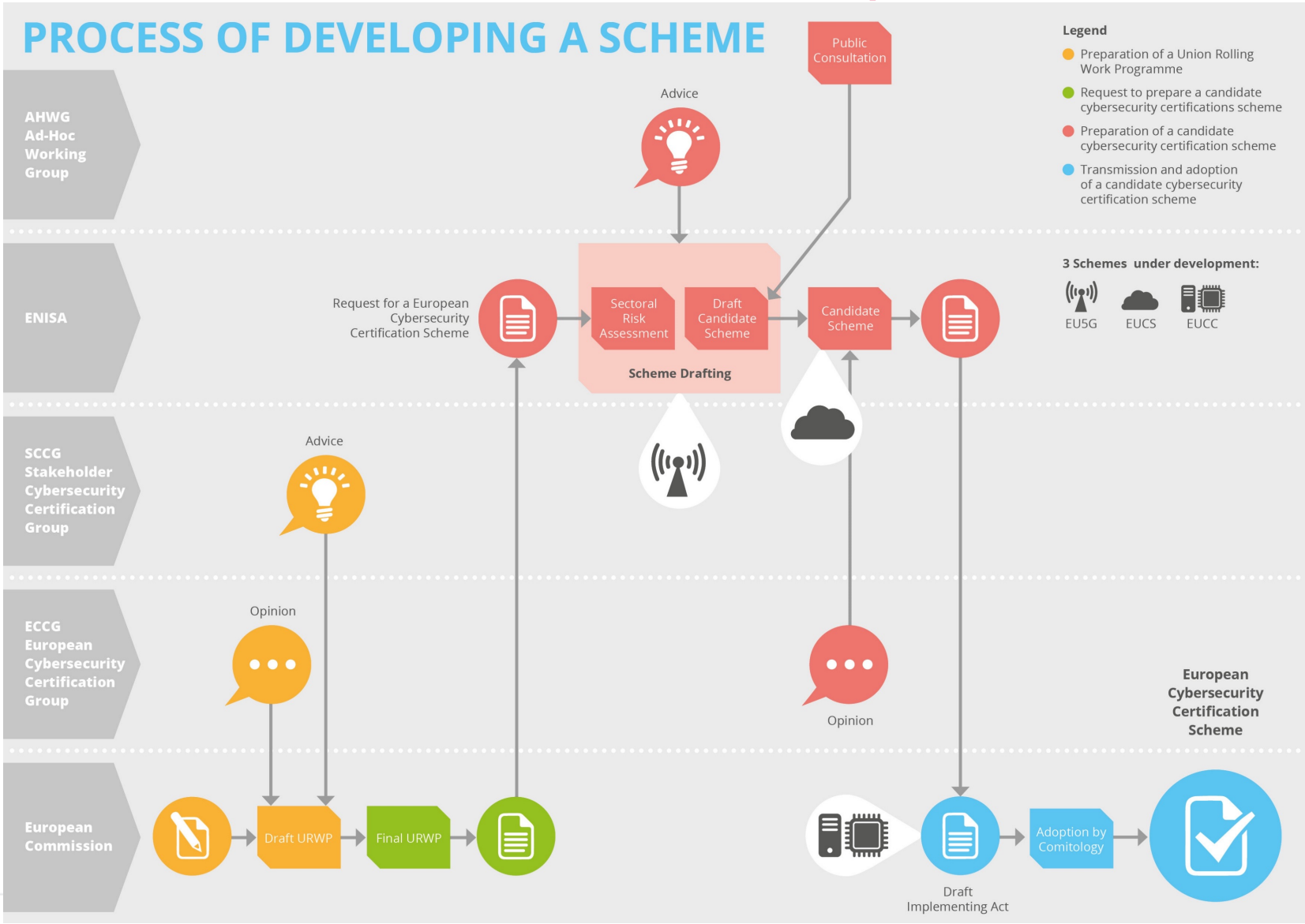
- Internal market, article 114 TFEU

Innovation v. Precautionary principle

Cybersecurity act



Certification schemes accomplishment level



EUCC for ICT products

Based on international standards

Common Criteria

ISO/IEC 17065 ISO/IEC 17025

Horizontal

Scope of the scheme “How to certify”

Fit the scheme under Regulation 765/2008

“What to certify” is for risk owners to define through Protections Profiles or individual security targets

Two assurance levels

Assurance levels:

Substantial

High

Both levels require an assessment by an accredited third-party

SOGIS

Senior Officials Group
Information Systems Security

Implementing Act (Commission competence)

Supporting Documents

Guidance

Monitoring and maintenance

Cryptography

EUCS for Cloud services

All capabilities

Based on ISO/IEC 22123

All cloud capabilities are supported: Infrastructure, Platform, Application

Covers the full service and infrastructure stack

No mentioning of the actual deployment model

Horizontal

Defines a baseline of requirements that are applicable to all services

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

Three assurance levels

As defined in the European Cybersecurity Act

'basic'

'substantial'

'high'

All levels based on an assessment by an accredited third-party

Opinion of ECCG, pending

Implementing Act, pending

Follow up of standardisation work concerning security controls at CEN CENELEC/JTC13

Personal data and compliance with GDPR

EUCS: Three assurance levels

CS-Basic level

Minimise the **known basic** risks of incidents and cyberattacks

- Limited assurance
- Review of CSP evidence
- Focus on the definition of procedures and mechanisms
- Few constraints

CS-Substantial level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources**

- Reasonable assurance
- Design effectiveness
- Operating effectiveness

CS-High level

Minimise the risk of **state-of-the-art** cyberattacks carried out by actors with **significant skills and resources**

- Same as substantial, plus
- Stronger requirements, including automated monitoring
- Penetration testing

Risk assessment to determine the desired assurance level sought by the consumer of the Cloud service concerned

The notion of risk is not monolithic; it evolves over time

NB: Assurance levels concern legislated mitigation measures in the Digital Single Market

EUCS: In the press

2 minute read · March 7, 2023 12:25 AM GMT+2 · Last Updated 2 months ago

Tech-sponsored study criticises plan to exclud

NTN National Technology News

TechCentral.ie About Contact Advertise

Life Pro Trade Blogs Radio Insights #teche

ET Telecom.com From The Economic Times

Internet · 2 M

urity labelling rules fo

crosoft

The Register®

TAGESSPIEGEL BACKGROUND

ntakt | Preise

Suchen

bersecurity **Digitalisierung & KI** Energie & Klima Gesundheit & E-Health Smart City & Verwaltung Sustainable Finance Verkehr

Digitalisierung & KI

CLOUD COMPUTING

Cloud-Zertifizierung: Deutschland will breitere Deb

riticised b

TAGESSPIEGEL BACKGROUND

gie & Klima Gesundheit & E-Health Smart City & Verwaltung Su

Cybersecurity

EUCS

Die Büchse der Pandora?

NETWORK DIGITAL 360

CYBERSECURITY360 Cybersecurity Nazionale

L'ANALISI

Fornitori di servizi cloud, da ENISA un bollino di provider "sicuro": una stretta sulle big tech

Les acteurs mondiaux du cloud s'alarment du projet de certification de l'UE

enisa

EU5G Overview

Cybersecurity certification scheme operated & recognized across the EU

- EU public authorities support and enhance cybersecurity of 5G
- Legally-supported way to meet cybersecurity requirements

Contains

- Cybersecurity requirements and objectives for products
- Cybersecurity audit on product development process and product lifecycle process & product evaluation on the network equipment

NB: The EU cybersecurity certification framework is voluntary

EU5G scheme, structure and timeline

GSMA NESAS
Processes & Products

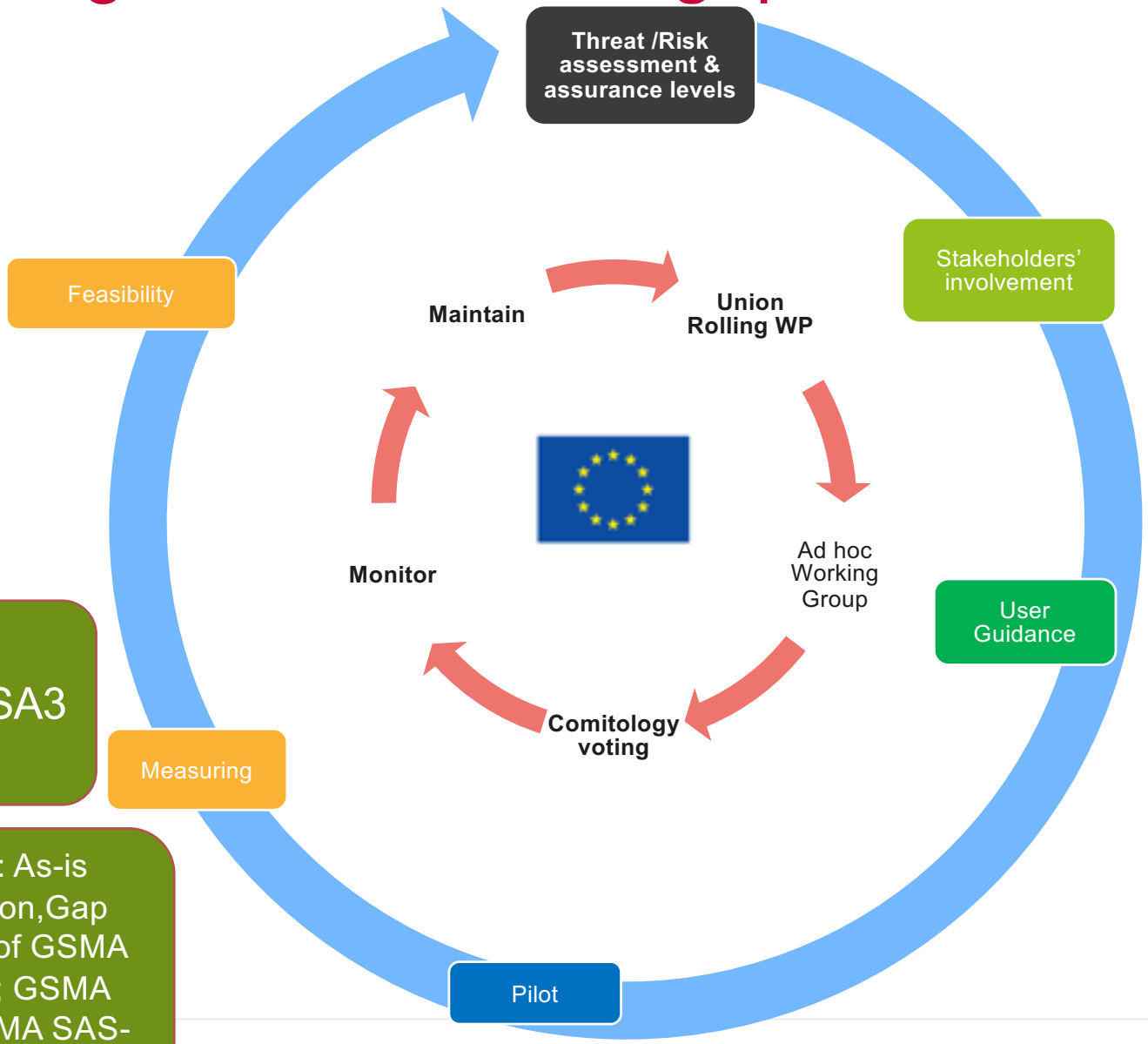
GSMA SAS SM/SAS UP processes
Subscription management
eUICC personalisation

eUICC product
- PP(s) updates + augmentations
- eIDAS/Wallet support

Phase I (WS1-3): appraisal of GSMA NESAS, SAS-SM, SAS-UP and eUICC, plus risk assessment and gap analysis across all components **- Q3 2022**

Phase II (WS4): Phase 2 (WS4) to follow (development of the candidate scheme) - **2023**

Filling standardisation gaps



CEN/CLC/JTC 13 WG 3 Guidelines on sectoral cybersecurity assessment

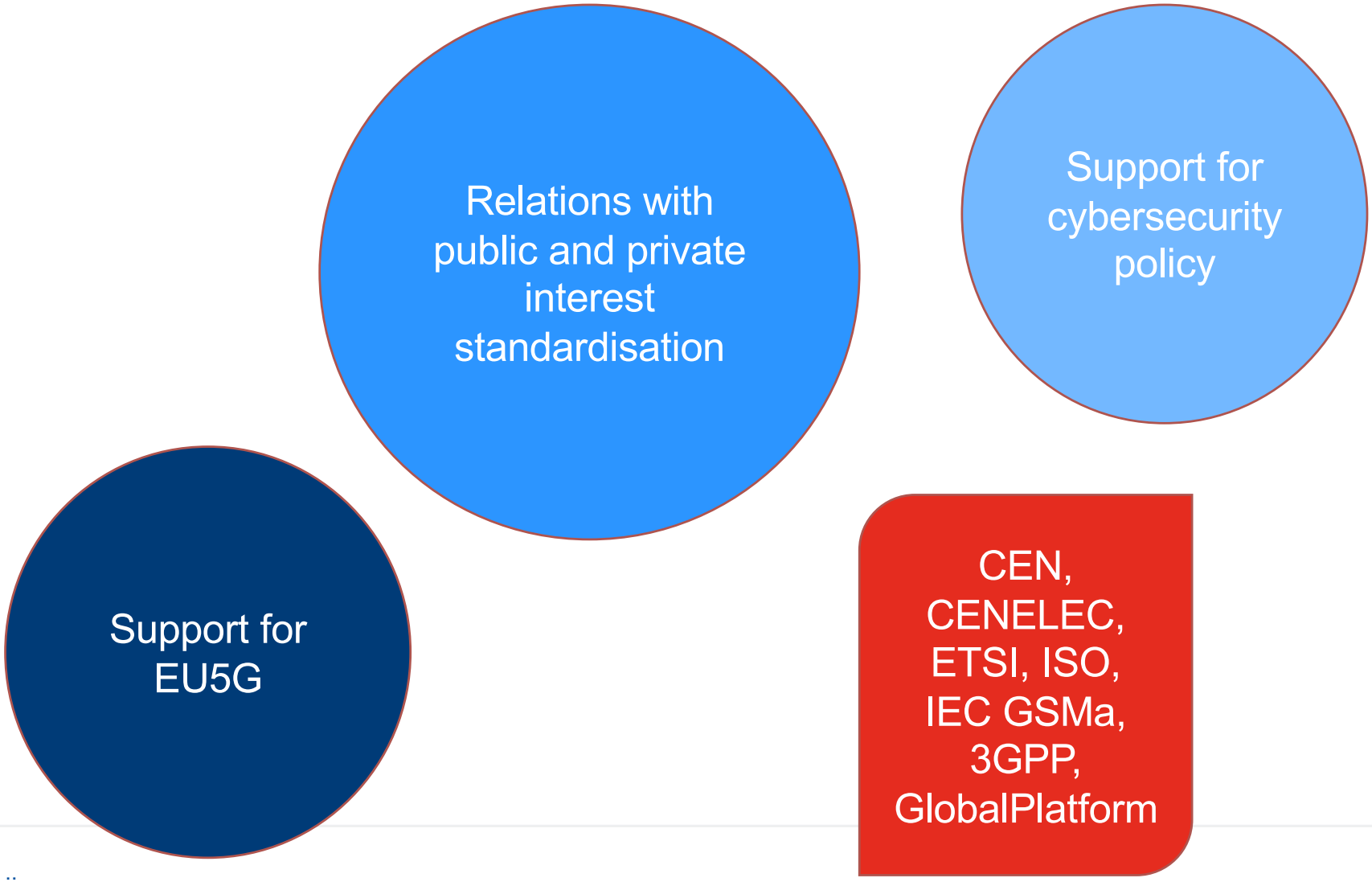
CEN/CLC/JTC 13 /WG2: EUCS1 Security Objectives and Requirements for Cloud Services

CEN/CLC/JTC 13/WG3: EUCS2 Requirements for Conformity Assessment Bodies certifying Cloud Services

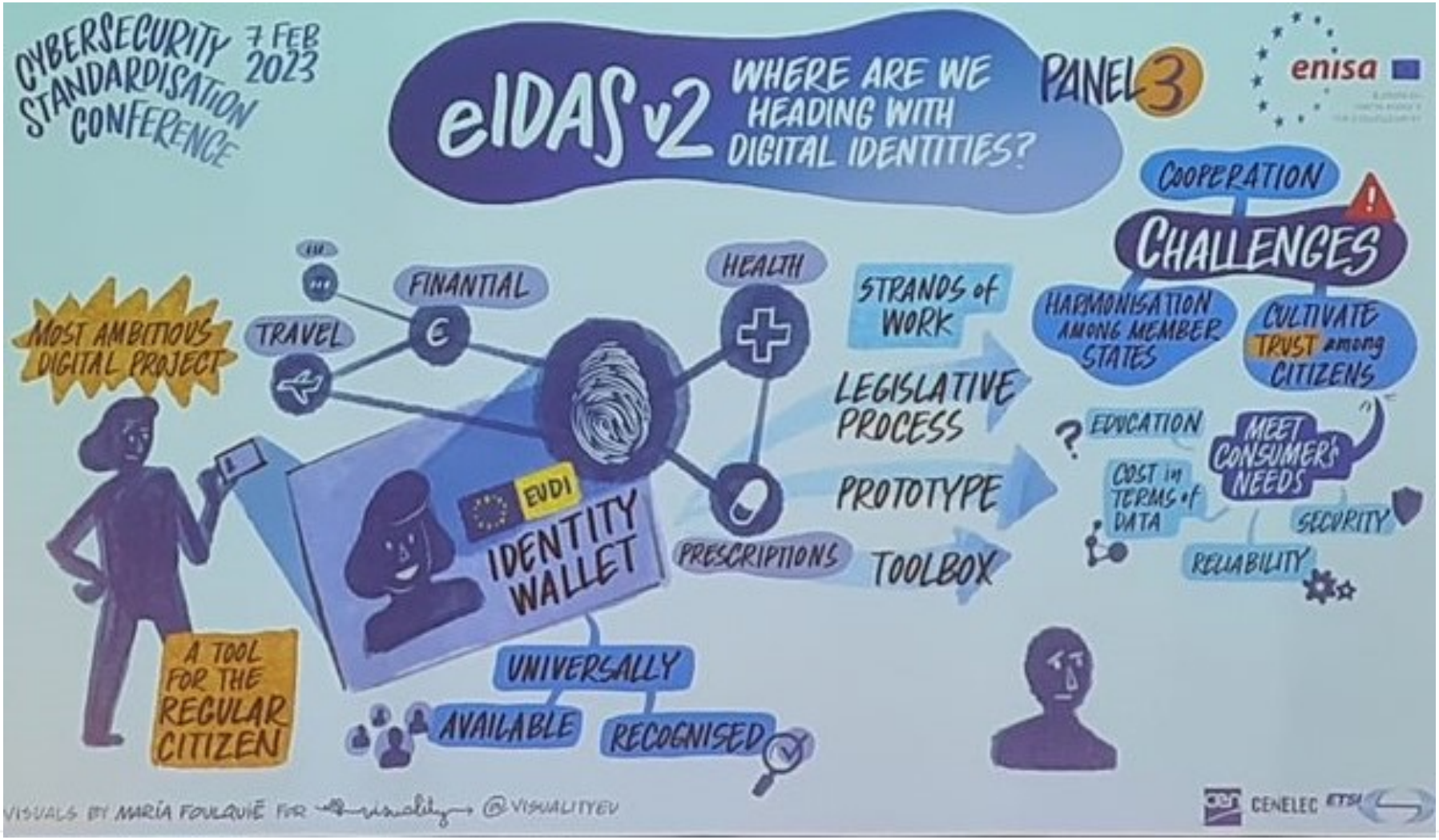
3GPP: SA3

GSMa: As-is translation,Gap analysis of GSMA NESAS; GSMA SAS; GSMA SAS-UP and eUICC

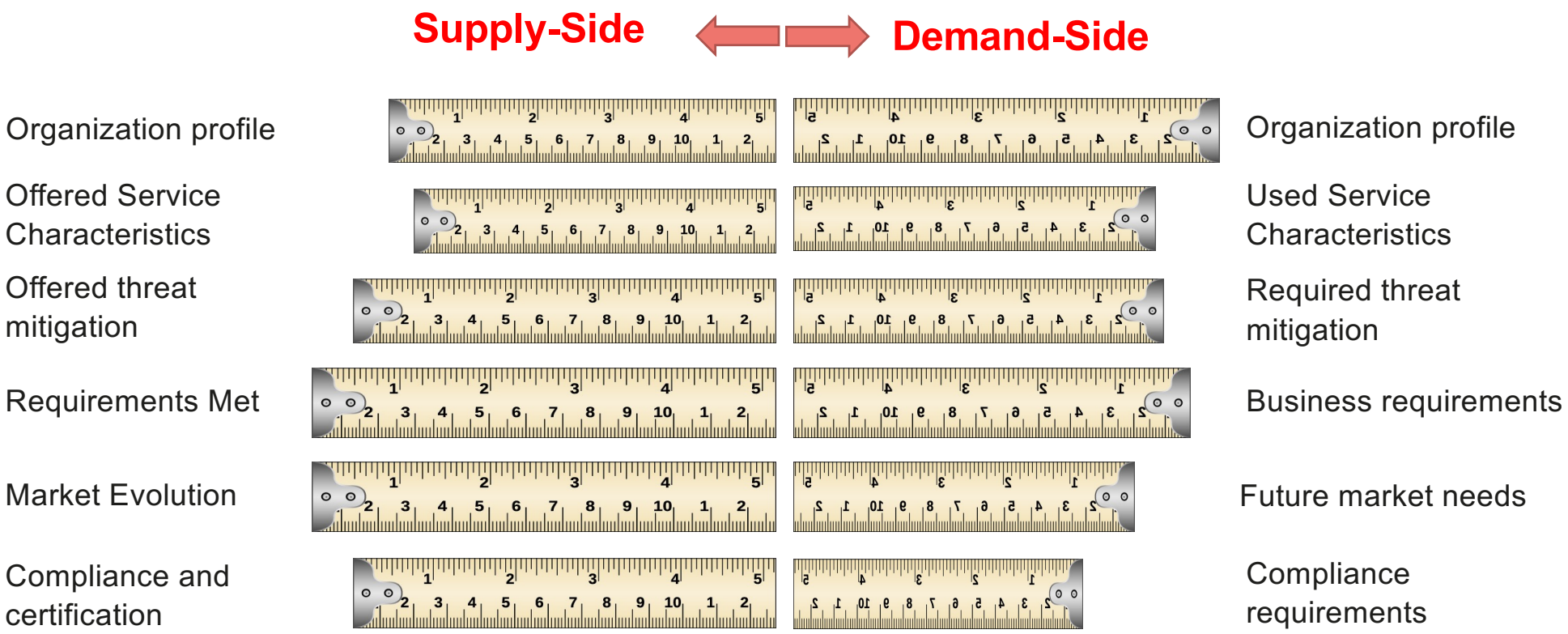
ENISA reaching out towards cybersecurity standardisation



EU Digital identity wallet



Cybersecurity market analysis



Compare perspectives: coverage of market needs, market gaps and more

Conclusions on market trends

- Dilution of distinguishable cloud cybersecurity features
- Research trends towards mobile cloud computing /fog computing / edge computing and secure cloud architectures
- Vendors follow an ‘all in one’ approach, as opposed to security-solution integration or ‘chaining’ done by customers or system integrators
- Secure computation outsourcing and privacy in multi-tenancy cloud systems to be the important challenge

What the future brings

https://certification.enisa.europa.eu/

THANK YOU FOR YOUR ATTENTION

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europe.eu