EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity certification & standardization in the EU

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

Workshop on cybersecurity assurance practices, International Telecommunication Union, ITU-D

23 | 05 | 2023

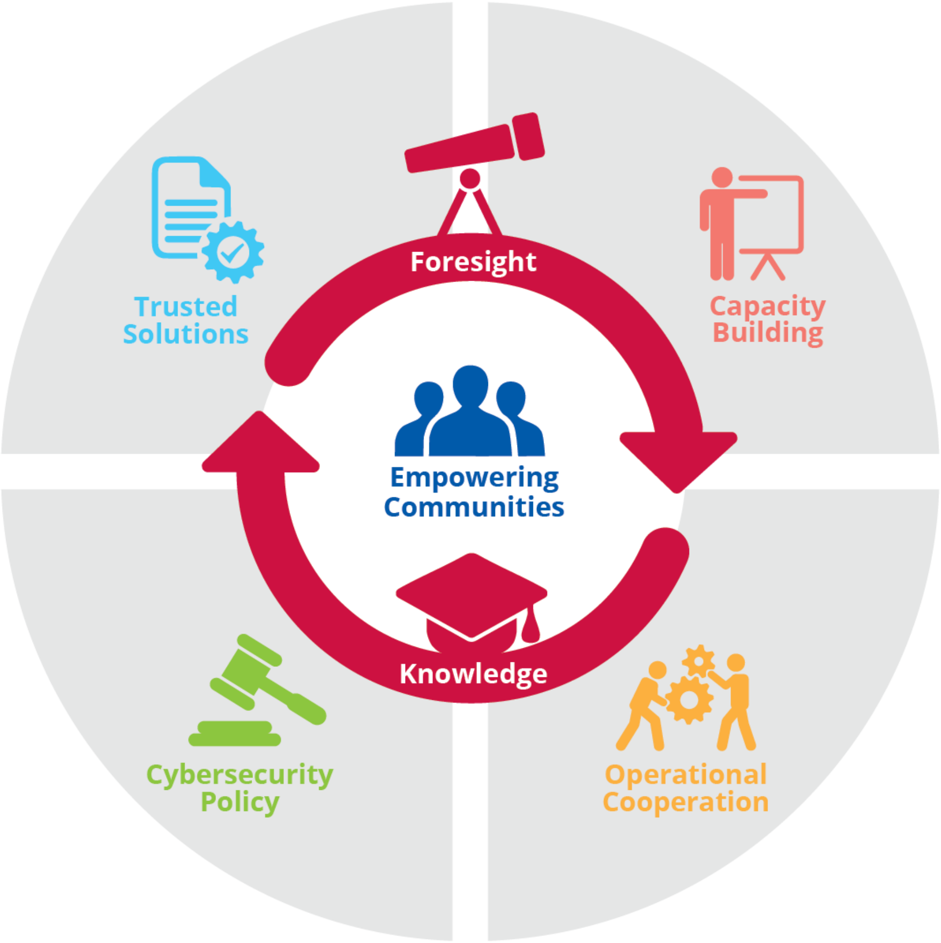
Agenda

Measurable Trust

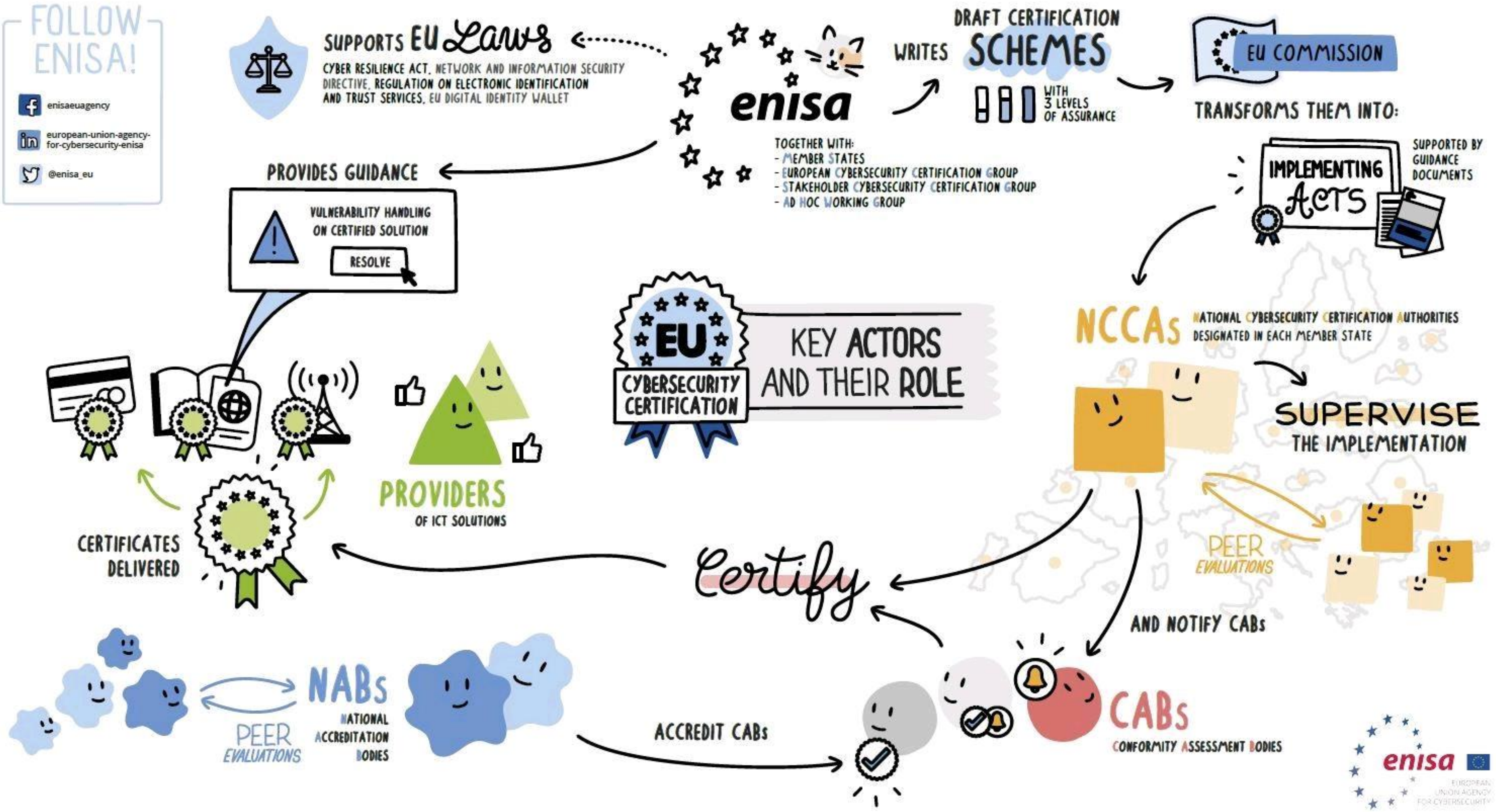
Approach towards implementation

Tangible outcomes

ENISA: What we do



Cybersecurity act


FOLLOW ENISA!
enisaeuagency
european-union-agency-for-cybersecurity-enisa
@enisa_eu
SUPPORTS EU LAWS
CYBER RESILIENCE ACT, NETWORK AND INFORMATION SECURITY DIRECTIVE, REGULATION ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES, EU DIGITAL IDENTITY WALLET
enisa
WRITES
DRAFT CERTIFICATION SCHEMES
WITH 3 LEVELS OF ASSURANCE
TOGETHER WITH:
- MEMBER STATES
- EUROPEAN CYBERSECURITY CERTIFICATION GROUP
- STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP
- AD HOC WORKING GROUP
EU COMMISSION
TRANSFORMS THEM INTO:
IMPLEMENTING ACTS
SUPPORTED BY GUIDANCE DOCUMENTS
PROVIDES GUIDANCE
VULNERABILITY HANDLING ON CERTIFIED SOLUTION
RESOLVE
EU
CYBERSECURITY CERTIFICATION
KEY ACTORS AND THEIR ROLE
NCCAs
NATIONAL CYBERSECURITY CERTIFICATION AUTHORITIES DESIGNATED IN EACH MEMBER STATE
SUPERVISE THE IMPLEMENTATION
PEER EVALUATIONS
AND NOTIFY CABs
PROVIDERS OF ICT SOLUTIONS
CERTIFICATES DELIVERED
Certify
NABs
NATIONAL ACCREDITATION BODIES
PEER EVALUATIONS
ACCREDIT CABs
CABs
CONFORMITY ASSESSMENT BODIES
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

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

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

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

EU5G Overview

Cybersecurity certification scheme operated & recognized across the EU

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

The EU cybersecurity certification framework is voluntary

EU5G scheme, structure and timeline

GSMA NESAS
Processes & Products

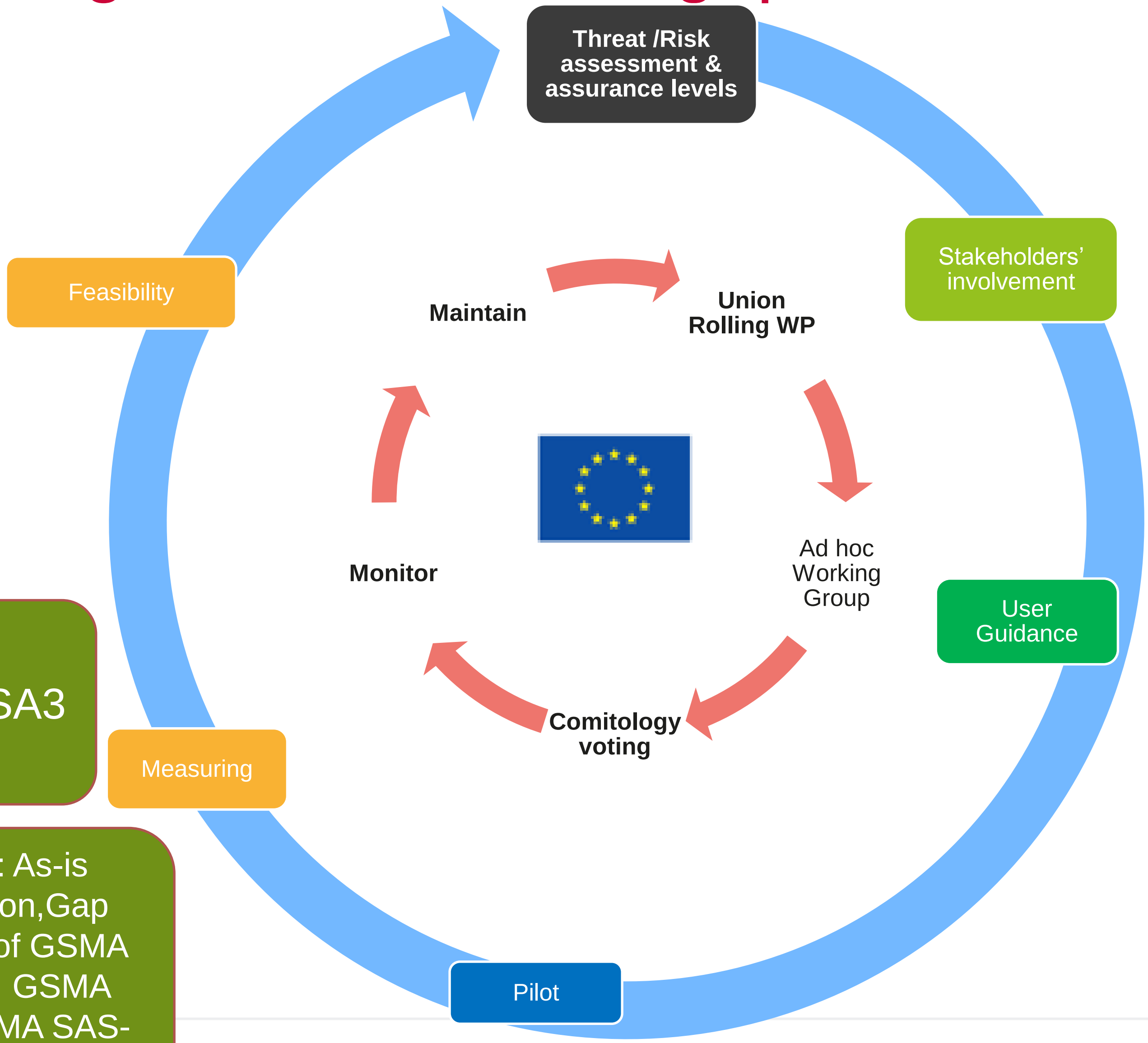
GSMA SAS SM/SAS UP processes
Subscription management
eUICC personalisation

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

Phase I (3WSs): 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



Threat /Risk assessment & assurance levels

Stakeholders' involvement

User Guidance

Pilot

Measuring

Feasibility

Maintain

Union Rolling WP

Ad hoc Working Group

Comitology voting

Monitor

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

Reaching out: cybersecurity standardisation

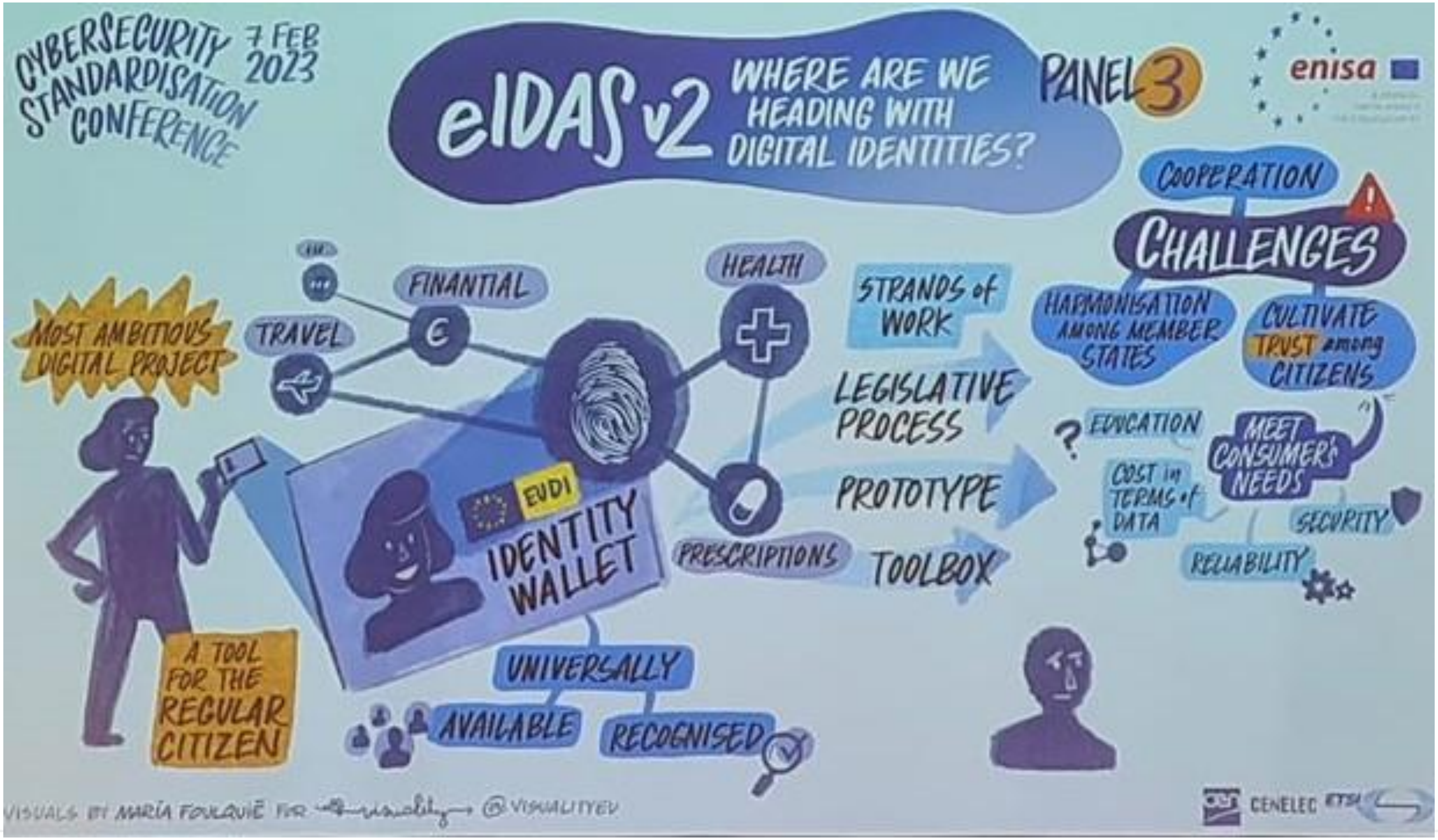
Relations with public and private interest standardisation

Support for cybersecurity policy

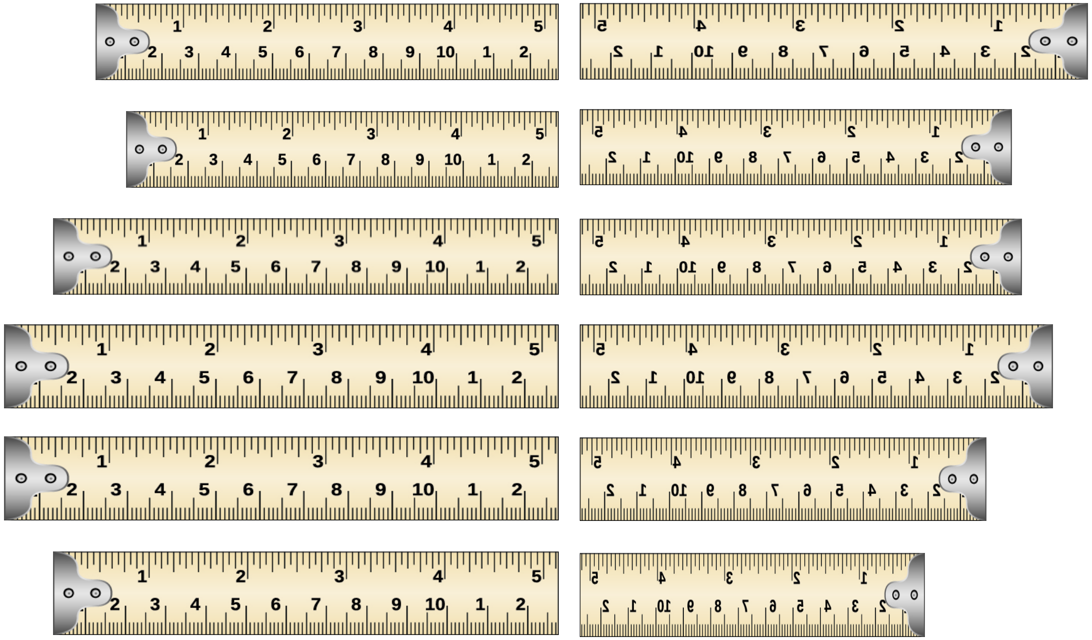
Support for EU5G

CEN, CENELEC, ETSI, ISO, IEC GSMa, 3GPP, GlobalPlatform

EU Digital identity wallet



Cybersecurity market analysis



Supply-Side	Demand-Side
Organization profile	Organization profile
Offered Service Characteristics	Used Service Characteristics
Offered threat mitigation	Required threat mitigation
Requirements Met	Business requirements
Market Evolution	Future market needs
Compliance and certification	Compliance requirements

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

CONCLUSIONS ON MARKET CHARACTERISTICS AND TRENDS

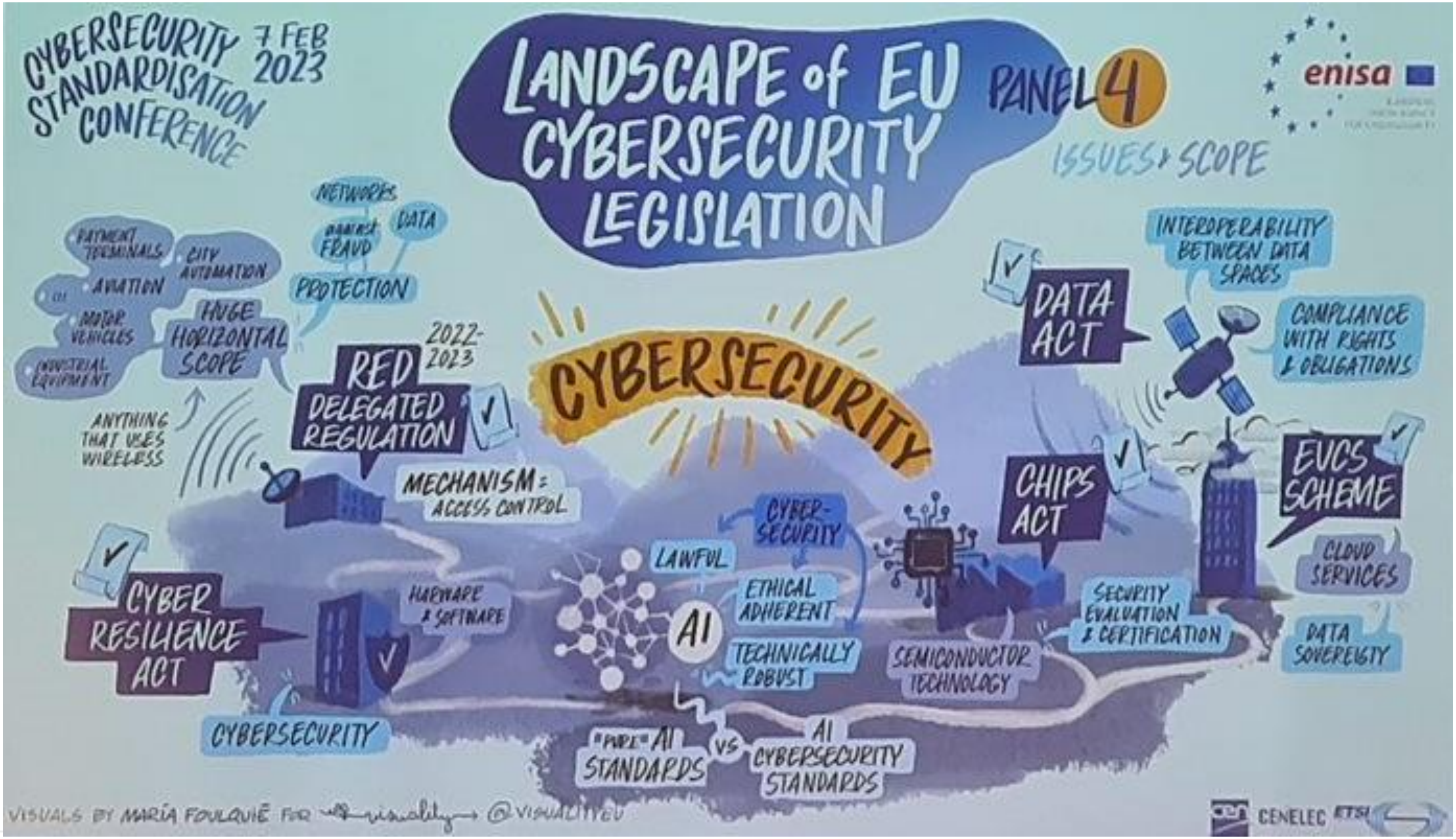
Dilution of distinguishable cloud cybersecurity features

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



THANK YOU FOR YOUR ATTENTION

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europe.eu