



At a glance on Digital Europe developments | Ukraine's opportunities on joining European Single Digital Market

Vilma Misiukonienė
17.02.2023



High stakes for the Digital Decade

✓ EU dependencies

- ✓ **Only a 10% share** of the global microchips market
- ✓ **Less than 4%** of top online platforms are European, with new developments such as virtual worlds also originating from outside of the EU
- ✓ **90% of the EU's data** is managed by US companies

✓ EU's untapped potential

- ✓ Reaching a high level of digital skills, for **digital empowerment of citizens** and to fulfil the need for ICT specialists for key areas such as **cyber security and data analysis**
- ✓ **Cost of non-Europe in digital transformation is 1,3 trillion by 2033**

EU Digital Decade Policy Programme (DDPP) 2030

The DDPP builds on already existing **policies / funding programmes/ strategies** (including RRF) and targets as set up in the Digital Decade Communication along **four domains**:

Objectives

Sovereignty,
resilience,
sustainability, etc.

Government

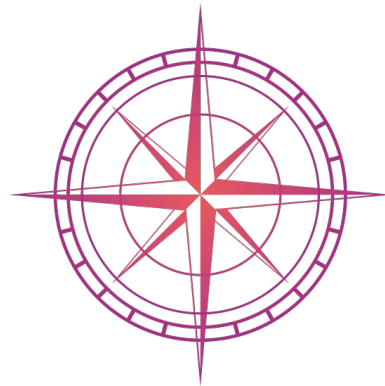
Key Public Services - 100% online
Everyone can **access health records online**
Everyone can use **eID**

Digital Rights & Principles

Solidarity and inclusion,
freedom of choice, safety,
privacy, etc.

Skills

ICT Specialists: 20 millions + gender balance
80% of adults can **use tech** for everyday tasks



Business

75% of EU companies using **Cloud, AI or Big Data**
Double the number of **unicorn startups**
90% of **SMEs taking up tech**

2030 Digital Targets

KPIs set -> Skills,
Infrastructure, Businesses,
Public services

Infrastructures

Gigabit connectivity for everyone, **high-speed mobile coverage** (at least 5G) everywhere
EU produces 20% of world's **semiconductors**
10 000 **cloud edge nodes** = fast data access
EU **quantum computing** by 2025

- ✓ Annual monitoring & reporting
- ✓ National Digital Decade strategic roadmaps
- ✓ Joint Commitments and Multi-Country Projects

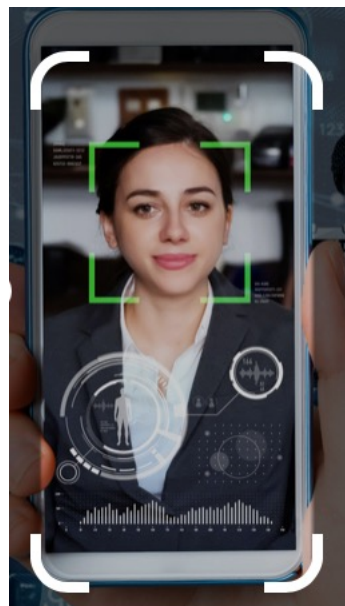
Digital Decade Policy Programme (DDPP) 2030 and multi-country projects planed to reach the targets



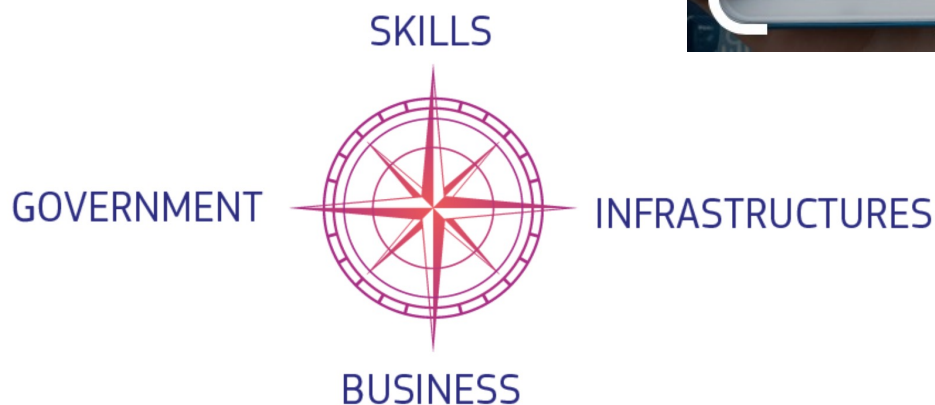
- European **Common Data Infrastructure and Services;**
- Endow the EU with the next generation of low power trusted processors;
- Pan-European **deployment of 5G corridors;**
- Acquiring supercomputers and quantum computers, connected with the EuroHPC Joint Undertaking;
- Developing and deploying ultra-secure **quantum and space-based communication infrastructures;**
- Deploying a **network of Security Operations Centres**, as part of the EU Cybersecurity Strategy;
- **Connected Public Administration;**
- European **Blockchain Services Infrastructure;**
- European Digital Innovation Hubs;
- High-tech **partnerships for Digital Skills** through the Pact for Skills;
- Skills and **training in cybersecurity**



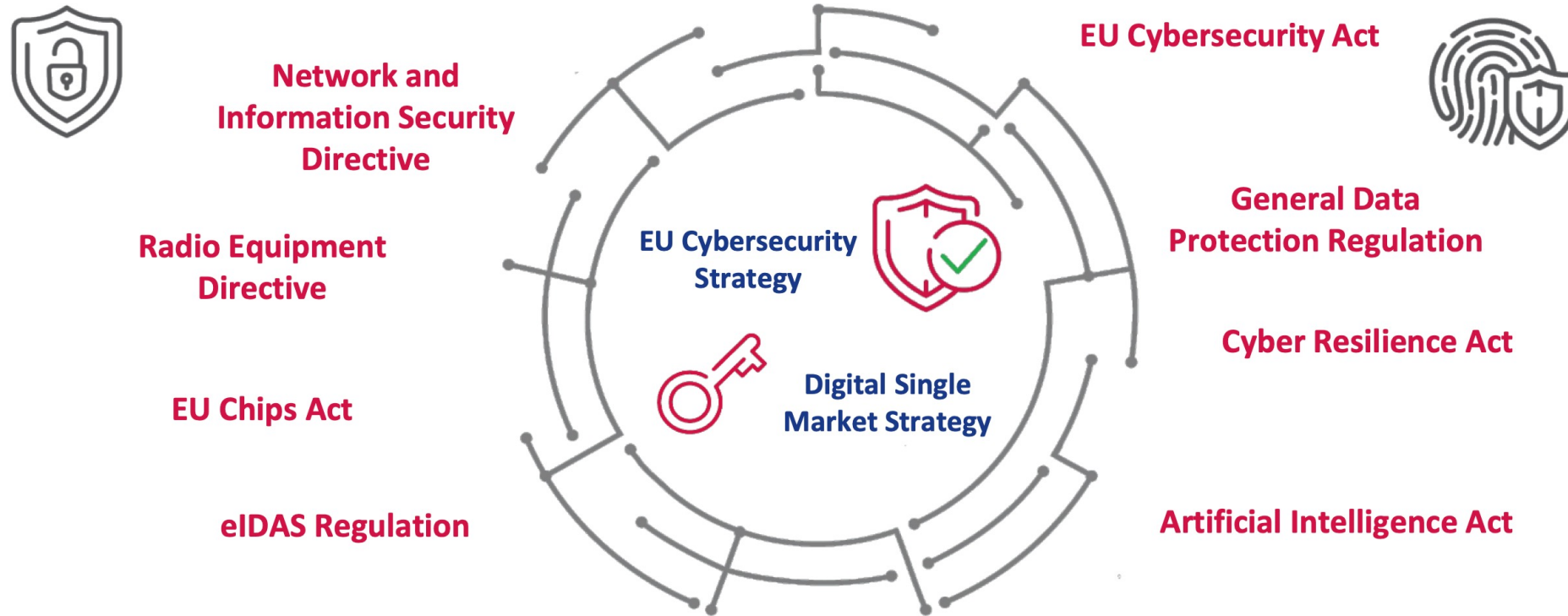
Towards self-sovereign Digital Europe -> change of rules in Digital Governance



- Digital Market Act
- Digital Services Act
- Data Act
- eIDAS Regulation update
- NIS2 Directive
- Cyber Resilience Act
- CyberSecurity Act
- Artificial Intelligence Act
- EU Interoperability Act
- Digital rights and principles Declaration



EU CyberSecurity in (pro)-action





European
Commission



CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU
2022

SEPTEMBER 2022

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.



Cyber Resilience Act



Main elements of the proposal

- ❖ **Cybersecurity rules** for the placing on the market of hardware and software
- ❖ Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- ❖ **Obligations** for manufacturers, distributors and importers
- ❖ Cybersecurity **essential requirements** across the life cycle (5 years)
- ❖ Harmonised **standards** to follow
- ❖ **Conformity assessment** – differentiated by level of risk
- ❖ **Market surveillance and enforcement**



Cyber Resilience Act (CRA)



proposal released on 15th of September, 2022

- **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle that business users and consumers benefit from **better protection**.
- Ensure that **products with digital elements** placed on the EU market have **fewer vulnerabilities** and that manufacturers remain **responsible for cybersecurity** throughout a product's life cycle;
- **Improve transparency** on security of hardware and software products;
- **Set Manufacturer's obligations (in planning, design, development, production, delivery and maintenance** phases; obligations on risks documented, report vulnerabilities and incidents to ENISA);
- **Security updates** to be made **available for at least five years**.





EU digital identity

Free

Safe

Voluntary

Linked to national eID

Available across the EU

Keeps you in control of your data



#DigitalEU

The ambition: Towards a European Digital Identity



Universally Available
all EU citizens and
businesses may use it
on a voluntary basis



Universally Useable
recognised by private
and public service
providers for all
transactions that require
authentication



Protecting Personal Data
users are able to take
control of their identity
and the disclosure of
personal data/attributes

European Digital Identity – User benefits



User control

- User can request, obtain, store, select, combine and share personal data and attributes to authenticate for access to public and private services
- No tracking of data not necessary for the provision of wallet services; physical and logical separation of other data
- Portability

Identity/attributes/credentials

- The wallet will allow users to link attributes (e.g. proof of age) and credentials (e.g. driving licence, university diploma, professional accreditations) to their identity

ARF- European Digital Identity Wallet Architecture and Reference Framework



- ver. 1.0 released in 10th of Feb, 2023
- **Technical and Operational Specifications and Reference Standards**
(taking into account certification aspects) - *Implementing Act following Article 6a(11)*
- **Certification Requirements** – *Implementing Act following Article 6c(4).*
- developed by Expert Group with support by ENISA and the Wallet contractor



eIDAS v2.0-> processes in paralell



- I. Member States work on **common tech Toolbox** (Architecture and Reference Framework). Identify tech standards, specifications, guidelines and best practices (v 1.0 on 10th of Feb 2023);
- II. European **EU Digital Wallet prototype** (MVP in Q4/2023). At least three versions of subsequent releases (e.g. extended functionalities, feedback from pilots). Wallet tested, certified and ready for deployment (Q1 2024 tbc);
- III. **Legal framework** (eIDAS2 Regulation) – trilogue will start in March, 2023. (adoption expected in 2023)
- IV. Large-scale **piloting projects** (start in Q2, 2023);
- V. **EUDIW certification**. ENISA together with standardisation bodies work in parallel defining the **certification scheme** (standards, requirements, etc), supported by the EC and experts from Member States.



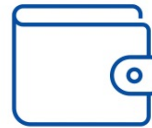
4 work strands

Legislative Process

Negotiation of the proposal for the revision of the **eIDAS regulation** underpinning the European Digital Identity Framework

LSPs pilot the Wallet Prototype and provide feedback for the Wallet Prototype

Toolbox provides the specifications for the Wallet Prototype



Wallet Prototype

Development of a **reference application** of the European Digital Identity Wallet based on the technical standards agreed by the toolbox.

Wallet Prototype is delivered to LSPs for re-use

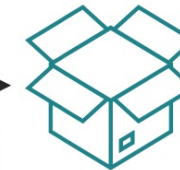
Wallet Prototype implements the Toolbox and provides feedback for the Toolbox



Large Scale Pilots

Toolbox provides the specifications for the LSPs

LSPs pilot the Toolbox Specifications and provide feedback for the Toolbox



Toolbox (ARF)

Establishing a **common toolbox** consisting of an **architecture and reference framework**, common standards and specifications and guidelines and best practices

Large-scale pilots around use-cases for the European Digital Identity Wallet including mobile driver licences, ePayments, eHealth and educational/professional qualifications

Article 6c(4) (GA)

4. *Within 6 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish:*

a) *list of cybersecurity certification schemes* pursuant to Regulation (EU) 2019/881, required for the certification of the European Digital Identity Wallets as referred to in paragraph 3;

aa) *specifications, procedures and reference standards for their use under relevant cybersecurity certification schemes* listed in accordance to point (a);

aaa) *a list of specifications, procedures and reference standards establishing common certification requirements not covered by relevant cybersecurity certification schemes* pursuant to Regulation (EU) 2019/881 for the purpose of certification referred to in paragraph 1 aiming to demonstrate that a European Digital Identity Wallet meets the requirements as referred to in paragraph 1;

b) *technical, procedural, organisational and operational specifications for the designation of conformity assessment bodies referred to in paragraph 1, and, for what regards the certification requirements established pursuant to point (aaa), for the monitoring and review of the certification schemes and related evaluation methods these bodies use and the certificates and certification reports they issue;*



Article 6c (GA) – Certification of the EUDIW

GDPR & privacy

- Optional certification
- Art.6c(2) As regards compliance with the data protection requirements under Article 6a(7), the certification under paragraph 1 may be complemented by a certification pursuant to Article 42 of Regulation (EU) 2016/679.

Cybersecurity

- Mandatory CSA certification
- Art.6c(1) The conformity of European Digital Identity Wallets with the requirements laid down in article 6a(3), (4), (5), with the requirement for logical separation laid down in paragraph Article 6a(7), and where applicable with the requirements laid down in Article 6a(11a), shall be certified by conformity assessment bodies accredited in accordance with Article 60 of the Cybersecurity Act and with the schemes, specifications, standards and procedures referenced in accordance with **paragraph 4 points (a), (aa) and (aaa)**, and designated by Member States. The certification shall not exceed five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled.
- Art.6c(3) The conformity of the European Digital Identity Wallets, or parts thereof, with the cybersecurity relevant requirements set out in Article 6a(3), (4), (5), (7) and where applicable (11a), shall be certified by the conformity assessment bodies referred to in paragraph 1, under **relevant** cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 as they are **referenced** in accordance with paragraphs 4(a) and 4(aa).

Non-cybersecurity

- Mandatory certification
- Art.6c(1) The conformity of European Digital Identity Wallets with the requirements laid down in article 6a(3), (4), (5), with the requirement for logical separation laid down in paragraph Article 6a(7), and where applicable with the requirements laid down in Article 6a(11a), shall be certified by conformity assessment bodies accredited in accordance with Article 60 of the Cybersecurity Act and with the schemes, specifications, standards and procedures referenced in accordance with **paragraph 4 points (a), (aa) and (aaa)**, and designated by Member States. The certification shall not exceed five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled



EUDIW certification strategy - summary

Cybersecurity requirements

ICT products

• **EUCC**

- **Security Sensitive functions** - CSA high (EAL4+ AVA_VAN 3/4/5)
(e.g. crypto functions, memories -- PP104 (CSP), PP084 (SoC), PP117 (3S on SoC), remote HSMs and/or external cards PPs)
- **Security Less sensitive functions** – CSA substantial
(Security interfaces, EUDIW applet based on CSP, EUDIW App)
- **Security Low functions** – No certification / CSA substantial (EUDIW App)

ICT products

ICT processes

ICT services

- **EUCC supplemented by means of eIDAS IAs, via specifications, procedures and reference standards** (e.g. EU5G GSMA SAM / RSP, EUCS); **and/or**
- **ISO/IEC 17065 supplemented by means of eIDAS IAs, via specifications, procedures and reference standards → harmonisation of national schemes**

Non-cybersecurity requirements

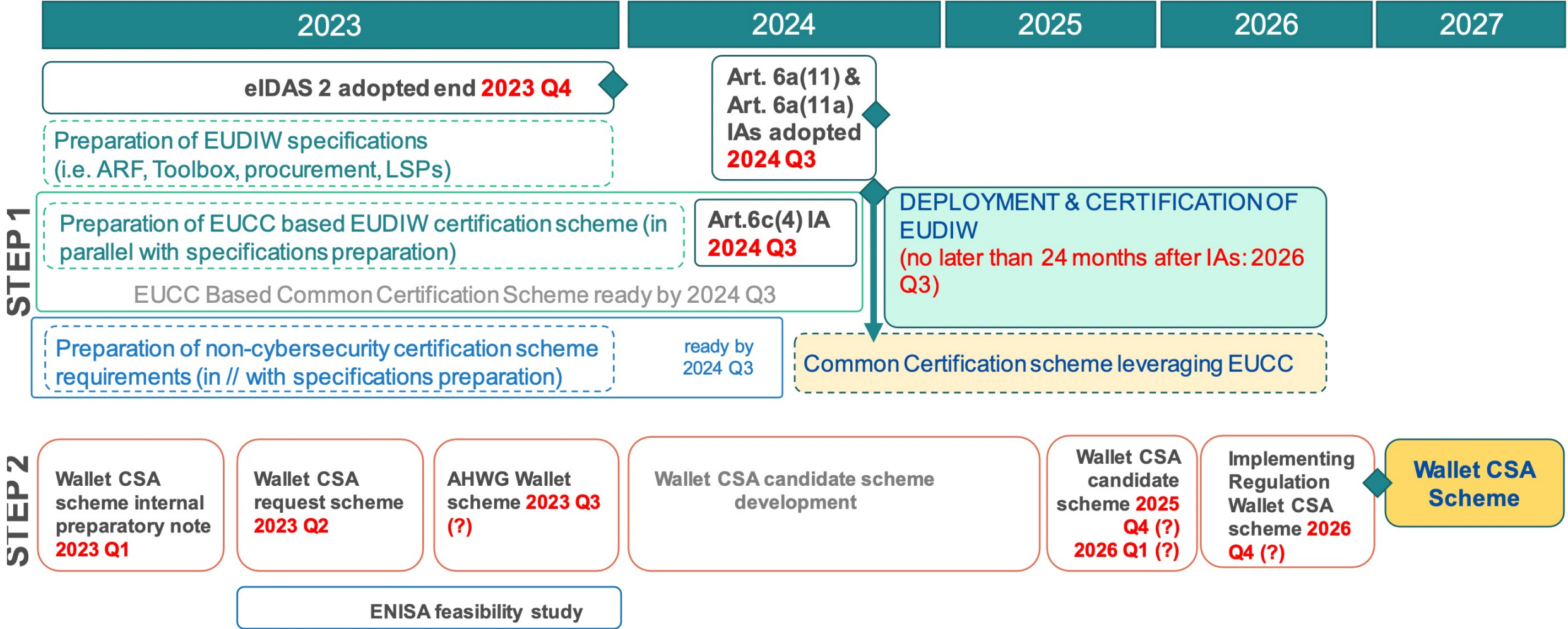
ICT products

ICT processes

ICT services

ISO/IEC 17065 supplemented by means of eIDAS IAs, via specifications, procedures and reference standards → harmonisation of national schemes

Indicative Timeline





Enabling Ukraine's approach on joining European Digital Single Market

EU expert Vilma
Misiukonienė
12.10.2021



Ukraine as EU candidate -

LT expert team assistanced with Application (quality check)



Hearing and Consultations session at RADA

with Trust Services national Supervisors (RRT,RIA)



Комітет цифрової
трансформації



Круглий стіл на тему: «Реалізація функцій наглядового органу у сферах електронної ідентифікації та електронних довірчих послуг»

14 липня 2022 року, м. Київ,

11:00 – 13:00

Організатор: Комітет Верховної Ради України з питань цифрової трансформації



EU project POTENTIAL



EUDI LSP POTENTIAL Consortium





Project partners



**148 organizations -
public & private**

Our memberstates

Austria

Belgium

Cyprus

Czech Republic

Estonia

Finland

France

Germany

Greece

Hungary

Italy

Lithuania

Luxembourg

Netherlands

Poland

Portugal

Slovakia

Slovenia

Spain

Ukraine



Final status of UCs and their respective leads

Status: 2022-07-06 Use case coordination call

Use Case Scenarios	Use Cases	20																			
eID (PID)	Electronic identification / authentication for eGov services	15	✓	✓	✓	✓			✓	✓	✓		✓		L	✓	✓	✓	✓	✓	
	Electronic identification for bank account opening	8	✓	✓						L	✓				✓			✓		✓	
	Electronic identification for mobile SIM registration	8	✓	✓			✓			L	✓					✓	✓				
Mobile Driving License (mDL)	Online car rental using electronic attestations of driving license	17	L	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote Qualified Electronic Signature	Remote qualified electronic signature	11	✓	L	✓	✓				✓	✓				✓			✓	✓	✓	
eHealth	ePrescription	11	✓	✓		✓	✓				✓	L	✓				✓	✓			✓ *

Large-scale pilots for testing European EU ID wallet

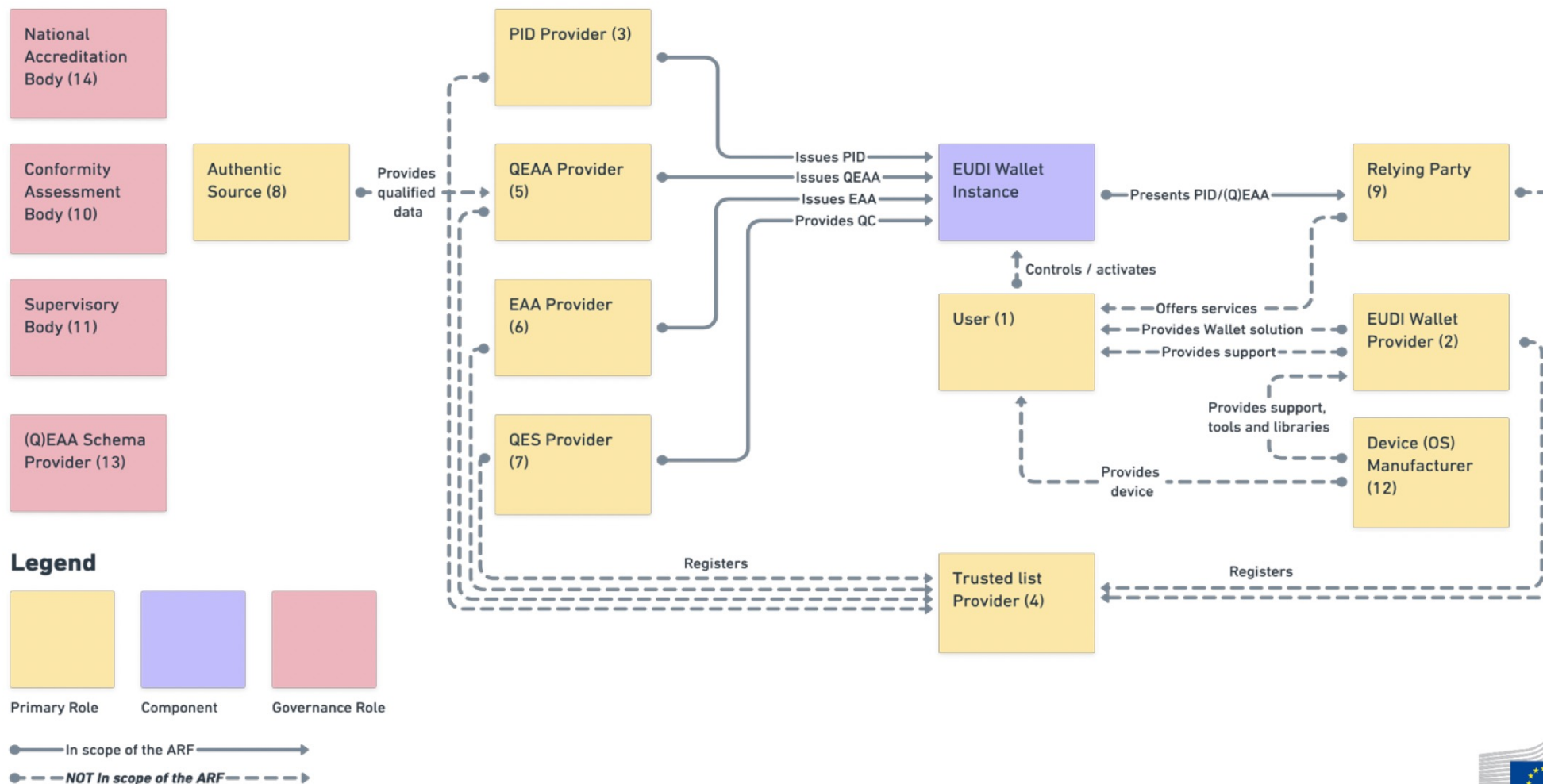


- Consortium of 19 EU MS + **Ukraine**
- + other three other consortiums



e-Gov Services
Mobile Driving License
e-Payments
e-Prescription
SIM cards registration
e-Signatures

Roles in the EUDI Wallet Ecosystem





Thank you | Дякую за увагу !

Vilma Misiukoniene, EU Affairs & Digital Policies

Vilma.Misiukoniene@vrm.lt | vilmuze@gmail.com

mob.:+370-69817037

