EU4Digital

Thematic session: Trust and Security

DAY 5

Online | 9 October 2020

EU4Digital Steering Committee Meeting Week

- EaP – Current policy agenda and results
- EaPConnect 2 – Kick-off meeting

- Future of EaP – policy beyond 2020
- Digital transformation in EaP

- Telecom Rules thematic session
- eHealth thematic session

- Digital Skills thematic session
- ICT innovation thematic session

- eTrade thematic session
- Trust and Security thematic session

EU4Digital

DAY 5: Trust and Security session – Agenda

Time	Item	Duration
10:30 – 10:55	Trust and Security thematic area state of play & plans	25 minutes
10:55 – 11:00	Feedback from Trust and Security Network	5 minutes
11:00 – 11:25	Q/A and Common discussion	25 minutes
11:25 – 11:35	Short break	10 minutes
11:35 – 12:00	Cybersecurity project state of play & plans	25 minutes
12:00 – 12:05	Feedback from Trust and Security Network	5 minutes
12:05 – 12:30	Q/A and Common discussion	25 minutes

EU4Digital

EU4Digital Facility in Trust and Security area

Through EU4Digital Facility the EU will:

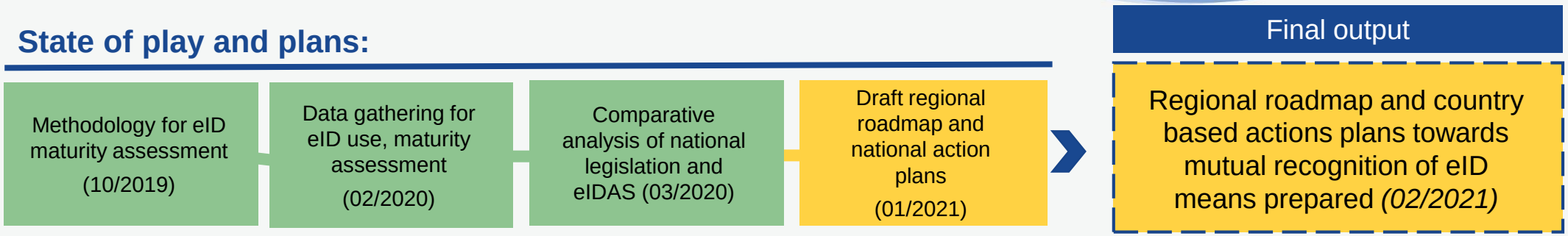
- Support development and implementation of a **regional roadmap and national action plans** for the mutual recognition of electronic identification in the Eastern partner region
- Pilot an interoperable **cross-border eSignature** in the region
- Support development of a **regional framework** for cross-border eServices
- Support development of a standard set of **cyber-security guidelines** for the Eastern partner region

EU4Digital

Completed | In progress | Planned for the upcoming 6 months

1. Recognition of eID

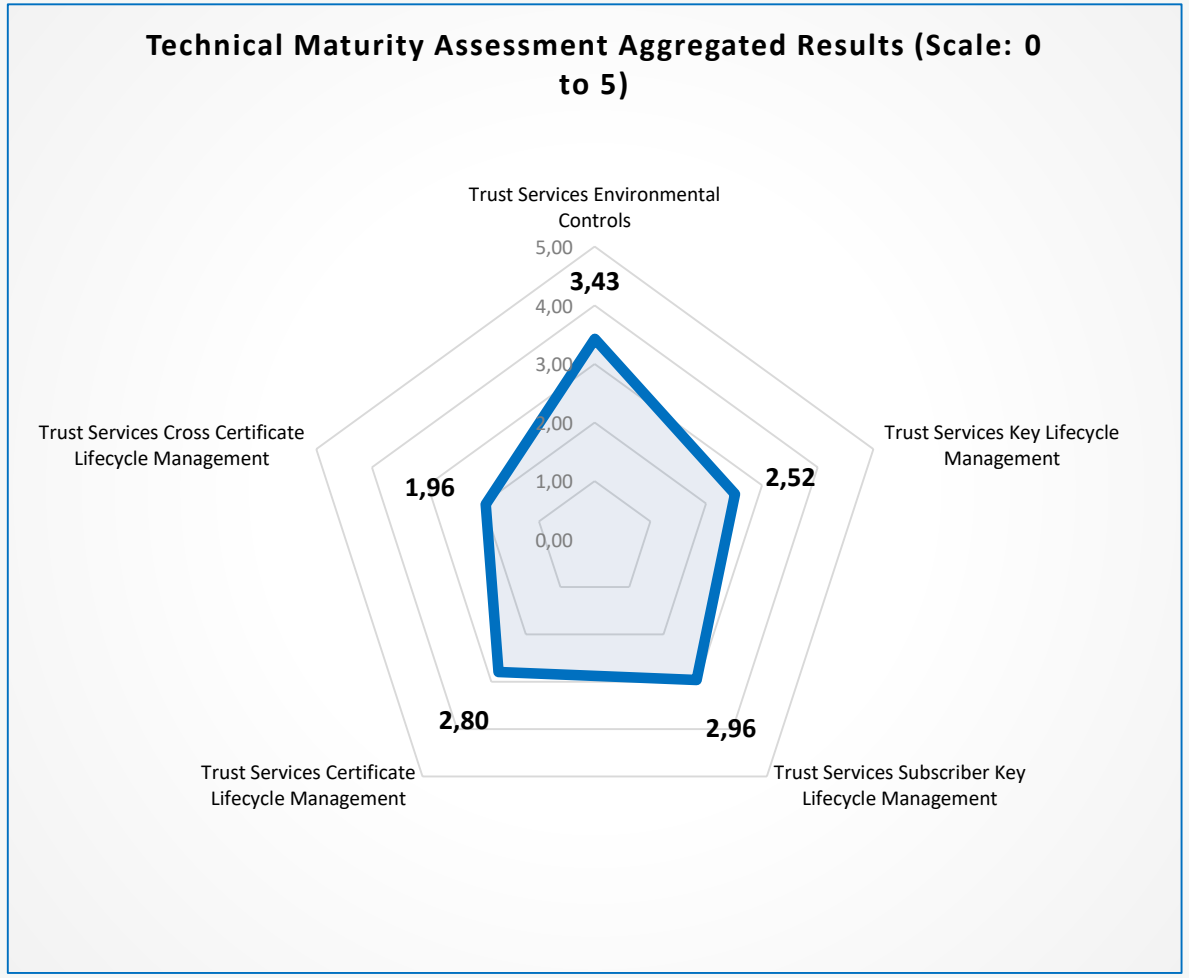
State of play and plans:

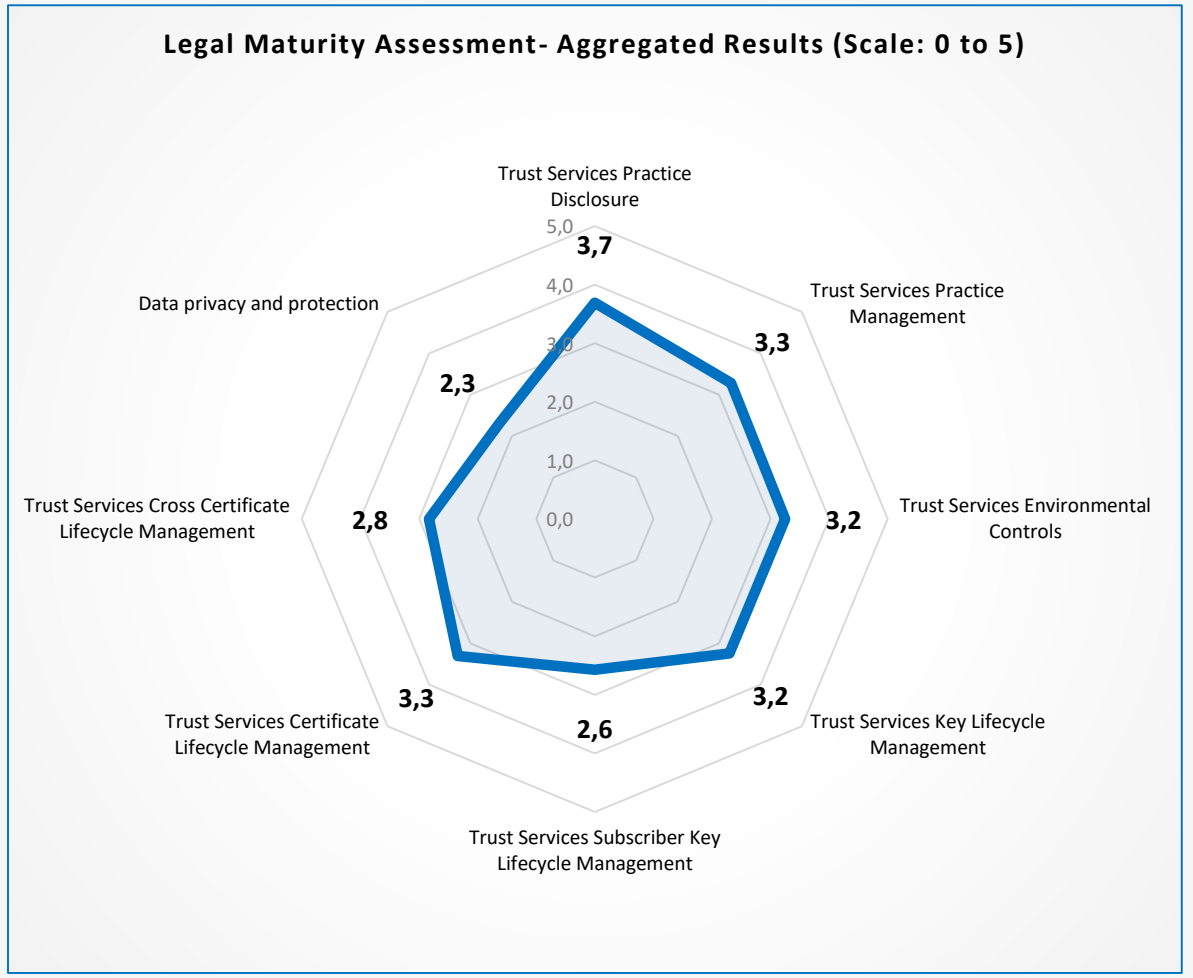


- The analysis on eID use and penetration in society, assessing eID maturity in each Eastern partner country was finalized and results aligned with country representatives
- The analysis has showed that:
  - most countries use eIDAS compatible technologies and standards, as well as international standards and guidelines. Significant area for improvement remains in **process design and technical configuration compatibility for eSignature cross-validation between countries**
  - The **data privacy and data protection regulations all together with the data protection processes** should be updated to comply with EU requirements for cross-border personally identifiable information (PII) transfer and processing that is needed for mutual validation eSignatures and eIDs
- The activity will continue with consultations of the national implementation teams for technical or legal questions that may arise related to the developed national action plan

1. Recognition of eID

Technical and Legal Maturity Assessments:





Completed | In progress | Planned for the upcoming 6 months

2. Pilot eSignature

State of play and plans:

Analysis of eSignature use in EaP countries (04/2020)	Requirements for eSignature use in cross-border interactions (06/2020	eSignature pilot countries selection and scope specification (05/2020)	Piloting cross-border eSignature (12/2020)

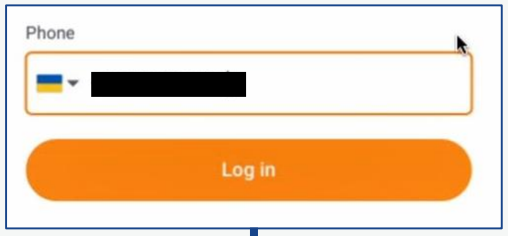
Final output

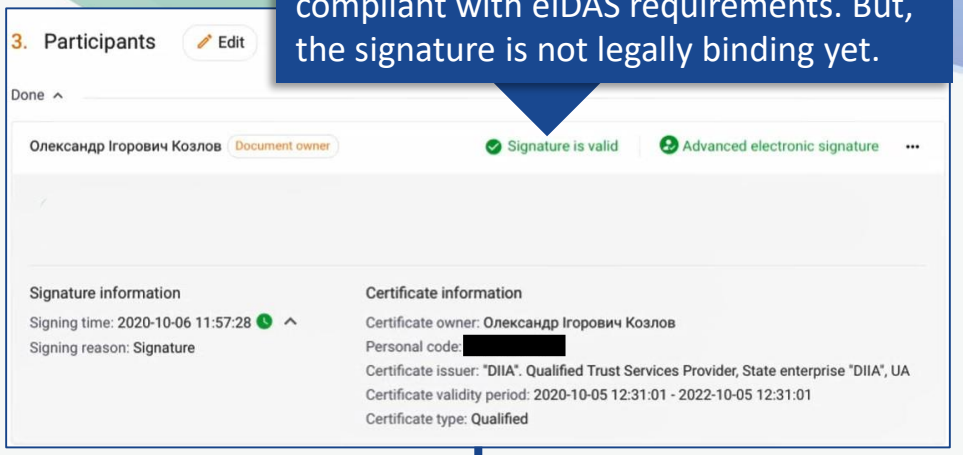
Piloted cross border eSignature. Recommendations and best practices on cross-border mutual developed. *(01/2021)*

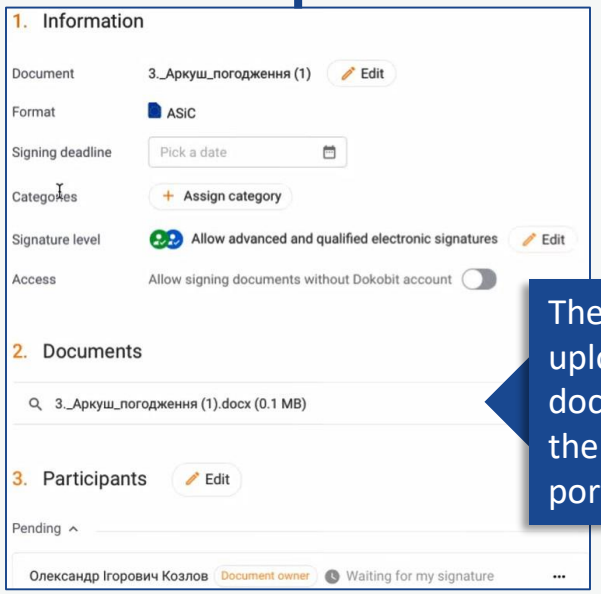
- **Scope of the activity:** eSignature pilot with UA – MD and UA – EE
- **Aim of the eSignature pilot:** technically operational cross-border eSignature to validate and identify the common practices and recommendations required to achieve cross-border mutual recognition
- EU4Digital Facility expert team has been supporting **with technical activities** to achieve technical compatibility between countries for cross-border mutual validation of trust services and eIDs
- **Focus on the upcoming period:** continuing piloting activities and identifying best-practices from the pilots which will serve in preparing an action plan for other EaP countries. As a post-pilot activity, the action plan will focus on readiness of cross-border mutual recognition from a regulatory, organizational and technical perspective, including actions that of eIDAS compliance audits

The signature is technically valid and compliant with eIDAS requirements. But, the signature is not legally binding yet.

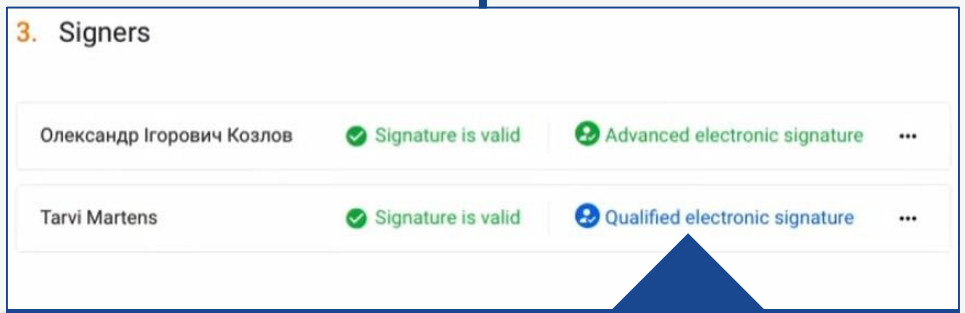
The signature is technically valid but the identity of the citizen is unknown because trust relationships between UA and EE (EU) were not established yet.







The UA citizen uploads a document in the eSignature portal.

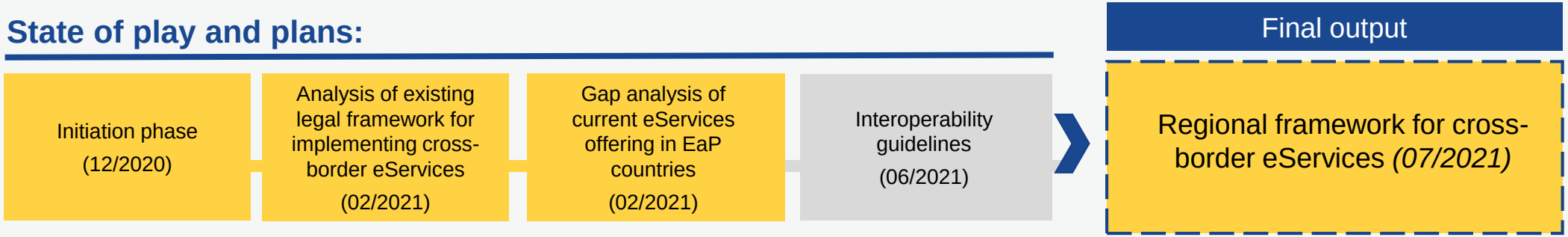


Both signatures are valid and recognized in the portal because the portal has established trust relationships with both UA and EE. The portal acts as a third party technical validation service between UA and EE. (the UA signature is still not legally binding in EU, yet)

Completed | In progress | Planned for the upcoming 6 months

3. Interoperability framework

State of play and plans:



- Differences in maturity and readiness levels of eServices, as well as data protection and privacy implementation are the key challenges, to resolve in order to achieve cross-border eServices enablement
- **Next steps in interoperability framework development:**
  - **Existing legal framework analysis and regulatory harmonization guidelines** - analysing legal frameworks for implementing cross-border eServices and creating regulatory harmonisation guidelines based on the EU example
  - **Identification of existing eService platforms, defining gaps in current service offering** - analysis on existing eServices platforms and current service offering gaps to businesses and citizens based on EU best practices
  - **Cross-border eServices capability building and interoperability guidelines** - detecting organizational, infrastructural and technical barriers for cross-border usage capabilities and providing interoperability guidelines
  - **Combined regional framework for the cross-border eServices enablement** - preparing the final regional framework for the cross border eServices enablement

Completed | In progress | Planned for the upcoming 6 months

4. Cybersecurity guidelines

State of play and plans:

AS-IS situation in EaP (09/2019)	Country specific cybersecurity reports on measures, priorities and gaps (01/2020)	Cybersecurity guidelines for EaP region (03/2020)

Final output

Cybersecurity guidelines for the EaP region developed *(06/2020)*

- **Common cybersecurity gaps and obstacles** based on analysis conducted**:**
  - Lack of qualified personnel, insufficient dedicated and systematic funding, and not established national-level contingency plans
  - No National Cyber Strategy (NSC) or it is outdated and not aligned with NIS Directive; not defined or incomplete Critical Information Infrastructure (CII) lists at a national level; and not performed cyber risk assessments at national level
- **Recommended next steps:**
  - Strengthening **cross-border cooperation** to support international cyber security operations and ensuring effective fight against cybercrime
  - Supporting Eastern Partner countries in **identification of CI/CII**, e.g. by providing reference list of security measures and guidelines on the criteria to be used for the identification of CI/CII
  - Supporting with **cyber awareness sessions** for public institutions and providing expert capability to strengthen **cyber security legislations** and harmonize with the NIS Directive

Trust and Security area beyond 2021

Considerations for the future

- Extend **eSignature piloting** to all Eastern Partner countries to establish cross-border mutual recognition of digital signatures within the region
- **Country action plans** implemented to achieve cross-border mutual recognition for trust services
- **Cross border eServices** piloted in all Eastern Partner countries
- **National Interoperability frameworks** established and **national interoperability platforms** operating in all EaP countries
- Strengthening cross-border cooperation to support **international cyber security operations** and ensuring **effective fight against cybercrime**
- Supporting EaP countries in **identification of CI/CII**, and strengthening of **cyber security legislations**

EU4Digital

EU4Digital

Feedback from Trust and Security Network

EU4Digital

Q/A
Common discussion

EU4Digital

Thank You

EU4Digital Facility | Trust and Security
Team leader | Martynas Daugirdas | martynas.daugirdas@lt.ey.com
(in cc: EU4Digital@lt.ey.com)