EU4Digital

EU4Digital: supporting digital economy and society in the Eastern Partnership

eSignature pilot extension Technical memorandum

December 2021

Table of Contents

Disclaimer: The views and opinions expressed in this document are entirely those of the EY-led consortium and do not reflect the official opinion of the European Commission. Neither the Commission, nor any person acting on the Commission's behalf may be held responsible for the content of the information contained in the document.

1. Context

EU4Digital[1] is European Union's regional facility which aims to bring the benefits of the harmonised digital market to the Eastern partner countries. EU4Digital aims to extend the benefits of the European Union Digital Single Market to the Eastern partner states, channelling the EU support to develop the potential of the digital economy and society, to bring economic growth, generate more jobs, improve people's lives, and help businesses. As part of the EU4Digital project the Trust and Security stream implements activities related to the promotion and increased usage of trust services between the EU member countries and the Eastern partner countries, including eSignature pilot extension activity.

The eSignature pilots are delivered as technical pilots and include the testing of cross-border eSignature interoperability.

The eSignatures issued during the pilot activities is not legally binding at the end of the pilots yet, nevertheless the results and the outcome of the pilots serve as an input for the development of the action plan, which outline future activities needed to achieve mutual recognition between the piloting countries.

The main characteristics of the eSignature pilots are detailed in the table below.

Characteristic	Description
Pilot scope	• Technically operational cross-border eSignature pilot compatible with eIDAS Regulation requirements which includes timestamping, and certificate validation mechanisms.
Pilot principles	• Technical pilot focused on the implementation of technologies and processes to enable eSignature creation and validation between pilot countries. • Non-legally binding unless mutual recognition (validation) of eSignatures is agreed between the pilot countries.
Pilot outcome	• Tested readiness of national infrastructure for cross-border eSignature interoperability compatible with eIDAS practices. • Practical recommendations to piloting countries for technical and organizational interoperability.

[1] For more information about EU4Digital Facility, please visit https://eufordigital.eu/

2. Pilot principles

The following principles shall be adhered to during the pilot's implementations:

- In order to pilot cross-border eSignature, signature creation tools (eIDs) and their certificates of participants shall be consistent with international cryptographic standards;
- No new eID service are implemented for the pilot, only existing eIDs shall be involved. Certification of participating eIDs shall be conformant with "qualified" level of corresponding national legislation;
- Parties will use eSignature and container format (hereinafter "Common format") as specified further in this document;
- Parties provide test eIDs and trust information (service certificates and/or Trust service list) to the "Reference platform";
- Parties enhance domestic publicly available eSignature tool(s) to verify signatures created with Common Format by eID holders of other participating countries.

3. Reference platform and interoperability levels

Parties may create their own eSignature creation tools and shall for validation, eSignatures of all parties shall be also interoperable with the Reference platform.

The Reference platform is needed for eSignature piloting activity, and the purpose of the Reference platform is to validate eSignatures in common format from all participating parties. In case of Interoperability level 1 or Interoperability level 2 (as per definitions provided below), there will be a need to create eSignatures by using eIDs of participating parties.

There are three interoperability level options considered for implementation during piloting activity:

- **Interoperability level 1** denotes that eSignature creation and validation for a party happens only by using the Reference platform.
- **Interoperability level 2** (nominal) adds requirement for a party to have self-maintained eSignature validation tool that also verifies cross-border signatures.
- **Interoperability level 3** foresees both creation and validation with self-maintained eSignature tool providing total independence from the Reference platform. However, the Reference platform shall successfully validate eSignatures created by such a tool.

Note: In previous eSignature pilot during 2020-2021 the Dokobit eSignature portal (dokobit.com) was the Reference platform for participating eIDs and provided eSignature creation, exchange, and validation capability in the Common Format. The Reference platform for the current pilot should be decided in each case.

4. Common format

The eSignature format shall be XAdES [1] at X-L and A level (also known as -LT and -LTA level in newer version of standards).

Timestamp and certificate validity data (OCSP) shall be obtained at the time of signing. Software implementations may limit support for XAdES elements to level specified in BDOC [2].

Time-marks (section 6.1 of BDOC[2]) and logging (section 7.1 of BDOC[2]) shall be disregarded. The container method for encapsulating original documents and signatures shall be ASiC-E [3].

Sample file can be found in [4]. In addition to DSS [5], source code libraries implementing the format are available for Java [6], C++ [7] and as a multiplatform desktop client [8].

References:

[1] ETSI TS 101 903 v1.4.2 – XML Advanced Electronic Signatures (XAdES)
https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf

and its Baseline Profile ETSI TS 103 171 v 2.1.1

https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.

Note: XAdES has been adopted as a EN ETSI EN 319 132{-1,-2}

[2] BDOC – Format for Digital Signatures https://www.id.ee/public/bdoc-spec212-eng.pdf

[3] ETSI TS 102 918 V1.3.1 - Associated Signature Containers (ASiC) https://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/ts_102918v010301p.pdf

[4] Sample file https://www.id.ee/wp-content/uploads/2020/05/bdoc21-ts.asice

[5] https://github.com/esig/

[6] DigiDoc Java library - digidoc4j https://id.ee/index.php?id=36972, https://github.com/open-eid/digidoc4j

[7] DigiDoc C++ library - libdigidocpp https://id.ee/index.php?id=36484

[8] DigiDoc4 Client https://github.com/open-eid/DigiDoc4-Client

5. eSignature pilot testing and acceptance criteria

The expected result is a file signed by two or more Pilot participants and successfully verified by Reference platform and/ or validation tools of the Parties (when applicable).

The pilots test cases will be designed based on the following high-level functional requirements presented in the following scenario:

Requirement	Scenario
Signing an electronic document	Citizen A (Country A) creates an eSignature using his own qualified digital certificate and signs an electronic document. The document is sent to Citizen B (Country B).
eSignature validation and co-signing	Citizen B (Country B) receives an electronic document signed with an eSignature from Citizen A (Country A). Citizen B validates the eSignature of Citizen A and after that Citizen B adds his own eSignature to the same electronic document. The document is sent back to Citizen A (Country A).
eSignature validation of the signed document	Citizen A (Country A) receives the electronic document co-signed by Citizen B (Country B). Citizen A (Country A) validates the eSignature of Citizen B (Country B).