Version 2021-03-19

FOR REVIEW

Revised outline of the Commission implementing act on the technical and operational specifications of the technical system for the cross-border exchange of evidence and application of the "once-only" principle

Chapter I – General provisions

Definitions

For the purposes of this Regulation, the following definitions should apply:

1. ‘once-only technical system’ (OOTS) means the technical system for the cross-border automated exchange of evidence referred to in Article 14 of Regulation (EU) 2018/1724;
2. ‘evidence provider’ means a competent authority that lawfully issues evidence falling within the scope of Article 14(2) of Regulation (EU) 2018/1724;
3. ‘evidence requester’ means a competent authority responsible for one or more of the procedures referred to in Article 14(1) of Regulation (EU) 2018/1724;
4. ‘eDelivery Access Point’ means a communication component that implements an electronic delivery service, complying with technical specifications referred to in Annex 4;
5. ‘eIDAS Node’ means an implementation of the technical specifications developed in line with Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, and with Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework, enabling the communication with other nodes of the eIDAS Network for the purpose of cross-border authentication;
6. ‘intermediary platform’ means a technical solution through which evidence providers or evidence requesters from one Member State connect to the common services referred to in Article 4(1) and to evidence providers or evidence requesters from other Member States;
7. ‘data service directory’ means a registry containing the list of evidence providers, the evidence they provide and their descriptive elements;
8. ‘evidence broker’ means a service allowing an evidence requester to determine which evidence type from another Member States is equivalent to the evidence it requires for the purposes of a national procedure;

9. ‘semantic repository’ means a collection of semantic specifications, linked to the evidence broker and the data service directory, which stores and shares machine-readable definitions of names, data types and data elements associated with specific evidence types to ensure the mutual understanding and cross-lingual interpretation for evidence providers, evidence requesters and the user, when exchanging evidence through the once-only technical system;
10. ‘data service’ means a technical service through which an evidence provider handles the evidence requests and dispatches evidence;
11. ‘data model’ means an abstraction that organises elements of data and standardises how they relate to one another. It specifies the entities, their attributes and the relationships between entities;
12. ‘preview space’ means a functionality enabling to temporarily store the evidence to allow its preview by the user;
13. ‘structured evidence’ means any data or document in electronic format in the scope of Article 14 of Regulation (EU) 2018/1724, that is organised in predefined elements or fields that have specific meaning and technical format allowing for processing by software systems;
14. ‘unstructured evidence’ means any evidence in electronic format in the scope of Article 14 of Regulation (EU) 2018/1724, which is not organised in predefined elements or fields that have specific meaning and technical format, but mapped to at least the minimal attributes of the relevant data model as documented in the semantic repository to enable its identification and automated exchange;
15. ‘incident’ means a situation where the once-only technical system is not performing, transmits wrong evidence, or where the evidence has changed during the transmission, as well as any event of security breach.

Object and structure

1. The OOTS should enable communication between evidence requesters and evidence providers with the support of the common services for the purpose of the automated cross-border exchange of evidence, at the user’ explicit request, for the online procedures listed in Article 14(1) of Regulation (EU) 2018/1724.
2. The OOTS should consist of:
    a. the relevant evidence requesters’ procedure portals and evidence providers’ data services;
    b. intermediary platforms, where relevant;
    c. eIDAS Nodes for user authentication and identity matching;
    d. eDelivery Access Points;
    e. the common services;
    f. the integration elements and interfaces required to connect this different components.

Chapter II – Services of the OOTS

eIDAS Nodes and eDelivery Access Points

1. The Member States should ensure that evidence requesters are connected to an eIDAS-Node to perform the user authentication either directly or through an intermediary platform.
2. Member States should ensure that eDelivery Access Points are installed, configured and integrated in the evidence requesters’ procedure portals, evidence providers’ data services or in intermediary platforms, as the case may be.

3. Member States should decide on the number of eDelivery Access Points they use for the OOTS. The eDelivery Access Points to be used as of 12 December 2023 should be notified to the Commission at the latest by 12 June 2023. After 12 June 2023, Member States can notify additional eDelivery Access Points to the Commission. Such additional eDelivery Access points can be taken into operation for the purpose of the OOTS as of 30 June and 31 December of each year, provided that a period of at least 6 months has lapsed since their notification.

Common services

1. The Commission in cooperation with the Member States should establish the following common services of the OOTS:
    a. the data service directory;
    b. the evidence broker;
    c. the semantic repository;
    d. the common user feedback tool.
2. The Member States should ensure the integration between the procedure portal of the evidence requesters and the data services of the evidence providers, directly or through intermediary platforms, and with the common services. The integration should be based on the exchange protocols and technical specifications set out in Annex [X] and aligned with the semantic assets stored in the semantic repository.
3. The Member States should ensure that only evidence requesters and evidence providers are connected, directly or through the intermediary platforms, to the common services and can make use of the OOTS.

Data service directory

1. The Member States should ensure that each evidence provider and each type of structured or unstructured evidence issued by each of these evidence providers is registered in the data service directory in accordance with the associated information, data models, definitions and data formats as documented in the semantic repository.
2. The Member States should ensure that each type of evidence registered in the data service directory is accompanied by an indication of:
    a. the level of assurance of the electronic identification means notified by Member States in accordance with Regulation (EU) 910/2014; and
    b. where applicable, any additional attributes beyond the attributes exchanged using the electronic identification means notified in accordance with Regulation (EU) 910/2014
    c. required for its exchange through the OOTS.
3. The data service directory should make a clear distinction between the additional attributes referred to in the previous paragraph (b) and the attributes exchanged using the electronic identification means notified in accordance with Regulation (EU) 910/2014.
4. The level of assurance and the additional attributes referred to above should correspond to the level of assurance and attributes required by the evidence provider from a national user requesting this type of evidence directly from the evidence provider.
5. The Member States should be responsible for keeping the information in the data service directory up to date.
6. The Commission should provide validation support for the Member States to verify the compliance of the evidence with the data models.

Evidence broker

The Commission should establish, in cooperation with the Member States, an evidence broker that allows an evidence requester in a Member State to determine which evidence type it can request from an evidence provider in another Member State, in the context of a particular procedure.

Semantic repository and the data models

1. The Commission in cooperation with Member States should ensure that the semantic repository provides access to data models, associated schemata and data formats for all types of evidence that can be requested on the basis of Article 14 of Regulation (EU) 2018/1724.
2. The evidence providers or intermediary platforms where applicable should apply all updates and adaptations to the data models, associated schemata and data formats according to schedules for updates and adaptations that are regularly announced and discussed in the gateway coordination group. Such updates and adaptations should apply twelve months after their publication in the semantic repository.

National registries and services

1. Member States that have national registries or services that are equivalent to the data service directory or evidence broker should have the option to either use the data service directory or the evidence broker or to:
    a. connect their national registries or services to the data service directory or evidence broker; or
    b. replicate data in the national registries or services in the data service directory or evidence broker.
2. In case a Member State chooses to connect a national registry or service to the common services, the providers of national registries or services should comply with the technical specifications set out in Annex [X] to ensure interoperability of their services.

Common user feedback tool

The common user feedback tool established by the Commission in accordance with Article 25 of Regulation (EU) 2018/1724 should be used to enable users to provide feedback, such as to specify why they decided not to use the evidence after previewing it. Articles 10(1) and 11 of Commission Implementing Regulation (EU) 2020/1121 should apply to the collection and transmission of such user feedback.

Chapter III – Obligations on evidence requesters

Explanation to users

Evidence requesters should ensure that their procedure portals contain explanations about the possibility to use the OOTS and its features, including, in particular, the information that:

- users have the option to preview the evidence and decide whether or not to use it for the procedure; and that,
- if the user decides not to use it for the procedure, the previewed evidence will be deleted automatically from the separate preview space referred to in Section X below.

Evidence selection

1. Evidence requesters should give users the possibility to select and request the types of evidence that they would accept in the same procedure by direct submission, provided that evidence providers make these types of evidence available through the OOTS.
2. If multiple pieces of evidences can be retrieved, the evidence requester should ensure that users can select all, a sub-set or a specific type of evidence.

User Authentication

1. Evidence requesters should rely on electronic identification means notified in accordance with Regulation (EU) 910/2014 for authenticating the identity of the users.
2. Once the user has selected the evidence to be exchanged through the OOTS, and based on the level of assurance of electronic identification means and, where applicable, the

additional attributes referred to in Section X(2)(a) and (b), the evidence requesters should inform users about:

a. the electronic identification means available for authenticating its identity for the purposes of evidence exchange through the OOTS; and

b. where applicable, any additional attributes that the user needs to provide.

3. Where a user has already identified and authenticated himself to access the procedural portal using an electronic identification means notified in accordance with Regulation (EU) 910/2014, the user should only be required to identify and authenticate again for the purpose of requesting the exchange of evidence where the level of assurance of the electronic identification means required by the evidence provider and presented in the data service directory is higher than the assurance level of the electronic identification means used by a user to access the procedural portal.
4. The previous paragraph also applies in cases when the user requests multiple pieces of evidence from different evidence providers in the same or different Member States.

Explicit request

In order for a user to be able to provide his/her explicit request to exchange the selected evidence through the OOTS, the evidence requester should provide the user with:

- the name(s) of the evidence provider(s);
- the evidence type(s) or data fields that will be exchanged.

Evidence request

1. The evidence requester should ensure that the explicit request made by a user is transmitted to the evidence provider with the following parameters:

a. the evidence type that is requested;

b. date and time when the explicit request was made;

c. identification of the procedure for which the evidence is required;

d. name of the evidence requester or intermediary platform, where applicable;

e. the personal identification data of a user;

f. the level of assurance of the electronic identification means used by the user;

g. the additional attributes provided by the user for the purpose of the request of evidence;

h. the identification of the evidence provider.

2. The evidence requester should ensure that the digital representation of that request, including the parameters listed in paragraph 1, is provided in a format that makes it possible to transmit electronically together with the evidence request, in accordance with the technical specifications set out in Annex [X].

Preview of evidence

1. The Member States should ensure that the preview space where a user can preview the evidence exchanged through the OOTS is available as part of the evidence requester's online procedure.
2. The Member States should ensure that the preview space is separate by equipping with features that:

a. allow only the user to access it and only as long as the user is in the procedure environment and until the user decides whether or not to use it in the procedure;

b. do not allow the evidence requester or any of its systems or any third parties to access, view or copy the evidence which is in the preview space;

c. permanently delete the evidence and any cached data from the preview space in case a user decides not to use the evidence for the procedure or when the user leaves the preview space or the procedure portal not explicitly approving the use of the evidence;

d. provide users the possibility to leave their feedback, including about why they decided not to use the previewed evidence in the procedure.

Chapter IV – Obligations on evidence providers

Role in the exchange of evidence

The Member States should ensure that for the purpose of the evidence exchange through the OOTS, the evidence providers or intermediary platforms should, where applicable, implement application services allowing in particular to:

- receive and interpret evidence requests delivered by an eDelivery Access Point. Such requests should be considered as the input to the "Evidence Query Service";
- retrieve any pieces of evidence or evidence references, matching the request, subject to successful authorisation;
- return evidence responses, including possible errors, and submit them to an eDelivery Access Point for transmission to the evidence requester;
- include in the response evidence references instead of actual evidence, where an evidence reference is requested instead of evidence.

Identity matching

1. Evidence providers or intermediary platforms where applicable should be responsible for ensuring that evidence is only exchanged through the OOTS if the identification data held by them unambiguously matches the identification data of the user in the evidence request referred to in Section X(1)(e) above.
2. Where process of identity record matching does not result in an unambiguous match enabling the attribution of the evidence to the user in the evidence request, the requested evidence should not be exchanged. In such a situation:
    a. the user should receive an automated message explaining that the evidence cannot be provided and be redirected to the evidence requester's procedure portal; and
    b. an error message should be sent to the evidence requester.

Evidence entering eDelivery Access Point

The evidence providers should be responsible for the quality and integrity of the evidence entering the eDelivery Access Points.

Chapter V – Governance of the technical system and ensuring the functioning of the 'once-only' technical system

Gateway coordination group

The Commission, in cooperation with Member States in the framework of the gateway coordination group established by Article 29 of Regulation (EU) 2018/1724, should:

- oversee the establishment and launch of the OOTS;
- set priorities for further developments and improvements to the OOTS;
- define and adapt where necessary the high-level principles of the technical specifications to the extent that these are not yet set out in this Implementing Regulation and its Annexes;

- determine the indicative schedule for regular updates and adaptations of the technical specifications;
- determine criteria for conformance testing to ensure correct implementation of the technical specification and the correct functioning of the OOTS;
- review and adopt risk management plans to identify risks, assess their potential impact and plan responses with appropriate technical and organisational measures in case of incidents.

Single points of contact

1. The Commission and each of the Member States should designate a single point of contact to ensure a coordinated development, operation and maintenance of the relevant parts of the OOTS for which they are responsible pursuant to Chapter VI.
2. The single points of contact should, in particular, each in its area of responsibility:
    a. provide expertise and advice to evidence providers and evidence requesters for all technical problems encountered in relation to the operation of the OOTS;
    b. handle any possible downtimes of the eDelivery Access Points or possible security breaches;
    c. investigate and solve any other incidents.
3. The Member States and the Commission should ensure that their respective single points of contact ensure business continuity and are able to provide assistance at short notice.
4. The single points of contact should report any substantial incidents to their SDG national coordinators and should support them in exercising their tasks related to the OOTS in the gateway coordination group.
5. The Member States and the Commission should communicate the contact details of these contact points to each other and inform each other immediately of any changes thereof.

Cooperation with other governance structures

The Commission should inform the gateway coordination group about discussions and decisions of different relevant governance structures, including those established under Regulation (EU) No 910/214, relevant for the functioning of the OOTS.

Chapter VI – Responsibility for the maintenance, operation and security of the components of the OOTS

Commission responsibilities

The Commission should be the owner of and responsible for the common services referred to in Section X(1). This responsibility includes in particular:

- the development, availability, monitoring, updating, maintenance and hosting of the common services;
- ensuring the security of the common services by preventing any unauthorised access, entry of data and consultation, modification or deletion of data and detecting any security breaches;
- establishing security plans concerning the common services.

Member States responsibilities

The Member States should be the owners of and responsible for the respective national components of the OOTS referred to in Article 2(2)(a)-(d) and (f). This responsibility includes in particular:

- their establishment where applicable, maintenance and management, including deploying updates;

- ensuring the security of those components by preventing any unauthorised access, entry of data and consultation, modification or deletion of data and detecting any security breaches.

Uninterrupted operation of the OOTS

1. The Commission and the Member States should ensure uninterrupted operation of the components of the OOTS for which they are responsible.
2. The Commission should inform the Member States of changes and updates to the common services.
3. The Member States should inform the Commission of changes and updates to the components under their responsibility that may have repercussions on the functioning of the OOTS.

Assessment of the electronic systems

1. The Commission and the Member States should conduct regular assessments of the components of the OOTS for which they are responsible.
2. The Commission and the Member States should inform each other of any activities that might result in a breach or a suspected breach of the security of the OOTS.

Chapter VII - Final provisions

Onboarding to the OOTS

The Member States and the Commission should test the functioning of the OOTS before it is put into operation. Only when the tests yield positive results, the OOTS should be made available to users.

Processing of personal data

In relation to the processing of personal data occurring in the system components that they own and are responsible for pursuant to Section X above, the Member States act as controllers as defined in Article 4(7) of Regulation (EU) 2016/679 and comply with the obligations laid down in that Regulation.