

CEF TELECOM – 2020-1 CALLS FOR PROPOSALS

FREQUENTLY ASKED QUESTIONS

eDelivery – 8 April 2020 version

All information in blue has been added or updated since the previous version.

For more technical information on eDelivery, please see the CEF Collaborative Platform: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>

Commonly used abbreviations in this FAQ:

AP	Access Point
AS2/4	Applicability Statement 2/4 Profile (open standards for eDelivery)
DSIs	Digital Service Infrastructures
eIDAS	electronic IDentification, Authentication and trust Services
ERDS	Electronic Registered Delivery Service
PEPPOL	Pan-European Public Procurement Online (set of artifacts and specifications enabling cross-border eProcurement)
QTSP	Qualified Trust Service Provider
SML	Service Metadata Locator
SMP	Service Metadata Publisher

1. What is the difference between this call and the previous eDelivery calls?

The main difference between the 2020-1 and previous eDelivery calls is that priority will be given to proposals deploying Access Points within activity (a)¹ as per call text in networks where CEF eDelivery is not already in use. As of the 2017-2 eDelivery call there has been no longer funding available for deploying an AS2 Access Point.

Apart from this change, the objectives/activities of the call remain the same. However, to be noted that under the current call, only 2 entities from one or more Member State(s) are required for the consortium composition. Please refer to section 6.1 of the call text for more information.

2. What are the definitions of an "Access Point" and "setting up an Access Point"?

As referred to in section 2.1 of the eDelivery call text, an Access Point is an implementation of the CEF eDelivery AS4 Profile² developed by e-SENS and now maintained by the Connecting Europe Facility (CEF). The specifications of CEF eDelivery are profiles, meaning that several options of the AS4 technical specifications from OASIS were narrowed down in order to increase consistency and interoperability, as well as simplify deployment.

The setting up of an Access Point involves:

- The installation of the software (Open Source or commercial) in a production environment (server, network, storage, etc.).
- The successful passing of connectivity tests³ from the connectivity testing service offered by the CEF eDelivery Core Service Platform.
- When applicable, the confirmed connectivity to a Service Metadata Publisher (SMP) and Service Metadata Locator (SML).
- The successful passing of conformance tests⁴ from the conformance testing services offered by

¹ <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-edelivery>

² <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4>

³ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Connectivity+testing>

⁴ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing>

the CEF eDelivery Core Service Platform, in case of installing software other than those previously found conformant with CEF eDelivery specifications as listed here:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions>

3. What is the definition of a "Service Metadata Publisher"?

The Service Metadata Publisher (SMP) is an implementation of the CEF eDelivery SMP profile⁵ developed by e-SENS and now maintained by the Connecting Europe Facility (CEF), on top of the OASIS SMP Specification.⁶ The specifications of CEF eDelivery are profiles, meaning that several options of the SMP technical specifications from OASIS were narrowed down in order to increase consistency and interoperability, as well as simplify deployment.

The setting up of an SMP involves:

- The installation of the software (Open Source or commercial) in a production environment (server, network, storage, etc.).
- The successful passing of connectivity tests from the connectivity testing service offered eDelivery Core Service Platform.
- The successful passing of conformance tests from the conformance testing service offered by the eDelivery Core Service Platform, in case of installing software other than those previously found conformant with CEF eDelivery specifications as listed here:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/OASIS+SMP+conformant+solutions>

4. What is the definition of the "Service Metadata Locator"?

The CEF eDelivery Service Metadata Locator (SML) enables Access Points to dynamically discover the location of the destination Access Point. Instead of looking at a static list of IP addresses, the Access Point consults a Service Metadata Publisher (SMP) where information about every participant in the document/data exchange network is kept up to date, including the IP addresses of their Access Point. For dynamic discovery to work, every participant must be given a unique ID in the form of a website's URL which must be known on the internet's Domain Name System (DNS) thanks to the SML. By knowing this URL, the Access Point is able to dynamically locate the right SMP and therefore the right Access Point.

The SML uses DNS lookups to find information concerning a given participant in a message exchange network. This approach does not need a single, central server to run the discovery interface (with its associated single point of failure). Instead, the use of the DNS makes it highly resilient. At runtime, the SML uses decentralised DNS for load balancing of requests, thus supporting a full European-wide upscaling of performance. Since CEF eDelivery interfaces with the global DNS system, the SML can virtually operate 24/7/365. In case of failure, participants would still be able to discover each other based on the information stored on the DNS.

5. Will the funding be provided for the connector that is part of access point localization?

No. Domain-specific connectors are out of scope of this call. In other words, no funding is foreseen beyond basic connectivity between back offices and the Access Point.

6. Is it mandatory to use the REM (registered electronic mail) evidences in the connector?

This is optional as the use of REM evidences depends on the needs of the project/message exchange network. There is no single policy on the use of REM evidences. As noted in Q5 above, the connector is in any case out of scope of the 2020-1 eDelivery call.

⁵ <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+specifications>

⁶ <http://docs.oasis-open.org/bdxc/bdx-smp/v1.0/cspr01/bdx-smp-v1.0-cspr01.html>

7. What is the minimum number of public bodies required in an eDelivery consortium?

As indicated in section 6.1 of the call text, the consortium composition must "consist of at least two entities, public and/or private, based in one or more Member States and/or EEA countries participating in the CEF Telecom programme." There is no requirement concerning the minimum number of public bodies in the consortium.

8. We are a commercial secure electronic mail service provider using a solution which runs on specific standards and does not support AS4 or SMP integration. Would the development of a background integration module for this system (to facilitate the transition to the new standard and to enable users of the current system to access the AS4 network) be covered under this call?

The deployment of an eDelivery Access Point (implementing the CEF eDelivery AS4 profile) can be done by buying, reusing or building. In this case, the deployment would be achieved by building and is therefore within the scope of this call.

9. Can interoperability testing be funded under this eDelivery call?

Yes, interoperability testing between eDelivery solutions can be funded under this call provided that activities specifically listed under section 2.1 of the call text (a, b or c) are also covered by the proposed Action.

10. The eSENS AS4 protocol has foreseen business transactions (service actions etc) for defining service choreography. Will there be future service procedures on how to e- service mail to EU citizens over the eDelivery building block?

The CEF eDelivery team has published a Security Controls guidance document which addresses the security controls and recommendations applicable to CEF eDelivery's message exchange Use Case. The document defines and explains several security options that can be used in this context and maps the Qualified ERDS (QERDS) requirements from the eIDAS Regulation to the security controls of eDelivery. More specifically, the document suggests and recommends a list of security controls to be implemented when using eDelivery, possibly, as a QTSP (Qualified Trust Service Provider).

However, it must be stressed that the recommended security controls do not grant or ensure the QTSP status, since this decision can only be made by the national supervisory bodies in the relevant Member State countries.

The Security Controls guidance document is publicly available via:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance>.

11. The "four-corner" model is discussed as if it is part of eDelivery. In one of the EU documents describing the eDelivery building block, it is stated that the four-corner model is not necessarily part of it. Can you explain this?

Please note that CEF eDelivery is not a "one size fits all" solution. There are several possible architectural set-ups that one can opt for depending on the business needs. eDelivery supports 3 different topologies of message-exchange models:

1. In the 2-corner model, backend systems communicate directly with each other through a point-to-point connection. As a result, there is a need to set up bilateral channels between every participant (when there is no common messaging protocol) or change backend systems to support the common protocol and impact the backends. This is also known as the "fully connected network".

Pros: Best suited for simple integration with few participants

Cons: Not easily scalable, heavy impact on backends

2. In the 3-corner model, backend systems communicate with each other through a central hub.

Thanks to the fully centralised approach, parties exchange messages with each other via the central hub in 2 steps:

- a. Party A exchanges information with the central hub
- b. Central hub exchanges information with Party B. This is also known as the "star network".

Pros: No need to set up bilateral channels between participants, central management and control of all processes, central monitoring processes

Cons: Central Access Point may become a bottleneck/single point of failure in the network; risk of service provider lock-in, scalability.

3. In the 4-corner model, the backend systems of the users do not exchange data directly with each other, but do this through Access Points. These Access Points are conformant to the same technical specifications and therefore capable of communicating with each other. As a result, users can easily and safely exchange data even if their IT systems were developed independently from each other. This is also known as the "mesh network".

Pros: Eliminates risk of single point of failure, eliminates risk of service provider lock-in

Cons: Need to enhance security between Access Points, need to conform to common message exchange protocol

Please be aware that depending on your business requirements, you may only implement a subset of the CEF eDelivery technical specifications. For instance, it is possible to implement the dynamic discovery model of CEF eDelivery based on the SMP and SML specifications without implementing the eDelivery Access point specification.

The CEF eDelivery self-assessment tool - a survey that assesses your requirements - might be of interest. The tool maps your requirements to the CEF eDelivery Service Offering. During the selfassessment, you assign different scores to the relevant needs of your organisation. Based on the answers provided, the tool calculates how CEF eDelivery can help you achieve your goals and which components of CEF eDelivery are suitable for re-use. All eDelivery-related resources are available on CEF Digital:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>

Additionally, to help you elicit your requirements, the CEF eDelivery team provides support via workshops to guide you through the user journey. Contact the CEF Stakeholder Management Office at CEF-BUILDING-BLOCKS@ec.europa.eu for more information. Please note that all services from CEF eDelivery are provided for free to public administrations.

12. Are there any specifications documents and/or open source software available for implementing a national connector to an Access point?

Currently, the Access Point specifications promoted by CEF eDelivery (the e-SENS AS4 profile) only defines the message exchange between Access Points (also called corner 2 and corner 3 in a 4-corner network - see Q11 above).

The backend integration between corner 1 and corner 2 (or similarly between corner 3 and corner 4) is not defined and can be product-specific based on the software implementation used. Domibus, the sample Access Point implementation maintained by the CEF eDelivery team uses a plug-in mechanism to facilitate the backend integration.

Every version of Domibus is released with a default web-service, folder based (file system) and JMS plug-in, also maintained by the CEF eDelivery team. Moreover, the plug-in mechanism allows users to develop their own custom plug-ins by following the guidelines in the plug-in cookbook (an implementation manual available on the release page of every Domibus version).

Other conformant implementations can choose to support different type of connector or custom backend integration mechanisms. They can do this out of the box or via a custom component based on specific needs. For more information on conformant implementations and related contact options, please refer to

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions>

13. Will the installation of AS2 Access Points and PEPPOL SMPs be supported under this call?

No. Please see Q1 above.

14. Will the projects have to verify compliance with the eDelivery DSI?

Yes, the projects will need to pass the conformance and/or connectivity tests that are provided by the CEF eDelivery Core Service Platform. More information on both tests can be found on CEF Digital website: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing>

15. We understand that the eDelivery call does not fund the development of domain-specific connectors. Could you please explain that?

'Domain-specific connectors' means connectors that are specific to the fields of another CEF Telecom Digital Service Infrastructure (DSI), for example eInvoicing. Therefore applicants that wish to fund a domain-specific connector must instead look at the call for proposals of the relevant DSI. Several DSI calls include eDelivery, allowing both the setup and implementation of the connectors to be funded.

16. Do we need to test our AS4 access point with the "CEF core service" connectivity test if we are only operating in the PEPPOL network? Could we obtain funding if we only test with the OpenPEPPOL testbed?

It would depend on the activities of the Action. The connectivity tests with the CEF eDelivery Core Service Platform are mandatory for a newly deployed AS4 AP/SMP or in case of an upgraded solution to become conformant with CEF eDelivery specifications. This is also applicable for the transformation of a PEPPOL Access Point from AS2 to AS4 profile. Furthermore, in case of an upgrade, the conformance tests with CEF eDelivery Core Service Platform are also mandatory (the links to the tests are provided in the call text).

The costs of testing with the PEPPOL network could also be eligible, if the testing is necessary for interoperability within the PEPPOL network, and the relevant task is mentioned in the work plan (i.e. in the Grant Agreement).

17. When upgrading to AS4 – can I also apply for making my application more efficient on parts related to AS4 but not only to the upgrade of AS4?

It depends under which priority/DSI of 2020-1 call you would like to apply for. Under the eDelivery call, such an Action could only be envisaged under call objective c). However it should be recalled that proposals will first and foremost be judged on their degree of alignment with the priorities of the Call/Work Programme, i.e. the compliance with the CEF eDelivery standards, to which only the upgrade to AS4 directly contributes. In other words, although additional work on efficiency of AS4 related parts could be assessed on a case-by-case basis, if the focus is on improvement of other parts the proposal is unlikely to be awarded under the eDelivery call.

When eDelivery is implemented under the calls of other DSIs, the related costs to AS4 AP should be justified and directly necessary for meeting the objectives of the particular DSI. The intended upgrades should be also included in the work plan (part A of the proposal).

18. Are there any recommendations on how much an AS4 upgrade should cost – the maximum of cost for an upgrade?

There is no fixed ceiling in the Call 2020-1 for an upgrade of AS4 Access Point, taking into account the fact that the situation and context of each beneficiary varies. However, the applicants should respect the basic principles of sound financial management (e.g. value for money). The relevant information on the costs and planned budget will be assessed and the application may receive a lower

score if the solution is too costly and/or the relevant information on the envisaged costs was not satisfactorily provided.

19. Are the costs related to the Conformity Assessment for becoming a qualified service provider pursuant to eIDAS Regulation eligible under the e-Delivery 2020-1 call? The Qualified Electronic Registered Delivery Service will be developed and offered as a result of the project implementation.

Yes, the costs associated with the Conformity Assessment could be considered as eligible within an Action aiming to develop and deploy a Qualified Electronic Registered Delivery Service. Please note that in order to consider those costs as eligible, the supervisory body would need to grant qualified status to the service provider (to become eIDAS qualified trust service provider) in line with the Article 21 of the eIDAS Regulation⁷, within the duration of the Action.

20. Can Ukrainian civil organisations apply for the 2020 CEF eDelivery call for proposals?

The rules for participation of entities established in third countries are provided in section 6.1 of the call text. Third countries and entities established in third countries may only participate as part of a consortium with applicants from EU/EEA countries. The application must contain the agreement of the Member State concerned by the proposed Action and a declaration from the European partner involved in the proposal on why the participation of the third country applicant is indispensable. Applicants that are entities established in a third country must also provide proof of the support of the third country authorities concerned by the action. The participation of entities from third countries must be well justified and they may not receive funding under the CEF Regulation, except where it is indispensable to achieve the objectives of a given project of common interest.

Furthermore, if the civil organization intends to deploy an AS4 Access Point or a SMP, the proposal needs to provide proof that the network to which the AP or SMP will be connected does not object to the role the third country applicant plays in the consortium.

21. What does evidence of eIDAS conformity of eDelivery implementations mean, as there are no standards mentioned for this?

eIDAS conformity evidence is requested for actions aiming to establish a Qualified Electronic Registered Delivery Service (QERDS) in line with the requirements set in Art. 44(1) of Regulation (EU) No 910/2014 (the eIDAS Regulation).

According to paragraph 2 of the same Article, the Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. However, no such implementing acts have been adopted.

Therefore, if an action aims to establish a QERDS, compliance with the requirements has to be established by way of a conformity assessment report issued by an eIDAS accredited conformity assessment body.

⁷ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

A list of conformity assessment bodies (CABs) accredited against the requirements of the eIDAS Regulation can be found here: <https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation>.