CEF TELECOM – 2017-2 CALLS FOR PROPOSALS

FREQUENTLY ASKED QUESTIONS

eDelivery – version 29 August 2017

For more technical information on eDelivery, please see the CEF Collaborative Platform:

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

All information marked in blue has been added since the previous FAQ version.

Commonly used abbreviations in this FAQ:

ERDS	Electronic Registered Delivery Service
QTSP	Qualified Trust Service Provider
SML	Service Metadata Locator
SMP	Service Metadata Publisher

1. What is the difference between this call and the 2016-2 eDelivery call?

The main difference between the 2017-2 and 2016-2 eDelivery calls is that there is no longer funding available for deploying an AS2 Access Point under the 2017-2 call. (See section 2.1 of the call text for more information).

Apart from this change, the priorities and objectives of the call remain the same. The overall budget of the call (€0.5 million) and the consortium requirements (at least 4 entities from one or more Member State(s) are unchanged from the 2016-2 call. Please read 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 e-SENS AS4 Profile[1] developed by e-SENS. The specifications of CEF eDelivery are profiles, meaning that several options of the original technical specifications 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 conformance tests from either a well-recognised conformance/interoperability testing organisation or from the conformance testing service offered by the eDelivery Core Service Platform.
- When applicable, the confirmed connectivity to a Service Metadata Publisher (SMP) and Service Metadata Locator (SML).

[1] http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4

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

The Service Metadata Publisher (SMP) is an implementation of the SMP profile developed by e-SENS[2] on top of the OASIS SMP Specification.[3] The specifications of CEF eDelivery are profiles, meaning that several options of the original technical specifications were narrowed down in order to increase consistency and interoperability, as well as simplify deployment.

The setting up of a SMP involves:

- The installation of the software (Open Source or commercial) in a production environment (server, network, storage, etc.).
- The successful passing of conformance tests from either a well-recognised conformance/interoperability testing organisation or from the conformance testing service offered by the eDelivery Core Service Platform.

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

In order to send a message, a sender needs to discover where the information about a receiver is stored. The SML (Service Metadata Locator) serves this purpose, and guides the sender towards this location, which is called SMP (Service Metadata Publisher). The SML is used to add/update/delete information about the participants' SMP location on a Domain Name System (DNS). The SML is centrally run by the eDelivery Core Service Platform.

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?

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 2017-2 eDelivery call.

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 4 entities from one or more Member State(s)." 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 e-SENS 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.

[2] Idem

[3] http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/csprd01/bdx-smp-v1.0-csprd01.html

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/x/cAqGAQ

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 don’t 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 self-assessment, 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.

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 and JMS plugin, also maintained by the CEF eDelivery team. Additionally, it is planned that Domibus will make available a file system plugin during the second half of 2017. 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/x/foGOAQ

13. Will the installation of AS2 Access Points 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 eDelivery Core service platform. More information on both tests can be found on CEF Digital website: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services