EUROPEAN COMMISSION

DIGIT | DG CNECT
Connecting Europe Facility

SML and SMP

Component Offering Description

CEF eDelivery Building Block

Version [1.10]

Status [Final]

Date: 26/09/2018

Document Approver(s):

Approver Name	Role
Adrien FERIAL	CEF eDelivery

Document Reviewers:

Reviewer Name	Role
Adrien FERIAL	CEF eDelivery Technical Office
Ioana DRAGUSANU	CEF eDelivery Technical Office
João RODRIGUES-FRADE	CEF eDelivery
Cosmin BACIU	CEF eDelivery Technical Office
Adam Yves	CEF eDelivery Technical Office

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.01	03/06/2016	Pedro TAVARES – CEF eDelivery Technical Office	Creation and preparation for external review
0.02	13/03/2017	Yves ADAM – CEF eDelivery Technical Office	Integrate changes after discussion with João RODRIGUES-FRADE and Adrien FERIAL
0.03	16/03/2018	PwC EU Services	Final draft updates
1.00	24/05/2018	Adrien FERIAL – CEF eDelivery Technical Office	Finalisation for publication
1.10	25/09/2018	Caroline AEBY	End of standby service

Table of Contents

Contents

APPROACH AND PURPOSE OF THE DOCUMENT

This document presents the Component Offering Description (COD) of the CEF eDelivery Service Metadata Locator (SML) and Service Metadata Publisher (SMP) components. Key content includes the description of CEF eDelivery messaging infrastructure and its dynamic discovery model, the functional and technical specifications of the SML and SMP components and their usage. This document provides guidelines to service providers, software providers and policy domain owners on how to implement the SMP and SML components in order to benefit from CEF eDelivery in their organisation ensuring the data exchange of electronic data and documents.

The following figure summarises the objectives, target audience and main outputs of this document.

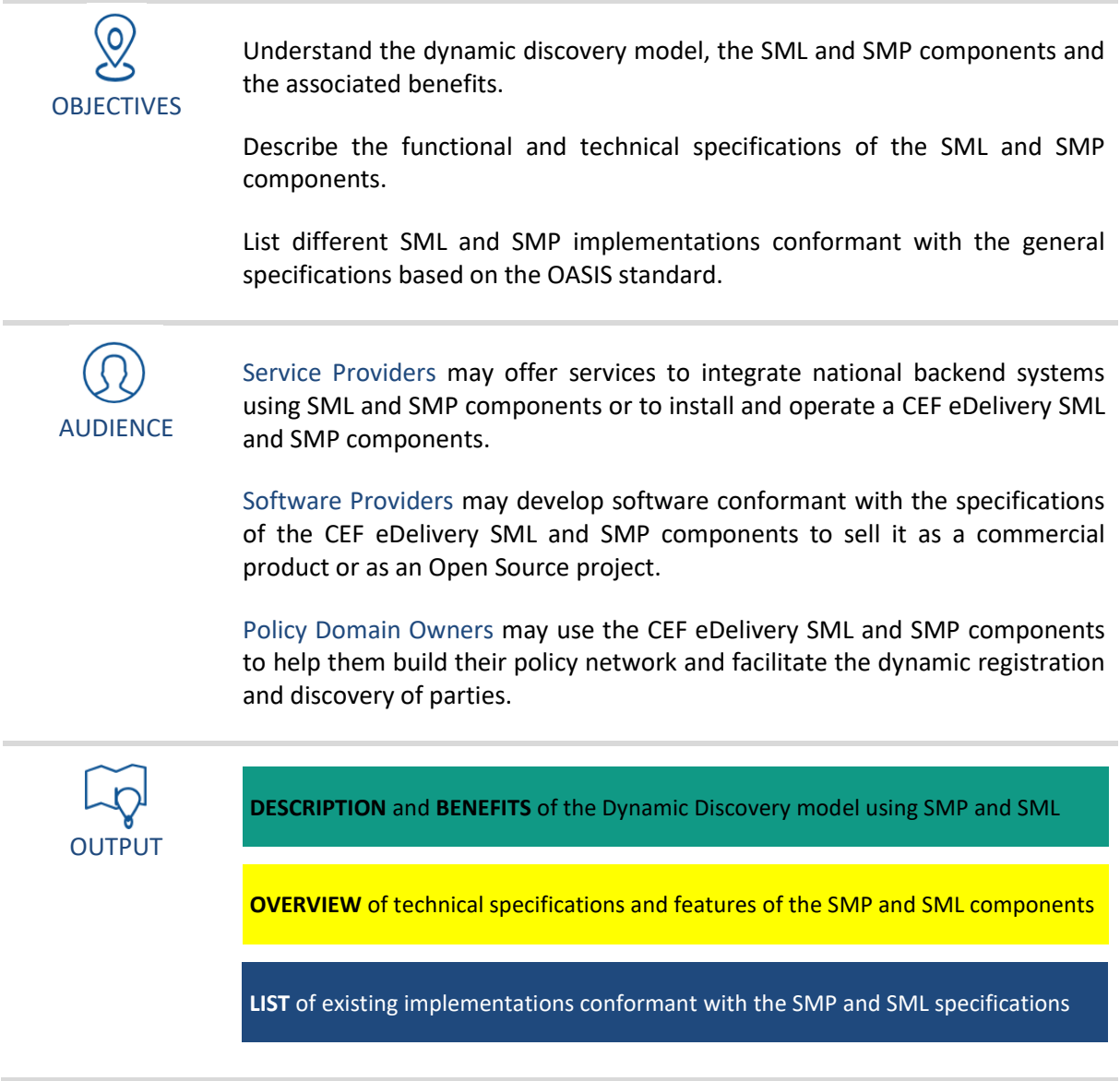

Figure 1: Summary of the objectives, audience and outputs of this document

The applicable terms and conditions of CEF eDelivery can be consulted in the Master Service Arrangement, available on the CEF Digital Single Web Portal [1].

GLOSSARY

The key terms used in this **document** are defined in the table below. The key acronyms used in the eDelivery Building Block are defined in the CEF Glossary [2] on the CEF Digital Single Web Portal:

Table 1. Key Terminology

Term	Description
Access Point (AP)	The Access Point (AP) of CEF eDelivery implements the AS4 message exchange protocol according to the CEF eDelivery AS4 profile [3]. This ensures standardised, interoperable, secure and reliable data exchange. For more information, please refer to the CEF Digital Portal [1].
AS4	The AS4 profile of CEF eDelivery is the AS4 Usage Profile/ implementation guidelines initially defined by e-SENS based on the AS4 specification of OASIS, itself a profile of OASIS ebXML Messaging Services Version 3.0, which in turn is based on various Web Services specifications of OASIS. The eDelivery AS4 profile is now maintained by CEF.
Backend system	In the context of CEF eDelivery, the Backend systems represent the IT systems used by the business and public administrations, which are exchanging data through CEF eDelivery. In that purpose, Backend systems are connected to CEF eDelivery Access Points via their default interfaces or through custom connector components.
Business Document Metadata Service Location (BDMSL)	The existing sample implementation of the SML software which implements the CEF eDelivery BDXL profile as well as the PEPPOL SML specification.
Capability Lookup	Capability Lookup is a technical service to accommodate a dynamic and flexible interoperability community. A capability lookup can provide metadata about the communication partner's interoperability capabilities on all levels defined in the European Interoperability Framework (Legal, Organizational, Process, Semantic and Technical interoperability levels). The metadata can be used to dynamically set interoperability parameters between the Sending and Receiving Parties.
CEF eDelivery	CEF eDelivery is a building block helping public administrations businesses and citizens to exchange electronic data and documents with each other in an interoperable, secure, reliable and trusted way.
Domain Name System (DNS)	The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
e-SENS	The electronic Simple European Networked Services (e-SENS) was a large-scale pilot project (ended in 2017) with the aim of consolidating, improving, and extending technical solutions based around common building blocks, in order to foster digital interactions among public administrations across the EU.
ISO/IEC 6523	Information technology – Structure for the identification of organisations and organisation parts. International standard for defining the structure for uniquely identifying organisations and its containing parts.
ISO 9735	International standard for electronic data interchange for administrations, commerce and transport.
ISO 20022	International standard for electronic data interchange between financial institutions.
ISO/IEC 27001	International standard for information security management systems.

Policy domain	Policy domains are typically linked to the Directorate-Generals of the European Commission, e.g. DG Justice and DG SANTE that are the business owners of domains such as the eJustice domain and eHealth domain respectively. Policy domains use CEF eDelivery to create a secure messaging infrastructure for the exchange of data and documents.
Public Administration	According to eIDAS regulation a Public Administration means a state, a regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.
Service Metadata	Information necessary for invoking a service using CEF eDelivery components. It is a combination of information on the end entity recipient (such as its identifier, certificate, supported business documents and processes in which it accepts those documents) and its associated endpoints (such as the transport protocol and its address).
Service Metadata Publisher (SMP)	Service Metadata Publisher (SMP) is a component of CEF eDelivery that is responsible for Capability Lookup: once the Access Point of the Sending Party discovered the address of the Receiving Party's SMP (Service Metadata Publisher), it is able to retrieve the required information to interoperate with the Receiving Party (i.e. metadata). SMP are registers of the message exchange capabilities and location of parties (i.e. metadata). SMP's are usually used in a distributed way.
Service Metadata Locator (SML)	Service Metadata Locator (SML) is a component of CEF eDelivery that is responsible for Dynamic Service Location: in order to send a message, the Access Point of a Sending Party needs to discover where the information about a Receiving Party is stored. The Service Metadata Locator (SML) serves this purpose, and guides the Access Point of the Sending Party towards this location, which is called the Service Metadata Publisher (SMP). In other words, the SML is used to retrieve/add/update/delete information about the Receiving parties and SMPs location on a Domain Name System (DNS). The SML is a centralised component.

REFERENCES

[1] "CEF Digital," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+services.

[2] "CEF Glossary," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Glossary.

[3] "Access Point Software," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software.

[4] "CEF eDelivery SMP specifications," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+specifications.

[5] "CEF eDelivery SML specifications," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+specifications.

[6] "CEF conformance testing service," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing.

[7] "Service Metadata Publishing (SMP) Version 1.0," [Online]. Available: http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.pdf.

[8] "OASIS ebCore Party Id Type Technical - Specification Version 1.0," [Online]. Available: http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/PartyIdType-1.0.pdf.

[9] "eDelivery ebCore Party ID profile," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+ebCore+Party+ID.

[10] "Business Document Metadata Service Location Version 1.0," [Online]. Available: http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.pdf.

[11] "Access Point specifications," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications.

[12] "SMP software," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP.

[13] "eefacta Server," [Online]. Available: http://www.unimaze.com/solutions/enterprise-solutions/eefacta-server.

[14] "phoss SMP - a PEPPOL and OASIS BDXR SMP Server, CEF eDelivery compliant," [Online]. Available: https://github.com/phax/peppol-smp-server.

[15] "SML software," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML.

[16] “Getting started with the Dynamic Discovery Client for SMP,” [Online]. Available: https://ec.europa.eu/cefdigital/code/projects/EDELIVERY/repos/dynamic-discovery-client/browse.

1. INTRODUCTION

This document introduces the dynamic discovery for the CEF eDelivery messaging infrastructure and describes the CEF eDelivery components used to facilitate such process.

1.1. What is CEF eDelivery?

The CEF eDelivery building block of the Connecting Europe Facility (CEF) enables businesses and public administrations to exchange electronic data and documents in digital format in an interoperable, secure, reliable and trusted way.

The CEF eDelivery is a messaging infrastructure working as a collection of distributed nodes conformant to the same technical rules capable of **interacting with each other**. The CEF eDelivery prescribes technical specifications that can be used in any Policy Domain of the EU (e.g. Justice, Procurement, Consumer Protection, etc.) while enabling a **secure, reliable and trusted exchange** of documents and data (structured, non-structured and/or binary) both cross-border and cross-sector.

The CEF eDelivery building block uses the decentralised four-corner model messaging topology, allowing direct communication between different parties without the need to set up bilateral channels. The parties use their own Backend systems to connect to the CEF eDelivery Access Points for the message exchange, as illustrated in the figure below. The Access Points are interoperable and implement the same message exchange protocol following the same implementation guidelines.

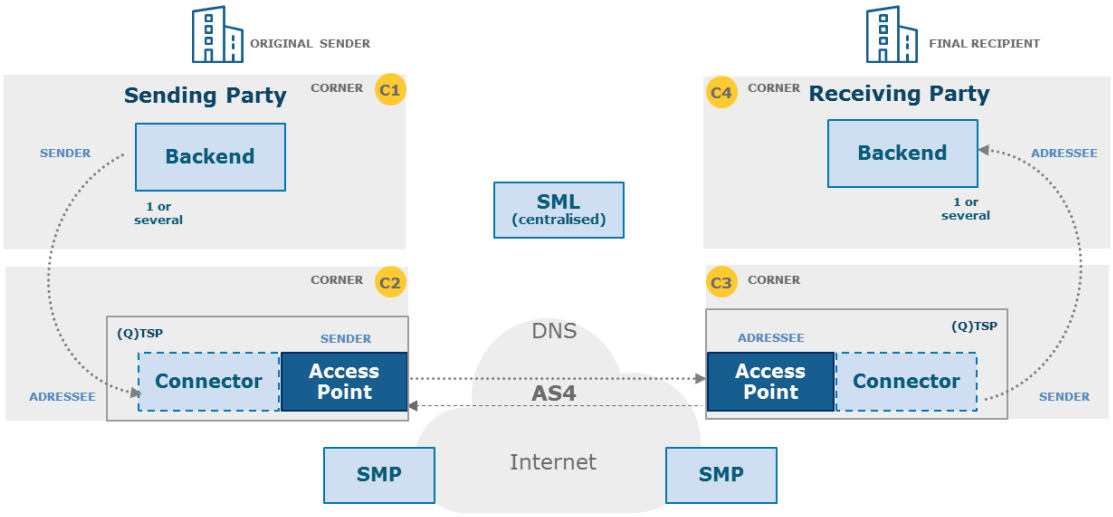

Figure 2 – CEF eDelivery four-corner model

Additional CEF eDelivery descriptions, technical specifications, software and services are available in the CEF Digital Portal [1].

1.2. What is Dynamic Discovery?

To send messages using the CEF eDelivery messaging infrastructure, the access point of the sending party needs to obtain the communication information of the receiving party, e.g. lookup address and the communication capabilities. Such information can be obtained via a **Static** or a **Dynamic** discovery process.

The **static** discovery process uses a static list of the receiving parties stored on the sending access point and their configuration which is programmatically selected and added to the message. **Dynamic** discovery allows the sending access point to query an external service storing up-to-date information about every receiving party in the network. The dynamic discovery in CEF eDelivery is implemented with three components, namely the Service Metadata Publisher (SMP), the Service Metadata Locator (SML) and the DNS.

This document discusses **Dynamic discovery** and associated CEF eDelivery components.

2. STATIC VERSUS DYNAMIC DISCOVERY MODELS

The **static model** requires sending Access Points (APs) [3] to have the information on the receiving parties statically available, including the lookup address and the communication capabilities. Hence, in the static model the AP stores a list with static information related to all the other APs (e.g. IP addresses). To send a message, the sending AP looks at this static list of IP addresses locating the AP of the receiving party (usually configured in the PMode). In contrast, in the **dynamic model** the sending AP obtains this information dynamically from a dedicated provider storing the up-to-date version. The table below summarises the major differences between the two models.

Table 2. Dynamic vs. Static discovery models

	Static model	Dynamic model
Pro's	Low lookup overhead	Extra automation, scalable and flexible
Con's	Low flexibility for reference changes	Extra lookup overhead

Table 3 below provides policy domain owners with a short guideline and criteria to select the best option. If two factors or more are in favour of Dynamic Discovery, this option should be considered as the most appropriate one.

Table 3. Choosing dynamic or static discovery

Factor	Static model	Dynamic model

Network Scale	*Best suited for small networks*. Static discovery requires few efforts to setup. Static configuration is applicable if the number of interoperating parties is limited (limited network scale).	*Best suited for medium to large scale networks.* As the number of interoperating parties grows, the configuration maintenance efforts grow quadratically. If the network is large or mid-sized, investments on more complex dynamic discovery solution provides a quick return on investment.
Network Topology	*Best suited for hierarchical or star topologies.* In a hierarchical or star topology implying 1-to-N communications, only the centralised component needs to be aware of satellite ones. In such circumstances, static discovery is easy to maintain while dynamic discovery brings limited added value (at least to value to small or mid-size networks).	*Best suited for meshed network.* In meshed network implying M-to-N communications, each node potentially needs to be aware of other's communication capabilities. Configuration of such type of topology increases exponentially with the number of interoperating parties. Dynamic – i.e. automatic – configuration is consequently an asset in meshed networks.
Network Stability	*Best suited for stable networks.* If the network is (almost) never changing, static configuration will be stable i.e. safe and with no recurrent costs.	*Best suited for evolving networks.* If the network's participants and participants' capabilities are changing frequently, dynamic discovery will avoid extensive human interventions proportionally avoiding costs and risks of errors.
Business continuity needs	*Best suited for networks accepting temporary downtime.* Since static configuration requires human intervention, it may imply human errors and downtime because of configuration delays (sometimes days or weeks when administration issues arise).	*Best suited for sensitive networks.* Dynamic discovery does not require human intervention and therefore provides secure instant distributed configuration.
Admin model	*Best suited for centralised administration model.* Maintaining the configuration manually is easier in a central location, therefore static configuration is more suitable for systems that are maintained in a central system administration service.	*Best suited for distributed administration model.* Distributed administration implies distribution and synchronisation of information (metadata) which is better implemented with Dynamic discovery.

3. CEF eDELIVERY IN DETAILS

The CEF eDelivery building block uses the decentralised four-corner model messaging topology, allowing direct communication between participants without the need to set up bilateral channels, as depicted in Figure 3. In this topology, the message exchange is done between the sending party and the receiving party via Access Points (APs).

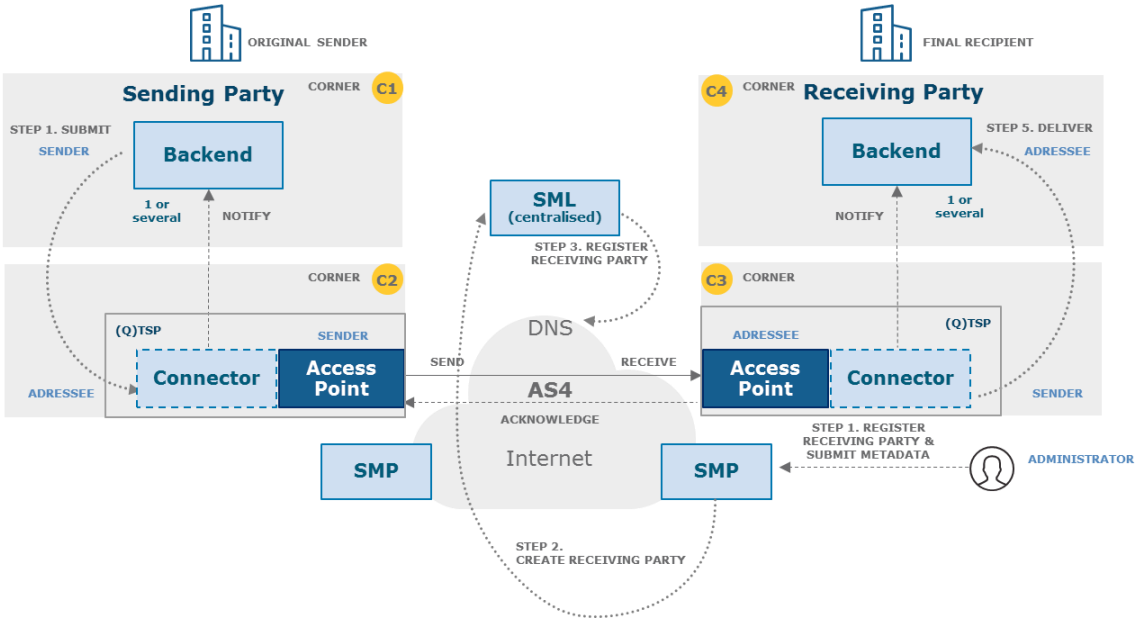

Figure 3 – CEF eDelivery four-corner model

In order to ensure and establish the communication between Access Points, the sending Access Point requires the service metadata information of the receiving party. The Sending Access Points retrieve the service metadata information either via a static list or via a dynamic discovery mechanism.

The Service Metadata Provider (SMP) [4] and the Service Metadata Locator (SML) [5] components enable the process of dynamic discovery of service metadata information. In opposition to the static process based on static lists, the dynamic discovery process provides:

- **Automation** of the discovery process increasing the efficiency of the configuration;
- Increased **flexibility** for communicating with different receiving parties operating different business processes;
- Improved **scalability** through the smooth addition, removal and update of parties.

This document outlines the functional and technical specifications of the SMP and SML components in the four-corner model using dynamic discovery, including some implementation examples. Since SMP and SML enable the dynamic discovery model, this document will only elaborate on the dynamic discovery process and not the static discovery process. Additional information about the CEF eDelivery components is available at the CEF Digital Portal [1].

The table below summarises the main actors involved in the CEF eDelivery messaging exchange.

Table 4. Actors in the CEF eDelivery messaging infrastructure

Actor	Description
Backend system	Backend systems represent the IT systems used by the business and public administrations, which are the origin of the documents and data to be exchanged through eDelivery.
Sending Party and Receiving Party	Represent both the businesses and public administrations operating the Backend systems which use and connect to CEF eDelivery Access Points.
Sending Access Point and Receiving Access Point	The sending Access Point (AP) is connected to the backend of the sending party. The sending Access Points converts the business message to the eDelivery AS4 profile format and sends it to the receiving Access Point. The receiving party uses a receiving Access Point to receive the AS4 message which delivers it to the backend system of the receiving party.
Connector	The connector component of eDelivery is an optional component used to facilitate the integration between the backend systems and Access Points.

4. DYNAMIC DISCOVERY IN DETAILS

This section describes the **Service Metadata Publisher (SMP)**, **Service Metadata Locator (SML)** and **DNS Server** components that facilitate and support the dynamic discovery process as follows:

The dynamic discovery involves three types of component actors:

- **Service Metadata Publisher (SMP):** The SMP provides the service location and capabilities of receiving parties, by storing, exchanging and performing capability lookups for other APs. The SMPs operate in a distributed manner in a CEF eDelivery network. The SMP stores the updated information of every receiving party of the network, each of them having its capabilities published in one and only one SMP. Hence, for the message exchange, the sending AP discovers the address of the SMP associated to the receiving AP in order to retrieve the required information (i.e. metadata) on the receiving AP and on the receiving party. This information is necessary for the receiving APs to send messages.

- **Service Metadata Locator (SML):** The SML is a centralised component that stores the locations of every SMP in the network and manages the resource records of the participants and SMPs in the DNS (Domain Name System) Server. The SML stores the unique identifier of all receiving parties and SMPs on the network in the DNS Server.

- **Domain Name System (DNS) Server:** The DNS Server stores DNS records identified by the unique identifier of each receiving party in the network. Each of these DNS records refers to the lookup information of the corresponding party's SMP. This service enables the sending AP to dynamically locate the SMP holding the service metadata of the receiving party.

The **SMP** provides the sending AP with the **Service Metadata** or **Service Capabilities** of the receiving party which includes the followings:

- The receiving Access Point lookup information (e.g. IP address, URL, transport protocol).
- The communication protocol (AS4);
- The available and possible business processes;
- The message types supported and required;
- The security setup (e.g. public key used for the encryption of the message);
- Any information relevant for the message exchange (customisable through extension anchors);

The dynamic discovery process is composed of the two following **phases**:

Registration: The registration phase consists of registering metadata of receiving parties in a CEF eDelivery network: the administrator registers the metadata in the SMP and entries referring to them in the standard internet DNS via the SML. The registration allows the sending Access Point to contact the SMP which serves the receiving party's capabilities that are necessary to communicate with it.

Operation: After the registration is completed, a sending Access Point can find the location of the SMP that serves a given receiving party from its unique identifier and collect the necessary information to interoperate with the Access Point of the receiving party.

4.1. Registration phase

The registration phase requires that each receiving party and the associated SMPs register their lookup information in the SML. The lookup information allows sending APs to locate the SMP of the receiving party and extract the service metadata required for the message exchange. This enables the sending AP to understand the communication capabilities and requirements of the receiving party and Access Point.

Registration of an SMP

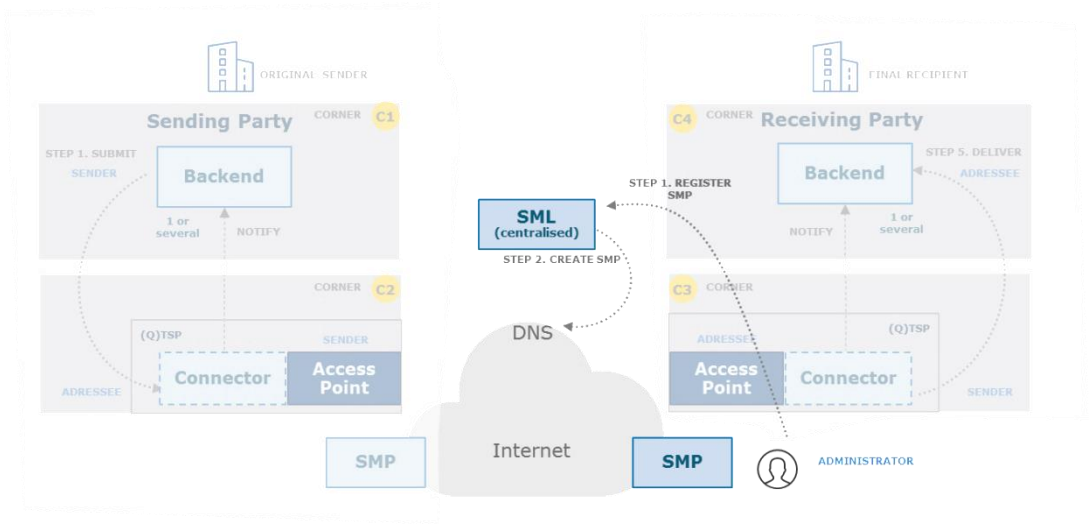

Figure 4 - Registration phase: registration of a SMP

STEP 1. **REGISTER SMP**: This represents a required action from the **administrator**, which from a technical perspective consists in calling a web service exposed by the SML with the appropriate metadata and credentials.

STEP 2. **CREATE SMP**: After the administrator registered the SMP with the SML, the SML automatically creates a new record in the DNS for this SMP. The record links the SMP's unique identifier to its location on the internet, making it accessible and discoverable by others.

Registration of a party

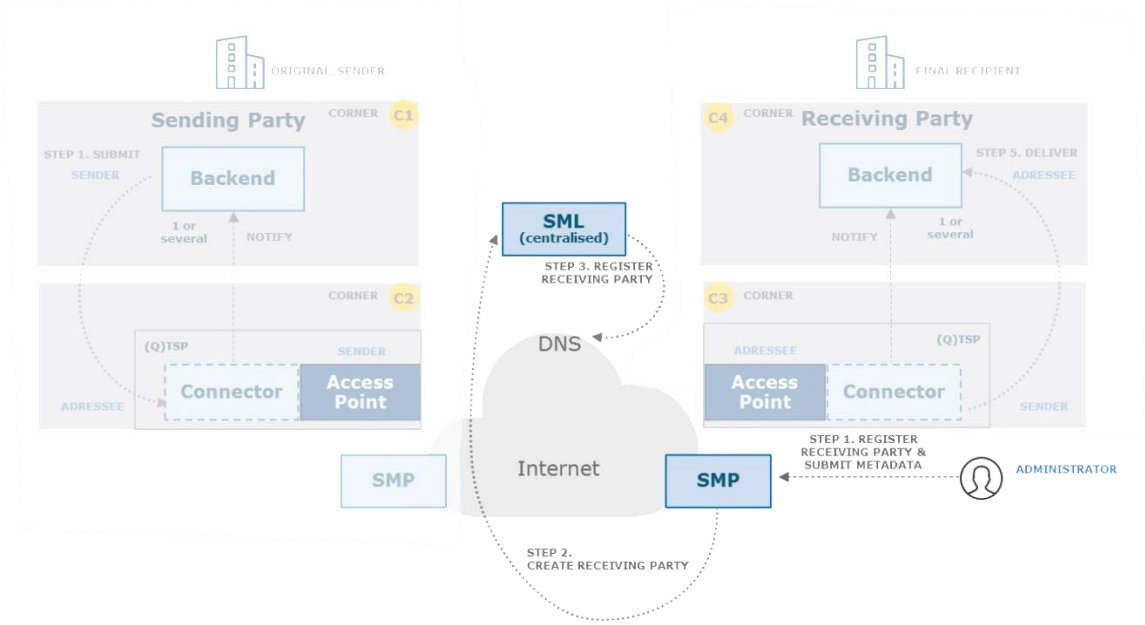

Figure 5 - Registration phase: Registration of a party

STEP 1. **REGISTER RECEIVING PARTY & SUBMIT METADATA**: This action assumes that the associated SMP is already registered with the SML (previous action). An SMP can serve metadata for multiple receiving parties, but each receiving party may be registered in one and only one SMP. During this action, the **administrator** registers the party and submits the associated service metadata to the SMP, through the call to a REST service as specified in the SMP specification [4].

STEP 2. **CREATE RECEIVING PARTY:** The registration of the receiving party and its metadata in step 1 automatically triggers a call from the SMP to the SML to create the new receiving party in the SML. This metadata will be later used during the operation phase.

STEP 3. **REGISTER RECEIVING PARTY**: The creation of the new party in the SML in step 2 automatically triggers the registration of the new receiving party in the local database of the SML. The SML also creates a specific record in the DNS server for that receiving party, making the receiving party discoverable by sending parties. As from there, the operation phase can be executed.

Note: The APs are not involved in the registration phase.

4.2. Operation phase

The operation phase enables parties to exchange messages using APs supported by the SMP and SML components. The figure below illustrates the operation phase process.

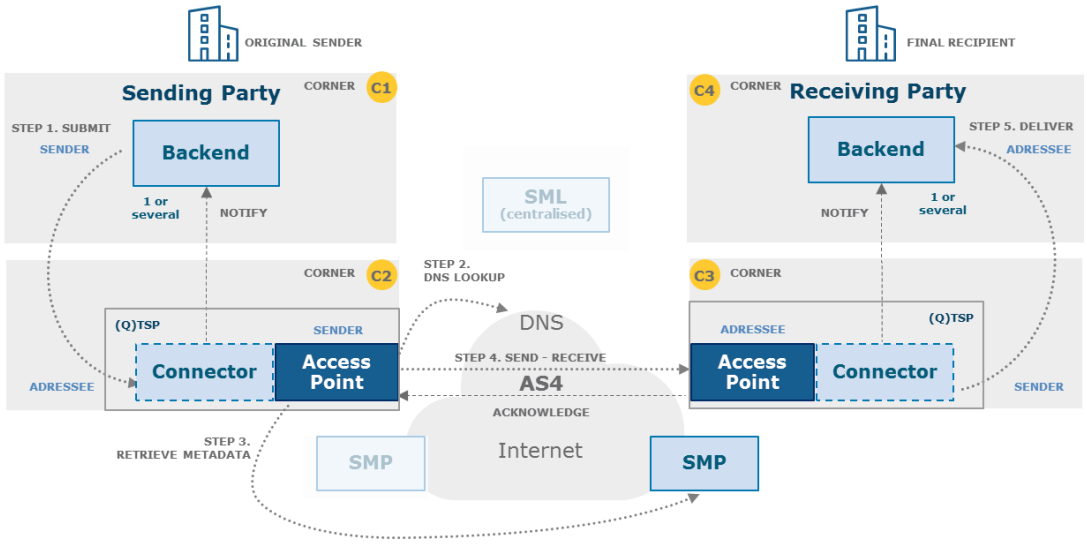

Figure 6 – Operation phase

The operation phase follows the five steps illustrated in the figure and described below:

STEP 1. **SUBMIT**: The sending party uses the backend system to create a message to be sent to a receiving party. At this stage, the sending party knows the unique identifier of the receiving party (e.g. a company VAT number) and the content of the data or document that he intends to send to the receiving party. After the message (in 'business' format) is created, the **backend system** submits it to its sending AP.

STEP 2. **DNS LOOKUP:** Upon submission of a message from the backend system, the sending AP converts the message to the AS4 format. In order to correctly create the AS4 message and route it to the receiving AP, the sending AP builds a canonical representation of the receiving party identifier by hashing it. The sending AP uses this canonical representation to perform a **DNS lookup**. As a result, the sending AP obtains the URL of the SMP publishing the metadata of the receiving party.

Step-by-step DNS lookup for Dynamic Discovery:

- Given the sample receiving party identifier: ***sample-party-id***,

  the sending AP calculates the hash of the party identifier as specified in the eDelivery SMP profile:

  hash(`sample-party-id`) =

  `JUQ5VICUBJQBZODMXVTEXA76NYU7KEEMASPUIJICR56O5OJ7HYAQ`

- The sending AP uses this hash to query the corresponding NAPTR record in DNS:

  `JUQ5VICUBJQBZODMXVTEXA76NYU7KEEMASPUIJICR56O5OJ7HYAQ``.sample-scheme-identifier.european-documents-exchange-system.eu. 60 IN` **`NAPTR`** `00 10 "U" "Meta:SMP" "!^.*$!https://`**`smp.company.com`**`!" ..`

  … referring to the logical address of the SMP: "***smp.company.com***"

STEP 3. **RETRIEVE METADATA:** The sending AP then queries the resolved SMP to **retrieve the metadata** of the receiving party. The metadata includes all the necessary information for the sending AP to send messages to the receiving AP, including IP location, communication capabilities and business characteristics;

STEP 4. **SEND:** The sending AP then builds and **sends** the AS4 message to the receiving party via the receiving AP according to the collected metadata.

STEP 5. **DELIVER:** The message from the sending AP is translated and delivered by the receiving AP to the receiving party.

Note: The SML is not involved during the whole operation phase. This means that even if the SML is down, operations will continue working as the lookup relies on the DNS which is highly replicated on the internet, preventing the 'single point of failure' problem, i.e. the risk of blocking operations when one single component is not available in the messaging infrastructure.

5. TECHNICAL SPECIFICATIONS

This section describes the technical specifications of the SMP and SML components by listing their key features and conformance tests. CEF eDelivery offers a conformance testing service of the CEF eDelivery SMP profile based on the OASIS standard, available via the CEF eDelivery Conformance testing service [6].

5.1. Specifications

The tables presented below show the evolution of the SMP and SML technical specifications. The specifications of the SMP and SML components have been built over time based on the original specifications developed by PEPPOL which have been standardised by OASIS. The CEF eDelivery profiles, transferred to CEF from e-SENS, are based on the OASIS standard and refine the specifications that are applicable to CEF eDelivery's SMP and SML components.

Table 5 - SMP Specifications

SMP	Description
OASIS SMP Specification [7]	Description of the protocol and its binding to a REST interface that Service Metadata Publishers ("SMP") and clients must support. Decisions regarding physical data format and management interfaces are left to implementers of the SMP and client applications.
eDelivery SMP profile [4]	The eDelivery SMP profile describes the request/response exchanges between a Service Metadata Publisher and a client wishing to discover AP metadata. The profile is based on the OASIS Service Metadata Publishing (SMP) Version 1.0 standard.

Table 6 - SML Specifications

SML	Description
eDelivery BDXL profile [5]	The eDelivery BDXL profile is an open specification for locating APs within a network. It offers a dynamic system to discover the URLs of other APs and their corresponding metadata.
OASIS ebCore Party ID Specification [8]	This specification specifies a formal mechanism for referencing party type identification schemes using a formal URN notation that leverages the three identification scheme catalogues: ISO 6523, ISO 9735 and ISO 20022.
eDelivery ebCore Party ID profile [9]	The eDelivery ebCore Party ID profile is based on the OASIS ebCore Party Id Type Technical specification. It provides a standard URN-based syntax for party identifiers and identifier types. A variety of naming identifier schemes are in existence and used internationally, such as GS1 Global Location Numbers (GLN), Dun & Bradstreet DUNS numbers, and various national business registry numbers. ISO is a global registration authority for such schemes and maintains the ISO 6523 catalogue. This CEF eDelivery specification provides additional implementation guidelines for the OASIS ebCore Party Id Type specification.
OASIS Business Document Metadata Service Location [10]	Definition of service discovery methods for use in DNS Resource Record service fields.

Table 7 - AP specifications

AP	Description
Profile enhancement Dynamic receiver and Dynamic sender of the **eDelivery AS4 profile [11]**	As from version 1.13 of the eDelivery AS4 profile, the optional profile enhancements Dynamic receiver and Dynamic sender specify how the dynamic discovery is profiled in eDelivery.

5.2. Features

The tables below show the features and specifications related to the SMP and SML. Table 7 below summarises the features and associated specifications of the SMP as defined by the CEF eDelivery SMP profile.

Table 7 – CEF eDelivery SMP profile key features

Feature	Specifications
Technical specification	OASIS BDX SMP
Core messaging	XML-based REST services
Encoding	UTF-8
Internet transport	HTTP 1.1
Transport Layer Integrity	Transport Layer (SSL/TLS) Security
Party scheme	eDelivery ebCore Party ID profile
Verification of integrity	XML-Signature [XML-DSIG1]
Authentication of origin	XML-Signature [XML-DSIG1]
Non-Repudiation of origin	XML-Signature [XML-DSIG1]

Table 8 below lists the features and specifications of the SML as defined by the CEF eDelivery BDXL profile.

Table 8 – CEF eDelivery BDXL profile key features

Feature	Specifications
Technical specification	OASIS BDX Location
Metadata service discovery mechanism	Dynamic Delegation Discovery System
Core messaging	DNS lookup, SOAP services
DNS Record type	U-NAPTR
Hashing algorithm	SHA256
Digest encoding	Base32
Party scheme	eDelivery ebCore Party ID profile
Transport Protocol defined in the DNS records	HTTP(S)
Transport Layer Integrity defined in the DNS records	Transport Layer (SSL/TLS) Security
Verification of integrity	DNSSEC
Authentication of origin	DNSSEC
Non-Repudiation of origin	DNSSEC

6. CONFORMANT IMPLEMENTATIONS

A growing number of software vendors and service providers already support the PEPPOL, OASIS and CEF eDelivery SMP profiles and the OASIS and CEF eDelivery BDXL Profiles (cf. §5.1). Some of them provide added-value services from integration to support of day-to-day operations, in addition to the SMP or SML software or service. The CEF eDelivery team maintains a list of vendors that have passed the conformance tests and a list of service providers with conformant implementations in its resources hub. Alternatively, organisations may decide to build their own SML and/or SMP component according to the one of these Profiles. It is therefore important to carefully consider the different options before deployment.

It is important to note that the OASIS and PEPPOL profiles are not compatible as they have different specifications and features. However, the component implementations may offer support for both specifications.

The European Commission maintains open source sample implementations of the SMP and SML solutions using profiles adhering to the aforementioned features and specifications. The end of this section lists the different CEF eDelivery SMP and SML implementations.

Table 9. Conformant Implementations

Component	Implementation	Description
SMP	**Sample CEF eDelivery SMP** [12]	The open source sample implementation of the Service Metadata Publisher (SMP) maintained by CEF.
	eefacta Server [13]	A customizable on-site business messaging server serving as a front end to the enterprise back end systems integrating a serviced or on-site OpenPEPPOL Service Metadata Publisher (SMP).
	phoss SMP [14]	A complete PEPPOL and OASIS SMP server with a management GUI and optionally an XML backend for simplified operations. It also supports the OASIS BDXR specification. It was the first SMP to be CEF eDelivery conformant.
SML	**CEF eDelivery BDMSL** [15]	The open source sample implementation supporting the CEF eDelivery SML specification provides support for the CEF eDelivery BDXL profile following the OASIS BDX-Location standard, as well as the PEPPOL SML specification. The PEPPOL SML specification continues to be supported to avoid disruption of the service to current legacy users of this service. The SML managed service offered by DIGIT uses this sample implementation and therefore benefits from its features. This version of the SML sample implementation is known as Business Document Metadata Service Location application (BDMSL).
Dynamic Discovery client	**CEF eDelivery Dynamic Discovery client** [16]	The CEF eDelivery **dynamic discovery client** is an open source Java library that handles all interactions with SMP and DNS on the retrieval and the usage of metadata about receiving party. It can be integrated with any Java-based AP. Major functionalities provided through this Java API are: • Locating the SMP of a given receiving party; • Querying the SMP;

Component	Implementation	Description
		• Signature Verifying of SMP signed responses; • Retrieving receiving party's supported documents and related ls.

7. CONTACT INFORMATION

CEF Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

Support Service: 8am to 6pm (Normal EC working Days)