Introduction to the Connecting Europe Facility
eDelivery building block

DIGIT
Directorate-General for Informatics
DG CONNECT
Directorate-General for Communications
Networks, Content and Technology

October 2015

eDELIVERY
connecting europe

DISCLAIMER

This document is for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein. References to legal acts or documentation of the European Union (EU) cannot be perceived as amending legislation in force or other EU documentation.

The document contains a brief overview of technical nature and is not supplementing or amending terms and conditions of any procurement procedure; therefore, no compensation claim can be based on the contents of the present document.

Introduction to the Connecting Europe Facility eDelivery building block

Created by: CEF eDelivery

DOCUMENT HISTORY

Version	Date	Modified by	Short Description of Changes
1.00	29/10/2015	CEF eDelivery	Final

Table of contents

Audience

This document describes the Electronic Delivery (eDelivery) building block which is one of the Connecting Europe Facility (CEF) Digital programme's essential digital services. These essential digital services, called building block Digital Service Infrastructures (DSIs) will play a vital role in the flow of data across borders and sectors.
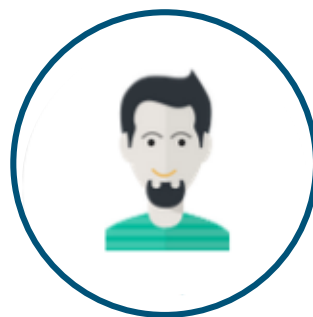
This document is intended for the following audiences:

POLICY OFFICERS

involved in the roll out of EU or national policies that require the secure exchange of documents and data

IT ARCHITECTS

involved in the design and operation of document and data exchange systems such as eDelivery

SERVICE PROVIDERS

involved in the implementation and roll-out of eDelivery

Whilst every effort has been made to ensure that the information contained in the document is correct, any comments on it should be submitted to the European Commission:
CEF-BUILDING-BLOCKS@ec.europa.eu

Audience

Even though this document should be considered and read in its entirety, some chapters are more relevant for readers wanting to understand the business reasons behind eDelivery while some others are more interesting for readers with a technical background.

CHAPTER

	Chapter	Business	Manager	Technical
1	Introduction	Main	Secondary	Secondary
2	Context	Main	Secondary	Secondary
3	Motivation	Main	Secondary	Secondary
4	Use cases	Main	Main	Secondary
5	Technical specification	Secondary	Main	Main
6	Implementations	Secondary	Main	Main
7	Governance	Secondary	Main	Main
8	CEF services to service providers	Secondary	Main	Main
9	Success stories	Secondary	Main	Main
10	Definitions	Secondary	Main	Main
11	Annex	Secondary	Secondary	Main

■ Main addressees   ▨ Secondary addressees

1 Introduction
What is CEF eDelivery?

Introduction to eDelivery

The **eDelivery** building block helps public administrations to **exchange electronic data and documents** with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way.

Through the use of this building block, **every participant becomes a node in the network** using standard transport protocols and security policies. eDelivery is based on a distributed model, allowing **direct communication between participants without the need to set up bilateral channels.**

The purpose of this document is to provide a general introduction to the eDelivery Digital Service Infrastructure (DSI), part of the Telecom Programme of the Connecting Europe Facility (CEF Telecom).

eDelivery is a building block of CEF. These building blocks are reusable specifications, software and services that will form part of a wide variety of IT systems in different policy domains of the EU.

The promotion of common building blocks is a way to lower barriers for technical integration and provide tried and tested solutions that will speed up the delivery of Digital Public Services, that work across borders, in a cost efficient manner.

More information about the CEF Telecom policy background, its Work Programmes and related information is available on the Digital Agenda website.

More information about eDelivery is available on the Joinup website.

The technical management of the eDelivery DSI is done by the Directorate-General for Informatics (DIGIT 🔗) of the European Commission.

Implementation of the EU policy directly related to eDelivery is the responsibility of the Directorate-General for Communications Networks, Content and Technology (DG CNECT 🔗) of the European Commission.

The Innovation and Networks Executive Agency (INEA 🔗) is responsible for the implementation of the CEF Telecom programme grants in cooperation with the Commission.

Introduction to eDelivery

eDelivery's main goal is to ensure that Public Administrations can exchange any type of data and documents across borders. This means enabling Administration to Administration communication (A2A) contributing to the creation of a EU single market which is fit for the digital age.

By connecting Public Authorities across Europe and bringing down digital barriers, eDelivery will support the 'European free flow of data initiative' part of the <u>Digital Single Strategy initiative</u> 🔗 a priority of the European Commission.

eDelivery can also be used in Administration to Business (A2B) and Business to Administration (B2A) scenarios as proven by the PEPPOL implementation of eDelivery in the eProcurement domain.

When behind a web-portal, eDelivery can also enable the interconnection of Public Administrations with Citizens (A2C and C2A). For example, eDelivery enables the eJustice portal to talk with other information systems.

The latter shows that the communication between Citizens (C2C) is out of scope of eDelivery.

The diagram on this page clarifies the positioning and scope of eDelivery.

- ● Primary Scope
- ◌ Secondary Scope
- ○ Out of Scope

* Through web-portals
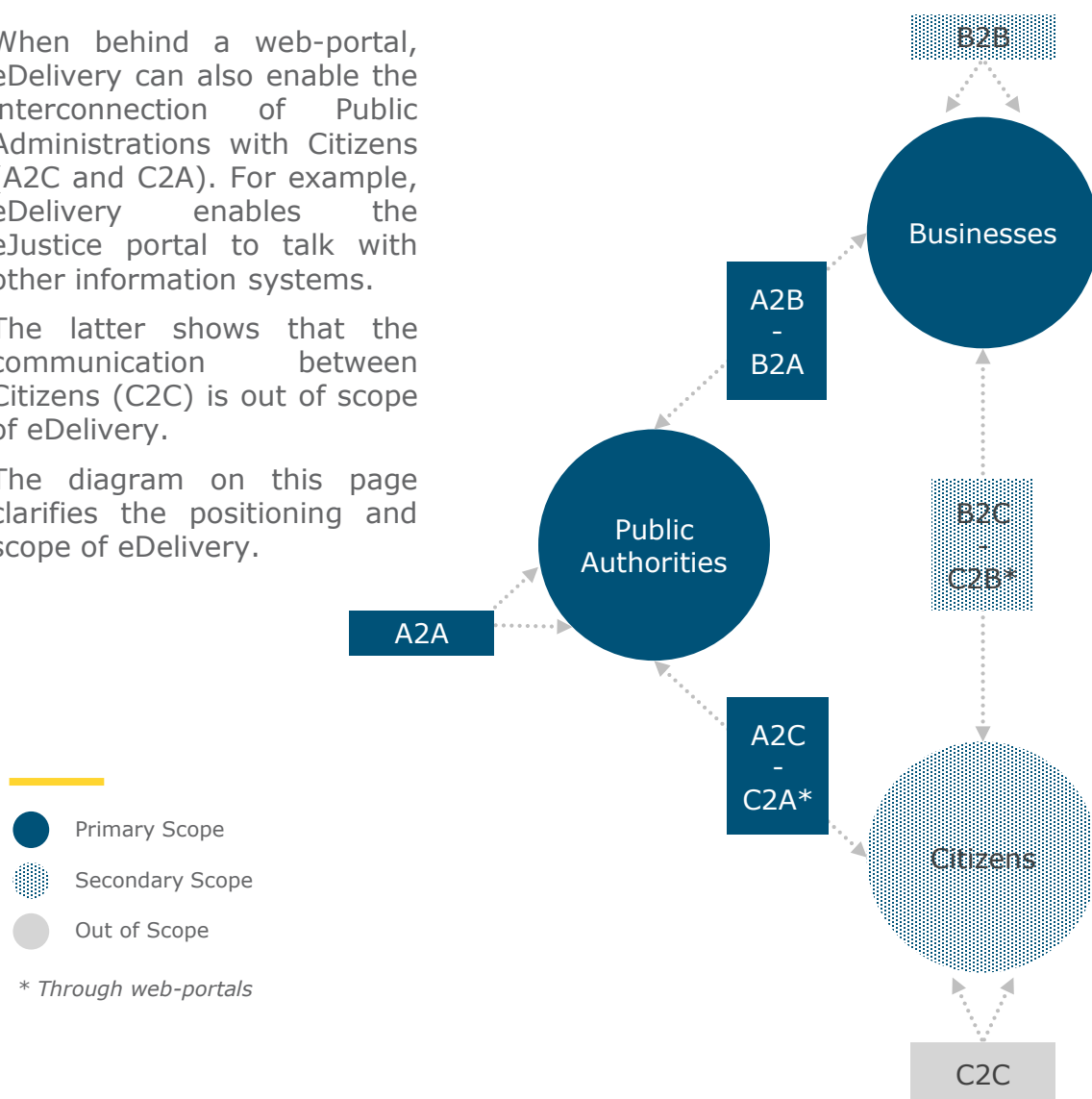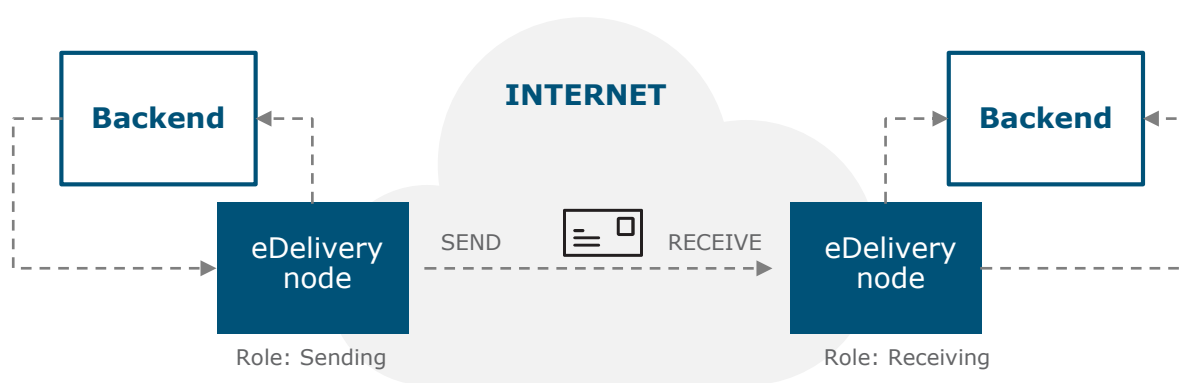
Introduction to eDelivery

eDelivery prescribes technical specifications that can be used in any Policy Domain of the EU (Justice, Procurement, Consumer Protection, etc.) to enable **secure and reliable exchange of documents and data** (structured, non-structured and/or binary), both across borders and sectors.

Once implemented, eDelivery works as a **collection of distributed *nodes* that are conformant to the same technical rules and therefore capable of interacting with each other**.

As a result of this, **organisations** that have developed their IT systems independently from each other **can start to securely communicate with one another once they have connected to a eDelivery node.**

It is important to note that there is **no single eDelivery node per Member State** but several ones. Each one of these nodes is deployed for a specific Pan-European Project within a given policy domain: eJustice, eProcurement, etc. Typically, the nodes of eDelivery are uni-domain and uni-project.

The eDelivery nodes can be implemented at any administrative level: national, regional, local or by single organisations. The deployment model must be defined upfront by the Pan-European project.

eDelivery: a high-level illustration

Introduction to eDelivery

eDelivery has strong links to Regulation [(EU) 910/2014](#) 🔗 on Electronic identification and trust services, commonly known as '**eIDAS**'.

In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and **electronic delivery services**, and for interoperable e-government services across the European Union.

The resulting leading-edge regulation, which most articles shall apply from 1 July 2016, establishes the principle that *an electronic document should not be denied legal effect on the grounds that it is in an electronic form.*

eDelivery supports this fundamental principle of the Digital age by promoting the **alignment between its technical specifications and the eIDAS regulatory framework.**

Some key concepts set forth by eIDAS, directly related to eDelivery, are shown below:

eIDAS Regulation

Article 3 - Definitions

(36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations

Article 46 - Legal effects of electronic documents

(1.) "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form."

Article 43 - Legal effect of an electronic registered delivery service

(1.) Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

(2) "Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service."

Introduction to eDelivery

As a result, to increase **interoperability in Europe**, the eDelivery DSI promotes technical specifications which are aligned with the legal and organisational principles of eIDAS.

Apart from evidences and the headers related to data exchange, data representation and meaning is not part of eDelivery's scope.

Individual Projects, and entire Policy Domains, are encouraged to deploy eDelivery within its specific legal context, in combination with their semantic and organisational models.

INTEROPERABILITY LEVELS	eDelivery DSI	Policy Domain	Project
Legal	eIDAS Regulation	Legislation	Legislation
Organisational		Organisational Models	Organisational Models
Semantic		Semantic Models	Semantic Models
Technical	CEF eDelivery Technical Specifications		

The scope of CEF's eDelivery DSI

More information about the European Interoperability Framework (EIF) can be found on the *ISA website*.

Introduction to eDelivery

Below is an overview of the expected **benefits** to the individual Projects and Policy Domains :

BENEFITS

Reduce risks	Reduce costs	Improve quality

Reduce the learning curve of service providers of document and data exchange networks

Make savings in the cost of creating, maintaining and operating document and data exchange networks as some of these costs may be shared with other service providers of eDelivery

The wide use of the same eDelivery specifications is expected to create incentives for software companies to offer eDelivery compliant solutions at a competitive cost

Accelerate the delivery time of a working document and data exchange network as eDelivery provides out of the box specifications and software components

Foster synergies at all levels with other service providers of eDelivery

Increase the quality of document and data exchange networks as eDelivery was already been tried and tested in multiple policy domains;

As use increases, the wide availability of IT engineers with knowledge and experience in eDelivery's technical specifications is also expected to increase

2

Context
What is CEF Digital?

Context

At present, most EU policies require the exchange of data and documents between citizens, businesses and administrations across borders.

Having this in mind, the ICT Policy Support Programme (ICT PSP) sponsored the piloting of eDelivery in several policy domains.

These Large Scale Pilots (LSPs) were carried out between 2007 and 2015:

PEPPOL

The Pan-European Public Procurement Online, the LSP of eProcurement, now transferred to the non-profit international association OpenPEPPOL

SPOCS

The Simple Procedures Online for Cross-Border Services, the LSP of simplified administrative procedures, now completed

e-CODEX

The e-Justice Communication via Online Data Exchange, the LSP of eJustice, running until May 2016

The piloting of eDelivery in these different domains was quite successful and as a result a dedicated eDelivery 'convergence' track was launched under the e-SENS 🔗 (Electronic Simple European Networked Services), the last LSP of the ICT PSP.

e-SENS

e-SENS was launched to consolidate, improve, and extend the technical solutions developed by the thematic LSPs

Context

The eDelivery DSI promotes the deployment of the technical specifications selected by the LSPs.

The technical specifications of eDelivery are:

Available for free	Supported by multiple programming languages	Independent from any specific vendor products	Supported by (Open Source and Commercial) solutions that can be purchased in a competitive environment

As decided by the LSPs, eDelivery is based on **technical specifications developed by international Standards Developing Organizations (SDOs)** such as OASIS and ETSI.

This strategic decision aims at the adoption of eDelivery's technical specifications by the software industry at large and not only by public authorities.

For example, eDelivery's message exchange specifications are based on OASIS' AS4/ ebMS3.0 specifications which have already been used in the e-CODEX LSP but also by major software vendors: over sixteen commercial products and several other Open Source products.

Context

The eDelivery DSI met the eligibility criteria of the CEF in 2014 and was, as a result, included in the CEF Telecom Work Programme 2014. The operation of the eDelivery core service platform is therefore ensured for 4 years, until 2018, with a budget of EUR 8 million. During this period, the Commission should accomplish the following tasks included in the aforementioned Work Programme:

Summary of technical tasks

i. implementation, testing and open-source publishing of software and specifications
ii. development and operation of a testing and reference centre

Summary of support and training tasks

i. support to the providers of access points through a helpdesk
ii. dissemination and training actions for actual and prospective users
iii. technical training and remote support for software companies and other parties

Summary of service administration and stakeholder engagement tasks

i. administration and operation; provision of statistics on the use of the services
ii. steering the extension of the service and monitoring its functional and geographical deployment
iii. support interaction with the stakeholder community

Grants will be used to promote the uptake of eDelivery. According to the CEF regulation, the grants should not exceed 75% of the eligible costs. These calls will be published on the website of the Innovation and Networks Executive Agency (INEA 🔗).

Parts of the funding under CEF will be made available in the form **of grants allocated following competitive Calls for Proposals**. Proposals shall be **submitted by one or more Member States or**, with the agreement of the Member States concerned, by **international organisations, joint undertakings, or public or private undertakings or bodies established in Member States.**

3

Motivation
Why should you reuse eDelivery?

Motivation

Nowadays, almost every EU policy requires some data to be exchanged and, as a result, the interconnection of specific IT systems in the Member States. eDelivery is usually implemented in support of Union policies: Procurement, Justice, Health, etc.
Each implementation has a different context and policy goals.

As explained in this chapter, a key motivation to deploy eDelivery is the creation of an interoperability layer among heterogeneous systems and to significantly raise the security level offered by the internet.
Furthermore, eDelivery also contributes to legal assurance and accountability as well as scalability and performance.

Network (internet)	HTTP (Hypertext Transfer Protocol)
	TCP/IP model
eDelivery	Secure message exchange of structured, non-structured and binary data
Legacy systems	Web-portals, Back Office systems, etc.

The role of eDelivery

Motivation

In order to better grasp how eDelivery works, how it can help, and to better understand the remainder of the document, some definitions are needed.

Why

Policy Officer · IT Architect · Service providers

GOALS

The high-level objectives your organization can achieve by adopting eDelivery

(Example: *Interoperability)*

BUSINESS NEEDS

The detailed business needs, linked to your goals, which can be satisfied through the adoption of eDelivery

(Example: *You can exchange documents and data using different communication channels)*

How

Policy Officer · IT Architect · Service providers

USE CASES

User-centric and functional view of what eDelivery can do

(Example: *Message exchange)*

What

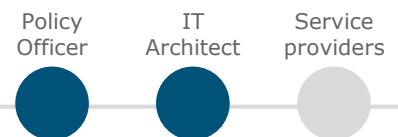Policy Officer · IT Architect · Service providers

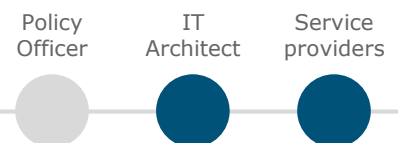### COMPONENTS

The technical components you need in order to start a successful eDelivery project

(Example: *Access Point)*

Tools

Policy Officer · IT Architect · Service providers

ASSESSMENT

An online questionnaire that will help you understand if goals and needs can be satisfied by eDelivery
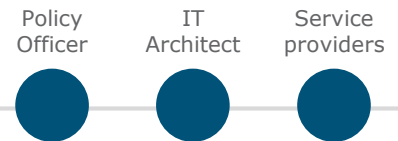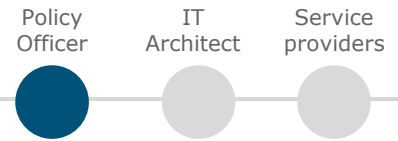
Motivation

The implementation of eDelivery may be triggered by a new EU regulation, a new Large Scale Pilot sponsored through EU funding (H2020 or other) or a new cooperation initiative between EU Member States.

Even if eDelivery is conceived for the exchange of documents and data across borders, it is also possible to use it to link up different regions, municipalities, etc. in one Member State.

A success factor for implementing eDelivery is to clearly understand the motivation for its use, its scope and (business) needs.

Below are the most usual **goals** that eDelivery helps to tackle:

Interoperability

Security

Scalability & Performance

Legal Assurance & Accountability

Motivation

In details, here are the goals that eDelivery helps achieve:

Goals	Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
What it is about	Implementing common technical specifications that enable diverse organisations to exchange data and documents.	Promoting an atmosphere of trust among all participants in the message exchange network.	Enabling the number of participants in the data exchange network to grow as well as the number of exchanged messages.	Promoting a high level of transparency and confidence among all participants in the message exchange network.
Examples	It is difficult to enable the exchange of data between Member States because their information systems were developed independently and have, as a result, no common data structures (not addressed by eDelivery) and data exchange protocol (addressed by eDelivery).	E-mail is widespread and reaches the intended recipients most of the time, but its delivery is not guaranteed. Furthermore, e-mail is usually not encrypted meaning that its contents may be intercepted and compromised along the way. A number of document and data exchange systems, deployed in the late 1990s/ early 2000s, no longer match the modern-day security demands.	EU systems based on a hub and spoke architecture, where the systems of the Member States connect to a hub operated by the European Commission, are hard to scale as the hub becomes a bottleneck. Data exchange systems that rely on e-mail are not easy to automate and consequently not easy to scale.	The evidences produced during the exchange of data and documents should have a legally recognised evidential value.

Motivation

To understand how eDelivery helps achieving these goals, here are the business needs it helps satisfy:

Goals

What it means for you

Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
Int.1 You can exchange documents and/ or data using a standardised messaging protocols other than e-mail	**Sec.1** You are certain that data and documents are secured against any modification (integrity)	**ScP.1** You can exchange documents and data files larger than 50 Mb	**LAA.1** You have the guarantee that data and documents are delivered once and only once (retries, receipts, duplicate elimination)
Int.2 You can exchange attachments in addition to messages (XML documents)	**Sec.2** You are certain that documents are encrypted during transmission (confidentiality)	**ScP.2** Your back-office has different ways to connect to the message exchange network	**LAA.2** You are certain that messages are delivered even if sent to temporarily unavailable channels (store and forward)
Int.3 The information about the participants (what messages they can process, the message protocol that they support, …) is easily discoverable and accessible to you and to everyone else in the data exchange network	**Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy	**ScP.3** You are certain that that the message exchange network will adapt to an increasing number of nodes, as opposed to a stable number of nodes	**LAA.3** You receive evidences, possibly with legally recognised evidential value, of the several steps of the exchange of documents and data
Int.4 You can easily change and discover the registered address of nodes	**Sec.4** You have access to advanced and configurable logging of events related to the exchange of data and documents	**ScP.4** You are certain you can handle increasing messaging loads in a day, hour, etc.	**LAA.4** You are certain of the non-repudiation of receipt and/or origin of every exchange through signature
Int.5 You can execute asynchronous request-response interactions		**ScP.5** You are certain you have access to advanced and configurable monitoring of the system	**LAA.5** You are certain of time synchronization in the message exchange process

Through the use of this building block, **every participant becomes a *node* in the network** using standard transport protocols and security policies.

eDelivery is based on a distributed model, allowing **direct communication between participants without the need to set up bilateral channels.**

——— ## What are the elements in play?

1 / Message exchange

At its core, public administrations adopting the same eDelivery Building Block can easily and safely exchange data with each other - even if their IT systems are independent from each other - through an Access Point.

3 / Dynamic Service Location

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).
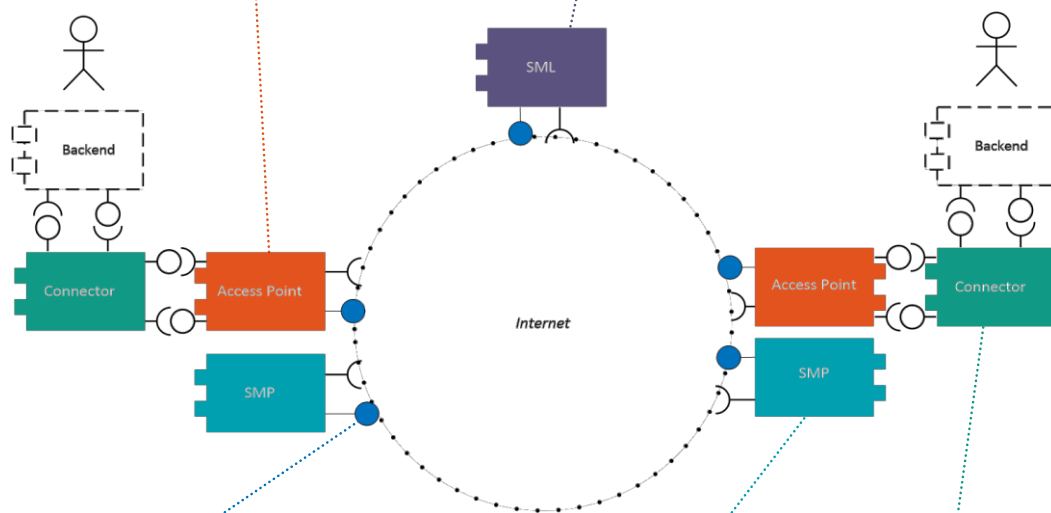
2 / Trust Establishment

In order to activate this exchange, two public administrations' Access Points need to establish trust between each other. This is done through digital certificates.

4 / Capability Lookup

Once the sender discovers the address of the receiver's SMP (Service Metadata Publisher), it is able to retrieve the needed information (i.e. metadata) about the receiver. With such information, the message can be sent.
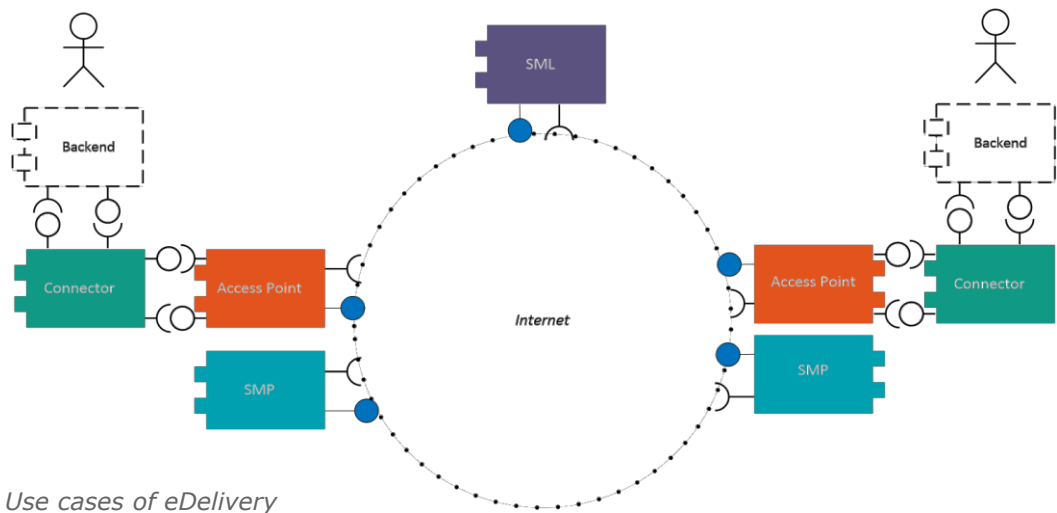
5 / Backend integration

In order to further facilitate the integration between a public administration's IT systems and an Access Point, a Connector can be put in place.

Motivation

The following illustration describes the use cases of eDelivery, with details of components and features behind each of them.

Use cases of eDelivery

	1 / Message Exchange	2 / Trust Establishment	3 / Dynamic Service Location	4 / Capability Lookup	5 / Backend Integration
Components	**Access Point**	**Digital Certificates**	**Service Metadata Locator (SML)**	**Service Metadata Publisher (SMP)**	**Connector**
	The access points of eDelivery implement a standardised message exchange protocol which ensures secure and reliable data exchange.	Trust is established using digital certificates. This can be implemented through a PKI model or mutual exchange of certificates.	The SML is used to add / update / delete information about the participants' SMP location on a Domain Name System (DNS). The SML is centralised.	The SMP is a register of the message exchange capabilities and location of participants. The SMP is usually distributed.	The Connector facilitates the interaction between the Access Point and the Backend Systems.
Features	Message sending	PKI model	Dynamic address resolution	Capabilities resolution	Document submission
	Message receiving	Mutual trust			Document delivery
	Transport level security				
	Transport message process				

_____

Motivation

Experience shows that the EU-wide projects that decided to implement eDelivery have different goals and, as a result, different business needs.

The importance of each goal can easily be quantified, once the business needs of the particular project are identified and well understood e.g. by linking the business needs associated with each goal.

CEF makes available an **assessment tool** to help you understand how your organization can benefit from eDelivery.

Step 1 - Fill the Questionnaire

- Provide some general information about your organization and your context
- Self-assess your business needs (on a scale from o to 2)

ASSESS YOUR SITUATION

REAL ASSESSMENT

STEP		ANSWERS	
1	ABOUT YOUR ORGANIZATION	8/8	✓
2	BACKOFFICE INFORMATION	4/4	✓
3	FACTS AND FIGURES	9/9	✓
4	**BUSINESS NEEDS**		
4.1	INTEROPERABILITY	5/5	✓
4.2	SECURITY	2/4	

SECURITY

	0	1	2
Ensure that data and documents are secured against any modification (integrity)			X
Ensure that data and documents are secured against any modification (integrity)			X
Ensure that the origin and the destination of the data and documents are trustworthy			
Advanced and configurable logging of events related to the exchange of data and documents			

NEXT ▶

4.2	SCALABILITY and PERFORMANCE	0/5
4.4	LEGAL ASSURANCE & ACCOUNTABILITY	0/5

VIEW RESULTS ▶

Motivation

STEP 2 – View the results and start a project

- Discover what goals and components are most relevant for you
- Discover which architecture design fits your needs
- Get in touch ✉ with CEF team, or read more online 🔗

Illustrative

Goals: what you can achieve

Radar chart axes: INTEROPERABILITY, SECURITY, SCALABILITY and PERFORMANCE, LEGAL ASSURANCE & ACCOUNTABILITY
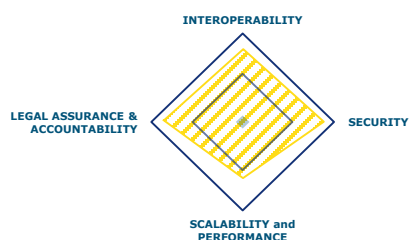
TOP GOALS

1st **SECURITY**
Promoting an atmosphere of trust among all participants in the message exchange network.

2nd **LEGAL ASSURANCE & ACCOUNTABILITY**
Enabling the number of participants in the data exchange network to grow as well as the number of exchanged messages.

3rd **INTEROPERABILITY**
Implementing common technical specifications that enable diverse organisations to exchange data and documents.

4th **SCALABILITY and PERFORMANCE**
Promoting a high level of transparency and confidence among all participants in the message exchange network.

Components: what you need

Radar chart axes: ACCESS POINT, TRUST ESTABLISHMENT, SML, SMP, CONNECTOR
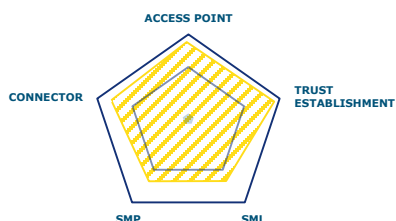
TOP COMPONENTS

1st **TRUST ESTABLISHMENT**
Trust is established using digital certificates. This can be implemented through a PKI model or mutual exchange of certificates.

2nd **ACCESS POINT**
The access points of eDelivery implement a standardised message exchange protocol which ensures secure and reliable data exchange.

3rd **CONNECTOR**
The Connector facilitates the interaction between the Access Point and the Backend Systems.

4th **SMP**
The SMP is a register of the message exchange capabilities and location of participants. The SMP is usually distributed.

5th **SML**
The SML is used to add / update / delete information about the participants' SMP location on a Domain Name System (DNS). The SML is centralised.

Architecture design: what you can re-use

50%

0%   100%

BB DSI – eDelivery
% of features that can be re-used
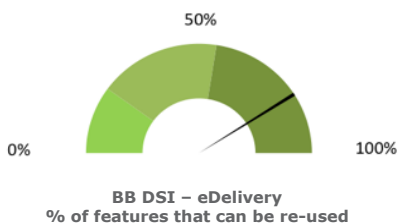
Start your eDelivery project

START CONVERSATION   ONLINE CATALOGUE

Take the self assessment

4

Use Cases
A deep-dive into CEF eDelivery

Use cases

The Use Cases introduced in this document are all **domain-neutral** as eDelivery can be used for the exchange of any type of document and data.

This is why the first Use Case is called 'Message Exchange' instead of 'Invoices Exchange' or 'Claims Exchange'. These domain-specific Use Cases are all specialisations of the 'Message Exchange' Use Case. What is important to keep in mind is that eDelivery is an **enabler** of a wide variety of services which will exchange specific types of documents and data, below are a few examples.

For example:

DOMAIN-NEUTRAL USE CASE

Message Exchange
Exchange of electronic data and documents among public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way

Examples of DOMAIN-SPECIFIC USE CASES

Consumer Protection	Procurement	Justice
Complaints	Invoices	Claims
Exchange of **complaints**	*Exchange of* **invoices**	*Exchange of* **claims**

Message Exchange

What eDelivery helps you achieve

Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
Int.1 You can exchange documents and/ or data using a standardised messaging protocols other than e-mail	**Sec.1** You are certain that data and documents are secured against any modification (integrity)	**ScP.1** You can exchange documents and data files larger than 50 Mb	**LAA.1** You have the guarantee that data and documents are delivered once and only once (retries, receipts, duplicate elimination)
Int.2 You can exchange attachments in addition to messages (XML documents)	**Sec.2** You are certain that documents are encrypted during transmission (confidentiality)	**ScP.4** You are certain you can handle increasing messaging loads in a day, hour, etc.	**LAA.2** You are certain that messages are delivered even if sent to temporarily unavailable channels (store and forward)
Int.5 You can execute asynchronous request-response interactions	**Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy		**LAA.4** You are certain of the non-repudiation of receipt and/or origin of every exchange through signature

Message Exchange

How does eDelivery help you achieve it

The technical architecture of eDelivery is based on a conceptual model called **'four-corner model'.** This means that Backend systems (corners one and four) do not exchange messages directly with each other but via Access Points (corners two and three) that, in any given exchange, play the sender or receiver role.

The Access Points of eDelivery are not operated centrally, instead they are deployed in the Member States under the responsibility of a public or private sector service provider.

The users of the Access Points are the Backend systems that need to exchange information with other administrations or businesses across borders.

During the exchange, the data and documents are secured by eDelivery's trust establishment mechanisms. This implies a choice of trust establishment model.
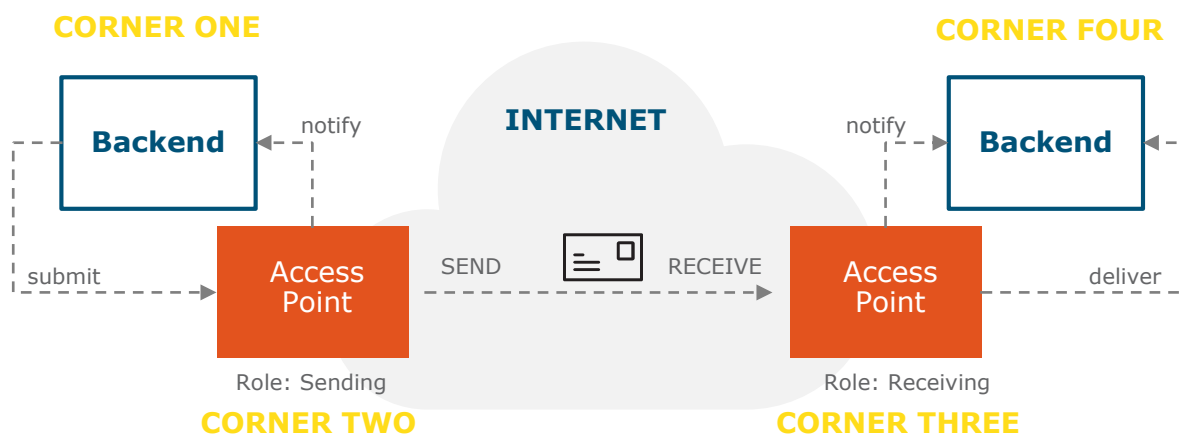
The four-corner model

Which components you need to achieve it

Component

ACCESS POINT
The access points of eDelivery implement a standardised message exchange protocol which ensures secure and reliable data exchange.

Standards

e-SENS profile of the **ebMS3** and **AS4 OASIS Standards**

PEPPOL profile of the **AS2 IETF and SBDH UN/CEFACT Standards**

Trust establishment

What eDelivery helps you achieve

Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
	Sec.1 You are certain that data and documents are secured against any modification (integrity) **Sec.2** You are certain that documents are encrypted during transmission (confidentiality) **Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy	**ScP.3** You are certain that the message exchange network will adapt to an increasing number of nodes, as opposed to a stable number of nodes	

Trust establishment

How does eDelivery help you achieve it

The trust models of eDelivery are all based on digital certificates. The way these digital certificates are used in 'run time' to secure the communication between Access Points is shown below.

1 / The sending Access Point uses its digital certificate to sign the data and documents, it may also encrypt it using the public key of the receiver

2 / The receiving Access Point confirms the digital signature of the sender and decrypts the data using its digital certificate

Access Point — TLS — Standard Protocol (HTTP,SOAP, ...)

INTERNET

Data

Receipt

Standard Protocol (HTTP,SOAP, ...) — Access Point

Role: Sending

CORNER TWO

Role: Receiving

CORNER THREE

3 / The receiving Access Point sends a signed receipt message to the sending Access Point

Two trust models are available to create, manage, distribute, store, and revoke the digital certificates of the Access Points: either a PKI model or a mutual exchange model of digital certificates.

The communication between the SMP and SML components is secured through two way TLS.

SMP — TLS

INTERNET DNS

Data

Standard Protocol (HTTP,SOAP ...) — TLS — SML

Which components you need to achieve it

Component   **Digital Certificates**

Trust is established using digital certificates. This can be implemented through a PKI model or mutual exchange of certificates.

Standards   **ETSI** - Electronic Signatures and Infrastructures

Dynamic Service Location

What eDelivery helps you achieve

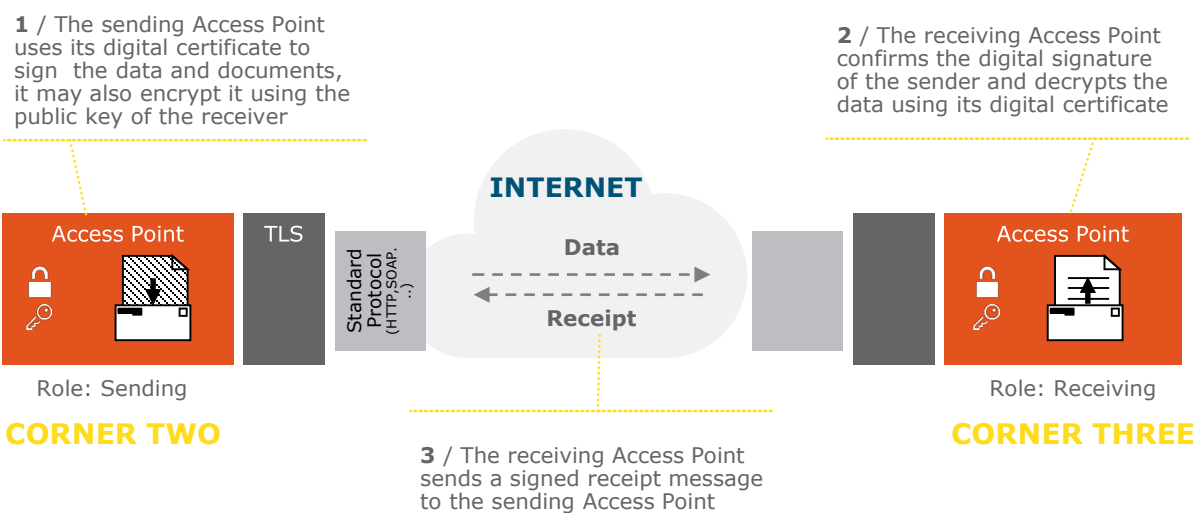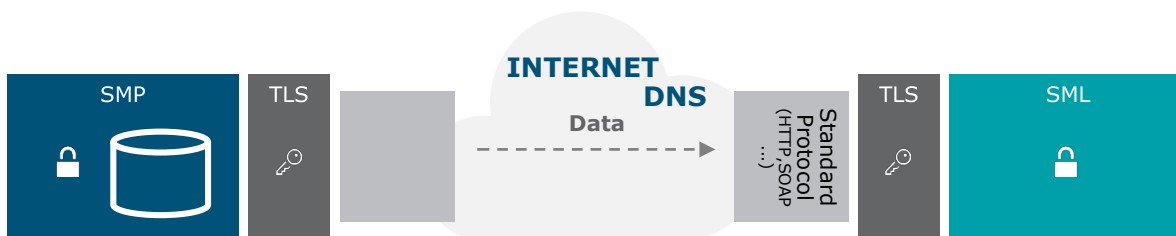| Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
Int.3 The information about the participants (what messages they can process, the message protocol that they support, …) is easily discoverable and accessible to you and to everyone else in the data exchange network	**Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy	**ScP.3** You are certain that the message exchange network will adapt to an increasing number of nodes, as opposed to a stable number of nodes	
Int.4 You can easily change and discover the registered address of nodes			

Dynamic Service Location

How does eDelivery help you achieve it

eDelivery's Dynamic Service Location enables the Sending Access Point to dynamically discover the IP address of the Receiving Access Point. Instead of looking at a static list of IP addresses, the Sending Access Point consults a Service Metadata Publisher (SMP) where information about every participant in the document and data exchange network is kept up to date, including IP addresses of their Access Point. As at any point in time there can be several SMPs, every participant must be given a unique ID in the form of a website's URL and this must be published by the Service Metadata Locator (SML) on the internet's Domain Name System (DNS). By knowing this URL, the Access Point is able to dynamically locate the right SMP and therefore the right Access Point.

Which components you need to achieve it

Component	**Service Metadata Locator (SML)**
	The SML is used to add/update/delete information about the participants' SMP location on a Domain Name System (DNS). The SML is centralised.

| Standards | **OASIS BDXL** Specification originally developed by PEPPOL |

Capability lookup

What eDelivery helps you achieve

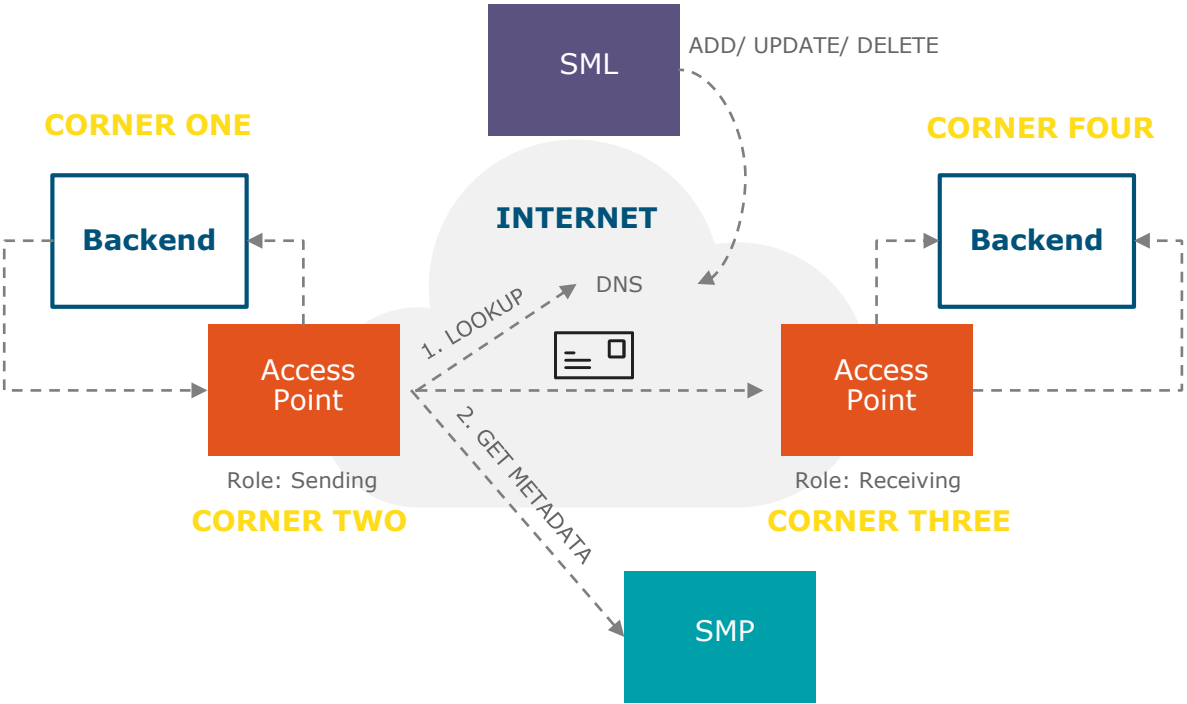| Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
Int.3 The information about the participants (what messages they can process, the message protocol that they support, …) is easily discoverable and accessible to you and to everyone else in the data exchange network	**Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy	**ScP.3** You are certain that that the message exchange network will adapt to an increasing number of nodes, as opposed to a stable number of nodes	
Int.4 You can easily change and discover the registered address of nodes			

Capability lookup

How does eDelivery help you achieve it

Capability lookup is about the delivery of metadata about the capabilities of each participant in a document and data exchange network. The metadata can be used to dynamically set interoperability parameters between the sender and the receiver.

1 / Participant A puts the metadata of the participant into the SMP

2 / Participant B retrieves the signed metadata of Participant A

TLS

REST/ HTTPS

SML

TLS

REST/ HTTPS

Participant A
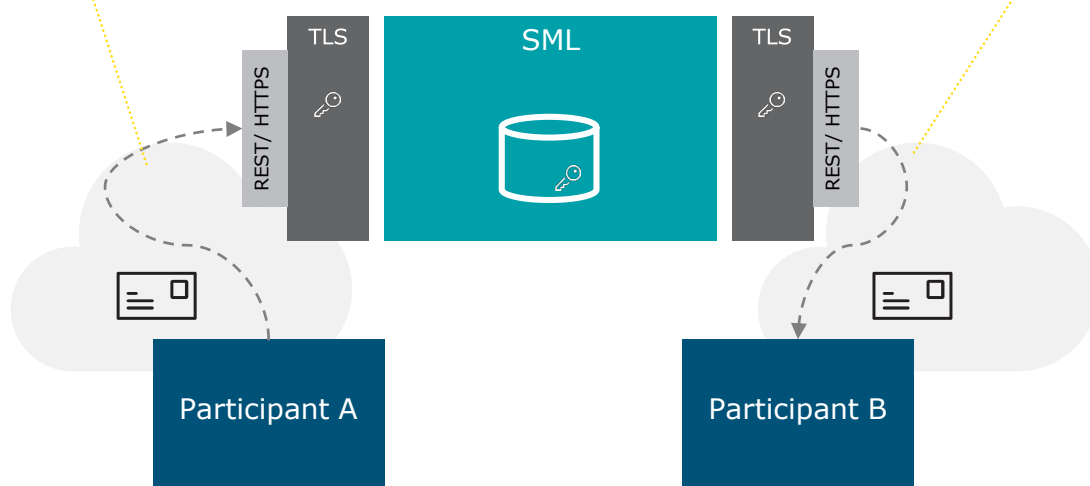
Participant B

Which components you need to achieve it

Component

Service Metadata Publisher (SMP)
The SMP is a register of the message exchange capabilities and location of participants. The SMP is usually distributed

Standards

OASIS SMP Specification originally developed by PEPPOL

Backend integration

What eDelivery helps you achieve

Interoperability	Security	Scalability & Performance	Legal Assurance & Accountability
Int.1 You can exchange documents and/ or data using a standardised messaging protocols other than e-mail	**Sec.2** You are certain that documents are encrypted during transmission (confidentiality)	**ScP.1** You can exchange documents and data files larger than 50 Mb	**LAA.2** You are certain that messages are delivered even if sent to temporarily unavailable channels (store and forward)
Int.2 You can exchange attachments in addition to messages (XML documents)	**Sec.3** You are certain that the origin and the destination of the data and documents are trustworthy	**ScP.2** Your back-office has different ways to connect to the message exchange network	**LAA.3** You receive evidences, possibly with legally recognised evidential value, of the several steps of the exchange of documents and data
Int.3 The information about the participants (what messages they can process, the message protocol that they support, …) is easily discoverable and accessible to you and to everyone else in the data exchange network	**Sec.4** You have access to advanced and configurable logging of events related to the exchange of data and documents	**ScP.5** You are certain you have access to advanced and configurable monitoring of the system	**LAA.4** You are certain of the non-repudiation of receipt and/or origin of every exchange through signature
Int.5 You can execute asynchronous request-response interactions			**LAA.5** You are certain of time synchronization in the message exchange process

Backend integration

How does eDelivery help you achieve it

An eDelivery Connector may also be used to facilitate the integration between backend systems and Access Points.

The next diagram shows the same exchange scenario with the eDelivery Connector. The connector offers capabilities like linking up to legacy systems, advanced monitoring and evidences.

CORNER FOUR

Backend

CORNER ONE

notify

Connector

Backend

deliver

notify

INTERNET

submit

Access Point

SEND

RECEIVE

Access Point

Role: Sending

Role: Receiving

CORNER TWO

CORNER THREE

Without Connector
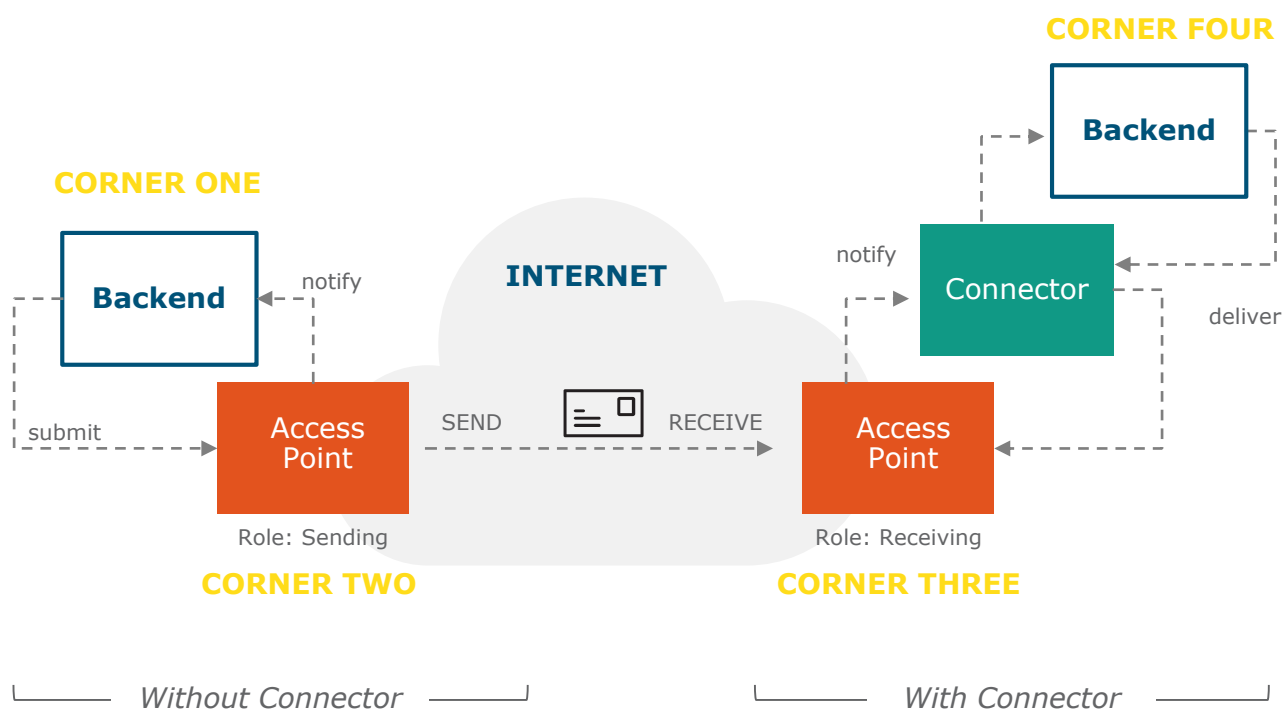
With Connector

Which components you need to achieve it

Component

Connector
The Connector facilitates the interaction between the Access Point and the backend systems.

Standards

ETSI REM

5 Technical specifications

What are the technical foundations of CEF eDelivery?

Technical specifications

This chapter provides more information on the technical specifications underpinning the eDelivery components. The approach employed by eDelivery is to promote the use of existing technical specifications and standards rather than to define new ones. The profiling work of e-SENS and PEPPOL on these standards, i.e. constraining configuration choices, is equally taken on board. Even though eDelivery makes software available implementing these specifications, the use of commercial software or other Open Source software projects is also possible.

Component	Key Specifications
Access Point	🔗 e-SENS profile of the ebMS3 and AS4 OASIS Standards. 🔗 PEPPOL profile of AS2 and SBDH
Digital Certificates	🔗 ETSI - Electronic Signatures and Infrastructures
Service Metadata Locator (SML)	🔗 OASIS BDXL Specification originally developed by PEPPOL 🔗 OASIS ebCore Party ID Type Technical Specification. September 2010
Service Metadata Publisher (SMP)	🔗 OASIS SMP Specification originally developed by PEPPOL 🔗 The original PEPPOL SMP specification
Connector	🔗 ETSI REM for evidences

6 Implementations
What are the existing CEF eDelivery implementations?

Your options

While considering an eDelivery project, three alternative implementation scenarios can be considered:
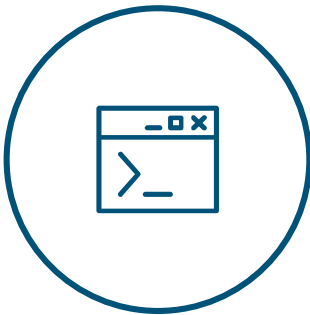
BUILD

You **build** and **test** your own components according to the specifications of the eDelivery DSI. This can be done using an in-house development team or by an external contractor.

BUY

You **buy** a product(s) that implements the specifications of the eDelivery DSI. This can be a Commercial or Open Source software product. Additional services can be involved.
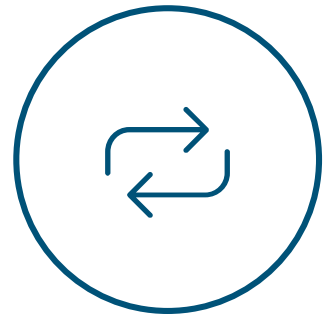
RE-USE

You **reuse** the sample software of the eDelivery DSI or one of its stand-alone services such as the Service Metadata Locator (SML) service.

Software Implementations

The European Commission maintains sample software compliant to the eDelivery specifications. The e-SENS project maintains a list of known commercial and non-commercial implementations of AS4. PEPPOL does the same for AS2.

Sample software maintained by the European Commission

	AS2 related stack	AS4 related stack
Access Point	OXALIS 3.1.0	DOMIBUS 3.0
Service Metadata Publisher (SMP)	CIPA	Available in 2016
Connector		Available in 2016

Download

Lists of software vendors and projects

	AS2	AS4
Access Point	List provided by PEPPOL	List provided by e-SENS

DISCLAIMER

These lists are for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein.

7 Governance

What is the CEF IT governance model?

Governance

CEF has a [governance model](#) 🔗 in place to ensure that eDelivery's reusable components correspond to user needs and expectations and that stakeholders can influence their evolution over time.

As shown below, the proposed model is multi-layered, designed according to guiding principles stemming from the CEF regulations.

CEF POLICY		
	CEF Coordination Committee ■	

CEF IT STRATEGY & COORDINATION

Project and Architecture Office ■ ← *support* / *guidance* → CEF Telecom Expert Group ■

CEF DSIs IMPLEMENTATION

BUILDING BLOCK DSIs
- DSI Operational mgmt board ■
- DSI Expert group ■

SECTOR SPECIFIC DSIs
- DSI Operational mgmt Board ■
- DSI Expert group ■

CEF DSIs STAKEHOLDERS

Standardisation Bodies	Private Sector	User Communities	Other Stakeholders

SCOPE OF DECISIONS

- ■ Policy implementation decisions
- ■ Strategic decisions
- ■ Tactical decisions
- ■ Operational & technical implementation decisions

CEF's governance model

Governance

The eDelivery Operational Management Board (OMB) is organised every month to discuss all types of operational matters (change requests, release planning, etc.). This governance body brings together:

- The eDelivery DSI (Policy) Owner, accountable for its policy and its translation into the functionality of the building block: this role is currently played by DG CNECT

- The DSI Solution Provider, accountable for the delivery side of eDelivery's components and related services: this role is currently played by DIGIT

- The Directorate Generals of the Commission that have decided to reuse, or are interested in reusing, eDelivery

The OMB works in close collaboration with, and is advised by, the eIDAS Electronic registered delivery service subgroup (composed of Member State representatives). Consultation processes ensure that standardisation bodies, the private sector, user communities and other stakeholders are involved as required. In case of issues, these can be escalated to the 'CEF Telecom Expert Group' (also composed of Member State Representatives). The CEF Telecom Committee is mostly involved in the formulation of the CEF Telecom Work Programmes and less in their implementation.

Governance

The European Commission	
The Director Generals (DGs) of the European Commission	eDelivery may be implemented in any policy domain of the EU, from agriculture to transport. This means that the deployment of eDelivery may be suggested by a DG of the European Commission to the Member States through the governance bodies of the policy domain.
The Director General for Informatics (DIGIT)	DIGIT provides the hosting environment for the SML and for the eDelivery testing environments. DIGIT also maintains sample implementations of the eDelivery software. DIGIT provides support to all service providers and is the custodian of the specifications of eDelivery. DIGIT reserves the right to delegate activities to private contractors through public procurement.
The Director General for Communications, Networks, Content and Technology (DG CNECT)	The eIDAS unit and the Public Services unit of DG CNECT are both responsible for the policy management of eDelivery and ensuring that the needs of the several policy domains are met.

Public Authorities	
eIDAS Electronic registered delivery service subgroup	Public Authorities that have been officially nominated to participate in the eDelivery Technical subgroup of eIDAS to provide recommendations to the eDelivery DSI on technical solutions and operational decisions regarding the implementation of eIDAS.
CEF Coordination Committee and CEF Telecom Expert Group	Public Authorities that have been officially nominated to participate in CEF's Committee or the CEF Telecom Expert Group .

Private Sector	
Software Vendors	Software Vendors may develop software compliant with the specifications of eDelivery to sell it as a commercial product or as an Open Source project.
System Integrators and Professional Services Companies	System Integrators and Professional Services Companies may offer their services to integrate national backend systems with eDelivery or to install and operate eDelivery.

Standards Developing Organizations (SDOs)	
OASIS and ETSI	The eDelivery specifications were developed on top of standards developed by OASIS and ETSI. These profiles were elaborated by e-SENS.

User Communities (examples)	
OpenPEPPOL	The OpenPEPPOL Association was established on the 1st of September 2012 after successful completion of the Pan-European Public Procurement Online (PEPPOL). Open PEPPOL uses eDelivery.
e-CODEX	e-CODEX is an e-justice project to improve the cross-border access of citizens and businesses to legal means in Europe. e-CODEX uses eDelivery.

8

CEF services to Service Providers
How can we help you accelerate the deployment of CEF eDelivery?

CEF services to Services Providers

The tables below shows the typical split of responsibilities between the eDelivery DSI and the Service Providers of eDelivery Services. These can be changed via a Memorandum of Understanding (MoU) with the CEF eDelivery DSI.

eDelivery DSI	Service Providers
• Hosting environment for the SML (when Dynamic Service Location is used);	• Hosting environment for the Access Point, Connector and Service Metadata Publisher (when Dynamic Service Location is used);
• Digital Certificates (when the PKI model of eDelivery is used);	• Digital Certificates (when the PKI model of eDelivery is not used);
• Testing environments;	• What is being exchanged (the electronic documents and data;
• Sample implementations of the eDelivery software;	• Data representation and meaning (data schemas, code lists, etc.);
• Deployment of sample implementations of the eDelivery software;	• Procedure for admitting members to the document and data exchange network;
• Support and training to the users of eDelivery specifications and eDelivery sample implementations.	• Coordination of deployment;
	• Operational supervision of the document and data exchange network.

CEF services to Service Providers

Before deployment

Testing services

- Conformance testing of any deployment of eDelivery in the dedicated test platform of the European Commission
- Provision of Test Certificates
- Support throughout the testing lifecycle

Installation and Training services

- Applicable for the sample implementations of the eDelivery software
- Support for on-site installation*
- On-site Training*
- eLearnings
- FAQ on dedicated website

* In case of a standard AS4 implementation, it is possible to request support for on-site installation and training.

For more information, please contact the Support Office (see below)

After deployment

PKI services

- Issuing of signing certificates
- Renewing of certificates after their lifespan

SML service

- 24/7 monitoring of the SML component hosted at the European Commission
- Support for updating/modification of participants

Single point of contact for all support related matters

- By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu
- By phone: +32 2 299 09 09
- Standard Service: 8am to 6pm (Normal EC working Days)
- Standby Service*: 6pm to 8am (Normal EC working Days)
    - Commission and Public Holidays
    - Weekends

* Only for critical and urgent incidents and only by phone

9 Success Stories

Success stories

What is PEPPOL

The Pan-European Public Procurement Online (PEPPOL) was a Large Scale Pilot (LSP) of eProcurement. It has now been transferred to the non-profit international association OpenPEPPOL 🔗

PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

What they do

PEPPOL connects suppliers to Public Administrations and has been in production since 2012. It has now:

- more than 40.000 end user organisations connected to the document and data exchange network; and
- around two million transactions on a monthly basis.

Most of the transactions are related to eInvoicing but the number of product catalogue and ordering transactions are also increasing.

Why they use eDelivery

The two main goals that eDelivery helps to tackle in the context of PEPPOL are:

Interoperability   Scalability & Performance

Which components they use

Use Cases	1 / Message Exchange	2 / Trust Establishment	3 / Dynamic Service Location	4 / Capability Lookup	5 / Backend Integration
Comp.	**Access Point**	**Digital Certificates**	**Service Metadata Locator (SML)**	**Service Metadata Publisher (SMP)**	**Connector**
Features	Message sending	PKI model	Dynamic address resolution	Capabilities resolution	Document submission
	Message receiving	Mutual trust			Document delivery
	Transport level security				
	Transport message process.				

Success stories

What is e-CODEX

e-CODEX 🔗 is a Large Scale Pilot (LSP) that aims to improve cross-border access to justice and is running until May 2016. The delivery network will continue to operate also after the project itself reaches its end.

What they do

e-CODEX is connecting national courts or other judicial authorities to support electronic handling of:

- European payment orders
- Small claims
- Mutual Legal Assistance (MLA)

It enables citizens, legal professionals and companies to electronically file these types of claims to courts abroad. In the case of MLA information in criminal cases are exchanged cross-border between public prosecution offices. There have been live transactions since 2013.

Why they use eDelivery

The two main goals that eDelivery helps to tackle in the context of e-CODEX are:

🛡 Security

⚖ Legal Assurance & Accountability

Which components they use

Use Cases	1 / Message Exchange	2 / Trust Establishment	3 / Dynamic Service Location	4 / Capability Lookup	5 / Backend Integration
Comp.	**Access Point**	**Digital Certificates**	**Service Metadata Locator (SML)**	**Service Metadata Publisher (SMP)**	**Connector**
Features	Message sending	PKI model	Dynamic address resolution	Capabilities resolution	Document submission
	Message receiving	Mutual trust			Document delivery
	Transport level security				
	Transport message process.				

1o Definitions

Definitions

A **Building Block** offers basic capabilities and services that can be combined with other building blocks or sector-specific applications to deliver architectures, solutions and sector-specific services.

Source: TOGAF® 9.1 and Regulation (EU) No 283/2014

Interoperability is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.

Source: European Interoperability Framework 2.0

e-SENS (Electronic Simple European Networked Services) is a large-scale pilot project with the aim of consolidating, improving, and extending technical solutions based around the building block DSIs to foster digital interaction with public administrations across the EU.

Regulation (EU) N°910/2014 on eID and trust services for electronic transactions in the internal market (**eIDAS Regulation**) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

eDelivery is a building block that enables secure and reliable exchange of structured, non-structured and/or binary data. Thematic DSIs such as eJustice, eProcurement, Social Security, etc. build their services by defining the content exchanged on top of eDelivery.

A **Digital Service Infrastructure (DSI)** enables networked services to be delivered electronically, typically over the internet, providing cross-border interoperable services for citizens, businesses and/or public authorities.

Source: Regulation (EU) No 283/2014

The **AS4 profile** of eDelivery is the AS4 Usage Profile defined by e-SENS based on the AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard. AS4 itself is based on other standards, in particular on OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard, which in turn is based on various Web Services specifications.

The **AS2 profile** of eDelivery is based on RFC4130 HTTP Applicability Statement 2 (AS2). AS2 was chosen by PEPPOL because of its popularity among EDI Service Providers.

eDelivery is based on the "**Four-Corner Model**" because a message passes four "corners" on its way: the original sender, the sending Access Point, the receiving Access Point and the final recipient.

Definitions

According to the eIDAS regulation a **Public Administration** means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such 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

Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

According to the eIDAS regulation an **electronic registered delivery service** means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

According to the eIDAS regulation an **electronic registered delivery service** means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

According to the eIDAS regulation a **Service provider** means a natural or a legal person who provides eDelivery services either as a qualified or as a non-qualified trust service provider

Source: http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

eDELIVERY
connecting europe

Visit the catalogue of building blocks on Joinup
https://joinup.ec.europa.eu/community/cef/

DIGIT
Directorate-General for Informatics

DG CONNECT
Directorate-General for Communications
Networks, Content and Technology

Contact us

✉ CEF-BUILDING-BLOCKS@ec.europa.eu

11 ANNEX
e-SENS / CEF requirements mapping

e-SENS Requirements

	Message Exchange	Int.	Sec.	ScP.	LAA.
R-MesExc-B1	Messaging must be secure, reliable, and asynchronous and must support non-repudiation.		Sec.1 Sec.2		LAA.2 LAA.4
R-MesExc-B2	Payload must be unified, size-scalable, in structured and unstructured format.	Int.1 Int.2		ScP.1	
R-MesExc-B3	The system must support originator and recipient Authentication.		Sec.3		
R-MesExc-T1	Secure Messaging		Sec.2		
R-MesExc-T2	Reliable Messaging: once-and-only-once guaranteed delivery (retries, receipts, duplicate elimination)				LAA.1
R-MesExc-T3	Support for non-repudiation of origin and receipt (gateway to gateway)				LAA.4
R-MesExc-T4	Support for asynchronous store-and-forward messaging	Int.5			LAA.2
R-MesExc-T5	Support for monitoring and routing based on business message metadata (identifiers, correlation, business process information and/or other)	-			
R-MesExc-T6	Support for business documents and attachments in a single message	Int.1 Int.2			
R-MesExc-T7	Support for large messages (where the definition of "large" is domain-dependent, but may be up to a few GB)			ScP.1	
R-MesExc-T8	Support for structured and unstructured payload.	Int.1 Int.2			
R-MesExc-T9	Ability to authenticate sending and receiving gateway.				
R-MesExc-T10	Ability to authenticate the original sender.				

	Trust Establishment	Int.	Sec.	ScP.	LAA.
R-TruSer-BL1	e-Signature validation services must be trustable		Sec.1 Sec.2 Sec.3		
R-TruSec-BL2	Nodes used to inter-connect national/ application domain trust circles must be recognizable as trustworthy; their underlying trust and service quality status, operational policy, governance model must be verifiable by all actors involved at any time.		Sec.3		

e-SENS Requirements

Dynamic discovery of Participants (Dynamic Service Location)	Int.	Sec.	ScP.	LAA.
R-SerLoc-B1	Obtain location information to route messages to end entities	Int.4			
R-SerLoc-B2	Location Lookup Services must be decoupled from transport protocols and security models it is used in conjunction with	Int.4			
R-SerLoc-B3	Ability to switch end entity identification information at the right point in time	-			
R-SerLoc-T1	Discover the location of a metadata service for an identified end entity	Int.4			
R-SerLoc-T2	Retrieve service metadata for an identified end entity from a discovered service location in a machine-readable format	Int.3			
R-SerLoc-T3	Ability to parametrize location for separate environments (production, test)	-			
R-SerLoc-T4	Ability to partition location information across communities (with community-specific terms and conditions, governance models etc.)	Int.3			
R-SerLoc-T5	Ability to locate service metadata for an entity using search criteria other than identifier	Int.3			

Capability Lookup	Int.	Sec.	ScP.	LAA.
R-CapLoo-S1	May provide metadata about receivers legal requirements for interoperability	Int.3			
R-CapLoo-S2	May provide metadata about receivers organizational requirements for interoperability	Int.3			
R-CapLoo-S3	May provide metadata about which standardized Business Processes (eProcess) is supported by receiver	Int.3			
R-CapLoo-S4	May provide metadata about which standardized Business Documents (eDocument) is supported by receiver	Int.3			
R-CapLoo-S5	May provide metadata about required and/or supported technical settings: Security, Evidence e.g. non-repudiation, Communication protocol	Int.3			
R-CapLoo-T1	May resolve receiver's communication address, based on receiver's other capabilities	Int.4			
R-CapLoo-T2	Ability for receiver to change its own capability settings within the agreed interoperability framework of the specific interoperability community	Int.4			
R-CapLoo-T3	Ability for an entity to control the visibility of its metadata	Int.4			
R-CapLoo-T4	Ability to verify authenticity and validity of metadata		Sec.3		
R-CapLoo-T5	Ability to partition metadata information across communities (with community-specific terms and conditions, governance models etc.)	Int.3			
R-CapLoo-T6	Ability to parametrize metadata for separate environments (production, test)	-			

e-SENS Requirements

Backend Integration (1/2)		Int.	Sec.	ScP.	LAA.
R-BacInt-B1	The system must support interoperability.	Int.1			
R-BacInt-T1	Availability of product implementations that can interface to national infrastructures using common backend integration protocols; including support for polling consumers using a standard interface.			ScP.2	
R-BacInt-T2	The system must provide interfaces that enable backend integration without changes to the national systems.			ScP.2 ScP.5	
R-BacInt-T3	The system must support interoperability in terms of Business Process between different backend systems by maintaining dynamic capability lookup services.	Int.3			
R-BacInt-T4	Message persistency: The e-Delivery platform should be able to keep messages in case of temporary connection delays.				LAA.2
R-BacInt-B2	Prevention of sensitive data persistency: The e-Delivery platform should be able to identify messages carrying sensitive date, and prevent their storage				
R-BacInt-T5	Transformation/encapsulation: The backend e-Delivery platform should be aware of different formats that are used between MSs and it should support modules that transform and encapsulate to the proper format.	Int.1			
R-BacInt-T6	Asynchronous communication: The backend e-Delivery platform should support asynchronous store-and-forward messaging.	Int.5			LAA.2
R-BacInt-T7	Message exchange pattern: There should be a clearly defined method describing how the messages are transferred from Corner 2 to Corner 1.	Int.1 Int.5			
R-BacInt-T8	Time stamping and time synchronization: All messages must be time stamped for logging and non-repudiation purposes.				LAA.3 LAA.4 LAA.5
R-BacInt-T9	User-selected gateway: It should be possible for an end entity connecting directly to the e-SENS delivery platform to select the e-SENS gateway.	-			
R-BacInt-T10	EE and GW software version cohabitation: Any new version of the EE connector software should be accompanied by a new version of e-SENS backend gateway and vice-versa.	-			

e-SENS Requirements

	Backend Integration (1/2)	Int.	Sec.	ScP.	LAA.
R-BacInt-T11	Backend implementation separated from e-SENS GW implementation: The e-SENS backend gateway software should be regarded as a separate piece of software.	-			
R-BacInt-T12	Network layer interface: There should be a clearly defined way to deliver structured messages and how the backend should communicate with the EE.	-			
R-BacInt-T13	Keep-alive/alarming: Corner 2 should know when Corner 1 has become unreachable even before an actual message is transmitted.	-			
R-BacInt-T14	Authentication information: The EEs must provide authentication information upon sending or receiving any message.				
R-BacInt-T15	Document signature: All structured messages sent or received MUST be digitally signed in order to demonstrate the authenticity of a digital message or document.				LAA.4
R-BacInt-T16	Signature validation: The digital signature contained in a message should be verifiable.				LAA.4
R-BacInt-B3	Non-repudiation: It should be possible to validate the origin of any message, and to determine the integrity of that message.				LAA.4
R-BacInt-T17	Document encryption: It should be possible to encrypt documents or structured messages.		Sec.2		
R-BacInt-B4	Connection security: The connection between the backend and the EE should be secure.		Sec.2		
R-BacInt-B5	Logging: All events occurring in the e-SENS backend gateway should be logged.		Sec.4		LAA.3
R-BacInt-B6	Security policy: EEs must be provided with a security policy.		Sec.3		