Introduction to eDelivery and Harmony eDelivery Access

Public Report
Credits

**GOFORE**

**Authors**

Gofore: Niall O’Donoghue

NIIS: Petteri Kivimäki
# Table of contents

Credits ............................................................................................................................. 3

Table of contents ........................................................................................................... 4

Glossary .......................................................................................................................... 6

Introduction .................................................................................................................... 8

1. eDelivery ..................................................................................................................... 11
   1.1. Role of eDelivery in Europe .................................................................................. 11
   1.2. Use Cases ............................................................................................................. 12
   1.3. Benefits ................................................................................................................ 14
   1.4. Features ................................................................................................................. 15
      1.4.1. Trust establishment ......................................................................................... 15
      1.4.2. Dynamic Service Location .............................................................................. 15
      1.4.3. Capability Lookup ........................................................................................ 16
      1.4.4. Message Exchange ........................................................................................ 17
      1.4.5. Backend integration ....................................................................................... 18
   1.5. eDelivery Architecture ........................................................................................ 20
      1.5.1. Message exchange ......................................................................................... 21
      1.4.2. Components ................................................................................................... 22
      1.4.3. Access Point .................................................................................................. 24
      1.5.4. Service Metadata Locator ............................................................................ 25
      1.5.5 Service Metadata Publisher ............................................................................ 25
   1.6. Discovery Models .................................................................................................. 27
      1.6.1. Static discovery model ................................................................................... 27
      1.6.2. Dynamic discovery model ............................................................................. 27
   1.7. Message Sending .................................................................................................. 29
   1.8. Trust and Security ................................................................................................ 31
      1.8.1. Trust Model ..................................................................................................... 31
      1.8.2. Security Requirements ............................................................................... 31
      1.8.3. Security Controls ......................................................................................... 32
   1.9. Roles and Responsibilities .................................................................................... 34
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2A</td>
<td>Administration-to-Administration</td>
</tr>
<tr>
<td>A2B</td>
<td>Administration-to-Business</td>
</tr>
<tr>
<td>A2C</td>
<td>Administration-to-Citizens</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>AS</td>
<td>Applicability Statement 4</td>
</tr>
<tr>
<td>B2A</td>
<td>Business-to-Administration</td>
</tr>
<tr>
<td>B2B</td>
<td>Business-to-Business</td>
</tr>
<tr>
<td>BRIS</td>
<td>Business Registers Interconnection System</td>
</tr>
<tr>
<td>C2A</td>
<td>Citizens-to-Administration</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CEF</td>
<td>Connecting Europe Facility</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>DSI</td>
<td>Digital Service Infrastructure</td>
</tr>
<tr>
<td>ebMS</td>
<td>electronic Business Messaging Services</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>e-CODEX</td>
<td>e-Justice Communication via Online Data Exchange</td>
</tr>
<tr>
<td>eDelivery</td>
<td>eDelivery in this document refers to the CEF eDelivery building block on which Harmony eDelivery Access is based</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EESSI</td>
<td>Electronic Exchange of Social Security Information</td>
</tr>
<tr>
<td>eHDSI</td>
<td>eHealth Digital Service Infrastructure</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>eIDAS</td>
<td>electronic IDentification, Authentication and trust Services</td>
</tr>
<tr>
<td>e-SENS</td>
<td>Electronic Simple European Networked Services</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUPL</td>
<td>European Union Public Licence</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>MDN</td>
<td>Message Disposition Notification</td>
</tr>
<tr>
<td>MEP</td>
<td>Message Exchange Pattern</td>
</tr>
<tr>
<td>NIIS</td>
<td>Nordic Institute for Interoperability Solutions</td>
</tr>
<tr>
<td>OOP</td>
<td>Once Only Principle</td>
</tr>
<tr>
<td>PEPPOL</td>
<td>Pan-European Public Procurement On-Line</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>SDG</td>
<td>Single Digital Gateway</td>
</tr>
<tr>
<td>SDGR</td>
<td>Single Digital Gateway Regulation</td>
</tr>
<tr>
<td>SML</td>
<td>Service Metadata Locator</td>
</tr>
<tr>
<td>SMP</td>
<td>Service Metadata Publisher</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Introduction

This document introduces you to Harmony eDelivery Access by the Nordic Institute for Interoperability Solutions (NIIS)\(^1\). Harmony eDelivery Access provides for you a free, productised and actively maintained open-source solution for joining eDelivery networks.

Firstly, so that you gain a broad understanding of how Harmony eDelivery Access will benefit your organisation, the role of eDelivery in Europe is introduced. Its features and benefits are described at a high level, supported by several use case examples. Then the eDelivery’s architecture, message exchange components, and trust and security enablers are introduced, amongst other aspects. After that basis for understanding the eDelivery concept, you are then introduced to the NIIS Harmony eDelivery Access product and its range of implementation alternatives, which emphasise eDelivery’s digital data exchange versatility.

eDelivery Digital Service Infrastructure (DSI) is one of the building blocks of the European Commission (EC) Connecting Europe Facility (CEF)\(^2\) that enables the exchange of data between networked organisations in an interoperable, reliable and secure manner. eDelivery is based on a distributed network model where every participant becomes a member of a network that applies standard protocols and policies, as simply depicted in figure 1. Constructing such organisational data exchange interconnectivity and interoperability both nationally and across borders continues to be a hot topic across the European Union (EU).

---

1 https://www.niis.org/
Figure 1. Variety of eDelivery cross-border solutions

The CEF building blocks are reusable software and services specifications that will support a wide variety of IT systems in various EU policy domains, for example in digitalised procurement, public services, justice, etc. Of the various CEF building blocks, the eDelivery building block helps public administrations throughout the EU to exchange data that can be structured, or non-structured, or binary, with other public administrations, businesses and citizens in a reliable and secure manner. Promotion of such a common eDelivery building block is a reliable and secure way to lower barriers for organisational onboarding\(^3\) and technical integration. eDelivery will speed up the rollout of digital public services that work within and across national borders in a cost efficient manner\(^4\).

The distributed nature of eDelivery facilitates direct data messaging exchange between organisations in an eDelivery policy domain without the need to set up bilateral channels. To do this, organisations connect to a technical access point which is based on common technical specifications and standards, e.g., open-source Domibus\(^5\) eDelivery access point implementation provided by the EC. This facilitates a flexible and fast way of integrating with any IT system backend of an organisation for reliable, secure and payload-agnostic exchange of data over the Internet. Each access point is an independent connection point within the distributed messaging network which is easily scalable and can accommodate thousands of access points. Furthermore, the use of a common protocol enables organisations to connect to one or

---

\(^3\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Stakeholders+onboarding](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Stakeholders+onboarding)

\(^4\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery)

more eDelivery-compliant access points to start exchanging data with other organisations in the same data exchange network, even when the organisations have differing backend IT systems. The eDelivery access point and associated components are explained in more detail in the section describing the eDelivery architecture.

The European Commission (EC) provides and maintains sample implementations of the eDelivery components, which are available as open source under the European Union Public Licence (EUPL) 1.2 licence. The EC’s sample implementations are the most widely supported. Harmony eDelivery Access is likewise based upon the sample implementations, as you will soon discover.

1. eDelivery

1.1. Role of eDelivery in Europe

The harmonising mission of the eDelivery DSI in Europe is clearly hinted at in the acronym CEF - it is about Connecting Europe. eDelivery enables Europe-wide interconnection of Member States’ public administrations with citizens (A2C and C2A) and with businesses (A2B and B2A) to reliably and securely exchange of any type of data across national borders. eDelivery's inclusive approach also presents opportunities in the eDelivery domain for service and software vendors to develop or upgrade their solutions to be conformant with the eDelivery technical specifications.

To promote widespread adoption of the eDelivery DSI across Europe, eDelivery applies the implementation guidelines as defined by the Member States in the electronic Simple European Networked Services (e-SENS) Large Scale Pilot. Hence, eDelivery is the default solution for cross-border data exchange in the EU. Also, CEF ultimately hopes for accelerated uptake and rollout of eDelivery amongst public and private entities not only in the EU but also more widely in the European Economic Area (EEA) countries.

It is important to note that there is no single way for how EU Member States connect to various eDelivery policy domains. Connections are for specific Pan-European projects within a given policy domain; for example, the eJustice domain, the eProcurement domain, and so on. Typically, eDelivery access points are uni-domain and uni-project and can be implemented at any administrative level; nationally, regionally, locally, or individually by organisations.

---

1.2. Use Cases

eDelivery can be utilised by domain-neutral use cases for the exchange of any type of data message. For example, the first use case in figure 8 refers to generic 'Message Exchange' instead of specific 'Invoices Exchange' or 'Claims Exchange'.

eDelivery can also be utilised by domain-specific use cases for specialisations of the 'Message Exchange' use case, such as exchange of invoices, public procurement documents, judicial claims, etc. as summarised\(^8\) in figure 2. This is how eDelivery is typically used.

Figure 2. Several eDelivery use cases

eDelivery is therefore an enabler of a wide variety of e-services that exchange either generic or specific types of data, with many success stories\(^9\), of which just several examples are as follows:

- **Estonia sets an example in e-invoicing**: A Nordic-Baltic cooperation applies CEF eDelivery and eInvoicing to achieve cost savings and efficiency in public sector electronic invoicing, as well as

---

\(^8\) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work

\(^9\) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Success+Stories
enhanced cross-border opportunities in the private sector. The consortium implemented standardised electronic invoicing with PEPPOL and by using specifications and technologies from the CEF eDelivery and eInvoicing building blocks.

- **Pan-European Public Procurement On-Line**: OpenPEPPOL is a non-profit association comprised of both public sector and private sector members. Its purpose is to enable European businesses to easily communicate electronically with any European public sector buyers in the business of procurement, thereby increasing opportunities for greater competition for government contracts and providing better value for tax payers’ money.

- **Electronic Exchange of Social Security Information**: EESSI is the system for exchanging social security-related data quickly and securely between social security authorities across the EU. For example, in Finland the authority owning and maintaining the Finnish access point for EESSI is KELA (Kansaneläkelaitos - the Social Insurance Institution of Finland) and over seventy Finnish Service Providers and Service Consumers representing employment, insurance, pension and other social services utilise the system for exchanging electronic data\(^\text{10}\).

- **eHDSI eDelivery Integration**: eHealth Digital Service Infrastructure enables cross-border healthcare services, with use cases such as Patient Summary providing access to health professionals to verify the health data of a patient during an unplanned care encounter while abroad, and ePrescription which enables patients to receive equivalent medication treatment while abroad to what they would receive in their home country.

\(^{10}\) [https://www.kela.fi/eessi](https://www.kela.fi/eessi)
1.3. Benefits

There are five main technical benefits derived from an eDelivery implementation:\footnote{https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Benefits+of+eDelivery}:

- **Interoperability**: Common technical specifications enable diverse organisations to exchange electronic data.
- **Security**: It promotes an atmosphere of trust and accountability among all participants in the data exchange network.
- **Reliability**: There is automatic recovery if transmission is unsuccessful due to temporary disruption.
- **Scalability and performance**: It enables the number of participants in the data exchange network to scale up, as well as the volume of exchanged messages, so there are no inherent limits on number of participants or messages.
- **Legal assurance and accountability**: It promotes a high level of transparency and confidence among all participants in the data exchange network.

There are also administrative benefits to becoming an eDelivery participant, as follows:

- **Vendor-neutrality**: The specifications are not proprietary and controlled by one vendor.
- **Multi-vendor**: Multiple products and solutions are available from different vendors.
- **eIDAS alignment**: The EU regulation for electronic IDentification, Authentication and trust Services for electronic transactions in the European Single Market enables trust.
- **Domain-independence**: It can be used in every policy domain of the EU.

On a more general level, an implemented eDelivery policy domain reduces risks, reduces costs, and improves quality for all involved organisations.
1.4. Features

1.4.1. TRUST ESTABLISHMENT

Digital trust establishment\(^{12}\) between communicating organisations ensures (a) all data exchanged between them is secured against unauthorised modification (integrity), (b) the data in transit between sender and receiver is encrypted (confidentiality), and (c) the origin and the destination of exchanged data and associated logs are verifiable (i.e. cannot be repudiated). To ensure end-to-end trustworthiness, organisations joining an eDelivery domain are required to go through an onboarding process. During this process, each organisation’s identity and access point is verified using unique organisational identifiers and digital certificates issued by a trusted Certification Authority (CA). You can consult CEF’s eDelivery Trust Models Guidance\(^{13}\) for further details.

![Figure 3. Trust establishment](image)

1. The sending Access Point signs the data, and it may also encrypt it.
2. The receiving Access Point verifies the digital signature and decrypts the data.

1.4.2. DYNAMIC SERVICE LOCATION

In order for a sending organisation to send a message to a receiving organisation, the sender must first discover where details about the receiver are stored. eDelivery's Dynamic Service Location\(^{14}\) enables the sender's access point to dynamically discover the internet protocol (IP) address of the receiver's access point. If the receiver's access point address changes, the new address will be automatically referenced by all other access points, so no manual changes are required.

---


\(^{13}\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Guidance+on+Digital+Certificates](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Guidance+on+Digital+Certificates)

\(^{14}\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Dynamic+Service+Location](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Dynamic+Service+Location)
To dynamically locate the receiver, the sender’s access point consults two components:

- the centralised registry of identifying information about receivers, known as a service metadata locator (SML), which enables the message sender to dynamically lookup and discover the receiver in the eDelivery network, and

- a decentralised registry of interoperability information about receivers, known as the service metadata publisher (SMP), which enables the message sender to retrieve the receiver’s messaging capabilities, which is described in the next section.

The SML and SMP components are explained in more detail in the eDelivery Architecture section. Dynamic service location is depicted simply in figure 4.

Figure 4. Dynamic Service Location

1.4.3. CAPABILITY LOOKUP

Capability lookup\textsuperscript{15} involves the sender querying the receiver’s message exchange capabilities. This is facilitated by the fact that every organisation’s SMP must be uniquely registered to the centralised SML with their IP address (physical address) and public web address (logical URL address). Once the sender discovers the address of the receiver’s SMP, the sender is now able to retrieve the receiver’s technical metadata. Metadata contains the receiver’s name and associated unique identifiers, amongst other details.

\textsuperscript{15} \url{https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Capability+Lookup}
Metadata dynamically sets the interoperability parameters between senders and receivers. Interoperability parameters include the business processes the receiver supports, their security setup (public key certificate), the supported transport protocol, and the location of the receiver's access point, amongst other details, as depicted simply in figure 5.

With such capability and interoperability information, the sender can now reliably send messages to the receiver.

Figure 5. Receiver capability lookup

### 1.4.4. MESSAGE EXCHANGE

Once the sending and receiving organisations are onboarded to the same eDelivery policy domain, and when the receiver location and capability lookups are performed, then reliable and trustworthy message exchange\(^{16}\) can be performed directly between the sender and receiver, as simply depicted in figure 6. Messaging confidentiality and integrity are based on secure end-to-end encryption, as described in the CEF’s Trust Model Guidance, and simplified as follows:

- The sending access point uses its digital certificate to sign the data message; it may also encrypt the data using the public key of the receiver.
- The receiving access point confirms the digital signature of the sender and decrypts the data using its digital certificate.
- The receiving access point sends a signed receipt message to the sending access point.

---

\(^{16}\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Message+exchange](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Message+exchange)
1.4.5. BACKEND INTEGRATION

An optional connector component can be utilised to further facilitate integration between a sender's backend system and their access point. The connector facilitates additional capabilities such as linking to legacy systems, advanced monitoring, and messaging evidences. Backend integration is depicted simply in figure 7.

**Figure 7. Connector facilitating integration between receiving backend system and access point**

Backend integration provides the following benefits:

- Interoperability

---

17 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Backend+Integration
- Security
- Scalability and performance
- Legal assurance and accountability
1.5. eDelivery Architecture

In this section we introduce more detail about the eDelivery architecture and about interactions between the already mentioned Access Point, Service Metadata Locator and Service Metadata components. The most typically implemented architectural model is the four-corner mesh network model\(^\text{18}\). In this model, participating organisations’ backend systems (C1 and C4) do not exchange data directly with each other but do so through their respective access points (C2 and C3), as depicted in figure 8. This message exchange model can be used by organisations acting as service consumers, service producers, or both. All that is required to be capable of communicating with each other is for their access points to be conformant to the same technical specifications. Consequently, sender A and receiver B can conveniently and securely exchange data even when their backend systems have been developed independently of each other.

![eDelivery 4-Corner model](https://slideplayer.com/slide/14667385/)

Figure 8. eDelivery 4-Corner model

\(^{18}\) [https://slideplayer.com/slide/14667385/]
1.5.1. MESSAGE EXCHANGE

Reliable and trustworthy message exchange is eDelivery’s core function. eDelivery supports asynchronous messaging of structured, non-structured, or binary data; this simply means that it is well suited for reliable, non-time-critical document and data exchange. Synchronous messaging is also possible but it requires additional connectors/plugins that are responsible for dealing with background asynchronous messaging.

eDelivery’s message exchange specifications are based on AS4 (Applicability Statement 4) OASIS and ebMS3.0 (electronic Business Messaging Services version 3.0) specifications\(^{19}\). AS4 is a web-based messaging protocol for securely exchanging electronic data between B2B organisations. The eDelivery AS4 Profile is an open specification for the secure and payload-agnostic exchange of data using web services. Table 1 summarises the features provided by the ebMS3 and AS4 specifications.

<table>
<thead>
<tr>
<th>Feature</th>
<th>ebMS3 and AS4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Messaging</td>
<td>Web Services</td>
</tr>
<tr>
<td>Internet Transport</td>
<td>HTTP 1.1</td>
</tr>
<tr>
<td>Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)</td>
<td>Transport Layer (SSL / TLS) Security</td>
</tr>
<tr>
<td>Message and Payload Packaging</td>
<td>SOAP 1.2 with attachments</td>
</tr>
<tr>
<td>Routing and Dispatching, SOA integration</td>
<td>Mandatory &quot;Service&quot; and &quot;Action&quot; header elements</td>
</tr>
<tr>
<td>Exchange Pattern</td>
<td>One Way or Two Way (*)</td>
</tr>
<tr>
<td>Exchange Pattern Bindings</td>
<td>Push, Pull and Sync (*)</td>
</tr>
<tr>
<td>Payload Compression</td>
<td>Gzip (**)</td>
</tr>
<tr>
<td>Message Identification</td>
<td>ebMS 3.0 &quot;MessageId&quot;</td>
</tr>
<tr>
<td>Message Correlation</td>
<td>ebMS 3.0 &quot;RefToMessageId&quot; and &quot;ConversationId&quot;</td>
</tr>
<tr>
<td>Message Timestamp</td>
<td>ebMS 3.0 &quot;Timestamp&quot; and WS-Security &quot;Timestamp&quot;</td>
</tr>
</tbody>
</table>

\(^{19}\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4++1.15](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4++1.15)
<table>
<thead>
<tr>
<th>Feature</th>
<th>ebMS3 and AS4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Repudiation of Origin</td>
<td>WS-Security 1.1 using XML Signature</td>
</tr>
<tr>
<td>Message Confidentiality</td>
<td>WS-Security 1.1 using XML Encryption</td>
</tr>
<tr>
<td>Non-Repudiation of Receipt</td>
<td>Signed Receipt Signal Message</td>
</tr>
<tr>
<td>Reliable Messaging</td>
<td>AS4 reception awareness feature for lightweight, interoperable reliable messaging (**)</td>
</tr>
</tbody>
</table>

Table 1. ebMS3/AS4 Functional Overview, (*) in ebMS3, not in AS4 (**) AS4 extension to ebMS3

The eDelivery AS4 Profile guarantees once and only once delivery of messages due to the exchange of receipts and other verification requirements for both the sender and receiver. In addition, the AS4 Profile supports two-way Message Exchange Patterns (MEP) with Push-and-Push and one-way MEP with Push because it is based on an extended subset of the AS4 ebHandler Conformance Profile.

1.4.2. COMPONENTS

The eDelivery architecture\(^\text{20}\) consists of the core technical components in Table 2.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point (AP)</td>
<td>A technical access point that implements the AS4 message exchange protocol according to the CEF eDelivery AS4 profile. The access point is the backend system's connection point to the eDelivery network and has two interfaces:</td>
</tr>
<tr>
<td></td>
<td>1. An interface to connect the backend system with the access point: typically, this interface is customisable as communication between access points and backend systems may use any messaging or transport protocol.</td>
</tr>
<tr>
<td></td>
<td>2. A standard messaging interface between access points: this interface is configurable according to the options of the profiles supported by CEF eDelivery. It is important to note that CEF eDelivery is</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>standardises only the communication between the sender's and receiver's access points.</td>
</tr>
<tr>
<td></td>
<td>Access points are not operated centrally, rather they are deployed independently by public authorities and businesses in a distributed manner. An organisation may decide to not operate its access point, but instead use a third-party service provider to host it for them.</td>
</tr>
<tr>
<td></td>
<td>Represents organisational IT systems that exchange data through the eDelivery network. Backend systems can be service providers and/or service consumers.</td>
</tr>
<tr>
<td></td>
<td>An optional component used to facilitate the integration between the backend systems and access points. When present, the connector is responsible for mapping from the backend's internal data format to eDelivery's internal data format. The communication and the mapping of the data can be done in both directions.</td>
</tr>
<tr>
<td></td>
<td>The centralised registration system that is responsible for Dynamic Service Location: in order to send a message, the access point of a sender needs to discover where the information about a receiver is stored.</td>
</tr>
<tr>
<td></td>
<td>A register of the location and message exchange capabilities of receivers. Organisations that only send data do not require to be registered in an SMP, only an access point is sufficient, whereas an SMP is necessary for an organisation to receive data when dynamic discovery is used.</td>
</tr>
<tr>
<td></td>
<td>The 'Internet phonebook' stores unique hostnames of eDelivery receivers as DNS records and converts hostnames into unique IP addresses. Each DNS record refers to the lookup information of the receiver's SMP. This service enables the sender's AP to dynamically locate the SMP holding the receiver's metadata.</td>
</tr>
</tbody>
</table>
Table 2. eDelivery DSI components

Supporting a full eDelivery policy domain deployment with all the various roles requires all three components: Access Point, SMP and SML. However, a minimal viable policy domain can also be deployed without the SMP and the SML. In the most basic setup, it is sufficient for organisations to only have an access point, but this very limited implementation doesn't scale up very well.

The digital certificates required by the eDelivery components may be self-signed or issued by a CA. In the latter case, a PKI service is required for issuing certificates. It is strongly recommended to use a PKI service rather than self-signed certificates in eDelivery production environments.

The three primary eDelivery components - Access Point, SMP and SML - are further described in the following sections.

1.4.3. ACCESS POINT

An AS4-compliant access point\(^\text{21}\) securely enables payload-agnostic data exchange between sending and receiving eDelivery access points. Therefore, in order to exchange information, organisations must install an access point or utilise an access point hosted by a service provider on their behalf.

Key aspects of an AS4-compliant access point are as follows:

- Support for SOAP 1.1 and 1.2 enveloping structure
- Payload agnosticism
- Support for single or multiple payloads contained either within the SOAP body or as SOAP attachment(s)
- Support for payload compression

\(^{21}\) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4++1.15
• Support for message-level security including various combinations of XML Digital Signature and/or XML Encryption
• Support for X.509 security tokens and username/password tokens
• Support for business receipt of non-repudiation similar to the Message Disposition Notification (MDN) used by AS2 and specified as an XML schema by the ebXML BPSS group
• Support for the ebMS 3.0 One-Way/Push message exchange pattern with support for either synchronous or asynchronous responses
• Support for the ebMS 3.0 One-Way/Pull message exchange pattern which is beneficial for exchanging documents with non-addressable endpoints

Setting up an access point involves:

• Installing the access point software in a production environment (server, network, storage, etc.)
• Integrating the sending entity’s access point connector to the backend
• Confirming the sending entity’s access point connectivity to the SMP of the receiving entity’s access point

1.5.4. SERVICE METADATA LOCATOR

The Service Metadata Locator (SML) component uses DNS lookups to find a participant’s information in the data exchange network. This approach does not require just a single central server to run the discovery interface (with its associated single point of failure). Instead, utilising the global DNS system makes it highly resilient. At runtime, the SML utilises the DNS for load balancing of requests. And since CEF eDelivery interfaces with the global DNS system, the SML can virtually operate 24/7/365. In case of failure, organisations would still be able to discover each other based on the information stored on the DNS.

1.5.5 SERVICE METADATA PUBLISHER

The Service Metadata Publisher (SMP) component is an implementation of the CEF eDelivery SMP profile developed by e-SENS and now maintained by the CEF. Typically, an SMP is provided to

complement an access point, but an SMP can also be hosted on behalf of an organisation by a service provider.

Setting up an SMP involves:

- Installing the software in a production environment (server, network, storage, etc.)
-Confirming the sending entities’ access points connectivity
- Testing connectivity to the policy domain’s SML where the SMP is connected
1.6. Discovery Models

A discovery model defines how the technical routing and communication capability information of eDelivery network's participants is maintained and distributed. eDelivery supports two discovery models: static and dynamic. The SML and SMP Component Offering Description 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.

1.6.1. STATIC DISCOVERY MODEL

In the static model, the sending access point is required to have the information on the receiver statically available, including the lookup address and the communication capabilities. Hence, in the static model the access point stores a list with static information related to all the other access points (e.g., IP address, etc). To send a message, the sending access point looks at this static list to locate the access point of the receiver (usually configured in a local configuration file).

Static discovery has the advantage that there is no overhead processing. However, there are several disadvantages. The receiver information must be configured manually by the access point administrator. Then it must also be exchanged through some external channel, for example, via email.

1.6.2. DYNAMIC DISCOVERY MODEL

In the dynamic model, the sending organisation's access point dynamically obtains details about receiving organisation. This enables the sender to discover the address of the receiver's SMP and retrieve their service metadata and service capabilities, which includes the followings:

- The receiving access point lookup information (e.g. IP address, URL, transport protocol)
- The communication protocol
- 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)

---

Having acquired this information, the sender can then send the message to the receiver.
1.7. Message Sending

When dynamic discovery is used, eDelivery message sending follows the five steps below and is depicted in figure 9:

1. **Submit**: The sender uses their backend system to create a message to be sent to a receiver. At this stage, the sender knows the unique identifier of the receiver (e.g. a company VAT number) and the content of the data that is intended to be sent to the receiver. After the message is created, the backend system submits it to its access point.

2. **DNS lookup**: The sending access point converts the message to the AS4 format and builds a canonical representation of the receiver's identifier by hashing it. The sender’s access point uses this canonical representation to perform a DNS lookup and obtains the URL of the SMP publishing the receiver's metadata.

3. **Retrieve metadata**: The sending access point then retrieves the receiver's metadata that includes all necessary information for the sender's access point to send the message to the receiver's access point.

4. **Send**: The sender's access point sends the message to the receiver's access point in accordance with the receiver's metadata.

5. **Deliver**: The sender's message is delivered to the receiver's access point and from there to the receiver's backend.

---

26 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Message+exchange
Figure 9. Message exchange in the eDelivery four corner model
1.8. Trust and Security

1.8.1. TRUST MODEL

A trust model is a collection of rules that ensure the legitimacy of the digital certificates used by the CEF eDelivery components. Digital certificates enable the identification of the organisations using eDelivery and are instrumental for the authenticity, confidentiality, integrity and non-repudiation of the exchanged data. A variety of trust models\(^{27}\) is possible based on various trust anchor models and rules to create, manage, distribute, store and revoke digital certificates.

eDelivery supports four trust models, as follows:

- **Dedicated Domain PKI**: Digital certificates are associated to a single trust anchor that serves a single policy domain, i.e. it is a dedicated anchor.

- **Shared Domain PKI**: Digital certificates are associated to a single trust anchor that serves multiple policy domains, i.e. it is a shared anchor.

- **Mutual exchange**: Relies on digital certificates from different trust anchors, and since there is no single trust anchor, organisations use the trust anchor of their choice (typically, according a set of well-defined criteria).

- **Domain trusted lists**: Relies on a list containing the trusted certificates and/or trust anchors complying with a common domain policy and organisations are free to choose their preferred trust anchor from that list.

1.8.2. SECURITY REQUIREMENTS

eDelivery’s security requirements are derived from the European Unions’ eIDAS (electronic IDentification, Authentication and trust Services) Regulation which stipulates at least the following security requirements\(^{28}\) for trust-based services:

- **Message Integrity**: Messages should be secured against any modification during transmission.

- **Message Confidentiality**: Messages should be encrypted during transmission.

- **Sender Identification**: Sender identity should be verified.

---


• **Receiver Identification**: Receiver identity should be verified before the delivery of the message.

• **Time-Reference**: The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp (audit log).

• **Proof of Send/Receive**: Sender and receiver of the message should be provided with evidence of message sending and receiving (non-repudiation).

### 1.8.3. SECURITY CONTROLS

eDelivery’s security controls\(^29\) are also derived from the eIDAS regulation which stipulates at least the following security controls for trust-based services:

• **Transport Layer Security (TLS) + Authentication**: TLS ensures the authenticity and integrity of messages.

• **Message Encryption**: Message encryption ensures confidentiality of the message payload so that only the correct receiver can access it.

• **Electronic Seal of message**: Sealing ensures integrity of the message header and payload and authenticity of origin.

• **Electronic Seal of evidence**: Applies an electronic seal to the receipt of a message, which guarantees the receiver received ‘that’ message.

• **Electronic Timestamp**: Binds accurate date and time to the exchanged data in such a way that there is no possibility to alter messaging dates and times undetectably.

Figure 10 summaries how all of the above-introduced security and trust requirements map to the eDelivery core components to facilitate reliable and trustworthy data exchange between sending and receiving organisations\(^30\).

---


\(^30\) [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2016/09/21/Towards+the+Digital+Single+Market%3A+Demonstrating+the+alignment+between+CEF+eDelivery+and+eIDAS%28Q%29ERDS](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2016/09/21/Towards+the+Digital+Single+Market%3A+Demonstrating+the+alignment+between+CEF+eDelivery+and+eIDAS%28Q%29ERDS)
Figure 10. Mapping of security requirements to the 4-Corner Model
1.9. Roles and Responsibilities

eDelivery can be used in administration to administration (A2A), administration to business (A2B), and business to administration (B2A) scenarios that are either policy domain-neutral or policy domain-specific implementations. When behind a web-portal, eDelivery can also enable the interconnection of public administrations and citizens (A2C and C2A). The commonality in all of these scenarios is that there are basically just two main roles; the domain owner and participating organisations. This means eDelivery can be adapted for almost any kind of organisational structure. The following sections explain the various roles in more detail.

1.9.1. POLICY DOMAIN AUTHORITY

An eDelivery Network requires a number of actors to work together in a trusted environment. To achieve this, two levels of governance are required.

Firstly, the Policy Domain Authority has authority over all of the central components of the domain’s network, meaning the technical and service specifications, the centralised SML, and the Transport Infrastructure Agreements and its annexes. The Policy Domain Authority can implement and operate all of this in-house, or optionally, may outsource the practical implementation and technical operation of the central components to a hosting provider.

Secondly, the Policy Domain must then ensure that access point and SMP services are provided in conformance to the technical standards and service specifications by entering into separate access point and SMP agreements with each of the respective participants within their domain, as part of their eDelivery onboarding process. These participants may also have the option of signing the access point and SMP agreements with the Policy Domain Authority directly, or with a commercial service provider who provides the access point and SMP as a hosted service.

1.9.2. PARTICIPANTS

Participants are organisations that are members of an eDelivery policy domain. Participants may have one or more eDelivery roles and a single organisation can have multiple roles simultaneously. Key participants are described in the following sections.

---

31 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Who+is+eDelivery+for
1.9.3. HOSTING PROVIDERS

The Policy Domain Authority has the option of outsourcing the practical implementation and technical operation of the central components to a hosting provider that hosts the access points and SMPs on behalf of the authority. Hosting providers may also host access points and SMPs on behalf of service providers and service consumers.

1.9.4. SERVICE PROVIDERS

Service providers publish their business services to the eDelivery policy domain in which they participate. There can be public sector and private sector service providers.

1.9.5. SERVICE CONSUMERS

Service consumers consume the data exchange services facilitated by the eDelivery policy domain in which they participate. There can be public sector and private sector service consumers.
1.10. Hosting alternatives

eDelivery access points are typically deployed by public authorities or businesses in a distributed manner. Alternatively, participating organisations may decide to contractually outsource the hosting of their access point and SMP to commercial service providers. Such third-party service provision is enabled by CEF eDelivery’s implementation guidelines, connectivity testing services, and conformance testing services for service providers. eDelivery service providers can offer a broad range of ancillary hosting services to organisational customers, such as cloud hosting, participant management, service desk, training, continuous monitoring and maintenance, and multi-tenancy.
2. Harmony eDelivery Access

Up to this point, you have been introduced at a reasonably high level to the overall eDelivery DSI concept. You also have pointers to referenced resources where you will find further in-depth descriptions and technical details. Hopefully already with this level of detail, you can start making informed decisions about the deployment model that best fits the requirements of your organisation.

In that regard, we introduce the NIIS Harmony eDelivery Access product as your most appropriate starting point for your eDelivery experience. NIIS is a non-profit association with the mission to ensure the development and strategic management of national and cross-border components for digital government infrastructure. Harmony eDelivery Access by NIIS is a free and actively maintained open-source component by NIIS for joining one or more eDelivery policy domains.

Harmony eDelivery Access assumes the most typically implemented four-corner network model whereby the organisations’ backend systems do not exchange data directly with each other, but do so through their respective access points. A variety of Harmony eDelivery Access configurations is also possible; a single access point can serve a single organisation (single tenancy), or the access point can serve several organisations and may be connected to one or more policy domains (multi-tenancy).

Harmony eDelivery Access provides a unified technology stack, an automated installation and upgrade process for selected platforms, and step-by-step installation and upgrade instructions. The security of Harmony eDelivery Access is assured by a third-party security assessment. When implemented, Harmony eDelivery Access enables you to exchange data in a standardised, reliable, secure, and trusted manner in the implementation model appropriate for your organisational needs.

Harmony eDelivery Access scope comprises just two components; the access point based upon the Domibus Open Source project\(^ {32}\) and the SMP\(^ {33}\). Harmony eDelivery Access supports both data exchange senders and receivers with the minimum viable implementation that requires only the sender’s and receiver's access points. Even with just these two components, there are multiple ways you can deploy them, as described in the implementation models section. Also, the access point comes with a default web service plugin that is used for backend integrations; however, in general a use case specific plugin is required.

2.1. Implementation Models

Harmony eDelivery Access facilitates the exchange of digitalised data between public administrations, private businesses and citizens, at national level and across borders, in an interoperable, secure and

\(^{32}\) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

\(^{33}\) https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP
reliable way. There are various implementation models that can facilitate this, and each has its pros and cons, as presented in the next sections. The implementation models are based on the decentralised four corner (mesh network) model whereby Harmony eDelivery Access participants can utilise an access point, a SMP, and the dynamic discovery model to interact reliably and securely with other domain participants. It is important to recognise that, in all implementation models, the infrastructure is only a means to achieve connectivity; standardised data exchange interoperability between participants is the ultimate goal.

The implementation models presented in the following sections are based on the technical capabilities of Harmony eDelivery Access. Technically, all the documented models can be implemented using Harmony. However, some eDelivery policy domains may have requirements and restrictions that make some of the models unsuitable for them. Therefore, it’s always recommended to consult with the Policy Domain Authority before deciding which model to implement.

2.1.1. NATIONAL ACCESS POINT

In the national eDelivery access point model, the National Authority of an EU Member State implements and maintains a single centrally-managed AS4-compliant access point, and if required, also a national SMP. In other words, the National Authority is both a participant and a service provider in one or more eDelivery policy domains. Potentially, the National Authority can also be a software provider if they decide to implement their own access point software and/or plugins for specific eDelivery policy domains.

The National eDelivery access point may be registered to multiple existing cross-border policy domains, such as PEPPOL[^34], EESSI[^35], Business Registers Interconnection System (BRIS)[^36], and the Single Digital Gateway (SDG)[^37], etc., as depicted in figure 10. This means that organisations that want to join an existing policy domain can utilise the national access point instead of having to set up their own private access point. This approach is also easily scalable since it can accommodate many participating organisations.

[^34]: https://peppol.eu/what-is-peppol/peppol-transport-infrastructure/
Figure 10. eDelivery national interoperability

A single national access point is an efficient solution because it is sufficient to setup, maintain and operate only one access point on a national level. Since high availability is a common requirement in production environments, the national access point should be run using a high availability setup. Also, policy domain specific connectors and/or plugins may be set up on a national level. However, the feasibility of using a national connector may vary between policy domains, therefore feasibility should be evaluated case by case. Overall, the national access point reduces the amount of infrastructure and the effort that is required on a national level to maintain and operate it.

The national access point is most likely connected to multiple policy domains that all have their own processes and operating models. Then a variety of organisations and information systems need to be able to connect to it. Therefore, connecting the same access point to multiple policy domains may require going through several, potentially quite different, onboarding processes. Also, a national access point must ensure continuous high availability and resilience against denial-of-service situations.

A potential downside of a single national access point is that operating it may become very complex. Managing all the organisational certificates and keys means additional work and complexity in operating the national access point. Also, the fact that the information systems that are connected to the national access point most likely run in different networks and data centers, which then requires some special
attention since all the connections between different components must be properly secured. Another disadvantage of this model is that it can be a single point of failure.

If for some reason a country wants to set up more than one national access point and SMP, that is also possible. However, that increases maintenance overhead and overall complexity, but on the other hand it also reduces the complexity of individual national access points.

2.1.1.1. Stakeholders in the national model

Stakeholders and their responsibilities in the national eDelivery access point model are:

- **Member State**: Mandates the establishment of the national access point.
- **National Authority**: Implements and maintains the national access point.
- **Service Providers**: Public sector and private sector organisations that publish services to some eDelivery policy domain.
- **Service Consumers**: Public sector and private sector organisations that consume services from some eDelivery policy domain.

2.1.1.2 Joining the Single Digital Gateway with a national access point

The Single Digital Gateway Regulation (SDGR)\(^{38}\) is an EU regulation stipulating that certain services must be fully digitally available for cross-border traffic within the EU. To meet this SDGR obligation (specifically Article 14), the EC and EU members states are building a system that will facilitate the Once Only Principle (OOP)\(^{39}\) whereby EU citizens, public services and businesses will exchange digital data only once to one authority/eDelivery instance, as depicted in figure 11. OOP will enable EU member state authorities to share data with their counterparts in other Member States in real-time and in accordance with data privacy regulations such as the General Data Protection Regulation (GDPR)\(^{40}\).

---


\(^{40}\) [https://gdpr.eu/](https://gdpr.eu/)
Figure 11. Single Digital Gateway structure

eDelivery is used as the data exchange solution in the OOP technical system. It means that each member state needs to connect to the OOP technical system using one or more eDelivery access point(s). The member states are free to decide how the connection is implemented; there may be just one national access point per member state, or multiple organisation-specific access points, or something in between. Each member state can make its own decision based on its requirements and existing national data exchange infrastructure.

Implementing the connection using a national access point means that multiple organisations do not need to setup and maintain their own access points. In addition, a single party is responsible for operating the national access point at the member state level. Overall, the national access point approach is more efficient compared to other more complex alternatives.

2.2.1. POLICY DOMAIN SPECIFIC MODEL

In the policy domain specific model, a single organisation within an EU Member State maintains a policy domain specific access point and all other organisations requiring access to that specific domain may use that access point, as simply depicted in figure 12. In this scenario, the organisation owning and maintaining the access point acts as a domain hosting provider for the other organisations. If required by the policy domain, the organisation maintaining the access point could also maintain the SMP. The policy domain specific model can be used in multiple existing eDelivery policy domains, for example, in PEPPOL and in EESSI that were introduced in the use cases section.
In this policy domain specific setup, every organisation doesn’t have to setup and maintain its own access point; rather there is just one access point per policy domain. Organisation identities are policy domain specific, therefore if an organisation is a member of multiple policy domains, it must have a separate identity with a related digital certificate and key for each policy domain.

How organisations are connected to a policy domain also affects the overall complexity. In some policy domains, it may be possible to use a single, shared identity that is used to represent multiple organisations. That single shared identity could be provided by the access point owner, whereby organisations in that policy domain would consume/provide services using the access point owner’s identity. However, this kind of approach may not be possible in all policy domains, and in that case, each organisation must join a specific policy domain using its own unique identity.

A potential downside of the policy domain specific model is that operating the shared access point is likely to be complicated since different organisations and information systems need to be able to access it.
2.2.1.1. Stakeholders in the policy domain specific model

Stakeholders and their responsibilities in the policy domain specific model are:

- **Authorities**: government organisations that drive, for example, PEPPOL or EESSI adoption
- **Hosting Providers**: host access points and SMPs on behalf of participating organisations
- **Service Providers**: publish their domain-specific services to the eDelivery policy domain
- **Service Consumers**: consume the policy domain data exchange services

2.3.1. ORGANISATION SPECIFIC MODEL

In the organisation specific model, each organisation has its own access point, and optionally its own SMP. The organisation specific access point and SMP can also be hosted by a commercial service provider. The centralised SML is hosted by the eDelivery policy domain owner.

![Figure 13. Organisation specific model](image-url)
There are certain benefits to the organisation specific model. Every organisation has its own access point and optionally an SMP, enabling them to exchange point-to-point data with other organisations. Organisations are in control of their own access point and SMP and are not relying on a third party for availability and quality of service. Management and maintenance of the organisation is also simpler since it is a single tenant setup.

A downside of the organisation specific model is that operating its own access point, and optionally its own SMP, necessitates the appropriate knowledge, resources and maintenance capability within the organisation. Also, the organisation will have to resolve any technical failures more or less on its own.

Overall, in comparison to the national access point approach, a lot more resources are required to setup, maintain and operate multiple organisation specific access points. Even if operating a single access point is less complicated, the overall overhead on a national level can potentially be very significant depending on the number the organisation specific access points.

2.3.1.1. Stakeholders in the organisation specific model

Stakeholders and their responsibilities in the organisation specific model are:

- **Organisations**: participants in the eDelivery policy domain
- **Hosting Providers**: host access points and SMPs on behalf of participating organisations
- **Service Providers**: enable the exchange of transactions
- **Service Consumers**: send and receive transactions
2.4. Start Now with Harmony eDelivery Access

You should by now have a broad understanding of how eDelivery functions and how it will benefit your organisation not only for the exchange of data across national borders, but also how it can link up different regions, municipalities, etc. across EU Member States. To summarise the benefits eDelivery affords your organisation; it enables paperless data exchange between eDelivery participants using standardised messaging protocols other than e-mail, it ensures the integrity and confidentiality of exchanged data with non-repudiation evidences that are legally valid, and the data exchange network is easily scalable in terms of access points and messaging loads. The sum of all these benefits is that eDelivery reduces risks, reduces costs, and improves quality.

An excellent starting point for your organisation to reap all of these benefits is with the NIIS Harmony eDelivery Access product. NIIS Harmony eDelivery Access provides you with free and actively maintained open-source components for joining one or more eDelivery policy domains. Technically, this solution includes both an eDelivery access point and SMP. Inbuilt versatility means you can utilise Harmony eDelivery Access as a service consumer, or a service producer, or both. Guiding documentation is available at the Harmony eDelivery Access product website41.

41 https://edelivery.digital/