Basic function *Addressing actors*

Introduction
Description
- Data model for an address
  - Participant identifier
  - Catalog identifier
  - Resource identifier
- Contact list management
- Public directory management
  - SMP SML as described in eIDAS

Applicability
Agreements
- Data format requirements for addresses
- Functional requirements for using addresses
- Requirements for publishing addresses
- Requirements for discovering addresses

Standards
Best practices
Suppliers
Administrators
Regulators
Costs
Open issues
- 01 Applicability of Decentralized Identifiers (DIDs)
- 02 Centralised versus federative addressing

Introduction

This document describes the basic function *Addressing actors* of the *TIP ecosystem*. Words printed in italic refer to definitions described in the document Basic functions and definitions for the *TIP ecosystem*.

> **Note**
>
> This document is published for consultation purposes and can be updated to a 1.0 version after implementation by Trusted Information Partners. **Comments on this document are appreciated via a message on our LinkedIn account.**

> **Note**
>
> At the moment of writing, this basic function is not yet included in the overview of basic functions. It can be considered part of *Exchanging data*, which is included in the overview.

Description

The basic function *Addressing actors* enables an *Actor* to discover, identify and record the online address of another *Actor*, given prior knowledge of their identity attributes. It also enables an *Actor* to manage multiple addresses and communicate an address change in an interoperable way. This function enables *Delivering messages*, or "delivery" in short.

The following features are out of scope for this basic function:

- Maintaining basic registrations of *Actors*.
- Addressing trust and other infrastructure services within an *Acting space*.
- Discovery of delivery provider addresses within a delivery network.
- Discovery of website or web-based API addresses.
- Discovery of public keys associated with addresses for end-to-end encryption.

We expect that in 2025, standards will be selected for interoperability within qualified electronic registered delivery providers, given Recital (52) of the (EU) 2024/1183 eIDAS amendment:

> Providers of qualified electronic registered delivery services should be encouraged by Member States to make their services interoperable with qualified electronic registered delivery services provided by other qualified trust service providers in order to easily transfer electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.

And Article 44(2a) and (2b):

> 2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. [...]
>
> 2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article.

For now, the identifier for natural persons is out of scope of this document while the discussion is still continuing.

Data model for an address

The following table describes the data model of an address. It describes which components constitute an address, specified with levels. The description of the components are given below the table.

Level	Component	Example
+	Address	`iso6523-actorid-upis::0007:2021005448/urn:oasis:names:specification:ubl:schema:xsd:Order-2::Order##UBL-2.0`
++	Participant identifier	`iso6523-actorid-upis::0007:2021005448`
+++	Catalog identifier	`iso6523-actorid-upis`
+++	Participant scheme identifier	`0007`
+++	Participant identifier value	`2021005448`
++	Resource identifier	`urn:oasis:names:specification:ubl:schema:xsd:Order-2::Order##UBL-2.0`
+++	Resource scheme identifier	`urn:oasis:names:specification:ubl:schema:xsd:Order-2`
+++	Resource type identifier	`Order`
+++	Resource subtype identifier	`UBL-2.0`

Participant identifier

Address within a delivery network. For example: `iso6523-actorid-upis::0007:2021005448` to indicate the Swedish Tax Authority as a participant identifier.

Typically a delivery network includes a fully qualified domain name (FQDN) directly in the address, or standardises metadata registration that enables finding an associated FQDN. Typically a delivery network applies the Domain Name System (DNS, RFC 1034) to resolve a FQDN to an Internet Protocol address (IPv4, RFC 791, or IPv6, RFC 8200). Some delivery networks require the use of DNS Security Extensions (DNSSEC, RFC 4033) to protect integrity of DNS records.

Catalog identifier

Within a delivery network, an address is typically structured hierarchically. For example, a network may segment its addresses into various registries, such as a value-added tax number registry (e.g. `NL:VAT` or `9944`), a chamber of commerce registry (e.g. `NL:KVK` or `0106`), or an organisation identifier registry (e.g. `NL:OIN` or `0190`). The second component of an address would then contain the registry identifier and an identifier of the *Actor* as registered within this registry.

For example, the Swedish Tax Authority may be identified with:

`iso6523-actorid-upis::0007:2021005448`

In this example, `iso6523-actorid-upis` identifies a scheme, `0007` identifies the Swedish organisation registry within that scheme (“organisationsnummer” or `SE:ORGNR`), and `2021005448` identifies the authority within that scheme.

Resource identifier

Depending on the delivery network design, the second component of an address may include a resource identifier. This could for example identify a specific delivery agent deployed by the *Actor*, or a specific context to group messages. Example contexts could be “finance” or “health”, or an organisation department or other sub-structure. The *Service or chain specifications* can promote harmonisation of such context identifiers.

Contact list management

An *Actor* can manage one or more contact lists, assigning locally meaningful identifiers to the identity attributes and/or addresses of other *Actors*.

Public directory management

A governing authority may manage, or delegate management of, one or more public directories. These directories enable discovery of addresses and their metadata, either by listing the data directly, or by providing locators to other resources that enable discovery of the data. Note that publishing a directory requires special attention to the addresses of natural persons, as these need to be protected as personal data. For organisations and some professions, the identifiers may be public information, which makes it easier to design a public directory.

SMP SML as described in eIDAS

Service Metadata Locator (SML) and Service Metadata Publisher (SMP) are core components of the eDelivery Building Block, which supports secure and interoperable electronic data and document exchange across the EU, as mandated by the eIDAS Regulation.

Service Metadata Locator (SML)

The SML acts as a centralized directory in the eDelivery infrastructure.

Its main purpose is to manage and store resource records of participants (such as public administrations, businesses, or service providers) and their associated SMPs in the Domain Name System (DNS).

When a sending party (Access Point) needs to communicate with a receiving party, the SML guides the sender to the correct SMP by resolving the unique identifier of the recipient to the corresponding SMP's address.

The SML enables dynamic discovery of where the metadata about a recipient is stored, making the network flexible and scalable for cross-border transactions as required by eIDAS.

Service Metadata Publisher (SMP)

The SMP is a distributed registry that holds detailed metadata about each participant's messaging capabilities.

Once the address of the SMP is located via the SML, the sending party can retrieve all necessary information to interoperate with the recipient. This includes:

- Endpoint information (e.g., URL, transport protocol)
- Supported business processes and document types
- Security credentials (e.g., public keys)
- Communication protocols and any additional requirements for message exchange.

The SMP ensures that the sending party has all technical and business information needed for secure and trusted message delivery, in line with eIDAS goals of interoperability and trust.

Role in the eIDAS Regulation Context

The eIDAS Regulation aims to create a secure, interoperable, and trusted environment for electronic transactions and identification across EU member states.

SML and SMP directly support these aims by:

- Enabling dynamic and automated discovery of participants and their capabilities, which is essential for seamless cross-border eDelivery.
- Facilitating interoperability between different national systems and service providers, as required by the regulation.
- Supporting the registration, location, and capability lookup of entities involved in electronic transactions, thus ensuring trust and efficiency in digital interactions.

Summary Table

Component	Main Purpose	How It Supports eIDAS
SML	Centralized directory for locating SMPs via DNS	Enables dynamic discovery of participant metadata, supporting interoperability and scalability
SMP	Distributed registry of participant capabilities and endpoints	Provides all technical/business info for secure, trusted cross-border message exchange

In summary, SML and SMP are foundational for the dynamic, secure, and interoperable exchange of electronic data and documents across borders as envisioned by the eIDAS Regulation

Applicability

The basic function *Addressing actors* is mandatory whenever an *Actor* needs to identify another *Actor* for the purpose of *Delivering messages*. This enables interoperability and reuse of generic infrastructure across vendors, technologies and sectors.

Agreements

TIP agrees on the following requirements regarding implementation of *Addressing actors*.

Data format requirements for addresses

An address SHOULD target a recipient, not their delivery provider.

An address SHOULD enable resilience in the ecosystem. Such a requirement will be posed by organisations for which their continuous digital presence is of the utmost importance. One such solution could be utilizing multiple delivery providers at the same time.

An address format SHOULD enable targeting a specific *Actor* resource. See Addressing *Actor* resources for use cases.

An address format SHOULD allow for extensibility towards identification schemes beyond EU initiatives. This should allow for interoperability with entities outside the EU. Potential foreign schemes can be national solutions outside the EU or international solutions such as vLEI.

Functional requirements for using addresses

An implementation SHOULD enable an *Actor* to specify where and how they are digitally available.

An implementation SHOULD allow for easy and trustworthy search of *Actors* for generic and specific exchange purposes. A public directory could allow for this.

An implementation SHOULD allow for entities to not expose their presence and addresses in public directories.

An implementation SHOULD NOT expose delivery provider selection or customer base.

Requirements for publishing addresses

An implementation SHOULD enable an *Actor* or an authorized person to manage its publications in the public directory.

The SML MUST be highly available.

The SMP MUST be protected with a qualified electronic seal as specified under *Signing data*.

Requirements for discovering addresses

A public directory MUST ensure integrity of the address and its metadata.

Standards

The Component Offering Description of the SML & SMP Building Block: SML And SMP

Chapter 5 & 6 of EN 319 522-4-3 v1.1.1 references OASIS Business Document Exchange (BDXR) standards for:

- SMP: https://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html
- SML: https://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html

Best practices

Peppol or other eDelivery implementations are inspiring examples to solve the addressing issues.

Suppliers

As stipulated in eIDAS, qualified trust services are provided by qualified trust service providers (Qualified Trust Service Providers or QTSPs). See the EU Trusted List Browser for an overview of QTSPs.

Administrators

For Service Metadata Locator (SML) resolution, we utilize the `brz.publisher.edelivery.tech.ec.europa.eu service`, operated by the European Commission's Directorate-General for Informatics (DIGIT), which is also used by Peppol.

For Service Metadata Publishers (SMPs), the publisher is a qualified trust service provider (QTSP) for qualified electronic registered delivery services. These can be found on the EU trusted lists. The QTSP could use a subcontractor for SMP services, but is still accountable for meeting the TIP requirements.

Addressing requires central management for TIP at least to maintain or delegate a list of recognized and/or connected QERDS providers and possibly also common infrastructure.

Regulators

As stipulated in eIDAS article 17, each EU member state is responsible for appointing a supervisory body that ensures that qualified trust service providers comply with the requirements set out in the eIDAS regulation. Rijksinspectie Digitale Infrastuctuur (RDI) is the Dutch supervisory body for QTSPs under the PKI-Overheid scheme.

Costs

Pricing for the use of the basic function are established on the basis of bilateral agreements between network providers and *Actors* who use this functionality via *Acting spaces*. There must be a party responsible for keeping the SMP and SML catalog operational. This costs money, and how these costs will be allocated must also be addressed later. Payment is made through the basic function *Making payments*.

Open issues

The following observations and requested changes may be evaluated in a next version of this document.

01 Applicability of Decentralized Identifiers (DIDs)

The DID Core v1 specification states similar goals as the current document under Towards portable addresses in a generic data space. However, the DID technology may introduce accidental complexity, given its broader purpose. It is not yet clear whether for example the EU Digital Identity framework will adopt DID, as evidenced in Architecture and Reference Framework issues #205, #264, #278. TIP will actively accept EUDI & DID credentials for the purpose of authentication to the Peppol Network when available, yet, for purposes of signage and decentralized adressing in Peppol tansactions it is sensible to await the further development of fully decentralised DID under the ARF and EUDI development.

TIP will actively accept EUDI & DID credentials for the purpose of authentication to the Peppol Network when available, yet, for purposes of signage and decentralized adressing in Peppol tansactions it is sensible to await the further development of fully decentralised DID under the ARF and EUDI development.

02 Centralised versus federative addressing

When multiple delivery providers participate in a single delivery network, the network needs to include a distributed system for address management. This enables the provider to answer the question: how do I know for sure the address of the recipient is correct and active? Can I look up whether the recipient has a provider? We consider two types of systems:

- Central address management: The network includes a shared directory, which aggregates all entries provided by each provider.
  - Advantages:
    - Competitors cannot see each other's customers.
    - It is applied in delivery deployments such as Peppol.
    - It enables central distrust of providers in the case of compromised integrity.
  - Disadvantages:
    - The shared directory can be implemented as a single point of failure.
    - Managing the shared directory requires significant resources.
    - It may not provide uniqueness for natural person addresses, if they cannot be centrally managed for privacy reasons.
- Federated address management: The network includes a mechanism for federation across provider directories, such as a shared list of IP addresses for discovery. Providers choose which other providers to trust. This enables each provider to access the network's address book, without any entity managing the primary source of truth for the whole network.
  - Advantages:
    - It has no single point of failure. Availability of the shared list is not a prerequisite for accessing other providers.
    - Managing the shared list requires fewer resources than managing a shared directory.
    - It enables providers to distrust other providers in the case of compromised integrity.
  - Disadvantages:
    - A provider may technically be able to abuse another provider's directory to learn about their customer base.
    - Managing the shared list still requires some resources.

We choose federated address management. No reasons to go for central management.