Basic function *Delivering messages*

Introduction

This document describes the basic function *Delivering messages* of the *TIP ecosystem*. Words printed in italic refer to definitions described in the document Basic functions and definitions for the *TIP ecosystem*, which can be found under Publicaties.

> **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 *Delivering messages* facilitates near real-time delivery of messages from and to *Actors*, while ensuring data availability, integrity and confidentiality. An *Actor* can be a natural person or a legal person, potentially acting with the role of a *Recognised profession* (Basic functions and definitions for the *TIP ecosystem*,version 1.3). This basic function may also generate evidence regarding the process of data transmission, including attestations of the time at which data has been sent or received, and attestations of attributes of the exchanging *Actors*. In these cases, *Delivering messages* not only protects the transmitted data itself against damage, loss and unauthorised modification, but also protects the proof of transmission. The function is often called “e-delivery” or “electronic data interchange (EDI)” outside of TIP.

Roles in *Delivering messages*

We specify the core function in terms of the following roles in *Delivering messages*, as illustrated in Figure 1.

- sender: an *Actor* who may send messages;
- recipient: an *Actor* who may receive messages;
- provider: an *Actor* who implements one or more functions in *Delivering messages*:
  - submitting messages;
  - receiving messages;
  - attesting registered delivery evidence;
  - addressing and routing;
  - contact management;
  - channel management;
  - key discovery;
  - network availability;
- agent: a system that uses one or more functions in *Delivering messages* on behalf of a sender or recipient;
- user: an *Actor* who operates an agent.

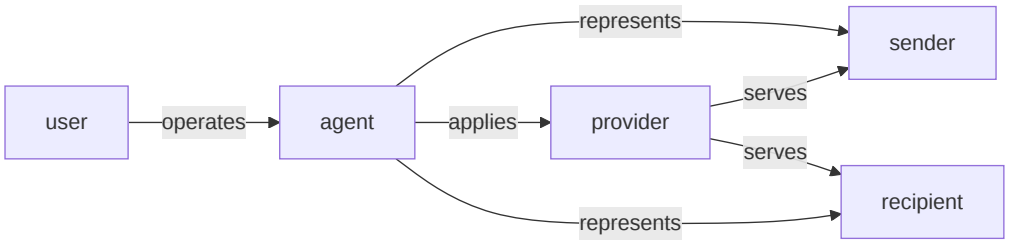

Figure 1: Relations between roles in *Delivering messages*

A user operates an agent to access a provider on behalf of a sender or recipient. The roles of sender, recipient, provider, and user may be performed by the same *Actor* or by different *Actors*. For example, a legal person acting as sender or recipient may delegate message handling to multiple natural persons acting as users. A sender or recipient may be its own provider or contract a provider for a service for *Delivering messages*. Furthermore, an agent may appear in several ways, for example as a web browser, as a dedicated purpose software application, or as a software process running on an organisation's internal infrastructure.

Networks for *Delivering messages*

A provider implements an access point to one or more networks for *Delivering messages*. A network enables its connected senders and recipients to exchange messages and can be either:

- centralised: the network only supports exchanging with other senders or recipients who subscribe to the same provider;
- federated: the network consists of multiple interoperable providers.

A federated network enables a four-corner model, in which the sender may use a sending provider that is distinct from the receiving provider used by the recipient. This is illustrated in Figure 2.

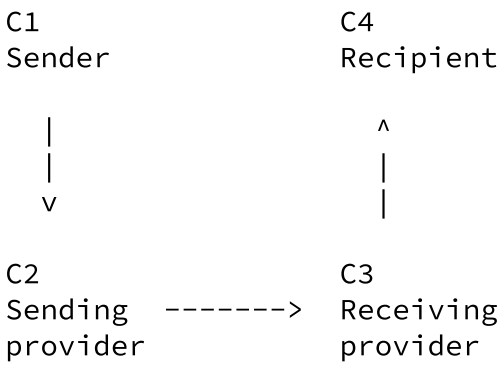

Figure 2: Four-corner model for *Delivering messages*

Each federated network may have its own policies regarding the functionality and quality of providers and agents, the recognition of senders and recipients and the authorisation of users. Example federated networks are:

- Internet with SMTP for global unstructured email;
- Internet with HTTPS for global web sites and APIs;
- Internet with XMPP for global structured messaging;
- Once Only Technical System for EU cross-border public administrative processes;
- Peppol for global business messages such as invoices.

Note that not all of these example networks conform to the standards and agreements set out below.

Note that some providers may use a federated network for notifications, e.g. email, and their own centralised network for payloads.

Delivering messages in data spaces

An implementation of *Delivering messages* can be part of a data space. In such cases, the Data Spaces Support Centre's Data Spaces Blueprint v1.5 terminology applies as follows:

- A provider for *Delivering messages* could be a data space "agency intermediary" providing (generic components of) local catalogue publication, contract negotiation, the transfer process, and the data plane.
- An agent for *Delivering messages* could be a data space "participant agent".
- A sender or recipient for *Delivering messages* could be a data space "data owner", configuring authorisation policies governing operations as "data provider" or "data consumer". For example, a "data owner" can receive requests for data as messages, or send data products as messages.
- A user of *Delivering messages* could be a data space "participant", with a "data provider" role when sending messages, and a "data consumer" when receiving them.

Lifecycle of *Delivering messages*

A provider is responsible for managing the process lifecycle of delivering a message, from the start of delivery to the end situation, whether successful or not. This lifecycle is defined as a sequence of events with the following types, based on EN 319 522-1 v1.2.1:

- SubmissionAcceptance or SubmissionRejection, after an authenticated agent has provided message content and requested submission on behalf of a sender;
- RelayAcceptance or RelayRejection or RelayFailure, after another provider has requested intermediation to submit to another provider or *Delivering messages* to a recipient at this provider;
- NotificationForAcceptance or NotificationForAcceptanceFailure, after the provider has tried to notify an agent of the the recipient and ask for their willingness to accept the delivery of the message;
- NotificationDelivered, after this notification and question about willingness was successful;
- ConsignmentAcceptance or ConsignmentRejection or AcceptanceRejectionExpiry, after the process of identification of the recipient, authentication of an agent acting on behalf of it, and acceptance by this agent;
- ContentConsignment or ContentConsignmentFailure, after trying to make the message content available to this agent;
- ConsignmentNotification or ConsignmentNotificationFailure, after trying to notify the recipient about the availability of the message content;
- NotificationAccessTracking, after observing that the recipient has accessed that notification;
- ContentAccessTracking, after observing that an authenticated agent acting on behalf of the recipient has started to access the message content;
- ContentHandover or ContentHandoverFailure, after trying to provide the message content to an authenticated agent on behalf of the recipient;
- RelayToNonERDS or RelayToNonERDSFailure or ReceivedFromNonERDS, after interacting with a network that does not provide electronic registered delivery services.

The provider may record explicit evidence of these events or apply a different logical model.

Qualified and non-qualfied registered *Delivering messages*

When the provider provides sending or receiving messages and attestation of *Delivering messages* lifecycle evidence as a service, this is considered an "electronic registered delivery service" (ERDS) under eIDAS. When the provider is qualified for this service, it is considered a "qualified electronic registered delivery service" (QERDS) under eIDAS. The exact formulation in Article 3(36) is:

> '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 unauthorized alterations;

Recital (52) of the (EU) 2024/1183 revision of eIDAS states ambitions for a cross-border high-assurance QERDS network:

> It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new Union-wide electronic registered delivery services. In order to ensure that data using a qualified electronic registered delivery service is delivered to the correct addressee, qualified electronic registered delivery services should ensure complete certainty the identification of the addressee while a high level of confidence would suffice as regards the identification of the sender. 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.

Delivering messages* from and to recognised *Actors

The *Delivering messages* agent may rely on a trust framework for electronic identification for originating and addressing outgoing messages. For example, the agent may rely on the provider's ability to authenticate the sender and recipient using eIDAS identifiers and pseudonyms, and its directory to map eIDAS identifiers and pseudonyms to addresses in networks for *Delivering messages*. A network may include shared services for federation of such provider directories.

Additionally, the agent may rely on it for sealing, authenticating and possibly encrypting incoming and outgoing messages. For example, a network may apply the Message Layer Security (MLS) protocol as specified in RFC 9420 for end-to-end encryption of highly confidential messages between *Actors*, relying on an MLS Authentication Service based on eIDAS qualified certificates. Such end-to-end encryption goes on top of the Transport Layer Security encryption as specified in RFC 8446 which encrypts between clients and servers of agents, providers, and other network services.

Delivering messages* and *Wallets

Users may be able to apply a *Wallet* to access an agent for *Delivering messages*.

Senders and recipients may be able to apply a *Wallet* to authorise an agent for *Delivering messages*. Additionally, they may be able to apply a *Wallet* to enrol for recognition as a sender or recipient, as described above.

A *Wallet* implements “wallet secure cryptographic device” (WSCD) functionality for identification, authentication and attesting attributes. An agent may apply this or a similar method to manage keys for end-to-end encryption as described above.

Applicability

The basic function *Delivering messages* is mandatory for all communication between *Actors* within the *TIP ecosystem*. This enables digitalisation of transactions with large financial or legal consequences in an open ecosystem.

Agreements

TIP agrees on the following requirements regarding implementation of *Delivering messages*.

General requirements

Implementers MUST apply a client-server model, in which the agent is a client and the provider is a server. This enables a store-and-forward technique, enabling sender’s business continuity even if the recipient’s infrastructure is temporarily unavailable.

Implementations that rely on signatures or seals to authenticate the sender MUST do so using the basic functions *Signing data* and *Validating signatures*.

Implementations that rely on *Wallets* to identify and authenticate senders and recipients MUST do so using the basic function *Attestation of attributes*.

When applying ERDS, the service MUST be QERDS. This simplifies quality assurance of ERDS within TIP, while leaving the option open to use non-registered non-qualified services for networks that require this, depending on legal, security or operational needs of the user.

Provider requirements

Providers MUST apply *Publishing service or chain specifications* at Level 1 (Embedded trust services) for potential integration into an *Acting space*. This allows *Actors* to configure an environment to manage and re-use the message content and evidence of *Delivering messages* easily and securely.

Providers MUST record at least the following events: SubmissionAcceptance, SubmissionRejection, ContentHandover, ContentHandoverFailure.

Providers MUST verify the identity of the sender with a high level of assurance.

Providers MUST verify the identity of the recipient with a high level of assurance.

QERDS providers MUST provide evidence using the basic function *Attestation of attributes*.

QERDS providers MUST seal evidence using the basic function *Signing data*.

Agent requirements

Agents MUST address messages to recipients, regardless of specific agents, providers or users. This enables traceability of the sender's intentions and portability across providers and agent solutions.

Agents MUST apply the basic function *Authorising an Actor* to manage user access.

Agents that validate QERDS evidence MUST validate this using the basic function *Validating signatures*.

Standards

> **Note**
>
> For an overview of applicable ETSI standards, see SR 019 050 v1.1.1. For an overview of ETSI standards development in the context of the eIDAS revision, see TR 119 520-1 v1.1.1 and TR 119 520-2 v1.1.1.

Implementations MUST NOT apply the EN 319 532 an TS 119 534 series of Registered Electronic Mail (REM) standards for QERDS.

Providers of registered evidence of *Delivering messages* MUST conform to:

- EN 319 401 v3.1.1: general policy requirements for trust service providers
- EN 319 521 v1.1.1: policy and security requirements
- EN 319 522-1 v1.2.1: framework and architecture
- EN 319 522-2 v1.2.1: semantic contents
- EN 319 522-3 v1.2.1: formats

If two QERDS instances interoperate, these instances MUST conform to:

- AS4 Profile of ebMS 3.0 Version 1.0 for message transmission between providers
- Business Document Metadata Service Location (BDXL) Version 1.0 for receiver identification services
- OASIS Service Metadata Publishing (SMP) Version 1.0 for capability discovery services
- EN 319 522-4-1 v1.2.1: message delivery bindings
- EN 319 522-4-2 v1.1.1: evidence and identification bindings
- EN 319 522-4-3 v1.1.1: capability/requirements bindings, with regard to BDXL, SMP, and EU Trusted List

If a QERDS provider claims that is QERDS is interoperable with other QERDS instances, it MUST succeed at:

- TS 119 524-1 v1.2.1: testing conformance
- TS 119 524-2 v1.2.1: test suites for interoperability testing

Best practices

When implementing QERDS, follow the business driven guidance provided in TR 119 500 v1.1.1.

Provide the agent as part of an *Acting space*. This allows *Actors* to configure an environment to manage and re-use the message content and evidence of *Delivering messages* easily and securely.

Apply the basic function *Attesting attributes* with a *Wallet* for agents authenticating users, senders and recipients and for enrolment of senders and recipients.

When applying *Delivering messages* in a federated network, prefer applying an existing network with a mature governance over setting up a new (sector-specific) network, provided that the existing network fully complies with the requirements in this document. For example, the Peppol network in the procurement and invoicing domain could be considered.

When applying *Delivering messages* in a service or chain specification, as specified in *Publishing service or chain specifications* Levels 2–3, typically the following process activities are useful to include:

- submit message, performed by a sender;
- receive message, performed by a recipient.

When displaying registered lifecycle status of *Delivering messages* to users, agents should provide unambiguous and recognisable user interfaces. For example, happy-flow status indicators could be:

Icon	Most recent lifecycle event
✓	SubmissionAcceptance
✓✓	NotificationDelivered
☑️☑️	ConsignmentAcceptance
✅✅	ContentConsignment
🫳	ContentHandover

Note that accessibility best practices need to be applied when designing such status indicators.

Suppliers

Providers of QERDS are listed in the EU/EAA Trusted Lists. Providers of ERDS may be listed there as well.

Providers of notified data intermediation services in the context of the Data Governance Act are listed in the EU register of data intermediation services.

Providers with access points to specific networks for *Delivering messages* may be listed by the governing authorities of these networks.

Administrators

Each network for *Delivering messages* is administered by its governing authority. Each *Delivering messages* sender or recipient administers which *Delivering messages* users may operate a *Delivering messages* agent on their behalf.

Regulators

Registered *Delivering messages* is regulated by EU member states under the eIDAS regulation. These member states designate a supervisory body, as listed in Supervisory bodies. This supervisory body ensures that trust service providers, including qualified trust service providers, comply with the requirements set out in eIDAS.

Intermediation services are regulated by EU member states under Digital Governance Act. See the list of National competent bodies and authorities under the EU register of data intermediation services.

Costs

Pricing for the use of *Delivering messages* is established on the basis of bilateral agreements between providers and *Actors* who subscribe as *Delivering messages* sender or recipient. Governance authorities or individual *Actors* may choose to cover the costs of messages to lower the barrier to interact digitally in an easy and secure manner.

Open issues

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

`01` Networks recognised by TIP

Does a TIP governance need to explicitly recognise networks for *Delivering messages*? For QERDS, is qualification sufficient?

`02` Directory standards for interoperable addressing

Should TIP require particular directory standards for interoperable addressing across providers? If so, should this be part of *Delivering messages* or of another basic function? See related notes in the TIP SharePoint under 5. Werkgroep Techniek › 3. Basisarchitectuur › Basic function Exchanging data.