Public

# Practice Statement Qualified Electronic Registered Delivery Service (qERDS)

## Aangetekend Mailen (Plus) / Registered Email (Plus)

## Aangetekend B.V.

Digitally signed by Aangetekend B.V.

Date: 26th of May2025

| Document | Version |
|---|---|
| Issued by | Aangetekend B.V. |
| Document owner | Wouter van den Brink |
| Telephone | +31 302006838 |
| E-mail | wouter@aangetekendmailen.nl |
| Date | 26th of May 2025 |
| Version | 1.6 |

This document describes what practices are in place for the provisioning of the Trust Services from Aangetekend B.V.

## Table of Content

# 1. Introduction and scope

Aangetekend B.V. is a qualified Trust Service Provider (qTSP) in accordance with the eIDAS and eIDAS2 Regulation and applies the trust service policy according to the practice statement.

Aangetekend BV is a provider of electronic Services, Trust Services and Qualified Trust Services.

Aangetekend B.V. provides the (qualified) Trust Service: (qualified) Electronic Registered Delivery Service ((q)ERDS) in accordance with the eIDAS Regulation.

Aangetekend B.V. and its services are periodically assessed by an accredited Conformity Assessment Body (CAB) for the requirements as set out in the eIDAS Regulation.

As a qualified Trust Service Provider, Aangetekend B.V. is under the permanent supervision of the Rijksinspectie Digitale Infrastructuur (RDI). RDI maintains the EU Trusted List for the Netherlands: eIDAS Dashboard

Aangetekend B.V. has been designated as a vital organization by the Ministry of Economic Affairs and Climate (Ministerie EZK).

This document describes the practices applied by Aangetekend B.V. with her office at Computerweg 22, 3542 DR Utrecht, registered with the Dutch Chamber of Commerce under number 52455289 for the provisioning of a qualified Electronic Registered Delivery Service (ERDS).

This Practice Statement includes a set of rules that Aangetekend B.V. applies in connection with its role as qualified Trust Service Provider in compliance with the Regulation (EU) No 910/2014 (eIDAS-Regulation) and EU Regulation No 2024/1183 (also called eIDAS 2)

# 2. Standards conformity

This Practice Statement claims conformity with:

- Regulation (EU) No 910/2014 (eIDAS-Regulation) and
- Regulation (EU) No 2024/1183 (eIDAS 2-Regulation)
    - in particular with the Articles 3.36, 13.1, 13.2, 13.3, 15, 20.1, 20.2, 20.3, 21.3, 23.1, 23.2, 24.2, 36.1 (a) to (d), 44.1, 44.1a, 44.2a
- Implementing Regulation (EU) 2015/806 laying down specifications relating to the form of the EU trust mark for qualified trust services
- Directive (EU) 2022/2555 Art. 21 measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- ETSI EN 319 401 V3.1.1 (2024-06) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 521 V1.1.1 (2019-02) Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 531 V1.1.1 (2019-01) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers

The Qualified Electronic Registered Delivery Service makes use of two other Trust Services: qualfied eSEAL and qualified Timestamp, according to eIDAS and eIDAS 2 to fulfill the obligations as set under article 44. These Trust Services claims conformity with:

- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319.421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

# 3. Overview and definitions qTSP,ERDS, qERDS, REM and REMS

Aangetekend B.V. was founded in April 2011 to implement the service Aangetekend Mailen / Registered Email. Via a 'track and trace' system, the sender can follow exactly where, when and how a document follows the digital route to the addressee and how it is subsequently handled. As a result of the speed and effectiveness of this way of mailing, an important - substantially cost-saving - contribution is made to the digital transformation of organizations. Hardly handling costs, no postage costs, no difficult conversion from digital to physical, certainty for the integrity of the content of the transmission and maximum conversion with the addressees are just a few advantages of the use of Aangetekend Mailen/ Registered Mail within the business processes. See websites for more information www.aangetekendmailen.nl .

Under eIDAS 2.0, Qualified Trust Service Providers (qTSPs) have enhanced obligations to ensure security, reliability, legal compliance, and cross-border interoperability of their trust services.

These obligations are laid out to maintain trust across the EU, especially as digital transactions become more widespread and critical (e.g., through the European Digital Identity Wallet). eIDAS 2.0 builds upon eIDAS 1.0 but introduces new responsibilities in light of emerging technologies and cross-border digital needs.

The obligations of a Qualified Trust Service Provider (qTSP) under eIDAS 2.0 can be summarized as followed:

**1. Supervision & Accreditation**
- A qTSP must undergo a conformity assessment by an independent body.
- It must be granted qualified status by the national supervisory authority.
- Once approved, the qTSP is listed in the EU Trusted List (EUTL), allowing cross-border recognition.

**2. Provision of Qualified Trust Services Only After Approval**
- A trust service can only be offered as qualified after the qTSP receives formal approval.
- This includes services like:
    - Qualified electronic signatures (QES)
    - Qualified electronic seals
    - Qualified electronic time stamps
    - Qualified website authentication certificates
    - Qualified electronic registered delivery services (qERDS)
    - Qualified electronic archiving services (new in eIDAS 2.0)
    - Qualified attestations of attributes

**3. Security and Risk Management**

- qTSPs must implement appropriate technical and organizational measures to:
    - Prevent misuse or unauthorized access,
    - Protect against compromise, fraud, and cyber threats.
- Must perform regular risk assessments and incident monitoring.

**4. Liability**

- qTSPs are presumed liable for damage caused by non-compliance with their obligations, unless they can prove no fault (i.e., they took all reasonable measures).
- This reinforces trust for users and relying parties.

**5. User Transparency & Consent**

- Clear, comprehensive terms and conditions must be provided to users.
- Information must include:
    - Description of the trust service,
    - Any limitations on use,
    - Procedures for complaints and redress.
- Explicit user consent must be obtained for processing personal data, in compliance with GDPR.

**6. Availability, Continuity & Revocation**

- Must guarantee high availability and continuity of service.
- Must have clear and secure revocation or suspension procedures for compromised certificates or services.
- Must maintain event logs and service evidence securely and durably.

**7. Use of Qualified Components and Procedures**

- Trust services (e.g., e-signatures, e-seals) must be based on:
    - Qualified signature/seal creation devices (QSCDs),
    - Qualified certificates, issued in accordance with strict standards.

**8. Compliance with EU Standards**

- Services must comply with:
    -ENISA and ETSI standards,
    - EU-wide technical specifications, including updates for newer technologies introduced in eIDAS 2.0.

**9. Cooperation with Supervisory Authorities**

- Must cooperate during:
    - Audits and assessments,
    - Incident investigations,
    - Monitoring of compliance.

**10. Interoperability and European Digital Identity Wallet (EUDI Wallet)**

- qTSPs must support interoperability across EU borders.
- eIDAS 2.0 introduces obligations related to issuance and verification of credentials for use in the EUDI Wallet (e.g., digital diplomas, professional qualifications, health credentials).

Aangetekend B.V. delivers two variants of the Qualified electronic registered delivery services (qERDS):

1. Electronic Registered Delivery Service **(ERDS)** - Aangetekend Mailen/ Registered Email (in short AM), whereby the mail can be sent to the recipient after an alert to the address of that recipient known to the sender (article 43.1 of the eIDAS Regulation);
2. Qualified Electronic Registered Delivery Service **(qERDS)** - Aangetekend Mailen Plus / Registered Email Plus (in short AM Plus), the qualified ERDS according to the eIDAS-

requirements whereby - after the sender has properly identified - the recipient must first go through an identification procedure before the mail becomes available (articles 43.2 and 44 of the eIDAS Regulation).

The qualified ERDS is according to ETSI EN 319 521 V1.1.1 (2019-02) Policy and security requirements for **Electronic Registered Delivery Service Providers (ERDSP)** and ETSI EN 319 531 V1.1.1 (2019-01) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Registered Electronic Mail Service Providers (REMSP)**.

The main difference between ETSI EN 319 521 and ETSI EN 319 531 is:

ETSI EN 319 521 defines policies and security requirements for qualified ERDS, but it does not prescribe specific technical message transmission protocols. ETSI EN 319 531 specifies the technical requirements for Registered Electronic Mail (REM), including message formats, exchange mechanisms, and delivery confirmation processes.

According to ETSI 319 532 standard, registered electronic mail service **(REMS)** is a specific type of electronic registered delivery service **(ERDS)**, which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

**Electronic Registered Delivery Service (ERDS)** means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations (source: eIDAS Regulation);

**Qualified Electronic Registered Delivery Service (QERDS)** means an electronic registered delivery service which meets the requirements laid down in Article 44 of eIDAS Regulation (source: eIDAS Regulation);

**Registered Electronic Mail (REM)** is a particular instance of An Electronic Registered Delivery Service (ERDS) (source: ETSI EN 319 532-4 V1.1.7), an enhanced form of e-mail transmitted by registered electronic mail service.

**Registered Electronic Mail Service (REMS)** is an electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

By simply words, REMS is a sub level of ERDS. The eIDAS Regulation does not describe such a service but yet this difference can be made according to ETSI standards.

This qualified variant Electronic Registered Delivery Service will be offered in the Dutch-speaking countries under the name Aangetekend Mailen Plus (AM Plus) and in other countries under the usual translations with the addition 'Plus'.

The Aangetekend Mailen / Registered Email service is also delivered in several European countries under the names: Digitaal Aangetekend (BE), Recommandé Electronique (BE/FR), Digital Einschreiben (DE), Registered Email (UK/IE) and E-Mail Certificado (ES).

Aangetekend B.V. has been ISO-27001 certified by LRQA since 2016 and eIDAS certified by Deutsche Telekom Security GmbH since 2019.

# 4. Policies and practices

## 4.1 Trust Service Practice statement

The current Practice Statement is approved by the Management Board of Aangetekend B.V. This document will be periodically reviewed by the Management Board which is scheduled in the ISMS calendar. This Practice Statement is made publicly available for subscribers and relying parties via the document repository of the website https://www.aangetekendmailen.nl/repository/

Any changes to this Practice Statement shall lead to a publication of the revised Practice Statement to the document repository. Old versions of the Practice Statement will still be available in the document store. Changes that have no impact on the subscribers or relying parties will not be notified up front. Changes that impact subscribers or relying parties and that do not impact the secure and compliant operation of the services will be notified via the Aangetekend Mailen – Registered Email website at least 2 weeks in advance of the implementation of the change. In case of changes that impact subscribers or relying parties that are urgent because they are required to maintain the security or compliance of the solution, a best effort will be performed to notify via the website as soon as possible.

Aangetekend will inform the Supervisory Body Rijksinspectie Digitale Infrastructuur at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities

The present Practice Statement supports the provisioning of the Electronic Registered Delivery Service (ERDS) that meets the eIDAS qualified level according to ETSI EN 319 521 V1.1.1 (2019-02) Policy and security requirements for Electronic Registered Delivery Service Providers **(ERDSP)** and ETSI EN 319 531 V1.1.1 (2019-01) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers **(REMSP).**

## 4.2 Terms and Conditions

Aangetekend B.V. publishes its General Terms and Conditions on the www.aangetekendmailen.nl websites and the Repository https://www.aangetekendmailen.nl/repository/

# 5. TSP Management

## 5.1 Internal organization

Aangetekend B.V. has a clear 'lean and mean' structure in terms of organization: TSP deliberately examine which activities can be performed in-house and which can be outsourced to reliable ISO27001 and/or ISO9001 and/or eIDAS-certified partners.
Aangetekend B.V. operates in a network of suppliers, resellers, business partners and (potential) subscribers. The supplying actors are always checked for delivery reliability and meeting the high requirements.

## 5.2 Human resources

For Aangetekend B.V. it is important to have a team of employees who, not only in terms of competency but also in terms of commitment and empathy capacity, are able to perform any related work. The team fully meets these job requirements.

The background of all internal employees is thoroughly investigated at the start of their employment relationship.

There is a procedure in place which provides the necessary instructions for checking the training, skills, experience and qualifications. These checks are aligned with the applicable laws and regulations.

## 5.3 Asset management

The TSP ensures that its information and other assets receive an appropriate level of protection. In particular, the TSP maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis. All media are handled securely in accordance with the requirements of the information classification scheme. Media containing sensitive data are securely disposed of when no longer required.

## 5.4 Physical and environmental security – datacentre Netherlands

To avoid compromise or theft of information and information processing facilities the following controls have been implemented:

- physical and logical access control;
- all equipment is protected from physical and environmental threats.

Therefore, the office fully meets the security requirements that can be set for this, such as permanent camera surveillance, compartmentalization, colocation, logging of access, external monitoring after office hours, motion detectors, etc. The datacentre which TSP uses for housing own hardware and the internet connection is heavily protected, is located above sea level on Dutch territory and is ISO27001 and NEN 7510 certified.

## 5.5 Operation security

Aangetekend B.V. ensures that the access to virtual infrastructure is limited to properly authorized individuals. In particular:

a) A firewall is implemented to protect the TSP's internal systems from unauthorized access.
b) The TSP ensures effective administration of user access required for the work of operators, administrators and auditors. In this way, the system security, including user account management, auditing, and timely modification or removal of access, is maintained.
c) Access to information and application system functions is restricted in accordance with the access control policy, and the TSP system provides sufficient computer security controls for the separation of trusted roles identified in the TSP, including the separation of security

administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled.

d) TSP personnel are properly identified and authenticated before using critical applications.
e) TSP personnel are accountable for their activities; to this end, event logs are retained
f) The local network components (e.g. routers) are kept in a physically secure environment, and their configurations are periodically audited for compliance with the requirements specified by the TSP.
g) Continuous monitoring and alarm facilities are provided to enable the TSP to detect, register, and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.
h) Interface connections are firewalled and are encrypted.

## 5.6 Incident management

In case of incidents and calamities, it is necessary to be able to act systematically in case of unforeseen incidents and calamities, so that the consequences can be mitigated as quickly as possible. TSP incident management is aimed at a fast and correct recovery of the processes affected by an incident or disaster in such a way that reliable services are provided to customers in the shortest possible time.

Aangetekend has effective communication plans in place that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols. This Service Level Agreement (SLA) includes incident response procedures including containment, eradication and recovery.

Aangetekend complies with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, such as DORA, CER, eIDAS, eIDAS2 including supervisory body Rijksinspectie Digitale Infrastructuur.

Incident detection and response process has clear interfaces between the incident handling and business continuity management (next chapter) functions to ensure a coordinated and cohesive response during incidents. Customer Succes Managers are in control of both under supervision of the Operational Manager.

Staff, contractors and customers can report possible network and information security incidents directly using contact details given on the website or support portal. Contact - Aangetekend or Kennisbank

In case of a Data Breach or Security breach Aangetekend has procedures in place and train their staff to follow the reporting procedure and to address the appropriate point of contact.

Aangetekend identifies the root cause in case of a severe incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents and ensures that each past incident led to a post-incident review.

## 5.7 Business continuity management

Continuity of service to all customers is of the utmost importance. For this reason, it is necessary to be able to act systematically in case of unforeseen incidents, calamities and/ or crisis, so that the consequences can be mitigated as quickly as possible.

The Business Continuity Plan focuses on the action perspective of those who are involved in any way in restoring the execution of the primary and secondary processes. In the continuity policy of Aangetekend B.V. the undisturbed service with regard to Aangetekend Mailen (Plus)/ Registered Email (Plus) has the highest priority for all customers. This means that in the preventive sphere the necessary measures are taken to mitigate risks in the service provision. This involves, among other things, the continuous inventory of potential risks, the SLA's with subcontractors, the necessary attention to guaranteeing continuity, determining the Single Points of Failure and determining the Recovery Time to Objective.

# 6. TSP Operations

## 6.1 Identification and authentication of sender

Before a legal person, as a sender/ subscriber/ client[1] (hereafter described as sender), is allowed to access to the platform he/ she has to go through the enrolment procedure. A natural person or non-subscriber cannot use the service as a sender. An authorized eIDAS Administrator has to register the sender in the platform first by email address and date of birth.

There are two methods for identifying the sender for the first time, namely using an eIDAS qualified identity provider and also through the implementation of a so-called 'physical presence'.

In the case of an eIDAS qualified identity provider the sender receives an activation link in their mailbox, when clicked, it allows them to identify themselves through their process.

In the physical presence method, the concerning delegate/ user is actually compared with his or her passport or other government-issued identity card, so that the identity can be determined on the spot. Supplier delegates can carry out these procedures.

In both cases, after validation of the name and the date of birth via the eIDAS qualified identity provider or on the official identity document, these personal details are unambiguously registered in the database by the eIDAS Administrator.

First time login of user, the name and date of birth received from the eIDAS qualified identity provider is stored in the database and when the name of the sender and the date of birth is validated compared with the information that was available by the eIDAS Administrator, access will be granted.

After the initial identifying the sender, the sender is asked for the phone number for two factor authentication. The next time the sender wants to access the platform, the sender is asked to provide their email address and password first after which they receive a code via SMS to their phone which they can enter on the login page. This code is validated and only then they are logged in.

Identifying and authenticating users is the same for ERDS as well as REMS, REMS is a sub level of ERDS.

[1] General Terms & Conditions; definitions: Subscriber - Client: the person who acts in the exercise of a profession or business with whom the Supplier enters into an Agreement for the delivery of the Service.

## 6.2 Identification and authentication of recipient/ receiver

A Recipient can be a legal and/ or a natural person. It is not necessary to be a subscriber of the Service to receive an Aangetekend Mailen (Plus)/ Registered Email (Plus).

There are different ways in which the recipient[2] can be identified:

1. Email address (Aangetekend Mailen/ Registered Email)
2. Email address plus 2FA using SMS (Aangetekend Mailen (Plus)/ Registered Email (Plus))
3. Email address plus 2FA using SMS plus personal data: name, surname and date of birth (Aangetekend Mailen Plus/ Registered Email Plus)
4. Email address plus personal data: name, surname and date of birth using qualified identity providers like eID and itsme (Aangetekend Mailen Plus/ Registered Email Plus)

After the identification process the Aangetekend Mailen (Plus)/ Registered Email (Plus) is shown to the recipient. The relevant data is attached to the “proof of receive” ticket for the sender.

Depending on the type of communication, the sender must choose the level of identification.

## 6.3 Sending Aangetekend Mailen Plus – Registered Email Plus

The use of Aangetekend Mailen Plus - Registered Email Plus begins after contracting and execution of the enrollment procedure with the customer.

If the end-user is connected to the Aangetekend Mailen Plus - Registered Email Plus service, a Registered Email Plus can easily be created via the used mail program, such as Outlook. Next to the well-known 'New Email' button there is a similar button with the title 'Registered Email Plus'. For workflow integration, a special suffix can be used instead of this button, as described in the Service Manual.

The content of email does not require any special treatment; it is a regular email, to which documents can also be added. When 'Send' is pressed, the mail - whether or not in batch - is sent to the company-specific mail server of Aangetekend B.V. via a secure connection. After this, the authorization process and the liability of the TSP starts in accordance with the eIDAS Regulation. The authorized Sender can be the identified end-user himself or a mandated manager, who has the mandate to approve and send a Registered Email Plus in accordance with the recorded data.

The approval for the sending can be done in batch. In this case, the messages are placed in a queue, which must be approved by the mandated person.

Optionally, the mobile phone numbers of recipients can be indicated if the 2FA is required by the sender via telephone validation. Other authentication options are personal data like: name, surname and date of birth.

After sending the notification(s) to the recipient(s), a proof of sending is created with the sender's name and integrity information, the proof of sending is sealed by an eIDAS qualified Hardware

[2] General Terms & Conditions Definitions 15: Addressee / Recipient/ Receiver: the person or organization with which User conducts or wishes to conduct e-mail correspondence via the user of the Authorized E-Mail Address with the intervention of the Service.

Security Module using a qualified eSEAL and timestamped using a qualified Timestamp and added to the proof of sending, so-called ticket, see sec. 6.6.

A detailed specification of this process can be found in the Service Manual.

How the users can submit messages is the same for ERDS as well as REMS. REMS is a sub level of ERDS.

## 6.4 Receiving Aangetekend Mailen Plus – Registered Email Plus

The receiver/addressee does not need to register or install any specific software. Upon receipt of a notification email, the recipient can accept or decline the email via a button in this notification email. Unlike the standard Service, a recipient must identify themselves before they can view the mail with attached documents. Identification can be at a substantial level when using qualified identity providers or at a low level when using 2FA with SMS and/ or given personal data: name, surname and date of birth.

Once the identification has succeeded, Once the e-mail and attachments have been downloaded and are visible through a secure web service (Store & Notify (S&N)), the recipient may individually choose to send the e-mail to their mailbox as well. The latter process falls outside the scope of Aangetekend Mailen Plus - Registered Email Plus except when secure forward is possible and succeeds (Store & Forward (S&F)).

A more detailed specification of this process can be found in section 6.8 of this document and in the Service Manual.

The Service has the option for all its users to send and receive messages in MIME format as per IETF RFC 2045 [4] and IETF RFC 5322 [5] over SMTP. The Service has the option for all its users to send message over SMTP and, receive messages over IMAP or POP.

## 6.5 User Agents

Several plug-ins (Outlook 2010, 2013, 2016, 2019, 2021, Outlook 365, Thunderbird and Lotus Notes) and or add-in for Microsoft 365 app for Office365 are available. To install the buttons Registered Email (Plus) in the email client you need an auto install plug-in.

Users do not need to install any plug-ins or apps to use the Service for workflow integration. For more information contact TSP.

## 6.6 Delivery evidence

During the sending and receiving process, different relevant statuses in the process are logged and displayed in a so-called ticket.

The proof of send and proof of receive tickets are created, sealed by an eIDAS qualified Hardware Security Module using an eIDAS qualified eSEAL and timestamped using an eIDAS qualified Timestamp the moment the message is sent / received, containing the identity information of the sender / receiver. The sealing is done and is available to inspect by the sender. The proof of send includes the integrity information, subject, send and receiver information, the name of the sender and an eIDAS qualified timestamp. The proof of receive contains the id of the message and the

identifying information of the receiver that opened the message, their name from their identity provider or their phone number. The eIDAS qualified seal of the proof of send is used to verify message integrity when displaying the message to the receiver.

The retention period of the evidence, the so-called ticket, is stored at least 7 years or longer when agreed with the customer and/or applicable legislation. There are no limitations on the evidence validity period.

Aangetekend Mailen (Plus) – Registered Email Plus will archive at least:

a) users identification data;
b) users authentication data;
c) proof that the sender identity has been initially verified;
d) logs of ERDS operation, identity verification of sender and recipient, and communication;
e) proof of the recipient's identity verification before the consignment/handover of the user content;
f) means to prove that the user content has not being modified during transmission;
g) a reference to or a digest of the complete user content submitted; and
h) time-stamp tokens corresponding to the date and time of sending, consigning and handing over and modifying the user content, as appropriate.

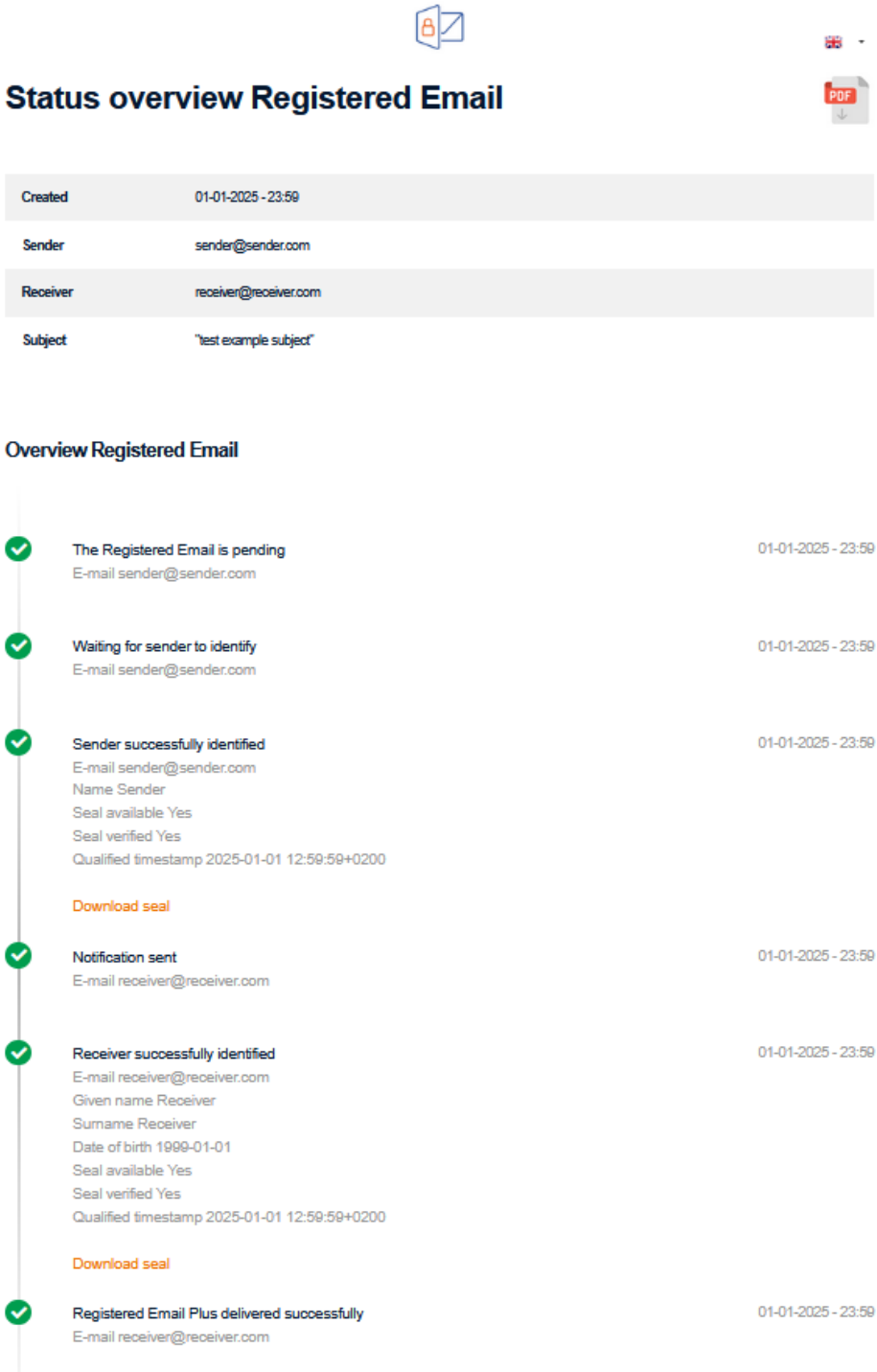
The provided evidence, the so-called ticket, are accessible to the user by a received email with a ticket included and/ or using the webservice dashboard with an enumeration of all created tickets and/ or downloadable from this mentioned dashboard.

The modalities of reversibility and portability apply in the sense that the content of the ticket cannot be changed and that it can be retrieved by means of the standards customary at that time.

The Service provides evidence for the events of successful and unsuccessful handover of user content.

In case if the S&F (see sec. 6.8) supports S&N style, the REMS shall provide evidence for the events capturing the acceptance/rejection/no-response by the recipient.

If the REMS supports S&N (see sec. 6.8) style and the user content which is processed in S&N style by this REMS is handed over to the recipient by this REMS, this REMS shall provide evidence for the consignment of that user content.



Status overview Registered Email

| | |
|---|---|
| Created | 01-01-2025 - 23:59 |
| Sender | sender@sender.com |
| Receiver | receiver@receiver.com |
| Subject | "test example subject" |

Overview Registered Email

The Registered Email is pending — 01-01-2025 - 23:59
E-mail sender@sender.com

Waiting for sender to identify — 01-01-2025 - 23:59
E-mail sender@sender.com

Sender successfully identified — 01-01-2025 - 23:59
E-mail sender@sender.com
Name Sender
Seal available Yes
Seal verified Yes
Qualified timestamp 2025-01-01 12:59:59+0200
Download seal

Notification sent — 01-01-2025 - 23:59
E-mail receiver@receiver.com

Receiver successfully identified — 01-01-2025 - 23:59
E-mail receiver@receiver.com
Given name Receiver
Surname Receiver
Date of birth 1999-01-01
Seal available Yes
Seal verified Yes
Qualified timestamp 2025-01-01 12:59:59+0200
Download seal

Registered Email Plus delivered successfully — 01-01-2025 - 23:59
E-mail receiver@receiver.com

**Fig. 1 Example ticket**

## 6.7 Interoperability

Aangetekend Mailen Plus - Registered Email Plus is a service in which, from the point of view of information security, it has been expressly chosen to deposit interoperability with other REMS with the sender or recipient of such a mail. The saving and reporting style of messages forwarded by another (non-) REMS is not supported. Currently the Service does not supports S&F style for messages relayed by another REMS. When other qualified Trust Service providers with ERDS are

added to the Dutch Trusted List supporting S&F style for messages relayed by another REMS will be considered.

Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 of eIDAS 44.2a and such compliance shall be confirmed by a conformity assessment body.

## 6.8 Store and Notify (S&N) and Store and Forward (S&F)

Each Aangetekend Mailen Plus - Registered Email Plus server can be configured according to client specific wishes of which one on them is set the time period for acceptance/ rejection. Final setting depends on determined legislation, policy rules or parameters given by client. The repetition of the notification email can also be set given by client.

The Service temporarily stores the content of the messages (Store) until it has been retrieved/rejected/deleted by the Notify notification email due to the expiry of the collection period by the recipient.

**Store & Notify (S&N)**

Once the notification has received and identification has succeeded (sec. 6.4), the e-mail and attachments have been downloaded and are visible through a secure web service, the recipient may individually choose to send the e-mail to their mailbox as well. The latter process falls outside the scope of Aangetekend Mailen Plus - Registered Email Plus, except when secure forward is possible (see S&F).

**Store & Forward (S&F – S&N)**

Once the notification has received and identification has succeeded (sec. 6.4), the e-mail and attachments are visible through a secure web service, and also directly been forwarded using regular email protocols. Delivery can only take place when the TSP system succeeds in the minimum set of requirements for secure delivery (for example Dutch NTA7516 standards). Secure delivery is possible when transport meets the security requirements as set by TSP such as TLS, DANE + DNSSEC, SPF, DKIM, DMARC. If secure delivery is not possible the fall back scenario is S&N, see above.

A detailed specification of this process can be found in the Service Manual.

## 6.9 Limitations on the use of Aangetekend Mailen Plus – Registered Email Plus

The limitations on the use of the QERDS Aangetekend Mailen Plus – Registered Email Plus are described in the General Terms and Conditions articles 2, 3, 4, 10 and 11.

## 6.10 Support

Although the use of Aangetekend Mailen (Plus) / Registered Email (Plus) is extremely simple, we help organizations with extensive support. The approach here is to explain key users / subscribers within the client organization how the product works, so that they can further implement this within their organization. Support therefore proceeds mainly through the designated contact persons within the

client organization.
Our business partners provide for the most part first-line support with the use of Aangetekend Mailen (Plus) / Registered Email (Plus). This means Aangetekend B.V. as second line support at the moment that the questions become more specific or more technical. In addition, Aangetekend B.V. gives support to the recipient of Aangetekend Mailen (Plus) / Registered Email (Plus). This is possible via the self-service helpdesk on the website of Aangetekend Mailen / Registered Email Support - Aangetekend and also via email support@aangetekendmailen.nl and telephone contact +31 30 200 68 38

# 7. QTSPs involved

Below the complete list of QTSPs involved in the provision of the QERDS Aangetekend Mailen Plus – Registered Email Plus.

| Modul Name | Modul Service | Module Provider | Adress | Conformity Certificate acc. to eIDAS | |
|---|---|---|---|---|---|
| | | | | ID | Valid until |
| e-Szigno Qualified Seal | Issuing service certificates for qualified electronic seals | Microsec Micro Software Engineeri ng & Consultin g Private Company Limited by Shares (trade name: Microsec Ltd.) | VATHU-23584497 , Ángel Sanz Briz út 13, 1033 Budapest, Hungary | HUNG-TJ-ESIGN-R-028-2024 as of 30.10.2024 | 30.10.2026 |
| QuoVadis Qualified Timestamp | Qualified timestamp service | QuoVadis Trustlink B.V. | Company number: 30237459 Nevelgaarde 56 noord 3436 ZZ Nieuwegein | Cert-ID 229/2023 as of 30.11.2023 KPMG Liechtenstein AG | 29.11.2025 |

# 8. Security policy

## 8.1 Information security policy

Aangetekend B.V. has set out all the security requirements and operational procedures in the information security policy that are required to implement the chosen risk management measures.

TSP has developed and implemented an Information Security Management System (ISMS) in accordance with ISO27001:2022. The scope of this ISMS includes all services provided by TSP.
The scope also includes the internal organization, employees, assets, data centre and suppliers that

independently support the services. It therefore relates to the management of information and all business activities that support these services.

Message integrity is secured against modification during transmission by sealing the message hashes with an eIDAS certified HSM using an eIDAS qualified e-Seal. Message hash and signature will be added to the Aangetekend Mailen Plus/ Registered Email Plus ticket, which creates an audit trail that proves that data has not been altered. Transmitted data is protected against the risk of loss, theft and damage by the use of TLS connections.

### 8.2 Risk assessment

The risk assessment is periodically updated in accordance with the ISO27001 standard by the management, supported by the privacy and security officer, of Aangetekend BV.

### 8.3 Cryptographic controls

The TSP ensures the security of cryptographic keys and cryptographic devices throughout their lifecycle.

Part of the information used or generated by Aangetekend B.V. is sent via an encryption. In the context of adequately securing the information, the management has established procedures for the management of the cryptographic control measures used.

### 8.4 Periodical audits

Aangetekend B.V. will be audited as a qTSP every 24 months, for ISO27001 every 12 months. The Certificates needed for ERDS are delivered by third party qTSP QuoVadis. Aangetekend BV shall be audited at their own expense at least every 24 months by conformity assessment body Deutsche Telekom Security GmbH according to eIDAS-Regulation and applicable ETSI-standards. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in the eIDAS-Regulation and in Article 21 of Directive (EU) 2022/2555. Qualified Trust Service Provider Aangetekend shall submit the resulting conformity assessment report to the supervisory body Rijksinspectie Digitale Infrastructuur (RDI) within three working days of receipt.

## 9. Obligations and liability

### 9.1 General

To enable a fully secured transport of data traffic from sender to receiver, various parties are involved, each with their own obligations and associated liabilities. For TSP services these are outlined in more detail in this chapter.

### 9.2 Subscriber/ Sender obligations

The obligations of Subscriber are defined in the General Terms and Conditions where is stated:

The Subscriber is and remains the party that is responsible and liable when using the Service at all times:

a. for all actions performed by Users via the Service; and
b. to verify when sending e-mail (s) to natural persons, whether the e-mail address that is entered actually belongs to the natural person to whom the User wishes to address the e-mail; and
c. when sending to natural persons who act on behalf of a company, to check whether the natural person to whom the e-mail is addressed is actually connected to - and authorized to communicate on behalf of - the company.
d. for the correctness of the link between the email address of the Addressee provided by or on behalf of the Supplier and the relevant natural or legal person.
e. in the case of the use of SMS with Registered Email Plus / Aangetekend Mailen Plus for identification of the Recipient that access to both the e-mail address and the SMS is expressly reserved for the authorized person.

Subscriber acknowledges that the Supplier is not responsible for the management and use of the e-mail client (including the inbox) of neither User nor Recipient. The Supplier is only responsible for the execution of the Service once the Registered Email has been received on the Registered Email-server.

The Subscriber must ensure that Users abstain from unauthorized use of the Service. This means that Users do not violate the applicable laws and regulations and behave in accordance with what may be expected of a careful User of the Service by the Supplier and third parties.

In the case of the use of AM Plus by an organization, the Delegate must carefully keep a list in which the subscribers who are authorized to use this service are registered.

The Subscriber as well as the Recipient / Addressee is independently at all times responsible for the maintenance and use of its E-mail client.

More obligations can be found in the General Terms and Conditions.

## 9.3 Recipient obligations

The liability of Subscriber are defined in the General Terms and Conditions where is stated:

The Subscriber as well as the Recipient / Addressee is independently at all times responsible for the maintenance and use of its E-mail client.

More obligations can be found in the General Terms and Conditions.

## 9.4 Relying party obligations

The provision of the service is based on chain liability that is covered by SLA's. At least ISO27001 is required from the key suppliers. The CAB, Deutsche Telekom Security GmbH, has included the most important suppliers in its eIDAS conformity audit.

## 9.5 Liability TSP

The liability of Aangetekend B.V. are defined in the General Terms and Conditions where is stated:

As a provider of trust services the TSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the eIDAS-Regulation.

The intention or negligence of the Supplier as an eIDAS qualified trust service provider shall be presumed unless the Supplier proves that the damage referred to in the previous paragraph has occurred without the intention or negligence of the Supplier.

When using Registered Email Plus, the Supplier acknowledges the possible legal consequences of electronic stamps and electronic time stamps in accordance with Articles 35 and 41 of the eIDAS Regulation.

More liability conditions can be found in the General Terms and Conditions.

## 10. Compliance

Aangetekend B.V. complies with all applicable laws, rules, regulations, decisions and orders when providing services based on this Practice Statement. Therefore provides TSP qualified trust services in accordance with the provisions of Regulation (EU) No 910/2014 (eIDAS) and Regulation (EU) No 2024/1183 (eIDAS 2). More relevant details described in section 2 of this document.

## 11. Procedures for changes in the Practice Statement

This Practice Statement will be changed in the case a mistake is detected, the need in updating arises, or proposals for changes come from related parties.

Periodical (and scheduled in the ISMS calendar) the Practice Statement will be updated by the Management under supervision of the Privacy and Security Officer.

## 12. Termination plan TSP

Although the 'set-up, existence and operation' are important focal points for every company to see if there are adequate control measures, the phase 'termination' must also be added to this.

Voluntary or unforeseen forced termination of all or part of the business activities must also be settled in the correct manner, with obligations towards suppliers and buyers being fulfilled.

Aangetekend B.V. has created a Termination Plan that deals with termination notification, subcontractors management, information maintenance, termination phasing and updating of the termination plan procedure.