SecuMailer

Qualified Registered Electronic Mail Service Policy and Practice

Versie: 1.1
Status: Final

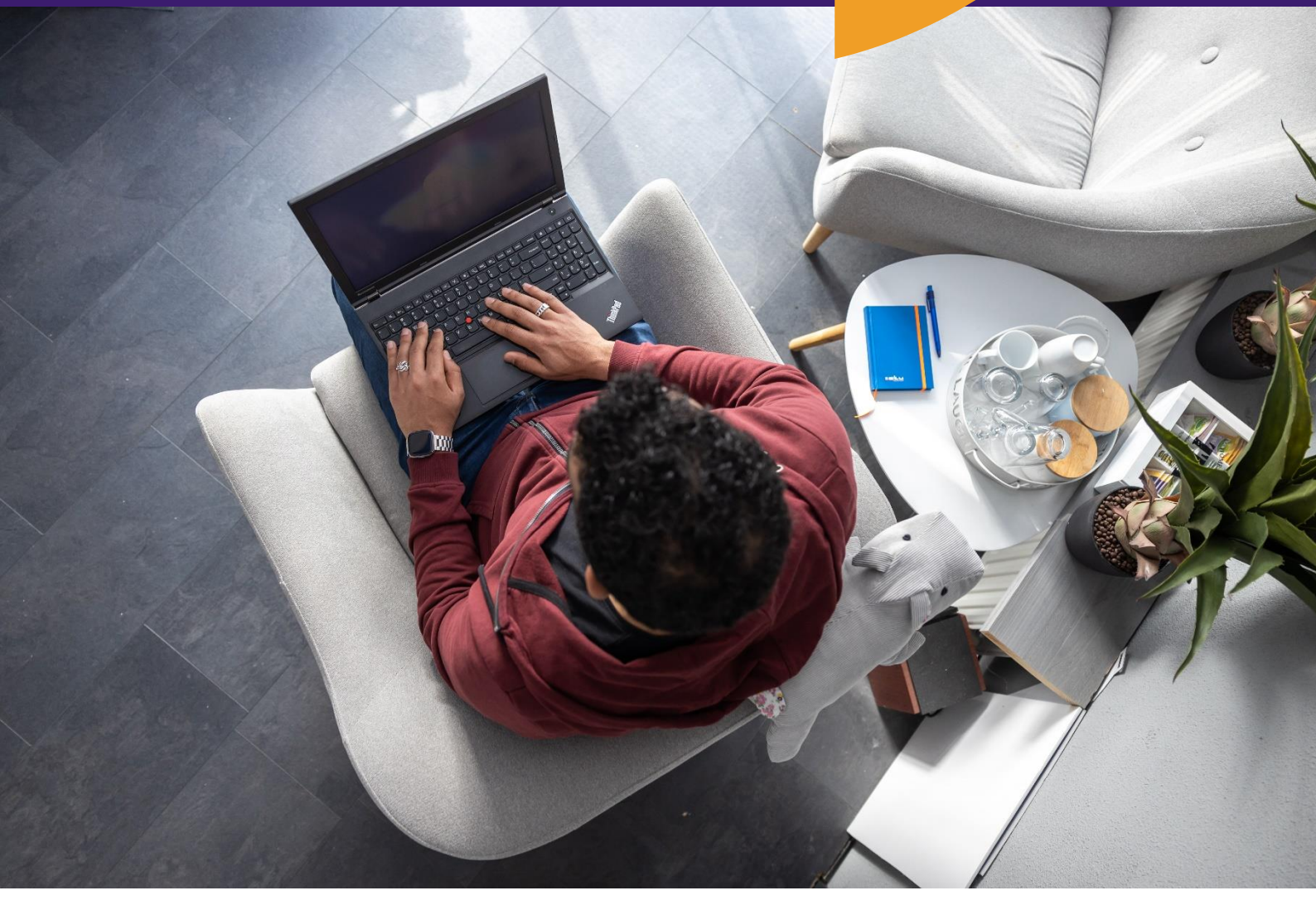


Table of Contents

1. Introduction

Secumail B.V. (hereafter SecuMailer) is a qualified trust service provider exercising activity in accordance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. As such the company is registered in the trust list of the European trust service providers (https://webgate.ec.europa.eu/tl-browser/#/tl/NL), as well as in the register of Dutch trust service providers maintained by the Rijksinspectie Digitale Infrastructuur (https://www.rdi.nl/onderwerpen/elektronische-vertrouwensdiensten/documenten/publicaties/2018/januari/01/digitale-statuslijst-van-vertrouwensdiensten).

SecuMailer provides to its users a highly reliable and secure qualified registered electronic mail service in accordance with Art. 44 of Regulation (EU) No. 910/2014.

1.1. Overview

This document describes the general rules and regulations applied by SecuMailer in the provision of the Qualified Registered Electronic Mail Service (QREMS). This document applies to a trust service provided by SecuMailer in line with Art. 44 of Regulation (EU) No. 910/2014 and in line with the applicable legislation in The Netherlands.

The Qualified Registered Electronic Mail Service (QREMS) provides secure and reliable delivery of electronic mails between the parties and offers evidence for the delivery process. The evidence can be considered statements by a trusted party, more specifically – SecuMailer, that a certain event related to the delivery process (sending, delivery, message denial, etc.) happens at a specific moment. The evidence can be transmitted immediately (together with the message or separately) or it can be stored in SecuMailer storage for later access. SecuMailer creates evidence in the form of digitally signed data.

Regulation (EU) No. 910/2014 provides the legal framework for facilitation of cross-border cooperation in the European Union (EU) for recognition of the existing national law systems related to the Qualified Registered Electronic Mail Service. The QREMS standards framework aims to cover the general and globally recognised requirements for registered electronic mail provided in a secure and reliable manner, irrespective of the applicable legislation.

This document defines the common requirements towards the activity of SecuMailer in its capacity as a Qualified Registered Electronic Mail Service Provider (QREMSP). This policy sets out the provisions that apply to company staff (competences, responsibilities, authorisation and obligations based on the role of each employee).

QREMS is a specific type of Electronic Registered Delivery Service (ERDS) that is based on the formats, protocols and mechanisms used in normal email messages. SecuMailer, as a provider of this service, meets a certain number of additional requirements set out in this document. The QREMS standards framework aims to cover the general and globally recognised requirements for secure and reliable registered electronic mail.

SecuMailer performs secure initial identification of the recipient and the sender and protection against loss, theft, corruption or unauthorised change of the data transmitted, thus ensuring the integrity of the user content.

It is important for SecuMailer users to familiarise themselves with the objectives and the role of this Policy and Practice so that this service can be used as intended. The relationships between SecuMailer and the users shall be settled through a Contract.

This document is in line with the standard ETSI EN 319 531 Electronic Signatures and Infrastructures (ESI) Policy and Security Requirements for Registered Electronic Mail Service Providers.

This policy is a public document. It can be changed at any time by SecuMailer and each new revision shall be approved by the Board of Directors and communicated to all relevant stakeholders through the company website (https://secumailer.nl).

1.2. Legislative references

This policy and practice is in line with the following legal documents, standards and recommendations:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); 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. 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 Electronic Time-Stamps;
- ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1 Framework and Architecture;
- ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents;
- ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats;
- ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1 Message delivery bindings;
- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2 Evidence and identification bindings;
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-3 Capability and requirements bindings;
- EN 319 532 Part 1 Registered Electronic Mail (REM) Services. Framework and Architecture;
- EN 319 532 Part 2 Registered Electronic Mail (REM) Services. Semantic Contents;
- EN 319 532 Part 3 Registered Electronic Mail (REM) Services. Formats;
- EN 319 532 Part 4 Registered Electronic Mail (REM) Services. Interoperability profiles;
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers;
- ETSI EN 319 531 Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic Mail Service Providers

1.3. Document name and identifier

The full name of this document is “SecuMailer Qualified Registered Electronic Mail Service Policy and Practice”. The identifier for the document is:

Policy name	Object Identifier (OID)
Qualified Registered Electronic Mail Service Policy and Practice	1.3.6.1.4.1.60954.1.1

SecuMailer ensures that it does not alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents, in any circumstances. SecuMailer follows an internal OID management procedure to this end.

1.4. Participants in the infrastructure

a. Users

Any natural or legal person who has a contract with SecuMailer for a Qualified Registered Electronic Mail Service is a QREMS user. Users can use the QREMS (electronic delivery/handover) as senders and/or recipients. Where practically feasible, the products used in the QREMS delivery are also accessible to people with disabilities.

b. Relying parties

Relying parties (third parties) are natural or legal persons who rely on the evidence provided by the provider in relation to the QREMS. They themselves are not QREMS users.

c. Other participants

SecuMailer reserves the right to enter into contracts with external parties for the provision of certain certification services, where necessary.

1.5. Application of Registered Electronic Mail

Registered Electronic Mail (REM) is a specific type of registered electronic mail that is based on the formats, protocols and mechanisms used in normal e-mail messages. Regulation (EU) No. 910/2014 defines a Qualified Registered Electronic Mail Service (QREMS), which is a specific type of ERDS and where the service and its provider shall meet a certain number of additional requirements.

The Qualified Registered Electronic Mail Service (QREMS) allows sending and/or receiving of a consignment that contains user content (e.g. electronic documents) related to it or to its transport metadata and REMS evidence for this process. This service is a useful tool for rapid and reliable delivery of information. SecuMailer ensures the security and safety of the communication with authentication of the time when the user content has been sent by the sender and authentication of the time of receipt of the user content by the recipient, as well as evidence for the communication that guarantees the authenticity of the exchanged deliveries. The evidence can be transmitted immediately (together with the user content or separately) or it can be stored in SecuMailer storage for later access.

The service is designed for legal entities, for administrations, healthcare organisations and organisations providing public services. The service is not intended and/or offered for private / personal / individual use.

1.6. Management of Policy and Practice

a. Management Policy Organisation

SecuMailer is responsible for managing this Policy and Practice. The document is maintained as part of the ISO/IEC 27001 ISMS management structure to ensure that the document is reviewed and updated as part of the ongoing ISMS planning cycle.

Any version of the Policy and Practice is in force until the approval and publication of a new version. Each new version is developed by SecuMailer employees and, after approval by the SecuMailer Board of Directors, is published on the SecuMailer website: https://www.secumailer.nl/eidas.

Users are required to comply only with the valid version of the Policy and Practice at the time of using the services of SecuMailer.

b. Contact person

The contact person in relation to the management of the "Qualified Registered Electronic Mail Service Policy of SecuMailer shall be the Chief Operations Officer of SecuMailer. Further information can be requested at the following address:

SecuMailer

Zilverparkkade 72

8232 WK Lelystad

Contact telephone: +31320337381

Website: https://secumailer.nl

Email address: info@secumailer.com

1.7. Definitions and abbreviations

a. Definitions

Electronic Registered Delivery Service (ERDS) – an electronic service that allows electronic data transmission between a sender and a recipient and presents evidence related to the processing of the data transmitted, including evidence for sending and receiving the data, which also protects the data transmitted from the risk of loss, theft, damages or any unauthorised changes;

ERDS evidence – data generated by the registered electronic mail service the purpose of which is to prove that a given event has happened during a specific period of time;

ERDS handover metadata – data related to the user content generated by the registered electronic mail and handed over to the recipient's agent/ERD;

ERDS notification/return receipt – an ERD message that contains evidence for ERDS and some metadata;

Delivery – an action where the sender's user content has successfully crossed the border with the user agent/application of the recipient;

Interface – in this case this term shall mean user interface, which constitutes a shared border between two separate computer components that exchange information which is used for access to resources.

NTA 7516 – Dutch national standard for transport of medical and confidential data via email

Qualified Registered Electronic Mail Services Provider (QREMSP) – a qualified provider of qualified trust services that provides a registered electronic mail service in accordance with Regulation (EU) No. 910/2014;

Qualified Registered Electronic Mail Service (QREMS) – registered electronic mail service that meets the requirements set out in Art. 44 of Regulation (EU) No. 910/2014;

Recipient – an individual or a legal entity to whom user content is addressed;

REMS consignment – data structure that contains the user content, REMS metadata and/or REMS evidence;

REM handover metadata – data related to the user content generated by REMS and handed over to the user agent;

Registered Electronic Mail Service (REMS) – a service that allows electronic data transmission between entities, provides evidence related to the processing of the data transmitted, including evidence for the data sending and receiving, which also protects the data transmitted against the risk of loss, theft, corruption or unauthorised changes;

REMS evidence – data generated as part of the registered electronic mail service, which have the purpose to prove that a certain event has taken place at a certain moment;

Sender – an individual or a legal entity that provides user content;

Store and Forward (S&F) – REMS operation style (REM Store and Forward) of SecuMailer, where the user content that has been created and sent by the sender is transmitted to the recipient without an express requirement for confirmation by the recipient; After the sender sends the content, the recipient is not required to perform any other action, except for identification and authentication. For this purpose, the user content shall be stored at the recipient's system.

User content – original data created by the sender that should be delivered to the recipient. It can consist of one or more files. The body of the e-mail message and all files attached, if any, constitute user content.

UA/User Agent – user agent/application. This is a system comprising of software and/or hardware components used by the sender/recipient to participate in the data exchange with the registered electronic mail service providers;

b. Abbreviations

DANE – DNS-based Authentication of Named Entities

DNSSEC – Domain Name System Security Extensions

ERDS – Electronic Registered Delivery Service;

IMAP – Internet Mail Application Protocol, protocol for accessing a mailbox

MDA – Mail Delivery Agent (mailbox service using protocols like IMAP/POP3)

MTA – Mail Transfer Agent (mail servers like Exchange, Microsoft 365, Gmail)

MUA – Mail User Agent (mail clients like Outlook, Apple Mail, Gmail)

POP3 – Post Office Protocol, protocol for accessing a mailbox

QTSP – Qualified Trust Service Provider;

QERDS – Qualified Electronic Registered Delivery Service;

QREMS – Qualified Registered Electronic Mail Service;

QERDSP – Qualified Electronic Registered Delivery Service Provider;

QREMSP – Qualified Registered Electronic Mail Service Provider;

REM – Registered Electronic Mail;

REMS – Registered Electronic Mail Service;

S&F – Store and Forward;

SMTP – Simple Mail Transfer Protocol – an internet standard for transfer of electronic mail;

UA (user agent) – user agent/application;

TLS – Transport Layer Security – a cryptographic protocol that ensures the security of internet communication.

2. Responsibility for publication and storage

The public register is available at: https://secumailer.nl/eidas

SecuMailer publishes communication related to the company activity and all significant documents that might be of interest for the users and the relying parties at its website.

Users and relying parties shall be informed about the Policy, Practice and General Terms of the Registered Electronic Mail Service before signing a contract. The documentation, including Policy and Practice, agreements, models, audit reports, etc. is published on the SecuMailer website immediately on each update. The operational certificates of the certifying authority are published immediately upon each issue of new certificates.

SecuMailer offers services related to access to the information stored in the repository (the public register), providing HTTPS based access to it. The information published in the SecuMailer repository is permanently accessible (24/7/365), except in the cases of events beyond SecuMailer's control.

3. Service delivery process

3.1. Requirements toward the qualified registered electronic mail service

QREMS allows transfer of user content between a sender and a recipient who are users of SecuMailer. This service provides evidence for the integrity and time of data transmission, including evidence for their sending and receipt. The service protects the data against loss, theft, breach of their integrity or unauthorised change and meets the requirements of QERDS in accordance with Regulation (EU) No. 910/2014.

The QREMS service provided by SecuMailer complies with the following requirements:

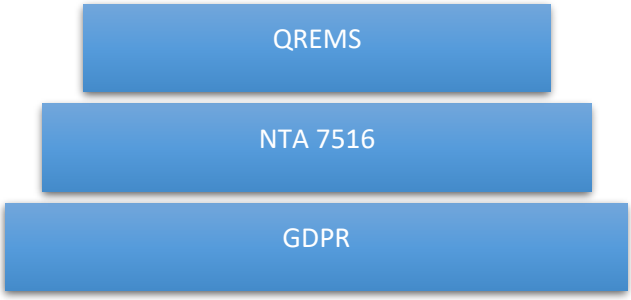
- SecuMailer guarantees the identity of the sending organization
- SecuMailer guarantees the recipient's identity before the delivery of data (the consignment/user content)
- Sending and receipt of the user content is backed by evidence signed with a qualified electronic seal of SecuMailer in a way that precludes any possibility for any unnoticed change in the user content (utilising the ETSI CAdES-T standard[1])
- The date and time of receiving, sending and delivery are noted with a qualified electronic time stamp
- The availability, integrity and confidentiality of user content is guaranteed from the time of receiving (by the QREMS platform), sending, until its receipt
- The integrity of the user content is protected during the exchange between the sender and the recipient or among the distributed system components of the service
- QREMS uses the qualified services of the QTSP SK ID Solutions for issue and management of qualified eSeal certificates (X.509v3) and QTSP DiSig for qualified time stamps
- The entire information on the provision of QREMS is stored for the duration of the contract with the customer

3.2. Technology layers

The SecuMailer QREMS is constructed of several technology layers. In order to ensure integrity of the service one first has to ensure the security of the service. This achieved by building the QREMS on top of two additional layers:

- GDPR security layer
- NTA 7516 security layer.

Visually this layering is represented as follows:



[1] ETSI TS 101 733

a. GDPR Security Layer

The GDPR layer takes care of the confidentiality and integrity of the transport layer. SecuMailer guarantees that a secure connection of sufficient quality is realised between the sender and SecuMailer and from SecuMailer to the recipient. If no such connection can be achieved then SecuMailer will deliver the message via a secure web portal with mandatory usage of 2FA for the recipient.

b. NTA7516 Security Layer

On top of the GDPR layer you will find the NTA 7516 layer. NTA 7516 is a Dutch standard[2], created by NEN, for the exchange of medical and highly confidential data via email. It provides a structure for technical requirements and process agreements to use email as the carrier for confidential data. The NTA 7516 layer takes care of 2FA requirements for both sender and recipient. eIDAS level 'Substantial' or 'High' is required for 2FA. NTA 7516 also adds additional requirements for transport security such as DANE/DNSSEC, SPF, DKIM and DMARC. NTA 7516 requires an advanced digital signature for protecting the payload of the message.

c. QREMS Security Layer

On top of the NTA 7516 layer SecuMailer has created its QREMS solution. QREMS adds the following capabilities:

- A CAdES-T digital signature will be applied to the message, based on a Qualified eSeal digital certificate combined with a Qualified Timestamp
- Full evidence capture of the QREMS process from submission to delivery
- Evidence at various processing stages is signed with a Qualified Timestamp before being stored
- Submission and Delivery notifications for the Sender
- Delivery notification for the recipient

The combination of the GDPR, NTA 7516 and QREMS layers constitute a complete QREMS solution that addresses all requirements from Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

3.3. Description of technology

SecuMailer is integrated with the senders mail system and accepts email as determined by the sender. QREMS emails are provided with a special header on the senders side to distinguish them from general GDPR or NTA 7516 messages. Senders have authenticated themselves with their mail server with two-factor authentication as determined by their NTA 7516 policy.

[2] https://www.nen.nl/en/nta-7516-2019-nl-254878

The connection between the senders mail server and the SecuMailer platform is a SMTP connection using mandatory TLS, certificate DN + hostname verification and SMTP authentication (based on SASL).

Upon receival of the QREMS message by the SecuMailer platform it will recognize the special QREMS header and do the following:

- Select the QREMS transport (which is built on top of the NTA 7516 transport)
- Retrieve the senders authentication mechanism from the database
- Initiate an out-of-band authentication of the recipient
- After successful authentication of the recipient the system will proceed with the QREMS message by adding a CaDES-T digital signature which includes a Qualified Timestamp
- The message will be sent to the recipient utilizing the NTA 7516 transport (using client certificate authentication, DANE/DNSSEC, Mandatory TLS, DKIM, SPF, DMARC)
- Upon receival or non-delivery of the QREMS message an evidence notification will be sent to the sender
- Upon delivery of the QREMS message to the recipient(s) a delivery evidence notification will be sent to recipient(s)
- All aspects of the QREMS message handling are stored in the SecuMailer database for possible later evidence handling

After the consignment enters the recipient's mail system, the consignment is considered handed over. At the moment of this event, the necessary evidence with integrated data about the type of event, including date, time, control/hash sum of the user content, which are electronically signed by the QREMS signing service and signed with a qualified time stamp. If no delivery to recipient mail system is possible, the system also automatically generates the necessary evidence for this event. Upon delivery of the QREMS message the recipient will receive an evidence notification.

3.4. Logical model of the process of delivery of QREMS

QREMS provides data about events that happen during the transmission of user contents (messages, documents and other objects) between the parties, e.g. evidence that the data have been sent by the sender or that they have been delivered to the recipient. This evidence can be used in order to proof to third parties or during court proceedings that the exchange of user content was conducted between the specific parties at a specific moment in time, which is confirmed by a qualified time stamp. All service users (senders and recipients) have a unique identifier that is logged in the REM messages and the evidence for ERDS. For REMS, the users' unique identifier is an e-mail address, as required by clause 5 of ETSI EN 319 532-3.

The evidence for QREMS Is signed with an qualified electronic seal provided by SK ID Solutions. The evidence contains information about a specific event related to the process of data transmission between the sender and the recipient, such as successful/unsuccessful sending or successful/unsuccessful receiving of the user content, as well as the specific moment when that event occurred. The evidence for QREMS can be downloaded from the sender's/recipient's system. SecuMailer stores all evidence for the duration of the customer contract for later access by stakeholders.

QREMS takes place through a "user agent" – an application directly interacting with the user. The user agents/programmes (UA) via which the sender and the recipient communicate with the system for registered electronic mail service are SMTP and IMAP clients that support TLS encryption.

In these cases, the client software uses standard e-mail protocols (SMTP/IMAP) for access to QREMS. The sender and the recipient have a unique identifier used to identify them in REM deliveries and evidence for REMS. For QREMS, the users' unique identifier is an e-mail address, as required by clause 5 of ETSI EN 319 532-3. For the purpose of submission of user content, certain metadata are transmitted by the sender to QREMS, e.g. the e-mail address of one or more recipients, the delivery options, etc. These metadata are transmitted with the electronic mail consignment. The additional specification of the content and the format of the metadata is in line with ETSI EN 319 532-2 and ETSI EN 319 532-3.

The logical model below illustrates the functionality of QREMS in individual components called "roles". The general QERDS model also applies to QREMS. The ERDS elements are described in the QERDS Policy (subsection 4.2.1 of ETSI EN 319 522-1).

REMS components that correspond to the general ERDS components:

REMS components	Corresponding ERDS components
REMS message delivery agent	ERDS message delivery system
REMS evidence provider	ERDS evidence provider
REMS evidence repository	ERDS evidence repository
REMS user directory	ERDS user directory

In addition to the general ERDS components, REMS also provides a component for temporary storage of REMS user content – REMS storage of user contents. This is required because authentication takes place before delivery, hence the REMS user content must be stored temporarily before actual delivery can take place. As soon as authentication and delivery have taken place then the temporary REMS user content will be removed from the REMS storage of user content.

REMS include the following main roles: REMS message delivery agent, REMS message store, and REMS evidence provider. In addition REMS include the REMS evidence repository and the REMS user directory.

3.5. Operational process of provision of service

SecuMailer customers access QREMS using application programs / Uis. In simpler terms, either a mail client like Outlook or a web browser like Google Chrome[3]. SecuMailer interfaces with the mail server and has no direct connection with the Mail User Agents (MUAs) of the customer. The customer must guarantee that the MUAs in use comply with the requirements as stated in the NTA 7516 standard. The use of the service requires initial identification of the sender and recipient. The data about the sender and recipient collected by SecuMailer are personal data, contact details, identity document data, etc. In compliance with GDPR, SecuMailer aims to store the minimum amount of personal data on its systems and if personal data is stored, to limit the duration of the data storage as much as is allowed by rules and regulations.

The SecuMailer QREMS service does not include the mail infrastructure of the sending party. The boundary of the QREMS service is determined by the sending mail server which sends emails of users on behalf of the customer/sending organization. The same applies to the recipient, the boundary of

[3] SecuMailer is fully agnostic with regards to mail clients and web browsers, as long as they support the required (open) standards mentioned in this document.

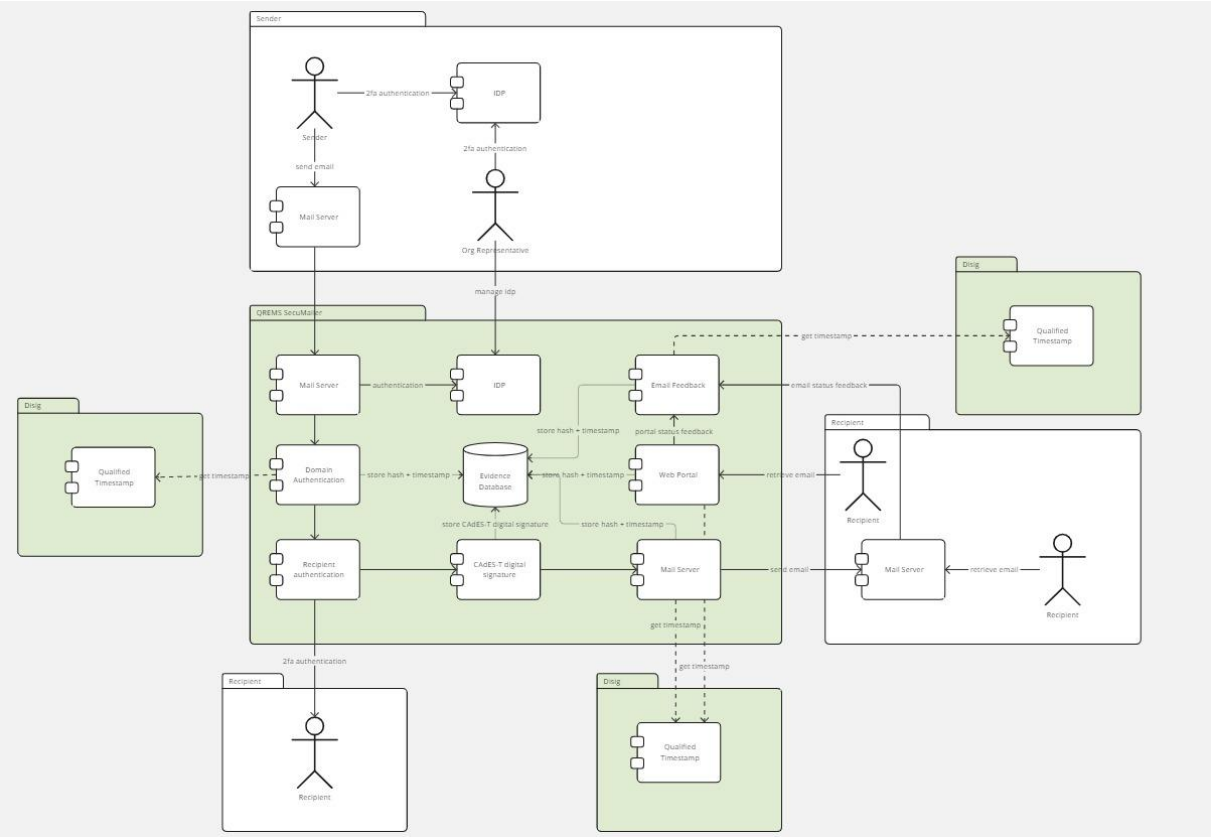
the QREMS service is determined by the recipient mail service. It does not extend to the recipient mail infrastructure.

QREMS provides users with the opportunity to send and receive user content in MIME format. QREMS provides users with the opportunity to send user content through SMTP and to receive user content through IMAP. The latter functionality is outside the scope of the QREMS facility.

The requirements of Regulation (EU) No. 910/2014 are applied for QERDSP and for QERDS for the user content, which is protected through a qualified electronic seal or signature issued by SecuMailer in a way that precludes any possibility for changes in the data without establishing this change. The date and time of sending, delivery and receiving of the user content are signed with a qualified electronic time stamp. The evidence for sending and the evidence for receipt is linked to the user content with a qualified electronic time stamp. The evidence includes a unique identifier, which is the e-mail of the individual or of the legal entity.

SecuMailer applies the Send and Forget (S&F) principle in the provision of QREMS. In this process, the user content provided by the sender is transmitted to the recipient without requesting their express consent. SecuMailer's system allows the user content to be available to the recipient for a certain period of time. After the user content is sent, no other action is required by the recipient, except for authentication.

The diagram below explains the various components of the QREMS, its structure and its boundaries.



a. Senders mail infrastructure

At the top of the diagram the senders' infrastructure is depicted. The sender (at the organization level) is required to use 2 factor authentication of at least eIDAS level Substantial when accessing the mail infrastructure. Mail intended for the SecuMailer QREMS is routed from the sending

organizations email infrastructure to the SecuMailer QREMS mail server. The Senders mail infrastructure is not part of the SecuMailer QREMS scope.

b. SecuMailer QREMS platform

The SecuMailer Mail Server denotes the first element of the QREMS platform. The Mail Server will check the authentication offered by the Sending organizations mail server with the Secumailer Identity Provider (IdP). The identity information for the Senders Organizations is managed by the Organization Representative. The server-to-server authentication is based on SMTP AUTH with the SASL protocol, using mandatory TLS, DANE/DNSSEC and server certificate hostname checking.

After successful authentication the email is considered received for processing and a notification is sent to the sender that the email has been received for processing. This stage is also captured as evidence by computing a hash value of the body of the email (which includes any attachments) and this hash value is signed with a Qualified Electronic Timestamp. The signed hash value is stored in the evidence database.

The next step is to authenticate the recipient(s) at eIDAS level Substantial using a 2 factor authentication utilizing a Time-based One Time Password (TOTP) sent via SMS. This step will be extended with DigiD authentication and eID authentication when it becomes available.

Upon successful completion of the two factor authentication of the recipient(s) a CAdES-T digital signature will be calculated for the email using the eSeal private key and certificate as stored in the QREMS Hardware Security Module (HSM). The CAdES-T digital signature is stored in the evidence database. The CAdES-T digital signature is attached to the email. Any changes to the email after this process step will lead to the repudiation of the digital signature.

The mail is now offered to the SecuMailer mail server for sending to the recipient. This can lead to four possible outcomes:

- Delivery: the email is correctly delivered to the recipient(s)
- Bounce: the email was rejected by the recipients mail server
- Complaint: the email was received by the recipient but tagged as unsolicited email (spam)
- Insecure: the recipients mail server was assessed as being insecure by the SecuMailer QREMS platform

In the situation where the recipients mail server is classified as insecure a new delivery is attempted via the QREMS web portal mail delivery. If the delivery is successful this is captured and a hash of the email will be signed with a Qualified Electronic Timestamp and stored in the evidence database.

In all other cases the Email Feedback component of the SecuMailer QREMS platform will capture the event, calculate a hash of the body of the email and have the hash signed with a Qualified Electronic Timestamp and stored in the evidence database.

In case of successful delivery the recipient will receive an evidence document for the delivery. The sender will have full access to all the evidence that is captured during the QREMS process.

The QREMS platform will send reminders in case the recipient(s) does not authenticate immediately. The platform will try for 4 weeks to deliver the email and send regular reminders during this timeframe to both sender and recipient. In case the recipient never authenticates in this time period the sender will be notified of non-delivery and this will be captured in the evidence database as well.

3.6. Creation of evidence

QREMS provides evidence of the sending and the receipt of user content. SecuMailer collects and stores data on:

- All events related to the initial verification of the identity of the recipient and its identification.
- At the initial verification of identity, the identification data of a natural person, identification data of a legal person and all other data that are necessary for its correct determination are verified.
- Data intended for initial identification of the sender/recipient.
- Authentication level of the sender/recipient.
- Evidence that the sender has been properly authenticated prior to accepting the consignment
- Data on the operation of QREMS confirming the authentication of the sender and the recipient, as well as the communication between them.
- Evidence that the recipient has failed to authenticate (properly) in the timeframe provided for authentication
- Evidence that the user content has been received by the recipient or evidence that the user content has not been received by the recipient
- Evidence that the user content has not been changed during the transmission.

a. Evidence related to the sender

REM fulfils additional requirements in the creation of evidence for REMS for each type of event. Sending is an action where the original user content coming from an external source passes through message submission interface of QREMS. The procedure includes sender authentication. Message submission is accessed through SMTP (Simple Mail Transfer Protocol), which is used for ensuring submission of the user content to SecuMailer QREMS. The sender may use a user agent or a mail transfer agent. After the submission, SecuMailer QREMS may process the submitted original user content in order to approve its acceptance; e.g. it may check it for malware, may check whether the titles of the user content are in line with the requirements for such types of messages, etc.

REMS processes the following events:

Event type under ETSI EN 319 522-1	Relevant interface	Issuer of REMS	Implementation
SubmissionAcceptance	REMS submission	SecuMailer Mail Server	SecuMailer accepts the original user content and it undertakes the responsibility to deliver it to all designated recipients by observing the rules for delivery given by the sender.
SubmissionRejection	REMS submission	SecuMailer Mail Server	SecuMailer rejects the presented user content and informs the sender about the reason for rejection

3.7. Evidence related to the recipient

The submission of user content is a process where the sender's user content (the consignment) is transferred to the recipient's mail server system. The process includes successful initial identification and authentication of the recipient. In this process, the relevant metadata and/or identification data for SecuMailer are transferred together with the sender's content.

The delivery of the user content takes place at the recipient's system. SecuMailer issues evidence for the successful or unsuccessful transfer:

Event type under ETSI EN 319 522-1	Relevant interface	REMS Issuer	Implementation
ContentHandover	REMS delivery	SecuMailer Mail Server	The user content has been successfully delivered to the recipient in their mail system
ContentHandoverFailure	REMS delivery	SecuMailer Mail Server	The user content has not been successfully delivered to the recipient in their system, within a certain period of time or for other reasons.

3.8. Evidence related to the delivery

The delivery is an operation of SecuMailer QREMS, which makes the user content available for the recipient and accessible to him/her/them after their authentication. SecuMailer issues evidence for successful or unsuccessful consignment for each user content to the recipients mail server. The delivery may take place by storing the user content in the recipient's system to which the recipient has access following authentication.

The evidence storage period is 7 years. No user content is stored on the SecuMailer QREMS platform.

SecuMailer QREMS issues evidence for successful or unsuccessful delivery of the user content to the recipient:

Event type under ETSI EN319 522-1	Relevant interface	Issuer	Implementation
ContentConsignment	REMS delivery	Email Feedback Service	SecuMailer delivers the user content to the recipient.
ContentConsignmentFailure	REMS delivery	Email Feedback Service	SecuMailer could not deliver the user content to the recipient within a certain period of time.

In line with the terminology used in ETSI EN 319 531 SecuMailer's Policy specifies the consignment and handover time of user content based on the specific implementation of the QREM service:

- By the recipient's use of a MUA:
  - Consignment: Upon receipt in the mailbox of the recipient(s).
  - Handover: The time of delivery to the recipients mail server.
- By the recipient's use of web interface for access to electronic mail:
  - Consignment: Upon receipt of the retrieval notification in the mailbox of the recipient(s).
  - Handover: At the time of visualisation as a new email in the recipient's browser through the web interface.

3.9. Protection of the data transferred against any risk of loss, theft, corruption or unauthorised changes

Data communication is securely protected by an encrypted channel, thus eliminating the risk of loss, theft, damage or unauthorized modifications of data. The evidence is reliably stored to prevent against any subsequent loss and theft in a protected environment under the control of SecuMailer QREMS for the duration of the contract.

3.10. Termination of service subscription

Termination of the service is available on week days from 08:00-17:00 CET. The time in the systems associated with the termination of a service contract for the provision of electronic registered email service is synchronized to UTC at least every 24 hours.

4. Identification and certification of identity

4.1. Names

The name requirements in the issued certificates are as specified in Recommendation ITUT X.509 or IETF RFC 5280 and ETSI EN 319 412. The names may be in accordance with the Domain Name Service (DNS) described in RFC 2247. This way allows subscribers to use two types of names: DN and DNS at the same time.

SecuMailer will use a qualified eSeal certificate issued to the entity “SecuMailer”. SecuMailer will sign email with this certificate on behalf of the user.

4.2. NTA 7516

NTA 7516 is a Dutch standard for the exchange of medical and highly confidential data via email. It provides a structure for technical requirements and process agreements to use email as the carrier for confidential data.

The standard distinguishes between two classes of recipients:

- Professional recipients: Healthcare professionals and healthcare organisations
- Consumer recipients: Patients, caretakers and other natural persons outside of a healthcare organisation with a valid interest in the information

Professional recipients must make use of a NTA 7516 solution offered by a certified vendor in order to receive secure email as a professional recipient. This is established by means of a special DNS resource record in the DNS of the NTA 7516 professional sender / recipient that contains the name (and gateway) of the vendor.

Recipients without the NTA 7516 resource record are by definition classified as consumers.

The distinction is relevant for the application of certain technical standards and the means of authentication.

Professional recipients must comply with the following technical standards: TLS, DANE + DNSSEC, DKIM, SPF and DMARC.

Professional recipients must also be onboarded with a special procedure that establishes the identity of the organisation, its representatives and the technical measures they have carried out to comply with the NTA 7516 standard. This includes mandatory 2FA authentication on the workstation of the employee using the NTA 7516 solution of a vendor. These informational elements are captured in a customer agreement. Only after signing the agreement will the customer be allowed to provide the NTA 7516 resource record to its DNS.

Consumer recipients must use a mail server that supports TLS, DKIM, SPF and DMARC. Most modern mail providers are able to comply with these requirements. Because there is no insight into the execution or availability of 2FA on the recipient side it means that the NTA 7516 sender will have to provide 2FA authentication to the recipient.

After the authentication of the recipient (either professional or consumer) the actual message is delivered to the recipient. In the case of SecuMailer this is via regular email protocols (SMTP / IMAP / POP3). This closely mimics the requirements of Registered Electronic Mail service with the exception of the qualified digital signature and qualified timestamp.

4.3. QREMS additions on top of NTA 7516

SecuMailer has built its Registered Electronic Mail Service on the foundation of the NTA 7516 standard and has added to its service:

- CAdES-T digital signature using qualified eSeal certificate and qualified timestamp
- QREMS evidence storage
- QREMS evidence notifications to the sender
- QREMS evidence notification to the recipient
- Qualified timestamp for QREMS evidence on the following positions in the process:
    - Upon receiving the email from the sender
    - Just before the delivery to the recipient(s) via email
    - Upon delivery to the recipient by email
    - Upon delivery to the recipient via web portal

4.4. Initial verification of identity

The SecuMailer system for QREMS allows sending user messages and attached documents/files (user content) as consignments. The difference with the simple electronic delivery is that the sender and the recipient must first undergo an initial identification process before using the system. In the process of service, the sender of electronic documents is authenticated and only after that he sends the consignment, and respectively the recipient has access to its content after it has been authenticated too.

SecuMailer verifies the identity of the sender in person or may use a third party organization for verification in person. During the personal identity verification the person must have a valid identity document available. The Identity Verification Officer needs to verify that the person and the presented identity document match. The process outcome is captured in a statement by the Identity Verification Officer. A number of document attributes (full names, date of birth, place of birth, start date and end date of the document) are captured in the statement. No copy of the identity document is stored by SecuMailer.

After verification of the information provided, identity / identity data shall be generated for the organisations who have been retained in the SecuMailer repository for the duration of the contract. SecuMailer fulfils the requirements under Art. 24 of Regulation (EU) No 910/2014 by retaining all relevant information in order to provide evidence in court proceedings and to ensure continuity in the provision of the service.

a. Establishing the identity of a natural person

The establishment and initial verification of the identity of a natural person is divided into two categories:

- Natural person as legal representative of the customer
- Natural person as recipient of a QREMS communication

The first category of users, natural person as legal representative of the customer, requires a minimum set of data consisting of:

- Family name (or names)
- Personal name (or names)

- Business address
- Job title
- Contact information

SecuMailer verifies the identity of the legal representative in person or may use a qualified third party organization for verification in person. During the personal identity verification the legal representative must have a valid identity document available. The Identity Verification Officer needs to verify that the person and the presented identity document match. The process outcome is captured in a statement by the Identity Verification Officer. A number of document attributes (full names, date of birth, place of birth, start date and end date of the document) are captured in the statement. No copy of the identity document is stored by SecuMailer.

Upon successful verification of the person, an agreement to enter into a QREMS contract will be signed by the verified legal representative.

The second category of users, natural person as recipient of QREMS communication, requires a minimum set of data consisting of:

- Family name (or names)
- Personal name (or names)
- Home address
- Mobile phone number
- Email address

This data is captured on the side of the QREMS sender, in accordance with the requirements of NTA 7516.

b. Establishing the identity of a legal entity

The minimum set of data for a legal entity shall contain the specific data listed below:

- Name of the legal entity (company)
- General phone number of the legal entity
- Business address
- Chamber of Commerce registration number
- VAT registration number
- Means of 2FA authentication for its users

4.5. Authentication

Senders are authenticated using the various means allowed by the NTA 7516 standard, requiring eIDAS level Substantial or High. The senders authentication mechanism is described in the NTA 7516 statement and a reference is stored in the SecuMailer QREMS database to be used in the creation of evidence.

Recipients are authenticated using two factor authentication (2FA) based on eIDAS level Substantial or High. Currently supported mechanisms are TOTP (RfC 6238) via SMS. Future supported mechanisms are DigiD[4] (Dutch national eID) and Itsme[5].

[4] https://www.digid.nl/
[5] https://www.itsme-id.com/

5. Control of physical and organizational security

5.1. Physical security controls

The measures taken with regard to the physical protection of SecuMailer are an element of the information security system developed and implemented in SecuMailer which complies with the requirements of the ISO/IEC 27001 standard. The SecuMailer ISO/IEC 27001 ISMS describes all controls in document “B10 Control of physical access”.

SecuMailer hosts its physical infrastructure with Amazon Web Services (AWS). SecuMailer uses the eu-west-1 region (Dublin/Ireland) and the eu-central-1 region (Frankfurt/Germany).

AWS supports 143 security standards and compliance certifications including ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015, and CSA STAR CCM v4.0, GDPR and ISAE 3402.

The measures related to the physical protection of information data, technology systems, premises and their related support systems are aimed at preventing:

- Unauthorised access, damage and interference with working conditions.
- Loss, damage or compromise of resources.
- Compromise or theft of information or information processing tools.
- The SecuMailer infrastructure is physically and logically distinct and is not used for any other *a*ctivities performed by SecuMailer.

a. Premises and premise construction

SecuMailer premises are purely used for office work and do not contain any sensitive data or equipment.

b. Physical access

Physical access to AWS data centres complies with the most stringent controls. A complete overview can be accessed at this location: https://aws.amazon.com/compliance/data-center/controls/

c. Access control

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access to SecuMailer systems is limited to authorized personnel.

5.2. Incident management

Any person who witnesses or suspects a security incident is required to inform the management. Reporting security incidents may be performed in any way (personally, by telephone or email) that enables the relevant management persons to be notified as soon as possible. The management is required to investigate the reported incident and to adopt or propose appropriate measures to prevent its recurrence. Every security incident is recorded in a protocol.

5.3. Human resource security

SecuMailer ensures that its employees perform administrative and management procedures and procedures that are consistent with information security management, thereby ensuring the reliability and security of its operations.

SecuMailer recruits staff and, where applicable, hires subcontractors who have the necessary experience, reliability and qualifications and who have undergone training in security and protection of personal data.

SecuMailer applies appropriate disciplinary sanctions to employees who violate company policies or procedures.

5.4. Audit procedure

The audits performed in SecuMailer concern the processing of information data and the management of key procedures. SecuMailer annually performs at least one internal audit. The provider has successfully undergone an audit from TüV Nord and Brand Compliance and is certified under the following standards: ISO/IEC 27001, NEN 7510 and NTA 7516.

5.5. Archiving

Information about significant events is periodically archived in an electronic form. SecuMailer archives all data and files related to: registration information, the system security, all requests submitted by customers, all customer information and all correspondence between SecuMailer and its customers. All documents and data used in the identity verification process are subject to archiving.

The information under Art. Article 24 (2) (h) of Regulation (EU) No 910/2014 (all relevant information in relation to data issued and received by SecuMailer, in particular with a view to providing evidence in court proceedings and insurance of continuity in the provision of the service) is stored for the duration of the contract.

a. Storage of data media

No removable media may be used. No data may be stored on premise. All data must be stored in controlled cloud environments.

b. Waste disposal

Procedures for safe destruction of media have been put in place to minimize the risk of leakage of confidential information to unauthorized persons. The procedures for safe destruction of media containing confidential information are consistent with the sensitivity of such information.

c. Asset management

SecuMailer ensures an adequate level of protection for its assets, including information assets. The provider maintains a list of all information assets and performs a risk assessment.

d. Records of events and keeping logs

All meaningful changes are captured in log files. Log files are append only and cannot be changed. Log files are stored for the shortest possible duration as allowed by rules and regulations. eIDAS evidence is stored for 7 years and automatically erased after that period.

5.6. Business Continuity Plan

SecuMailer has developed, documented, implemented and currently maintains control plans, procedures and mechanisms in line with the International Standard ISO 22301 to ensure the necessary level of business continuity and information security during adverse events.

SecuMailer ensures:

- An adequate management structure in order to prepare, mitigate and respond to a disastrous event using staff having the necessary authority, experience and competence.
- The development and approval of response and recovery plans and procedures, describing in detail how the company will manage a disastrous event and maintain the continuity of information security.
- Information security control mechanisms within the procedures and supporting systems and tools for business continuity and recovery after a disaster.
- Compensating mechanisms for control of the information security control mechanisms that cannot be maintained during an adverse event.

A business continuity plan is provided that involves duplication of critical systems. Backup is stored in geographically remote locations. The specific conditions are in line with the applicable standards, recommendations and regulations specified in the area of information security. SecuMailer reviews at regular intervals of time the mechanisms created for control of the information security continuity so as to ensure their effectiveness and efficiency during adverse events.

SecuMailer regularly creates backups of important information and software and ensures that all basic information and software can be recovered after a disaster or in case of loss of the archive.

Recovery mechanisms are reviewed regularly to ensure that they meet the requirements of the Business Continuity Plan.

6. Controls of technical security

6.1. Protection of private keys and cryptography module

SecuMailer has developed security controls for the management of all cryptographic keys and cryptographic devices during their entire lifecycle.

SecuMailer uses a Qualified eSeal certificate issued by SK ID Solutions, registered as a Qualified Trust Service Provider and included with the European Trust List.

The private key of the Qualified eSeal is stored in AWS KMS, a certified FIPS 140-2 level 3 Hardware Security Module[6] and does not exit the environment unprotected. This key is archived, stored and recovered only by employees on trusted positions. The number of employees authorised to perform this function is minimum and corresponds to the QREMS practice.

SecuMailer uses a remote Qualified Electronic Time Stamp service provided by DiSig A.S., registered as a Qualified Trust Service Provider and included with the European Trust List. As such no key storage requirement exists for the Qualified Electronic Time Stamp.

QREMSP uses modern protocols and algorithms for encryption of the data transmitted.

6.2. Computer security

SecuMailer uses Amazon Web Service cloud infrastructure as its hosting platform. AWS is responsible for ensuring the confidentiality, integrity and availability of its cloud infrastructure (Shared Responsibility Model[7]).

The architecture of SecuMailer uses serverless computing which results in computer systems that are only active for milli seconds after which they are discarded. There is no permanent compute infrastructure to attack and / or abuse.

Workstations of SecuMailer employees are protected with standard measures for anti-virus and malware. Documents are stored in Microsoft 365 cloud, there is no local storage on workstations.

6.3. Information system vulnerability assessment

SecuMailer classifies and maintains registers of all assets in accordance with ISO/IEC 27001. According to the SecuMailer Security Policy, an analysis of the vulnerability assessment is performed for all internal procedures, applications and information systems. Analysis requirements may also be determined by an external institution authorized to audit SecuMailer.

The analysis of the activities and the supervision of the performance of all procedures are automatically by the security systems of all information and communication devices of SecuMailer. The vulnerability assessment is based on analysis of logs, security events, and other important data.

SecuMailer uses intruder.io for continuous vulnerability management and AWS Security Hub for continuous security baseline monitoring.

[6] https://aws.amazon.com/kms/features/
[7] https://aws.amazon.com/compliance/shared-responsibility-model/

6.4. Network security

SecuMailer infrastructure utilizes modern technical means of information exchange and protection to ensure the network security of systems against external interventions and threats. The SecuMailer network at AWS is fully compartmentalised into various zones separated with access controls, firewalls and zone routing. Inbound traffic is only possible via clearly defined and controlled ingress points

6.5. Timestamp

SeuMailer QREMS uses the Qualified Electronic Time Stamp service from DiSig a.s.

7. Compliance audit and other assessment

The audits carried out at SecuMailer concerns the processing of information data. SecuMailer annually performs at least one internal audit. SecuMailer is annually audited by TüV Nord as part of its ISO/IEC 27001 and NEN 7510 certification.

7.1. Actions taken as a result of an audit

Reports of internal and external audits are transmitted to SecuMailer. On the basis of the assessments made in the report, SecuMailer's Management Team sets out measures and deadlines for remedying the identified gaps and inconsistencies. SecuMailer staff undertake specific actions for their removal within the specified deadlines.

8. Other business and legal issues

8.1. Financial responsibility

SecuMailer shall be financially liable to QREMS customers who rely on its business. The financial liability shall only be applicable if the damage is due to the fault of SecuMailer or the parties with which it has concluded an agreement. If SecuMailer confirms and accepts that damage has occurred, it undertakes to compensate the damages. The maximum payment limit shall not exceed the amount of damage and shall not exceed the monthly fee for the month the issue occurred.

8.2. Personal data privacy

SecuMailer is registered as a personal data processor under the terms of the Personal Data Protection Act. As a personal data processor SecuMailer strictly respects the requirements for the confidentiality and non-disclosure of personal data of natural and legal persons that have come to its knowledge in the performance of its activities as a Qualified Trust Service Provider.

The company uses in its activities:

- Only such information about the activities and the business of its customers and partners that is required to provide QREMS.
- Confidential information such as commercial, financial and technical documents (software, data, surveys, prices, contracts and other documents).

SecuMailer frequently informs its employees of their obligations.

8.3. Intellectual property rights

There are various data integrated in the QREMS operated by SecuMailer, which are subject to intellectual property rights and other proprietary or non-proprietary rights.

8.4. Obligations, responsibilities and warranties

a. Obligations, responsibilities and warranties of SecuMailer

SecuMailer warrants that it performs its activities by:

- Complying with the terms and conditions of this document, the requirements of Regulation (EU) No. 910/2014 and the national legislation.
- Its provided QREMS service not infringing the copyrights and licensed rights of any third party.
- Using technical equipment and technologies that ensure system reliability and technical and cryptographic security in the performance of the processes, including a secure and protected mechanism/device for generating keys in its infrastructure.
- Providing QREMS after verifying the information provided by means permitted by law.
- Securely storing and maintaining information related to the QREMS provided and the systems operational performance.
- Complying with the established operational procedures and the technical and physical control regulations, in accordance with the terms and conditions of this Policy.
- Providing conditions for the accurate determination of the time of sending and receiving data.
- Performing procedures of identification and authentication of natural and legal persons or of authorized representatives of legal persons;

- Taking immediate measures in the event of technical security issues.
- Informing customers about their obligations and due care in the use of the QREMS certification service provided by SecuMailer.
- Using and storing the collected personal and other information only for the purposes of its activities in accordance with the national legislation.
- Maintaining disposable funds, which enable it to carry out its activities.
- Concluding an insurance for the period of its activities.
- Maintaining trusted staff having the necessary expertise, experience and qualifications to perform the activities.
- Maintaining a Public Register in which it publishes electronic documents related to its activities.
- Providing permanent access to the Public Register by electronic means (24/7/365).
- Ensuring protection against the introduction of changes to the maintained Public Register from unregulated or unauthorized access or due to a random event.
- Performing periodic internal audits of the SecuMailer platform.
- Performing external audits by independent auditors and publishing the audit results on its website.
- Using in its activities certified software and hardware as well as secure and reliable technology systems.
- Providing maximum access to its services (365/24/7), except for the following cases:
    - Scheduled and pre-announced technical repairs to the infrastructure.
    - Unscheduled technical repairs to the infrastructure as a result of unforeseen failures.
    - Maintenance due to infrastructure failures beyond the provider's jurisdiction.
    - Inaccessibility of the service as a result of force majeure or extraordinary events.
- Declaring the maintenance or upgrading of its infrastructure at least three (3) days prior to the commencement of the repair.

SecuMailer is liable to its customers for any damages caused by gross negligence or intent:

- Resulting from failure to comply with the requirements of Regulation (EU) No. 910/2014 in the performance of its QREMS provision activities
- Resulting from failure to comply with its obligations to provide QREMS
- Resulting from faults in establishing the original identity of customers.

b. Obligations of senders and recipients

Natural and legal persons shall have the following obligations:

- To become acquainted with and comply with the terms and conditions of the Agreement, the General Terms and Conditions, Policies and Practices when using QREMS, as well as the requirements in the other documents published in the Public Register of SecuMailer.
- To use the qualified electronic registered delivery for legitimate purposes only and in accordance with its Policy and Practice.
- To agree with the terms and conditions set out in the Agreement between them and SecuMailer.

c. Release from liability

SecuMailer IS NOT liable for damages arising from:

- The use of QREMS beyond the limits of its listed intended uses and restrictions of its operation.
- Illegal actions by customers.
- Accidental events having the nature of force majeure, including malicious actions of third parties (hacker attacks, depriving of the device for the use of the electronic registered delivery, of the identification method, etc.).
- The use of electronic registered delivery in non-compliance with the requirements and procedures of the SecuMailer Practice and Policy.
- Poor quality and functionality of the software products and hardware devices used by customers.
- Incorrect and inadequate password protection.
- The disclosure of confidential data and irresponsible behaviour by customers.
- Damage to the infrastructure beyond SecuMailer's area of management.
- Inadequate customer behaviour when using the QREMS service.

8.5. Limitation of liability

For the Qualified service of Registered Electronic Mail, SecuMailer sets a liability limit of EUR 5.000.

8.6. Activity insurance

SecuMailer concludes a compulsory insurance for its activities as a Qualified Trust Service Provider.

8.7. Time and termination of Policy and Practice

This document becomes effective as soon as it is approved by the Board of Directors of SecuMailer and published in the SecuMailer Public Register. Appendices to this Policy and Practice take effect after their publication.

The provisions in this document are valid until the next version of this document is published on the SecuMailer website.

Upon termination of the operation of SecuMailer, the topicality of the Policy and Practice, as well as the provisions contained in this document, are terminated.

The Provider keeps all previous versions / editions of this document duly and securely.

8.8. Policy and Practice amendments

Changes in this document may result from observed errors, updates and suggestions from affected parties. In the event of an invalid Policy and Practice clause, the validity of the entire document is retained and the contract with the customer is not violated. The invalid clause is replaced by a legal norm.

SecuMailer may make editorial changes to this document that do not affect the content of the rights and obligations contained therein. In the event of changes to Policy and Practice, the Object Identifier of the document (OID) is retained and does not change. Changes that lead to a new version of the document are published on the SecuMailer website.

8.9. Dispute settlement

Any disputes or complaints concerning the use of QREMS provided by SecuMailer shall be settled through mediation on the basis of written information. Complaints shall be dealt with by the legal adviser of SecuMailer. Any complainant will receive a reply within 2 (two) business days after the submission thereof. In the event that no resolution is found for a dispute within 30 (thirty) days of the commencement of the settlement procedure, the parties may refer the dispute to the Dutch courts.

8.10. Applicable law

For all matters not covered by this document the provisions of the Dutch legislation shall apply.

8.11. Compliance with applicable law

SecuMailer warrants that the service operates legally and reliably. It is offered in accordance with the applicable legal requirements. Any issues not settled by this document shall be governed by the provisions of the Dutch legislation. In the event that national legislation changes, the legal rules shall apply until the harmonization of this Policy.

SecuMailer warrants that personal data are processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the processing of personal data and on the free movement of such data.

Wherever possible, the QREM service and the end-user products used in the provision of the service are accessible to disabled people.

8.12. General provisions

The obligations and responsibilities of consumers and SecuMailer are governed by contractual agreements. Relationships with trustworthy parties are governed by general law. Contracts for the provision of QREMS should be concluded in written or electronic form, subject to the provisions of Regulation (EU) No 910/2014, Regulation (EC) 2016/679 and the applicable legislation in the Kingdom of The Netherlands.

SecuMailer

2024.06.26 11:06:21 +02’00