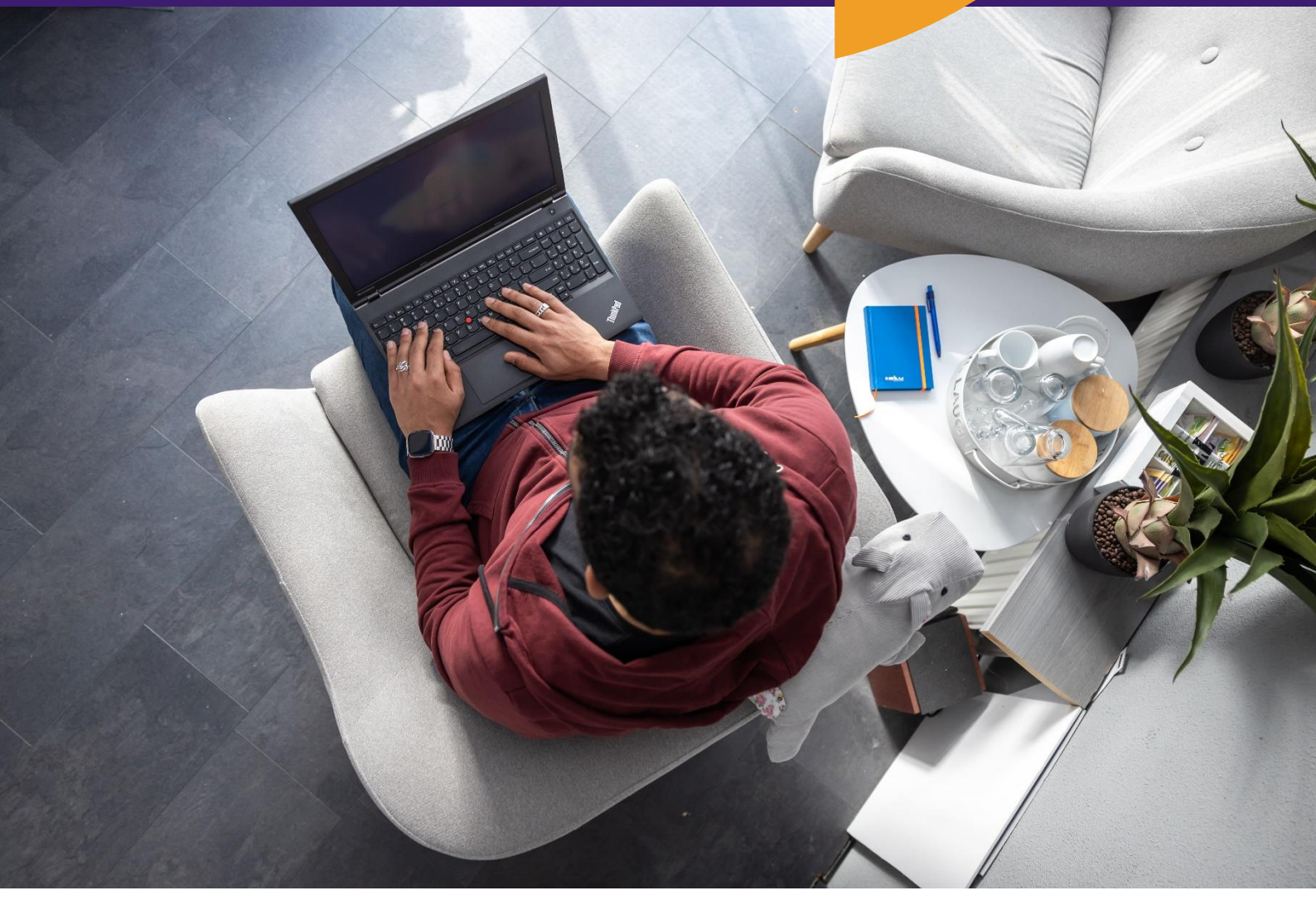
SecuMailer

Qualified Registered Electronic Mail Service

Termination Plan

Versie: 1.2
Status: Final



Contents

1. Introduction 3
2. Termination plan provisions 6
3. Termination plan project 9
4. Scheduled termination 10
5. Unscheduled termination 10
6. Compliance 11

1. Introduction

1.1. Overview

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 Supervisory Body (SB) Rijksinspectie Digitale Infrastructuur (RDI).

SecuMailer provides to its users highly reliable and secure Qualified Registered Electronic Mail service in accordance with Art. 44 of Regulation (EU) No. 910/2014.

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.

1.2. Document name and identifier

The full name of this document is "SecuMailer Qualified Registered Electronic Mail Service Termination Plan". The identifier for the document is:

Policy name	Object Identifier (OID)
Qualified Registered Electronic Mail Service Termination Plan	1.3.6.1.4.1.60954.3.1

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.

1.3. QTS to which the termination plan applies

This Termination Plan is specifically for terminating the SecuMailer Qualified Registered Electronic Mail Service (qREMS), as defined in ETSI EN 319 531.

1.4. Termination plan administration

Management Policy Organisation

SecuMailer is responsible for managing this Policy. 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 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.

This document shall enter into force upon its approval by the Board of Directors of SecuMailer. The provisions of this document are valid until the next version is published on the SecuMailer website.

Contact person

The contact person in relation to the management of the "Termination Plan" 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

1.5. Definitions and abbreviations

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;

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;

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;

Abbreviations

ERDS – Electronic Registered Delivery Service;

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;

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

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

2. Termination plan provisions

SecuMailer provides a Qualified Electronic Delivery Service (qERDS), specifically a Qualified Registered Electronic Mail Service (qREMS). A qREMS uses standard email protocols as part of its service delivery.

SecuMailer does not store any e-mails on its platform, it only stores meta-data for evidentiary purposes. The actual emails reside with the sender (mail system) and the recipient (mail system).

SecuMailer uses cryptographic material provided by 3rd parties, specifically a Qualified eSeal from SK ID Solutions[1] and a Qualified Electronic Timestamp from Disig a.s[2]. These cryptographic materials are provided by organizations with their own termination plans, therefore they are not part of the scope of this termination plan.

SecuMailer uses a CAdES-T digital signature, conforming to ETSI TS 101 733[3]. As a result the digital signature will be valid even when the underlying cryptographic infrastructure has expired. A cessation of activities by SecuMailer will have no impact on the validity or longevity of issued digital signatures.

2.1. Termination impact

On terminating the SecuMailer service the impact is relatively low compared to QTSP's that issue their own cryptographic key material and / or that store mail data on their platform. Because no email is stored on the SecuMailer platform, no export of customer data needs to take place. All email is available at the sender and / or the recipient(s). Because SecuMailer uses a CAdES-T digital signature based on 3rd party QTSP cryptographic material there is no impact due to unavailability of any cryptographic infrastructure.

The biggest impacts are:

- That the service terminates and that subscribers need to find an alternative solution.
- Stored evidence needs to be provided (exported) to the subscribers of the service

2.2. Termination Plan

The Termination Plans has as its scope the Qualified Electronic Registered Delivery Service, specifically Qualified Electronic Registered Electronic Mail, as defined by ETSI EN 319 531.

The obligations described below have been developed in order to minimise any interruptions in the users' and relying parties' operations as a result of SecuMailer's decision to terminate its activity. In its termination plan for its activity, SecuMailer applies the procedure that fulfils the requirements specified in clause 7.12 of ETSI EN 319 401.

SecuMailer periodically updates this termination plan. Exact periodicity is determined by the Information Security Planning procedure but will be at minimum annually.

[1] https://orderforms.skidsolutions.eu/en/services/Digital-stamp

[2] https://eidas.disig.sk/en/qualified-electronic-time-stamps/

[3] https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf

Scheduled termination encompasses the following scenarios:

- End of life cycle or decommissioning of the technical instance of the qREMS QTS
- Anticipated termination of qREMS QTS provisions
- Takeover, merging or acquisition of qREMS QTS activities by another legal entity

2.3. Granularity of the service

This Termination Plan is specifically for terminating the Qualified Registered Electronic Mail Service (qREMS), as defined in ETSI EN 319 531.

2.4. Scope

The Termination Plan applies to subscribers, relying parties and supervisory body. Terminating the QTS will be the responsibility of the COO of SecuMailer. The COO is responsible for setting and communicating the time line for the termination of the QTS. The COO is responsible for ensuring that the provisions for subscribers, relying parties and supervisory body as determined below are carried out as documented.

2.5. Termination notifications

The COO will inform subscribers, relying parties and supervisory body.

Subscribers

Subscribers will be informed via the default communication method for customer communications which is a service notification via email. In the service notification the COO will announce termination of the QTS and the time line for terminating the service. *This will be at minimum a period of three months between the announcement and the actual termination*. The COO will suggest alternative QTS solutions for the provided qREMS service. Currently there are no other qREMS S&F style solutions in the market which prohibit any potential migrations of the SecuMailer service to an alternative solution (due to technology mismatch). The COO will communicate about the provisioning of evidence as stored by SecuMailer for its subscribers. At the end of the communicated time period for termination SecuMailer will provide a zip file with all evidence documents pertaining to the subscribers usage. This zip file will contain a document per consumed qREMS service holding the evidence attributes as prescribed by ETSI EN 319 521 section 5.4.1 – 5.4.3.

Relying parties

Relying parties are informed by email by the COO of the intention of terminating the QTS and the timeline for termination. Currently identified relying partners are limited to resellers.

Supervisory body

The Supervisory Body (SB) is informed by email by the COO of the intention of terminating the QTS and the timeline and planning for termination. Planning will contain the steps required for terminating the service with subscribers, including the evidence export planning.

2.6. Impact of termination

SecuMailer only stores evidence on its SaaS platform, it does not store emails and it does not issue its own cryptographic material.

Emails are available on the source systems of both sender and recipient. They are not available on the SecuMailer platform due to the GDPR requirement of data minimisation. Therefore an export of processed emails is not possible and not needed.

SecuMailer doesn't issue cryptographic key material, it uses 3rd party supplied cryptographic material (qualified eSeal certificate and private key from SK ID Solutions and remote qualified electronic time stamp for Disig). Termination of QTS services has no impact on the validity of processed emails and the digital signature as SecuMailer uses the CAdES-T format which fixates the digital signature. This means that the digital signature will remain valid even when the underlying cryptographic material has expired. Availability of the original cryptographic material is not required for technically validating the digital signature, at any time in the future. SecuMailer will remove the cryptographic material from its protected storage as last item in its Termination Plan.

Legal validation of the digital signature requires availability of evidence. It is the responsibility of the COO to export all evidence and make this available to its subscribers before actual termination. The COO will create an export per subscriber of the evidence documents. The export will be a zip file containing the evidence documents. The zip file will be securely mailed to the subscriber. Each evidence document will use the message-id of the email as the file name identifier. This is a globally unique id so there is no risk of collision with other evidence documents.

SecuMailer currently only has the QTS qREMS on the EU trusted list. Termination of the qREMS service therefore does not impact any other QTS service of SecuMailer or any other relying partner.

2.7. Risk analysis

SecuMailer has identified the following risks specifically for the Termination Plan:

- Lack of available funds for executing the Termination Plan
- Lack of available knowledge/capacity for executing the Termination Plan

Availability, Integrity and Confidentiality of the QTS are not at risk as the platform will continue uninterrupted (business as usual) during a scheduled termination, in line with its ISO 27001 ISMS measures.

The identified risks are remediated in the paragraph "Financial resources".

2.8. Financial resources

SecuMailer will ensure appropriate finances to complete the provisions of the Termination Plan. To this end SecuMailer has incorporated the "Stichting SecuMailer[4]" which has sufficient financial means to ensure uninterrupted operation of its platform for at least three months. This includes required staff for the execution of the Termination Plan. At least one DevOps engineer needs to be available to carry out the evidence export as identified in paragraph "Expected impact".

Insurance will be continued until the end of the Termination Plan.

[4] NL Chamber of Commerce registration 91597234

2.9. Personal data impact assessment

SecuMailer does not permanently store emails. The only personal data attribute that has been identified in its platform DPIA is the subject line of an email. SecuMailer uses a Data Processing Agreement with its subscribers to safeguard this data attribute from a privacy perspective.

In case of termination of the QTS SecuMailer will remove the applicable statements from its audit log that contain the meta-data of qREMS processed emails.

2.10. Compensation for subscribers

SecuMailer uses a pay-per-use scheme for the qREMS service based on actual usage. Payment is after the fact. There are no additional subscription costs. When terminating the service there are no charges that need to be repaid. Therefore there is no need for compensation of the subscribers.

3. Termination plan project

Three months before its intended QTS termination SecuMailer will communicate its intention to the stakeholders as identified in “Termination notification”.

SecuMailer has a complete administration of all its subscriber representatives and will use this list to send the notifications. The SecuMailer COO will communicate the intention to the replying parties and the Supervisory Body.

SecuMailer will communicate that it will stop providing the service in three months’ time from the date of notification.

SecuMailer will create the solution for the evidence export activity. The solution will be developed and tested in the three months notification time frame.

SecuMailer will send reminder notifications of the intended termination every 4 weeks.

Upon reaching the termination date SecuMailer will deactivate its QTS processing logic. New qREMS messages will not be processed and the sender will receive a rejection notification. SecuMailer will initiate its evidence export process the day after the termination date. All subscribers will receive their evidence export. The export will be sent as a zip file to the original senders of the qREMS messages. In case of a bounce of the message the export will be sent to the organizational representative.

After the evidence export process has completed SecuMailer will delete its 3rd party cryptographic keys from the protected key storage. The evidence database will be stored in such a way that the data will be available for later requests.

SecuMailer will create a website that holds the public keys of its cryptographic material and it will provide contact information to answer any questions with regards to the evidence position for a period of 7 years after termination.

SecuMailer will inform the Supervisory Body of the completion of the Termination Plan and any issues that were found during execution of the Termination Plan.

4. Scheduled termination

In case of a scheduled termination the following provisions shall apply. Execution of the Termination Plan is the responsibility of the COO, supported by other Managing Board officers where required.

Scheduled termination describes the situation wherein SecuMailer voluntarily decides to terminate its eIDAS business. This can be due to business, legal or financial reasons. In a voluntary situation there is sufficient time and financial resources for terminating the eIDAS operations.

Before SecuMailer terminates its services, at least the following procedures apply:

- SecuMailer informs the following of the termination of its activity:
    - All subscribers and other stakeholders with which it has agreements
    - Stakeholders with an established relation among which relying parties, the relevant competent authorities such as supervisory bodies
- Upon terminating its services, SecuMailer terminates the authorisation of all subcontractors to act on their behalf in carrying out any functions relating to the process of issuing trust service certificates/tokens and/or reports
- Upon terminating its services, SecuMailer transfers its obligations to a reliable party ("Stichting SecuMailer") for maintaining all information necessary to provide evidence of the operation of the services for a reasonable period, unless it can be demonstrated that SecuMailer does not hold such information.
    - SecuMailer will maintain a website where its public key material will be available (https://secumailer.nl/eidas).
    - On this website a contact address will be available where concerned parties can raise requests for evidence provision during the 7 years validity period of its evidence database
- Upon terminating its services, the private key(s) of SecuMailer, including backup copies, are destroyed or withdrawn from use, in a manner such that the private key(s) cannot be retrieved
- Upon terminating its services, where possible, SecuMailer will endeavour to transfer the provision of trust services for its existing customers to another qualified trust service provider

5. Unscheduled termination

Unexpected or unscheduled termination of the QTSP may result from different causes such as severe incident or disaster from which incomplete or unsatisfactory recovery could be reached, bankruptcy, court orders, and any other unexpected reason forcing the QTSP to execute a termination

In case of an unscheduled termination the provisions of a scheduled termination will be followed as much as possible.

Before SecuMailer terminates its services, at least the following procedures apply:

- SecuMailer informs the following of the termination of its activity:
    - All subscribers and other stakeholders with which it has agreements
    - Stakeholders with an established relation among which relying parties, the relevant competent authorities such as supervisory bodies
- Upon terminating its services, SecuMailer terminates the authorisation of all subcontractors to act on their behalf in carrying out any functions relating to the process of issuing trust service certificates/tokens and/or reports

- Upon terminating its services, SecuMailer transfers its obligations to a reliable party ("Stichting SecuMailer") for maintaining all information necessary to provide evidence of the operation of the services for a reasonable period, unless it can be demonstrated that SecuMailer does not hold such information.
    - SecuMailer will maintain a website where its public key material will be available (https://secumailer.nl/eidas).
    - On this website a contact address will be available where concerned parties can raise requests for evidence provision during the 7 years validity period of its evidence database
- Upon terminating its services, the private key(s) of SecuMailer, including backup copies, are destroyed or withdrawn from use, in a manner such that the private key(s) cannot be retrieved
- Upon terminating its services, where possible, SecuMailer will endeavour to transfer the provision of trust services for its existing customers to another qualified trust service provider
- SecuMailer maintains or transfers to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period
- SecuMailer has an arrangement to cover the costs to fulfil these minimum requirements in case of bankruptcy or if it is unable to cover the costs by itself for other reasons, as far as possible within the constraints of applicable legislation. To this end a specific Legal Entity has been created ("Stichting SecuMailer") that contains sufficient financial funds to cover at least 3 months of operating the SaaS platform and covers the costs of a DevOps engineer to manage the SaaS platform during this period.

6. Compliance

The Termination Plan will be annually audited, both internally and externally. The results of these audits will be reported to the SecuMailer Managing Board. Any findings will result in a treatment plan.