



Terms and Conditions of the Electronic Registered Delivery Service

Access Level: Public



Copyright Notice

Terms and Conditions of Signaturit's QERDS

©2018 Signaturit Solutions, S.L., all rights reserved.

Notwithstanding the rights reserved in the foregoing and unless permitted below, reproduction, storage or entering into a storage system or transmission of any part of this publication in any manner and using any process whatsoever (electronic, mechanical, photocopy, recording or in any other manner) shall not be permitted without Signaturit's prior consent.

Change History

Version	Author	Approved by	Date of Approval	Comment
1.0	Pau Mestre	Coordination Committee	20 th November 2019	Initial Version of the Document
2.0	Pau Mestre	Coordination Committee	16 th December 2019	Modification of section 1.1., 1.5, 1.6, 1.7, 1.8, 1.9 and 1.15
3.0	Pau Mestre	Coordination Committee	15 th January 2020	Modification of section 1.6

Table of Contents

Copyright Notice	2
Change History	2
1.1 Scope	4
1.2 Qualified Electronic Registered Service Provider contact info	4
1.3 Certificate type, validation procedure and usage	5
1.4 Reliance limits	5
1.5 Obligation of subscribers	6
1.6 Delivery of the user content	6
1.7 Data availability for the recipient	6
1.8 Collection of evidence	7
1.9 Limitations of the service	8
1.10. TSU public key certificate status checking obligations of relying parties	10
1.11. Limited warranty and disclaimer/Limitation of liability	10
1.12. Applicable agreements and practice statement	10
1.13. Privacy policy	11
1.14. Refund policy	11
1.15. Availability of the service	11
1.16. Applicable law, complaints and dispute resolution	12
1.17. ERDSP and repository licenses, trust marks, and audit	12

Disclosure Statement

1.1 Scope

This disclosure statement contains the terms and conditions pertaining to the Qualified Electronic Registered Delivery Services (hereinafter “ERDS”) of Signaturit Solutions, SL. This document does not represent the integrity of the contractual relationship between Signaturit Solutions S.L., the Qualified Trust Service Provider (hereinafter, the “QTSP”), and the Subscriber and shall be considered a part of it and applicable to the whole.

1.2 Qualified Electronic Registered Service Provider contact info

Name of the ERDSP	Signaturit Solutions, S.L.
Address	Avila Street 29, Barcelona (08005), Spain
Email	legal@signaturit.com
Telephone	(+34) 935 511 480
Contact Person	Legal Department

For revocation purposes please contact the Qualified Electronic Registered Service Provider (hereinafter, “ERDSP”) and/or Certification Authority (hereinafter, “CA”) and follow the specifications established in Section 4.9 of the Certification Practice Statement (CPS) of the Certification Authority found in the following link:

http://pki.signaturit.com/pki/Signaturit_CPS_CA.pdf



Receive, reroute and deliver an email from a sending user to one or more receiving users, generating a digitally signed certificate that accredits sending email address, receiving email addresses, message content and delivery in the email inbox of the target server.

1.3 Certificate type, validation procedure and usage

This document relates to the QTSP's Electronic Registered Delivery service, for which the TSA signs qualified timestamps electronically using private keys that are specifically reserved for this purpose in order to provide ERDS.

Signaturit provides qualified timestamping service and the issuances of certificates for natural persons. Please review the applicable norms for these services in the following link:

<http://www.signaturit.com/en/pki>

For validation purposes please review Section 4.9.9 of the CPS.

For certificate usage please review Section 1.4 of the CPS.

1.4 Reliance limits

The QTSP only issues certificates that must be used compliant with its Basic Constraints. Uses not specified in the Certification Practice Statement, or in the certificate itself are forbidden. Also, certificates used against compliance of the Applicable Legislation are prohibited.

The ERDS is synchronized with UTC [ROA] with an accuracy of 1 second or better by using Network time protocol (hereinafter, "NTP").

The ERDS is synchronized with different NTP servers for which a polling is performed periodically making sure that the time accuracy is always under one second, which is the maximum allowed. If any error occurs and the time accuracy is detected to be over one second, the TSA will not issue time stamps as stated in ETSI EN 319 421.

Logs of issued qualified timestamps are preserved for at least fifteen (15) years in accordance to the Spanish “*Ley 59/2003, de 19 de diciembre, de firma electronica*”.

1.5 Obligation of subscribers

The subscriber is obligated to use qualified time-stamping service and qualified electronic certificates in compliance with this document and applicable agreements set out in Section 1.12.

1.6 Consignment and delivery of the user content

The delivery of the user content will be considered made at the time the message is received into Recipient user platform.

By accepting the receipt of the message, the recipient accesses to the content of the message and the time stamp is stamped on the document, once this occurred the sender will receive proof of delivery with the events recorded in the shipping process.

1.7 Data availability for the recipient

The sending of the user content will be valid for TEN (10) days from the date the sender sent the document. Once this period has elapsed, the shipment will expire.

1.8 Collection of evidence

The retention period of the evidence is at least FIVE (5) years unless otherwise agreed with the customer and/or applicable legislation. There are no limitations on the evidence validity period.

The QERDS will archive at least:

- a) user's identification data;
- b) user's authentication data;
- c) proof that the sender identity has been initially verified;
- d) logs of QERDS 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 (Audit Trail), are accessible to the user by a received email with and/ or using the webservice dashboard with an enumeration of all created events and/ or downloadable from this mentioned dashboard.

1.9 Limitations of the service

1.9.1. Certificate Life-Cycle Operational Requirements

Application to issue a certificate in line with this document may be submitted by:

- a) The Subject,
 - i. Directly to the Certification Authority or Registration Authority
- b) The Subscriber on behalf of the Subject
 - i. Directly to the Certification Authority or Registration Authority

1.9.2 Enrollment process and responsibilities

The registration process includes certificate application, generation of key pair, public key certification request, and signature of the contract. Each party involved in the process has specific responsibilities and jointly contributes to the successful certificate issuance:

- a) The Subject is responsible for providing correct and truthful information on his identity, reading carefully the material made available by the CA and following the CA instructions while submitting a qualified certificate application. If the Subject is a legal person, those responsibilities fall on the legal representative with Powers of attorney;
- b) For the Subscriber to use the QERD service of the QTSP, he/she must request the use of the service by contacting the QTSP and be identified in person (ID document, personal data and if needed Powers).
- c) The Subscriber, if present, is responsible for informing the Subject on whose behalf he is requesting a certificate about the obligations arising from the certificate, as well as for providing correct and truthful information about the

identity of the Subject and for following processes and indications given by the CA.

- d) The CA is ultimately responsible for Subject and Subscriber identification and successful registration of the qualified certificate.

1.9.3. Certificate application processing

The Subject and/or Subscriber must:

- Read carefully the Policy and Practice Statement and the applicable Terms and Conditions and the contract documents.
- Comply with the identification procedures adopted by the CA as described
- Provide all information required for identification accompanied by any appropriate documentation (where required);
- Sign the contract using the QTSP's advanced electronic signature.

The QTSP is not liable for defects in provided services occurred due to incorrect or unauthorized use of services provided under a contract for provision of certification services caused by the Subscriber and/or Subject, in particular, for defects occurred due to operations conducted contrary to requirements specified in this CPS, applicable CP, or for defects occurred due to force majeure events including temporary interruptions of telecommunication services etc. Furthermore, the QTSP limits its warranties to what is stipulated in the contract signed between the QTSP and the subscriber.

1.10.TSU public key certificate status checking obligations of relying parties

Must ensure that the qualified timestamps have been properly signed and check the CRL to confirm that the private key used for signing these qualified timestamps are not compromised. The CRL can be verified in the following link:

<http://pki.signaturit.com/crl>

Relying parties must also verify compliance with Section 1.4 of the CPS.

1.11.Limited warranty and disclaimer/Limitation of liability

The ERDSP is not liable for defects in provided services occurred due to incorrect or unauthorized use of services provided under a contract for provision of certification services caused by the subscriber and/or subject, in particular, for defects occurred due to operations conducted contrary to requirements specified in this CPS, applicable Certification Policy, or for defects occurred due to force majeure events including temporary interruptions of telecommunication services etc. Furthermore, the ERDSP limits its warranties to what is stipulated in the contract signed between the QTSP and the subscriber.

Furthermore, the ERDSP has a civil liability insurance that covers up to 3 million euros, in compliance with the Spanish “*Ley 59/2003, de 19 de diciembre, de firma electronica*”.

1.12.Applicable agreements and practice statement

The following documents are considered applicable to the relationship between the ERDSP and the subscriber:

- a. Certification Practice Statement of Signaturit
- b. Terms and Conditions for the PKI
- c. Terms and Conditions of the Timestamp Service
- d. Policy and Certification Practice Statement of the Electronic Registered Delivery Service.
- e. Subscription agreement

1.13. Privacy policy

Please review the following link:

<https://www.signaturit.com/en/privacy>

1.14. Refund policy

Please contact the ERDSP for further information.

1.15. Availability of the service

- The Supplier shall endeavour to offer an availability of 99.9% of the Service.
- With prior announcement, the Supplier is entitled to shut down the Service and/or the Website temporarily for the purposes of maintenance, modifying or improving the Service and/or the Website, the associated software and other facilities. The Supplier will ensure that any such shutdown as far as possible happens outside standard office hours and will notify (potential) users of the planned shutdown in good time; in the event of scheduled and essential corrective maintenance this will be done via the Website.

- Under no circumstances however is the Supplier liable to pay damages in relation to such a shutdown.
- The Supplier is entitled to make occasional modifications to the Service and/or the Website in order to improve its functionality and rectify any faults. If a modification results in a significant change to functionality, the Supplier will notify (potential) Users of this by means of the Website.
- The Subscriber as well as the Recipient are independently at all times responsible for the maintenance and use of its E-mail client.

1.16.Applicable law, complaints and dispute resolution

- Any complaint shall be communicated to the ERDSP, per Section 1.2, in order to amicably resolve any possible dispute. If for some reason it is not possible to amicably resolve the dispute, the parties involved in the contractual relationship, waiving any other jurisdiction that may correspond, are subjected to the resolution between them to the courts of Barcelona.
- Qualified timestamps service is provided under the jurisdiction of Spanish law
- ERDS is provided under the jurisdiction of Spanish law

1.17.ERDSP and repository licenses, trust marks, and audit

The ERDSP has undergone the conformity assessment in accordance to 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 and repealing Directive 1999/93/EC.