Policy and Practice Statement of the Qualified Electronic Registered Services

Access Level: Public

Copyright Notice

Certification Practice Statement of Signaturit's TSA

Change History

Version	Author	Approved by	Date of Approval	Comment
1.0	Pau Mestre	Coordination Committee	20th November 2019	Initial Version of the Document
2.0	Pau Mestre	Coordination Committee	16th December 2019	Modification of section 1, 6.3.1, 7.1., 7.2, 7.4, 7.7, 7.14
3.0	Pau Mestre	Coordination Committee	15th January 2020	Modification of section 7.3

Table of Contents

1 Overview

Signaturit Solutions S.L. (hereinafter, “Signaturit”) is a limited liability company duly incorporated under Spanish Law, having as a VAT number B-66024167 and corporate address in Avila Street 29, Barcelona (08005, Spain).

Signaturit is an Electronic Registered Delivery Service Provider, and this Policy and Practice Statement is intended to describe the rules and operational procedures adopted by Signaturit for the provision of time stamps according 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 and to comply with the requirements stated in ETSI EN 319 401 Electronic Signature and Infrastructures; General Policy Requirements for Trust Service Providers and ETSI EN 319 521 Electronic Signature and Infrastructures Policy and Security Requirements for Electronic Registered Delivery Service Providers.

Furthermore, this document expands on Signaturit’s Certification Practice Statement (OID: 1.3.6.1.4.1.50646.1.1) and shall prevail in case of contradiction.

1.1 Document Name and Identification

This document is named “Policy and Practice Statement of the Electronic Registered Delivery Service Provider”. It shall be unambiguously identified with Signaturit’s Object Identity Identifier (OID) provided by the American National Standards Institute (ANSI): 1.3.6.1.4.1.50646.11.1. Its latest version can always be found in the following link:

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

This document is modified and updated per Section 1.5 of the CPS.

2 References

2.1 Technical Standards

- Signaturit's Certification Practice Statement
- ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 521 - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Service Providers.

2.2 Legal regulations

2.2.1 International

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, relating to the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2.2.2 Spain

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

3 Acronyms and Synonyms

For the interpretation of this document, the following definitions have been added to those established in Signaturit's CPS:

- **Applicable Legislation**: Section 2.2 of this document
- **Certification Authority (CA)**: A trust system managed by a Trust Service Provider and responsible for issuing and revoking Certificates used in Electronic signatures. From a legal viewpoint, it is a specific case of a Trust Service Provider and, by extension, the provider is referred to as the Certification Authority.
- **Certification Practice Statement (CPS)**: It is a document from a Certification Authority which describes their practice for issuing and managing public key certificates.
- **Coordinate Universal Time (UTC)**: is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude.
- **Information Security Management Policy (ISMS)**: An ISMS, or information security management system, is a defined, documented management system that consists of a set of policies, processes, and systems to manage risks to organizational data, with the objective of ensuring acceptable levels of information security risk
- **Relying Party**: recipient of a time-stamp who relies on that time-stamp
- **Subscriber**: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
- **Terms and Conditions**: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties

- **Technical Standards**: Section 2.1 of this document.
- **Time-stamp:** data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
- **Time-Stamping Authority (TSA):** A TSP which issues time-stamps using one or more TSUs.
- **Time-Stamp Unit (TSU):** A set of hardware and software that is managed as a unit and which has a single active signature key at all times.
- **Qualified Trust Service Provider (TSP):** entity which provides one or more qualified trust services. It is the entity in charge of managing the CA. Signaturit Solutions, S.L. is the Qualified Trust Service Provider.
- **Sender and receipt** are natural persons (subscribers according to point “p”)who apply for and hold Signaturit’s trust services, for themselves or as representatives of a third party **and use Electronic Registered Delivery Systems.**
- **ERDS** Electronic Registered Delivery Service

4 General Concepts

4.1 Electronic Registered Delivery Services

The services offered is the qualified variant according to the eIDAS-requirements whereby - after the sender has properly identified - the recipient must first go through an identification procedure before the mail becomes available (articles 43.2 and 44 of the eIDAS Regulation).

- Time-stamping management: This service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service.

4.1.1 Uses of qualified time stamps

- To preserve integrity of a document after Signaturit's advanced electronic signature has been used
- To attest the moment in which an act or process has been carried out, for example when using Signaturit's electronic registered delivery.
- To certify documents uploaded to Signaturit's dashboard
- Qualified Timestamps can only be used in accordance to the CPS, this document and for legal purposes only.

4.2 Timestamping Authority

Signaturit's TSA is trusted by its subscribers and relying parties to issue qualified timestamps. The TSA is responsible for the operation of one or more timestamp services identified in section 4.1 above, and examples have been provided in section 4.1.1.

The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. Furthermore, the TSA is responsible for ensuring that the requirements identified in this Policy and Practice Statement are met.

4.3 Subscriber

A subscriber is the end user of the qualified timestamps issued by the TSA. Subscribers can be individuals or organizations (public or private), as well as technological equipment.

4.4 Sender and receiver

A Sender and a receiver are natural persons (subscribers according to the previous point who apply for and hold Signaturit's trust services, for themselves or as representatives of a third party and use Electronic Registered Delivery Systems.

4.5 QERDS policy and practice statement

This document should be read in conjunction with the current version of Signaturit's CPS, which is available in the following links:

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

https://pki.signaturit.com/pki/Signaturit_CPS_TSA.pdf

Furthermore, this document specifies the policy and practice statement for the Electronic Registered Delivery Services provided by Signaturit, which alongside the CPS and other internal documents, it is defined how Signaturit complies with the Applicable Legislation and Technical Standards.

4.6 Other services Involved and relying parties

Relying Parties are natural or legal persons, other than the Subscriber/Subject, that receive and/or use the trust services of the QTSP, therefore are Subject to the provisions. of the CPS when they effectively decide to place their trust in the trust services.

Below the complete list of QTSPs involved in the provision of the QERDS:

1. Certification Authority
2. Registration Authority
3. Certificate Subscribers and Subjects
4. Relying parties
5. Other participants

4.6.1 Time-stamp issuance

Qualified time-stamps are issued in accordance with the time-stamp profile defined in ETSI EN 319 422[5] and comply with RFC 3161 “Time Stamp Protocol (TSP)”.

Each TST contains the time-stamping policy identifier, a unique serial number and a certificate containing the identification information of the Signaturit TSA’s TSU if it is requested by the client.

The TSU accepts requests using SHA224, SHA256, SHA383 and SHA512 as the hash algorithm to obtain the digest.

The TSU key is a 2048 bits RSA key only used for signing TSTs.

For every qualified time-stamp request, the TSA generates audit records including data about the request time, request result, time stamp issued, and extra data to grant the audit records integrity.

The TSU does not issue any TST if the end of the validity of the TSU certificate has been reached, or if the system's time accuracy compared to a trusted set of NTP servers is over one second.

4.6.2 Clock synchronization with UTC

The QERDS is synchronized with UTC [ROA] with an accuracy of 1 second or better by using NTP protocol.

The QERDS 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.

5 QERDS Policies and General Requirements

5.1 General

The present Practice Statement supports the provisioning of the Electronic Registered Delivery Service (QERDS) that meets the eIDAS qualified level.

5.2 User community and applicability

The community of users for Electronic Registered Delivery Services of Signaturit include subscribers (sender and receiver) and relying parties.

This policy may be used for public time-Electronic Registered Delivery Services used within a closed community, as long as it is not used for any of restricted uses established in Signaturit's CPS.

5.3 Compliance

Signaturit is subjected to independent external and internal audits, in order to demonstrate that the Electronic Registered Delivery Service fulfills the obligations established in the Applicable Legislation and has implemented appropriate controls as described in Section 7.

6 Obligations and Liability

6.1 General

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

6.2 Subscriber/ Sender and Recipient obligations

The obligations of Subscriber and Recipient are defined in the General Terms and Conditions where is stated: The Subscriber is and remains the party that is always responsible and liable when using the Service:

a. for all actions performed by Users via the Service; and

b. to verify when sending e-mail (s) to natural persons, whether the e-mail address that is entered belongs to the natural person to whom the User wishes to address the e-mail; and

c. when sending to natural persons who act on behalf of a company, to check whether the natural person to whom the e-mail is addressed is connected to - and authorized to communicate on behalf of - the company.

d. for the correctness of the link between the email address provided by or on behalf of the Supplier and the relevant natural or legal person.

e. in the case of the use of SMS with Registered Email Plus for identification of the Recipient that access to both the e-mail address and the SMS is expressly reserved for the authorized person.

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

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

The Subscriber as well as the Recipient is always independently responsible for the maintenance and use of its E-mail client.

a) Subscribers 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 is not compromised. The CRL can be verified in the following link:

http://pki.signaturit.com/crl

b) Comply with Section 1.4 of the CPS.

6.3 Relying parties' obligations

Relying Parties are natural or legal persons, other than the Subscriber/Subject, that receive and/or use the trust services of the QTSP, therefore are Subject to the provisions of the CPS when they effectively decide to place their trust in the trust services.

6.3.1. Other participants obligations

The TSA oversees the creation, verification and validation of qualified time stamps and oversees that all legal, technical and organizational parts components are in place and compliant with the applicable legislation and technical standards. The Timestamping services are specified in the Policy and Practice Statement of the Timestamping Authority (OID: 1.3.6.1.4.1.50646.10.2).

a) 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 is not compromised. The CRL can be verified in the following link:

http://pki.signaturit.com/crl

b) Verify compliance with Section 1.4 of the CPS.

Signaturit's PKI allows the participation of Registration Authorities which have signed a collaboration agreement with Signaturit.

The QTSP involved in the provision of the QERDS is CAMERFIRMA Qualified Seal for Legal Persons and with Conformity Certificate acc. to eIDAS Validity of the service and Uanataca Qualified Time Stamp Service (Backup). Compliant with eIDAS Regulation.

Apart from this, the TSP does not use third party services to offer QERDS. However, if needed TSP can contract third suppliers for the provision of the service is based on chain

liability that is covered by SLA's. At least ISO 27001 will be required from the key suppliers with a eIDAS conformity audit. Any third party as a provider of trust services the TSP will be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the eIDAS-Regulation.

6.4 Liability

Signaturit is committed to operate the Electronic Registered Service in accordance with this Policy and Practice Statement of the Electronic Registered Delivery Service, the Policy and Practice Statement of the Timestamping Authority, the CPS, Technical Standards and Applicable Legislation. It doesn´t assume any expressed or implied responsibility or guarantee for (except in cases of agreements) the availability or accuracy of the qualified timestamp service.

7 QERDSP Management and Operation

7.1 Identification and authentication of sender

Before a natural person, as a sender/ subscriber (hereafter described as "sender"), can access to the platform he/ she has to go through the enrolment procedure.

A legal person or nonsubscriber cannot use the service as a sender. There is one method for identifying the sender for the first time, using the physical presence of the natural person directly in front the QERDSP.

The authentication process is done through username and password. Likewise, it is checked through access by notifications to the email provided

7.2 Identification and authentication of recipient/receiver

A Recipient can be a natural person. It is necessary to be a subscriber of the Service to receive a Registered Email. A natural person or nonsubscriber cannot use the service as a receiver. There is one method for identifying the sender for the first time, using the physical presence of the natural person directly in front the QERDSP.

The authentication process is done through username and password. Likewise, it is checked through access by notifications to the email provided.

7.3 Sending and receiving Registered messages

The use of Registered Email begins after contracting and execution of the enrollment procedure with the customer both sender and receiver.

Once the user writes the message in the application, it is transformed/modified into a .pdf format it is shown to the user for the acceptance and the sending of it.

After sending the notification(s)/message(s) to the recipient(s), a proof of sending is created with the sender's name and integrity information, the proof of sending is timestamped and added to the proof of sending. A detailed specification of this process can be found in the Audit Trail.

7.4 Delivery evidence

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

The proof of send and proof of receive are created, sealed and timestamped the moment the message is sent / received, containing the identity information of the sender / receiver.

The proof of send includes the integrity information, subject, send and receiver information, the name of the sender and a timestamp. The proof of receive contains the id of the message and the identifying information of the receiver that opened the message, their name. The seal of the proof of send is used to verify message integrity when displaying the message to the receiver

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link:
http://pki.signaturit.com/cert

b) The TSU does not issues a qualified timestamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.
c) When obtaining a signature verification (public key) certificate, the TSA verifies that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority)

The provided evidence (Audit trail), are accessible to the user by a received email with a Audit trail included and/ or using the webservice dashboard with all Audit trails created and/ or downloadable from this mentioned dashboard.

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

7.5 Physical and environmental security

Please review Section 5.1 of the CPS.

7.6 Risk assessment and information security policy

Signaturit has an ISMS, under which it performs various risk assessments and there are various information security policies which govern the company. As part of this risk assessments, the QERDS is part of the reviewable areas. The ISMS is managed by the Information Security Committee which review and make sure Signaturit as a company, and its employees adhere and comply to the ISMS.

7.7 Operation security

Message integrity is secured against modification during transmission by timestamping the message hashes with an eIDAS certified HSM using an eIDAS qualified timestamp. Message hash and signature will be added to the QERDS, which creates an audit trail that proves that data has not been altered. Transmitted data is protected against the risk of loss, theft and damage using TLS connections.

7.8 Network security

Please review Section 6.7 of the CPS.

7.9 Incident management

Please review Section 5.7 of the CPS.

7.10 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.

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

Please review Section 5.4 and 5.5 of the CPS.

7.11 Business continuity management

Please review Section 5.7 of the CPS.

7.12 QERDS termination and termination plans

Please review Section 5.8 of the CPS and the document “Termination Plan of the QERDSP”

7.13 Compliance

Signaturit offers its services in strict compliance with the Applicable Legislation and Technical Standards. Verification is performed through internal and external audits.

7.14 Limitations on the use

The limitations on the use of the QERDS are described in the General Terms and Conditions section 1.9.

8. Logical QERDSP Architecture

Signaturit QERDS defines two actors in the logical QERDSP Architecture: the user and the legal department of signaturit. Both connect seamlessly to Signaturit QERDSP service, but the legal department can review and approve identity verification documents from users.

Every interaction with Signaturit QERDSP is done by means of a web app.

8.1. Components

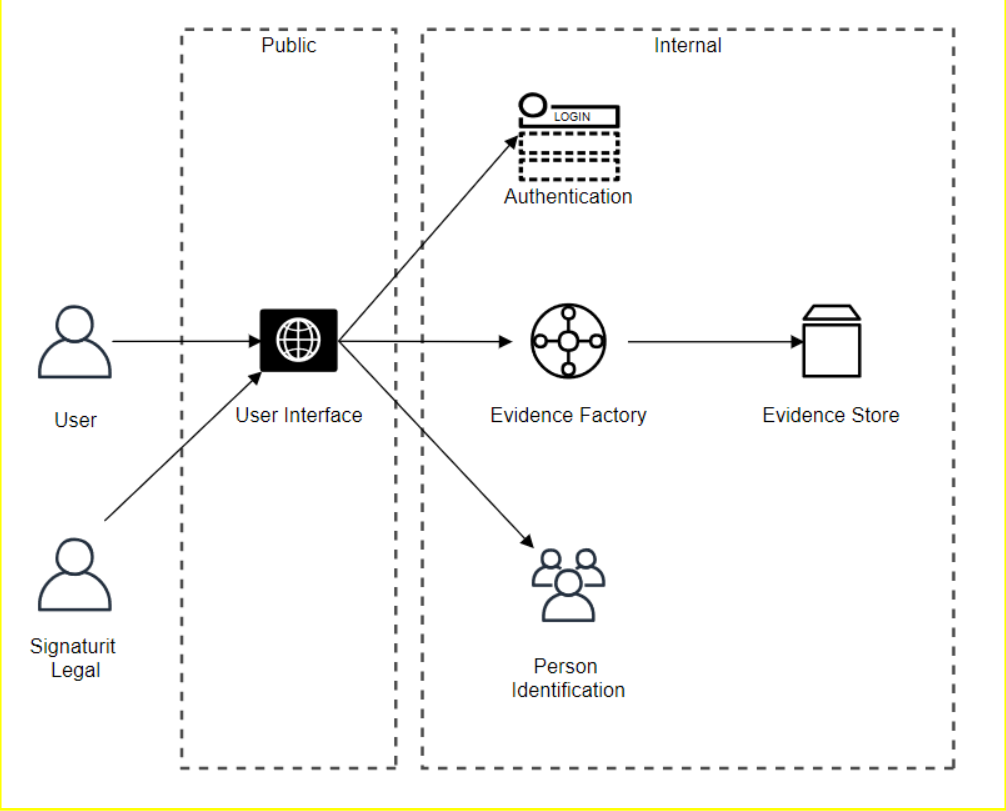
Logical components of Signaturit QERDSP are:

- User interface, responsible for giving the ERD-UA an interface to interact. There will be no programmatic users (no API for automation tasks)

- Evidence Factory, secure storage where all operations related to signing and evidencing occur.
- Evidence Store, general purpose storage, contains all data needed to run the QERDSP (user information, transaction status, web session, …)
- Person Identification, coordination module for the person identification process
- User, can be a sender or recipient
- Signaturit Legal, legal department from Signaturit

8.2. Diagram

We can see a diagram of the logical architecture here:



9. Physical Architecture

9.1. Introduction

The physical architecture of Signaturit QERDSP is based on two main centers: Amazon AWS and Colt.

Amazon Web Services is a cloud computing platform that provides a wide array of cloud services. We can define AWS (Amazon Web Services) as a secured cloud services platform that offers compute power, database storage, content delivery and various other functionalities.

Signaturit QERDSP works with Colt datacenter located in Barcelona. This datacenter has 4.8MVA or power, offers resilience and 24/7 onsite security (ISO 27001), secure with two door airlock.

9.2. Components

Physical architecture components are:

- HSM. Secure module where are the encryption keys are kept.

- HSM Hardserver. Secure server coordinating and managing the HSM

- Amazon EC2 (Amazon Elastic Compute Cloud). Provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Amazon EC2 to launch as many virtual servers as Signaturit QERDSP needs, configure security and networking, and manage storage. Amazon EC2 enables to scale up or down to handle changes in requirements or spikes in petitions, reducing the need to forecast traffic.

- Amazon RDS (Relational Database Service). Operates and scales a relational database in Amazon cloud.

- Amazon SNS (Simple Notification Service is a highly available). Durable, secure, managed pub/sub messaging service that enables Signaturit QERDS to decouple microservices, distributed systems, and serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. By using Amazon SNS topics, Signaturit QERDS systems can fan out messages to a large number of subscriber endpoints for parallel processing.

- Amazon Lambda. Lets run code without provisioning or managing servers in Amazon cloud.

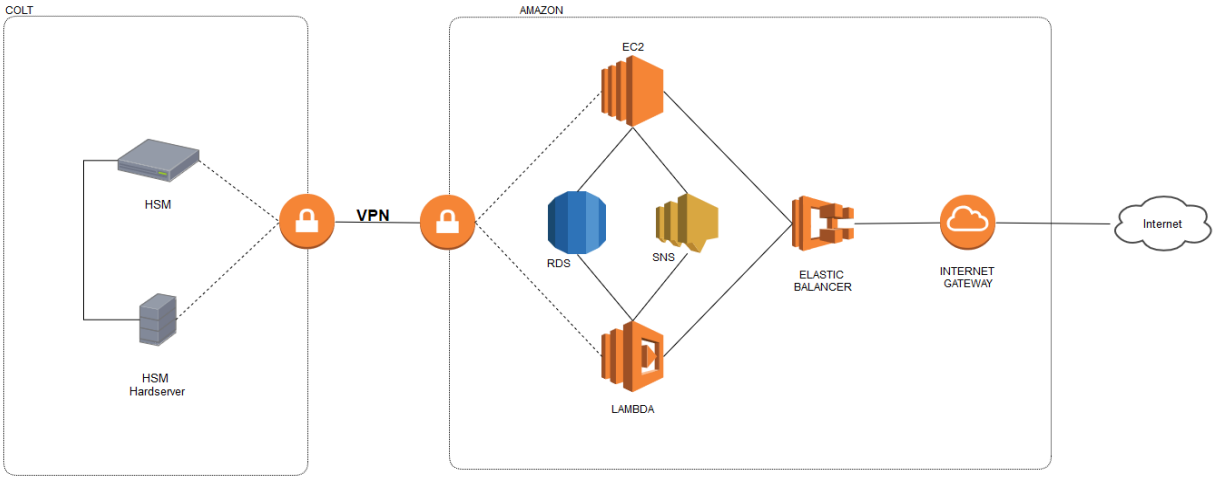
- Amazon Elastic Balancer. Automatically distributes incoming application traffic across Amazon EC2 instances and Lambda functions. It can handle the varying load of Signaturit QERDS application traffic in a single module. Elastic Load Balancing features the high availability, automatic scaling, and robust security necessary to Signaturit QERDS application fault tolerant.

- Amazon Internet Gateway. The piece of the schema that links all the pieces with user's computers. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances of this schema and the internet. It therefore imposes no availability risks or bandwidth constraints on network traffic.

- VPN. Provides secure communication between two datacenters in Signaturit QERDS service, Amazon and Colt.

9.3. Diagram

We can see a diagram of the logical architecture here:



10. Validity and Document Management

The owner of this document is the Legal Department, who must check and, if necessary, update the document at least every six months with the previous approval of the Coordination Committee and it will be notified and made available to all interested parties.