DECLARATION OF PRACTICES FOR THE PRESERVATION OF ELECTRONIC SIGNATURES AND STAMPS

TrustCloud

TYPE OF DOCUMENT				
				Secret Documentation
			x	Public Documentation
				Internal Documentation
				Confidential Documentation
TITLE			DECLARATION OF PRACTICES FOR THE PRESERVATION OF ELECTRONIC SIGNATURES AND SEALS	
ENTITY			TRUSTCLOUD SOLUTIONS	
FORMAT			Electronic - PDF	
PAGES				
VERSION	DATE OF ISSUE	OID	AUTHOR	
2.3	07/11/2023	1.3.6.1.4.1.5 2582.1.1.1	TRUSTCLOUD SOLUTIONS	
Reviewed by: Alberto Angón (CISO-RSI) Signed by ALBERTO ANGON on 2023-12-05 14:24:06 CET			Date:	
Approved Signed by Saioa Echebarria on 2023-12-05 14:36:10 CET By TRUSTCLOUD SOLUTIONS Management Committee S. L			Date:	

CHANGE HISTORY

Version	Date	Description of the action	Pages
1.6	02/11/2018	Inclusion of subscriber obligations	
1.7	21/03/2019	Updating legislation	
1.8	07/10/2020	General update	
1.9	25/11/2021	Change of references ETSI 102 573 to ETSI 119 511	
2.0	07/10/2022	Adequacy ETSI 119 511	
2.1	10/10/2022	Corrigendum item 17	
2.2	20/10/2023	Modification of Branddocs to Trustcloud Solutions.	
2.3	08/11/2023	Updating references regulatory framework (paragraphs 1, 3 and 4), and inclusion of shelf life (paragraph 15)	

Index

1 INTRODUCTION

This document is a Statement of Practice of the Electronic Signature and Seal Preservation Service, by means of which TRUSTCLOUD SOLUTIONS, as a trust service provider, sets out and describes the way in which it provides the service of preserving qualified electronic signatures and qualified electronic seals and ensures compliance with the legally required obligations, informing the public about the correct way to use these services.

This Statement of Practice is addressed to all natural and legal persons requesting, subscribers and in general users of escrow services, in accordance with the provisions of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services and Regulation 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.

To this end, TRUSTCLOUD SOLUTIONS has implemented an information security management system applied to the information and infrastructures that support the services of design, development and maintenance of applications, computer systems, professional cloud services and integral provider of trust services, obtaining its certification in ISO/IEC 27001, with the aim of developing and effectively implementing its services.

In addition, for the electronic signature and electronic seal storage service, TRUSTCLOUD SOLUTIONS follows the indications of the standards of the European Telecommunications Standards Institute -ETSI- following the technical specifications of the ETSI TS 119 511 standards, EN 319 401 (general requirements for trust service providers), EN 319-102-1 (procedure for creation and validation of AdES digital signature), TS 101 533-1 (European standard for preservation system) and ISO 14641-1 (specifications for the design and operation of an information system for the preservation of digital information). NOM-151 (Requirements to be observed for the preservation of data messages and digitisation of documents).

To this end, TRUSTCLOUD SOLUTIONS has designed and developed a technological infrastructure which, in an integrated manner, provides its Users with a tool through which they can keep qualified electronic signatures and seals for a long period of time, and re-seal them periodically, so as to guarantee sufficient legal probative effectiveness throughout the duration of the custody.

2 IDENTIFICATION OF THE DOCUMENT

In order to individually identify each type of service performed by TRUSTCLOUD, in accordance with this Statement of Practice on the Preservation of Qualified Electronic Signatures and Seals, an Object Identifier (OID) is assigned to each type.

This Certification Practice Statement describes the services related to the preservation of qualified electronic signatures and seals provided through the platform owned by TRUSTCLOUD, including, among other aspects of the description and functionality of the services provided, the following:

- The characteristics of each service.
- Treatment and operational flows.
- The identification of all parties involved, from the providers of documentation for qualified safekeeping to the certification service providers in charge of generating time-stamp tokens.

and electronic signatures.
- The obligations assumed in the provision of services.
- The technical and organisational security measures in place.
- The general conditions of use and contracting of services.

3 ACRONYMS AND DEFINITIONS

Acronyms

ACRONYM	DEFINITION
LSC	Law 6/2020 of 11 November 2020, regulating certain aspects of electronic trust services
eIDAS	Regulation 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
GDPR	Regulation 2016/679 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
LSSI	Law 34/2002 of 11 July 2002 on information society services and electronic commerce.
PCSC	Certification Service Providers
TSA	Time Stamp Authority - Autoridad de Sellado de Tiempo - Time Stamp Authority
CPD	Data Processing Centre
NTP	Network Time Protocol - Internet protocol for synchronising the clocks of computer systems.
PKI	Public Key Infrastructure - Infraestructura de Clave Pública - Infraestructura de Clave Pública - Public Key Infrastructure
WF	Work Flow - Workflows of each process
CRL	Certificate Revocation List
OID	Object Identifier - A value, hierarchical in nature and comprising a sequence of variable components, but always consisting of non-negative integers separated by a dot, which can be assigned to registered objects and which have the property of being unique among all other OIDs.

Definitions

CONCEPT	DEFINITION
DPC	**Certification Practices Statement**: Trustcloud statement made available to the public electronically and free of charge by Trustcloud as a Trusted Service Provider in compliance with the provisions of the Law.
TRUSTED SERVICE PROVIDER	Natural or legal person providing one or more trust services, in accordance with eIDAS
QUALIFIED TRUSTWORTHY SERVICE PROVIDER	Trust service provider that provides one or more qualified trust services and has been granted qualification by the supervisory body.
TIME STAMPING AUTHORITY	a natural or legal person who, in accordance with the regulations on time-stamping, issues electronic time-stamps.
ELECTRONIC TIME STAMP	Data in electronic format linking other data in electronic format to a specific point in time, providing evidence that the latter data existed at that point in time.
QUALIFIED ELECTRONIC TIME STAMP	Electronic time stamp that complies with the requirements set out in Article 42 of eIDAS.
USER	Natural or legal person using the qualified escrow services for qualified electronic signatures or qualified electronic seals, subject to acceptance of the conditions associated with the service and the CPD.
DOCUMENTATION	Set of digital evidences received by Trustcloud from the User, which comply with the requirements set out in these CPS.
CERTIFICATE	An electronically signed file by a certification service provider that links signature verification data to a signatory and confirms the signatory's identity.
PUBLIC KEY	A publicly known mathematical value used for the verification of a digital signature or data encryption. Also called signature verification data.
PRIVATE KEY	A mathematical value known only to the subscriber and used for the creation of a digital signature or decryption of data. Also called signature creation data.

HASH FUNCTION	An operation performed on a dataset of any size, so that the result obtained is another dataset of fixed size, independent of the original size, and which has the property of being associated.
HASH OR FINGERPRINT	A fixed-size result obtained after applying a hash function to a message and which has the property of being uniquely associated with the initial data.
EXPORT-IMPORT PACKAGE	Information extracted from the preservation service that includes the SubDO, preservation evidence and preservation-related metadata, allowing another preservation service to import it in order to further achieve the preservation objective based on this information

4 NORMS AND STANDARDS OF APPLICATION

1] Regulation 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.
[2] Law 6/2020 of 11 November 2020 regulating certain aspects of electronic trust services
[3] Regulation 2016/679 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
[4] Law 34/2002 of 11 July 2002 on information society services and electronic commerce.
[5] ETSI TS 119 511 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
[6] ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
[7] ETSI EN 319 102-1 v1.1.1 Procedures for Creation and Validation of AdES Digital Signatures: Creation and Validation
[8] ETSI TS 102 778-6 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles

[9] ETSI TS 101 533-1 Information Preservation Systems Security; Part 1: Requirements for Implementation and Management
[10] ETSI EN 319 421 v1.0.0 Electronic Signatures and Infrastructures (ESI); Policy and SecurityRequirements for Trust Service Providers issuing Time-Stamps
[11] ISO/IEC 14641-1 Electronic archiving
[12] ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection - Information security management systems
[13] ISO/IEC 27002;2022 Information security, cybersecurity, and privacy protection - Information security controls
[14] ETSI SR 019 510. Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardisation of long-term data preservation services, including preservation of/with digital signatures.

5 COMPLIANCE REQUIREMENTS

TRUSTCLOUD warrants, in line with its statement of applicability and legal requirements, that it complies with:

1) The Information Security Policy, which is aligned with the applicable legal regulation.
2) The Qualified Electronic Signature and Seal Preservation Service Policy defined in this Certification Practices Statement.
3) The organisational requirements as defined in point 8.1.1.
4) The obligation to provide the required information, where necessary, to its business partners, auditors and regulatory authorities, as specified in points 8.1.2 and 8.1.3. of this document, including organisational requirements.
5) That Trustcloud has implemented controls that comply with the requirements specified in Annex A of ETSI TS 119 511 [5], guaranteed by the implementation of an ISMS based on ISO/IEC 27001:2022, as a trusted service provider.
6) That Trustcloud takes into account the necessary legal requirements for the use of qualified electronic signatures and seals using secure signature creation devices.

6 IDENTIFICATION AND CONTACT DETAILS

- Company Name: TRUSTCLOUD SOLUTIONS S.L
- Trade name: TRUSTCLOUD
- VAT NO: B87142618
- Registered Address: Paseo Club Deportivo 1, 28223 Pozuelo de Alarcón, Madrid
- Customer Service Centre (SAC): +34 913 518 558
- E-mail: contact@trustcloud.tech
- Web: https://trustcloud.tech/es/
- Other contact details: +34 913 518 558

7 DESCRIPTION OF THE SERVICE

TRUSTCLOUD, as a trust service provider, offers a qualified service for the conservation of qualified electronic signatures and seals, whereby it carries out the conservation of the aforementioned qualified electronic signatures and seals by using procedures and technologies capable of extending the reliability of the qualified electronic signature data beyond the period of validity of the electronic certificate.

7.1 PARTIES INVOLVED IN THE TRUSTCLOUD SERVICES

The parties involved in TRUSTCLOUD services are:

Service users:

The users of the services are the natural and legal persons for whom the electronic signature and seal preservation services are intended, who wish to preserve qualified electronic signatures and seals over the long term, guaranteeing their integrity, authenticity and legality over time.

Custody Warehouse:

Warehouse and SQL database where the signed and stamped Declarations are stored, perfectly classified.

Qualified Certification Service Provider:

A legally constituted entity, duly qualified by one of the competent authorities of an EU member country, whose main activity is the issuance of qualified signature and seal certificates for the purpose of generating qualified signatures and seals.

There are two kinds of policies related to the adoption of the use of advanced electronic signatures, according to ETSI TS 101 533 [9]:

1) Standardised Policy Requirements (N), based on advanced electronic signatures
2) Extended Policy Requirements (N+), the use of which implies greater security by extending the standardised requirements with requirements for qualified electronic signatures, requiring the use of AdES formats issued with secure signature creation devices and based on qualified certificates.

TRUSTCLOUD requires Qualified Trust Service Providers, in any case, to use policy N+ (qualified electronic signatures) in this service.

Qualified Time Stamping Authority:

Authority that generates qualified time-stamp certificates with the file's summary hash, date and time obtained from a reliable time source, electronically signs it and provides it to TRUSTCLOUD, guaranteeing its existence and integrity over time from the time of sealing.

In the same way, the Qualified Time-Stamping Authority will carry out the time-stamping processes of the electronic signatures and seals kept, performing a new electronic time-stamping before their expiry, with the sole purpose of guaranteeing the longevity of the electronic signature, and therefore the reliability of the electronic signature over time.

Other service providers:

TRUSTCLOUD relies on the services of Cloud storage service providers for storage.

The description of the intervention in the different processes, in which the above-mentioned service providers are involved, is reflected in this CPD.

7.2 MAIN FEATURES OF TRUSTCLOUD SERVICES

Through the service provided by TRUSTCLOUD, the following aspects are guaranteed

1) That the files received by the User are, in any case, in PAdES format.

2) That the electronic signatures and seals retained are qualified, in such a way as to meet the following requirements:

✓ They have been made by means of a qualified electronic signature or seal certificate, issued under a Certification Policy for qualified electronic certificates.

✓ Which have been generated, in any case, on a secure signature creation device.

3) That the retained qualified signatures and seals meet the requirements of longevity, extending the reliability of the qualified electronic signature or seal data used beyond the period of validity of the electronic certificate with which the signature is made.

7.3 QUALIFIED ELECTRONIC SIGNATURE AND SEAL PRESERVATION SERVICE

The electronic signature and seal preservation service consists of a solution aimed at guaranteeing the integrity and legal validity of the files incorporated therein. The entire process is carried out in accordance with the guidelines of the qualified service for the preservation of qualified electronic signatures and seals.

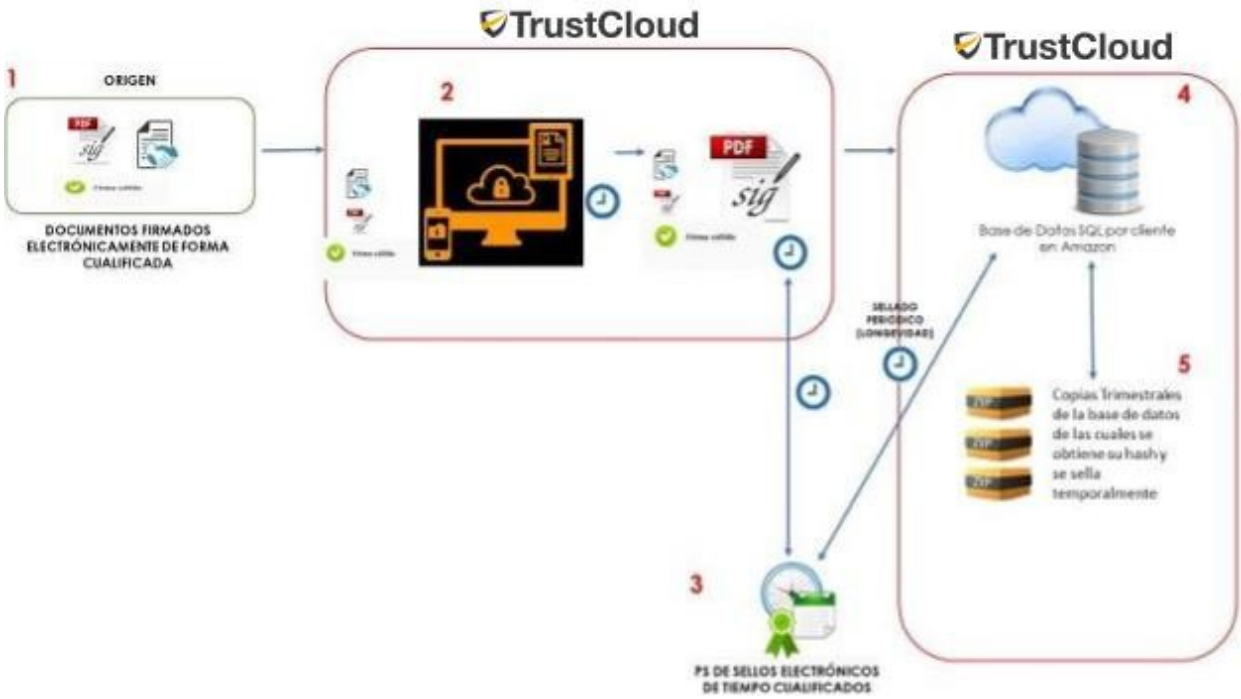
This service only preserves the electronic signatures and seals of the files (reception, revisions and recording of the electronic signatures and seals of each file, recording of operations to guarantee their integrity, authenticity and confidentiality over time), while the storage and preservation of the electronic files associated with these signatures and seals is the responsibility of the entity that generates the qualified signatures and seals.

The procedure for TRUSTCLOUD's electronic signature and qualified seal preservation service is as follows:

1. The User submits to TRUSTCLOUD's "TRUSTCLOUD" platform the electronic files in PAdES format, the integrity and authenticity of which the User wishes to preserve.
2. The system proceeds to verify that they are in PAdES format.
3. The system verifies that the files are electronically signed or stamped and if the signature or stamp is qualified.
4. If confirmed, the system proceeds to add a qualified time stamp issued by a qualified service provider for this service and the corresponding electronic signature.
5. The resulting file, duly signed and stamped in a qualified manner, is stored in the warehouse and in the supplier's SQL database.
6. From then on, TRUSTCLOUD incorporates the electronic time-stampings on the stored PAdES-LTV format files, before the expiry of the certificate of the time-stampings of the signature initially made, thus guaranteeing the integrity of the archived electronic signature.
7. In addition, TRUSTCLOUD makes quarterly incremental copies of the Database, from which it will

gets its hash and is stamped with a qualified time stamp.

The complete outline of the process can be seen in the following diagram:



The processes involved in these activities are detailed below.

7.3.1 ENTRY OF DOCUMENTATION INTO THE TRUSTCLOUD SIGNATURE ESCROW SYSTEM

Once the relationship between TRUSTCLOUD and the issuer of the signed/sealed files to be kept for the provision of the electronic signature preservation service has been formalised, and following acceptance of this Certification Practices Statement, TRUSTCLOUD will provide the User with keys to incorporate the documentation and/or associated digital objects into the TRUSTCLOUD preservation platform ("TRUSTCLOUD"), and TRUSTCLOUD will check that the signatures and seals received are qualified.

The conservation service is integrated with the management systems of its Users through a web application (API). The "TRUSTCLOUD" platform must check that the signature or stamp is qualified upon receipt of the file transfer in the information system;

7.3.2 QUALIFIED ELECTRONIC TIME STAMPING

TRUSTCLOUD requests the Time Stamping Authority (TSA) to issue a qualified time stamp, according to the ETSI EN 319 421 recommendation [10], by means of a summary of the information to be stamped. This TSA generates a time stamp that is composed of the digest or hash, the date and time that have been obtained from a reliable time source, and its electronic signature.

TRUSTCLOUD incorporates this seal into the file, to guarantee that it exists at that moment and its integrity over time.

7.3.3 SQL DATABASE PER CUSTOMER HOSTED BY SERVICE PROVIDER

Once the process has been completed, the qualified signatures and seals are stored by TRUSTCLOUD in a SQL database of a service provider whose servers are hosted in the European Union.

TRUSTCLOUD has ensured that the supplier has the appropriate security measures in place to guarantee the availability, integrity and confidentiality of the database and has the required quality certifications to securely store qualified electronic signatures and seals. The supplier shall have implemented the technical specifications, in accordance with European legislation, in accordance with these two standards:

- ETSI TS 119 511 [5].
- ISO 14641-1 [11]

This documentation is stored for an indefinite period of time on these servers.

Notwithstanding this, a service continuity plan is provided for in the event of a service stoppage by TRUSTCLOUD (point 10 of this CPS).

TRUSTCLOUD provides a unique storage and preservation service. The data to be stored

stored are preserved by TRUSTCLOUD, while the preserved evidence and data are delivered by TRUSTCLOUD to the client upon request.

TRUSTCLOUD provides a unique preservation with storage service. The data to be stored is preserved by TRUSTCLOUD, while the evidence and preserved data is delivered by TRUSTCLOUD to the client upon request.

7.3.4 QUARTERLY COPIES AND TIME STAMPING OF THE DATABASE

In order to increase the security of the conservation of the declarations, a quarterly incremental backup of the data in the database is made by means of a CSV file, on which a hash is generated by applying the SHA 256 algorithm, and incorporates a time stamp by TRUSTCLOUD.

8 OBLIGATIONS AND RESPONSIBILITIES

8.1 TRUSTCLOUD OBLIGATIONS

TRUSTCLOUD as a PCSC is committed to comply with a number of obligations detailed in this CPD, within the framework of eIDAS [1], its implementing provisions and other applicable legislation.

8.1.1 TRUSTCLOUD ORGANISATIONAL REQUIREMENTS

- Operate its digital signature associated service infrastructures as set out in this CERTIFICATION PRACTICES STATEMENT.
- To provide the service of preservation of electronic signatures and seals in an impartial and objective manner.
- Ensure the adequacy of its processes and services to the standards to which they adhere.
- Informing the service applicant of the characteristics of the service provision, the obligations assumed and the limits of liability.
- To reliably protect all User data, as well as activity and audit logs, by the means it deems most appropriate and for the period of time contemplated according to the nature of the data recorded.
- Ensuring the provision of the electronic signature preservation service in a timely and uninterrupted manner
- Communicate to its Users sufficiently in advance the unavailability of the system in the event of modification, improvement or maintenance processes that imply a paralysis of the service.
- Notify the parties involved as soon as possible whenever an incident is detected in the system that affects them.
- Ensure that digital signature systems operate in synchronisation with reliable time sources, using a

Qualified Time Stamping Authority.

- Publish the most recent versions of this document and other definitions of practices of other services prior to the application of the conditions contained therein.
- To have a channel of communication with Users and third parties for requests, queries, complaints and claims.
- Deal with requests, queries, complaints and claims from Users and third parties within a reasonable timeframe.
- In case of receiving a request for an export-import package, it would be handled at the contractual level where a detailed plan of how to carry out the associated process will be elaborated.
- Depending on the method of production of the package(s), the necessary security measures will be applied. For example: encryption, password, two-factor etc.
- The data obtained after the end of the transition period agreed with the client starts the corresponding blocking period and is deleted at the end of this period in accordance with the legislation in force.

8.1.2 INFORMATION FOR BUSINESS PARTNERS

Business partners who rely on the digital objects archived by TRUSTCLOUD and make use of its services shall perform the following actions

- Verify the validity, suspension or revocation of the certificates used using the revocation status information (OCSP or CRLs of the Certification Service Provider that issued the certificate), incorporated within the PAdES-LTA file itself.
- Respect the security measures indicated by TRUSTCLOUD to access the electronic signature and qualified seal preservation service.

8.1.3 INFORMATION FOR AUDITORS AND REGULATORY AUTHORITIES

TRUSTCLOUD undertakes to communicate to the competent Public Authority any confidential information or information containing personal data when required to do so and in the cases provided for by law:

- Notify the accredited supervisory and control authority (SETSI of MINETAD) of any changes to this Declaration of Electronic Signature Retention Practices.

- Notify the competent authority and the parties involved of any change in the infrastructure that may affect the provision of the service.

In particular, TRUSTCLOUD is obliged to disclose the identity of the signatories when requested to do so by judicial bodies in the exercise of the functions attributed to them, and in the other cases provided for in the RGPD / Data Protection Legislation in force [3].

TRUSTCLOUD will inform auditors, regulators and tax authorities who rely on the electronic signature and seal preservation service that they should:

• Verify the validity, suspension or revocation of the certificates used using the revocation status information (OCSP or CRLs of the Certification Service Provider that issued the certificate), incorporated within the PAdES-LTA file itself.
Respect the security measures indicated by TRUSTCLOUD to access the service for the conservation of qualified electronic signatures and seals.

8.2 RESPONSIBILITY

TRUSTCLOUD as a Trusted Service Provider is subject to the liability regime set out in article 13 of the eIDAS [1], and will therefore assume liability for damages caused deliberately or negligently to any natural or legal person under the terms set out in the legislation in force.

TRUSTCLOUD shall not be liable for any damages caused by the improper use of the service for the preservation of qualified electronic signatures and seals.

TRUSTCLOUD shall not be liable for damages caused by force majeure, unforeseeable or unforeseeable circumstances or which, although foreseeable, could not have been avoided according to the state of the art.

All cases contemplated by law as Limitations to t h e liability of the PCSC are excluded from liability.

TRUSTCLOUD shall not be liable for the acts or omissions made by the User, and the User shall be liable for all damages, direct and indirect, that may be caused to any person, property, company, public or private service, specifically for loss of profits, loss of information and data, or the corresponding damages, as a result of the acts, omissions or negligence of the User as well as of third parties linked to him/her, due to inappropriate use, being at the sole risk of the User.

For this purpose, TRUSTCLOUD has taken out liability insurance of 3,000,000 € (three million euros) to cover the risk of liability for damages that it may incur as a result of its failure to comply with its obligations under the eIDAS Regulation [1].

8.3 OBLIGATIONS OF THE SUBSCRIBER

On the other hand, the subscriber of the qualified Signature and Seal Preservation Service shall comply with the following obligations:

- The objects shipped shall comply with the requirements set out in ETSI 119 511.
- It shall ensure legal compliance and the accuracy of the objects to be preserved.
- You must send the objects accurately and completely, as set out in paragraph 7.3 of this CPD.
- It shall take any other precautions prescribed in the contract or agreement reached.

9 SECURITY CONTROLS

TRUSTCLOUD has developed and implemented an information security management system consisting of policies, rules, standards, guidelines and internal procedures that define the framework for security in the company's systems, services and processes, with the aim of ensuring that the highest level of security is achieved in all areas of the company.

9.1 PHYSICAL SECURITY

TRUSTCLOUD guarantees that it complies with the applicable regulations and the main standards and best practices regarding physical security, as described in this section.

At TRUSTCLOUD's facilities, different security perimeters have been established with security barriers and entry controls appropriate to the activities that take place in each one of them. The aim is to reduce the risk of unauthorised access or damage to IT resources.

TRUSTCLOUD's information systems are located in restricted access areas that have been adequately protected by appropriate physical access control mechanisms. These systems have also been protected against other environmental threats such as fire, flooding or power outages.

This protection extends to those systems whose physical security is delegated to a supplier. To this end, the appropriate clauses have been signed in the contracts and the necessary monitoring mechanisms have been established by TRUSTCLOUD. The processing of information outside TRUSTCLOUD systems is duly authorised, once compliance with the required level of security is guaranteed.

TRUSTCLOUD has also implemented an asset management policy based on inventory and classification, storage and input and output records. On the technical side, procedures have been adopted to ensure that the information contained therein is adequately secured, as well as to allow its use without any risk to the information.

Some of the measures taken by TRUSTCLOUD include the following:

- Authentication and Access Control. Building access control
- Access control to DataCentres based on biometric fingerprint identification and centralised authorisation with access registration, both incoming and outgoing.
- The temperature conditions are ensured by self-contained refrigeration equipment located within the DataCenter that keep the temperature of the DataCenter within the established margins.
- Redundant power supply, providing two power supply lines to the racks used to house the equipment.
- The cabling used in the Data Centre is category 6,7 and fibre optic.
- Uninterruptible power supply systems. - Fire detection, based on smoke and aspiration detectors.
- Continuous and adequate air conditioning of the DPC zones with n+1 redundancy in each zone. - Humidity detectors in the DPC and electrical room areas.
- An agreement is in place with a specialised service provider for the safekeeping of magnetic media,

The building is equipped with an earthquake-proof vault.
- Access to the DPC by outsiders (visitors)
- Exposure to water
- Information retrieval

9.2 LOGICAL SECURITY

TRUSTCLOUD uses logical security measures common to all systems. The specific systems used for the provision of the service covered by this CPS have been equipped with a second level of security measures.

Responsibilities and documented procedures have been formally established to ensure the correct configuration, administration, operation and monitoring of TRUSTCLOUD's information and communications systems.

An incident management procedure has been established and defined in order to minimise the impact caused by security incidents or system malfunctions, enabling a rapid reaction to possible incidents and the establishment of corrective measures to prevent their recurrence.

Adequate segregation of duties has also been established in the assignment of responsibilities with the aim of preventing inappropriate use of the information systems, establishing, in cases where such segregation is not feasible, other appropriate control mechanisms that allow for monitoring and control.

Procedures and controls are in place to adequately prevent the introduction of malicious software, ensuring the integrity of TRUSTCLOUD software and information.

Safeguarding measures have been established, including the necessary backup copies, periodically checking their validity by restoring them, together with the permanent monitoring of the systems, which guarantees the continuity of TRUSTCLOUD's systems, services and information and the services provided.

The information transmitted over public or private communications networks is adequately protected by means of the appropriate mechanisms to guarantee its confidentiality and integrity. The necessary controls have been established to prevent the impersonation of the sender, modification or loss of the information transmitted, both in communications with systems located in internal networks and with other external systems, such as those entities that TRUSTCLOUD uses in the provision of its services as an intervening party in the same.

Procedures have been established that regulate TRUSTCLOUD's information encryption strategy, describing the organisational and technical measures that guarantee the confidentiality and integrity of the information.

Procedures are also established that regulate in detail the storage, handling, transport and destruction of sensitive information, both on laptops, mobile devices, etc.) and, residually, on paper, in order to mitigate the risk of unauthorised access, loss or theft.

9.2.1 ACCESS TO SYSTEMS

Access by both internal and external personnel to TRUSTCLOUD's information systems, as well as to the information they process and store, is regulated on the basis of the information and operational needs of each user, granting access exclusively to those functions and information that are required for the correct performance of their work activity, in accordance with their function and/or operational profile.

Those responsible for the processing of information assets shall be responsible for defining the levels of access.

to resources and authorise any extraordinary access, all in accordance with the guidelines of the owners of the information, or, where appropriate, the owners of the process or business.

Without prejudice to further detail in its application, nor to the formal delegation of functions, the following positions are understood as owners of the process or business:

- Information Security Officer (RSI-CISO)
- Systems Manager (RS)

All access to TRUSTCLOUD's information systems by users will be associated with a process of identification, authentication and authorisation, establishing the appropriate controls to ensure that these processes are carried out securely.

To this end, mechanisms have been designed and implemented to record and monitor access to and use of the systems in order to ascertain the effectiveness of the measures installed and detect possible security incidents.

9.2.2 REFERENCE TO SYSTEM EVENTS

In relation to possible system events, taking into account the category of services provided, TRUSTCLOUD has designed a system of logs and controls that allow for the reactive inspection of, among others, the following events on its systems:

- Successful and unsuccessful login and logout attempts.
- Successful or unsuccessful attempts to create, modify or delete accounts in the system.
- Successful or unsuccessful attempts to create, modify or delete authorised system users.
- Successful or unsuccessful attempts to create, modify or cancel requests within the different components of the system.
- Successful and unsuccessful attempts to sign files.
- Successful and unsuccessful attempts at certification files.
- Successful or unsuccessful attempts to send communications.
- Changes in system configuration.

9.2.3 RECORDS MANAGEMENT

The integrity and availability of audit records shall be maintained at all times, keeping time sources synchronised with all systems that generate such records, centralising, whenever technologically possible, the control and monitoring of the records by means of a management tool.

Audit trails generated by systems handling confidential information must be stored in accordance with the law; for all other systems this time will be regulated by the appropriate procedures.

Information systems shall have sufficient capacity to ensure that the storage of audit trails does not degrade the level of service.

Any strictly necessary changes to the generation of audit trails shall be duly authorised by the security officer.

Disposal of records should be done by mechanisms that do not degrade the confidentiality of the records.

9.2.3.1 PROTECTION OVER RECORDS

Access to TRUSTCLOUD's archive and document storage systems is restricted to authorised personnel only. An access control, identification and authentication system has been set up in such a way that it is protected against unauthorised access, modification, deletion or other unauthorised manipulation.

The systems, supports and media containing the documentation and information subject to archiving and custody, as well as the applications necessary to process and treat the data under custody are maintained and can be accessed for the period of time established in this CPS.

9.2.3.2 RECORD RETENTION PERIOD

The above records, including evidence of service, shall be stored and retained as audit records generated by the system for a minimum period from the date of their creation of one (1) year for daily audits, two (2) years for monthly audits and four (4) years for annual audits.

9.2.3.3 REQUIREMENTS FOR TIME SOURCES

Certificates, CRLs, and other revocation database entries shall contain date and time information.

TRUSTCLOUD's systems record the exact instant of time at which the records are made, using a time stamp issued by a qualified TSA in the case of being part of the processes that are part of the qualified electronic signature preservation services provided by TRUSTCLOUD.

All TRUSTCLOUD systems synchronise their instantaneous time with reliable time sources based on the Network Time Protocol (NTP), self-calibrating by various means.

9.2.3.4 BACKUP OF RECORDS

Back-up copies of the files containing the records subject to retention a r e made and stored in the cloud.

These backups are performed on all components of the service.

9.3 VULNERABILITY ANALYSIS

Given the increasing risk of malicious code being embedded in software, it will be mandatory to adopt criteria to help protect Information Systems against such attacks.

The IT department shall put in place all technical and organisational measures available to it to prevent the entry and spread of malicious code on its IT systems.

These measures include, but are not limited to, the following:

TRUSTCLOUD's Information Systems must have antivirus, firewall, antispyware and mail filtering, DLP, all of which are automatically updated, provided that the systems technologically support these types of controls. We have corporate Defender, internal SonicWall firewall and firewall managed by Movistar for office network connection and AWS IS measures.

- TRUSTCLOUD's anti-virus and mail filtering systems shall check all incoming and outgoing e-mail messages, as well as all internal messages on its communications networks.
- When an email does not comply with the security criteria defined in the antivirus and content filtering applications, the email will not be delivered to its addressee and will be automatically deleted. This action will be carried out in accordance with the due legal guarantees and respect for privacy.
- The status of any portable device, regardless of how it was obtained, should be checked using malicious code detection tools.

TRUSTCLOUD, or an external auditor with sufficient knowledge and certification, will perform at least a vulnerability scan.

It is the responsibility of the analysis team coordinators to inform the TRUSTCLOUD service managers, through the Security Manager, of the results of the analyses carried out, of any problems that prevent the performance of the audits, or the delivery of the resulting documentation.

Security scans involve the initiation of the necessary tasks to correct the vulnerabilities detected and the issuance of a counter-report.

The vulnerabilities found will be detailed in a resulting document labelled as: "Vulnerability analysis on TRUSTCLOUD platform". If any vulnerabilities are found, the TRUSTCLOUD team will analyse them and categorise and weight them according to the degree of affectation and proceed to create a proposal with countermeasures.

Countermeasures will be implemented in the shortest possible time, notifying the parties involved if there are entities adversely affected by the vulnerabilities found.

9.4 PERSONNEL SECURITY

TRUSTCLOUD will determine the human and technical equipment necessary for the provision of the services, ensuring the required quality and operating conditions and guaranteeing the agreed level of service.

TRUSTCLOUD will use all the technical and human resources necessary for the execution of the services, with the capacity, qualifications and experience required to provide them.

TRUSTCLOUD reserves the right to make the technical and human changes it deems appropriate to maintain the quality of the service provided, notwithstanding which, it will try to ensure that the changes in the provision of the Service are as few as possible.

TRUSTCLOUD guarantees to provide its staff with the training courses that may be necessary for the provision of services to be carried out diligently and with the appropriate level of qualification for the optimal development of the service.

TRUSTCLOUD shall also be responsible for any training that may be necessary for the USER's staff using the contracted service. The duration and number of participants shall be agreed with the USER.

10 CONTINUITY AND CONTINGENCY PLAN

TRUSTCLOUD has established business continuity and availability management processes to minimise the impact on critical functions and processes in the event of a disaster, in order to reduce downtime to pre-established levels. These processes have the appropriate combination of organisational, technological and procedural controls, both preventive and recovery.

These processes are supported by a Business Continuity and Availability Plan that is tested periodically and kept up to date at all times. To this end, the risk of threats and the associated impact caused by the lack of continuity of the information assets that support or are involved in TRUSTCLOUD's business processes are assessed.

10.1 BUSINESS CONTINUITY and AVAILABILITY PLAN

Business Continuity is the tactical and strategic ability of TRUSTCLOUD to plan for and respond to incidents and business interruptions in order to continue critical business operations within an acceptable and manageable level of service for TRUSTCLOUD.

The scope of the Business Continuity and Availability Plan is the same as that defined for the implementation of the Information Security Management System (IS). It includes TRUSTCLOUD's services and processes at its headquarters in Madrid, as well as the information systems and assets on which they are based: information and data, software, equipment, communications, auxiliary elements, information supports, personnel and premises.

In a disaster situation, the protection of people has the highest priority. This aspect is not covered in this plan, as it is only technologically oriented. No activity will be considered until the safety and well-being of people is ensured.

Staff forming the recovery team will be familiar with the responsibilities and content covered in this Plan.

In the event of a disaster situation TRUSTCLOUD will contact the relevant material supply provider. If replenishment time cannot be assured, it may be necessary to purchase equipment and store it in an alternative location to the main facility.

Once the Recovery Procedure has been established, its maintenance is mandatory. The recovery process is feasible only if this document is up to date and complete.

TRUSTCLOUD has a financial plan in place to provide it with sufficient financial stability and resources to operate in accordance with these CPS and to respond to contingencies.

10.2 CONTINGENCY PLAN

TRUSTCLOUD has established a contingency response plan, which determines the strategy and treatment to be given to contingencies.

The services and processes of the IT department that are most critical for the business are determined. In the event of serious contingencies, the service will be suspended for the duration of the contingency and system users will be notified as soon as possible.

The contingencies envisaged that could pose some kind of risk to the quality of service are as follows:

- Response times so long as to be in clear violation of the quality of service policy.
- Loss of synchronism with primary and secondary time sources.

Contingencies that may pose a risk to the provision of the service are:

- Errors in the operating systems associated with the provision of the service.
- Errors in the communication systems associated with the provision of the service.
- Errors affecting the provision of the service detected in the software of any of the services.

In addition, procedures are defined for teams to reconstitute TRUSTCLOUD operations using backup data and backup copies of keys.

11 COMPLIANCE AUDITS

11.1 AUDITOR PROFILE

The external auditor or team of external auditors shall be selected at the time of planning each audit.

Any company or person contracted to perform a security audit of TRUSTCLOUD or any of its services must comply with the following requirements:

- Adequate and proven training and experience in information systems security and auditing processes.
- Organisational independence of the TRUSTCLOUD authority, in case of external audits.

The external auditor or team of external auditors shall not have any current or planned financial, legal or any other type of relationship that could lead to a conflict of interest with TRUSTCLOUD. In order to comply with current legislation on data processing, and if the audit process involves access to personal data, the auditor shall be considered the Data Processor, pursuant to the provisions of article 28 of the GDPR [3].

11.2 AUDIT CRITERIA

Without prejudice to being extended by documents of the particular services offered by TRUSTCLOUD, in this section we will define the set of minimum checks of the adequacy of the services offered with respect to what is defined in this CPS. The aspects covered by an audit will include, but not be limited to:

- Security policy.
- Physical security of the facilities of the audited service.
- Logical security of TRUSTCLOUD systems and services
- Technological assessment of service components.
- Administration of services, as well as service security.
- The present CPD and service policies in force.
- Compliance with applicable legal requirements

11.3 FREQUENCY

Compliance audits are carried out at least every two years, unless there are relevant or essential changes in TRUSTCLOUD's systems and services, in which case extraordinary audits will be carried out.

11.4 ACTION PLAN

The identification of deficiencies in the audit shall lead to immediate corrective action. The competent authorities as defined by the applicable legislation in collaboration with the auditor shall be responsible for the determination of these deficiencies.

11.5 COMMUNICATION OF RESULTS

The external auditor(s) shall communicate the results of the audit to the TRUSTCLOUD Security Manager, as well as to those responsible for the different areas in which non-conformities are detected, as well as to the competent authority as determined by the legislation in force.

12 CONFIDENTIALITY POLICY

There is a general duty of confidentiality with regard to the information that TRUSTCLOUD employees learn by reason of their job. Information considered confidential provided to TRUSTCLOUD will under no circumstances be disclosed to third parties unless it is covered by the requirements of collaboration with the competent institutions.

The Parties shall not be bound by the obligation of confidentiality under this Clause where confidential information is required to be disclosed by law or to comply with a judicial or administrative order, provided that they notify the Party to whom the confidential information pertains.

In this sense, it shall be considered as 'confidential' information (without prejudice to the fact that other information may also be 'confidential'):

- Business continuity and contingency plans.
- Information relating to the operation and maintenance of the service.
- Any information relating to the operations carried out by TRUSTCLOUD.
- Any information relating to security parameters, control and audit procedures.
- All personal information provided to TRUSTCLOUD during the certificate subscriber registration process, except as specified by the applicable Certification Policy and the certification contract.
- Business information provided by its suppliers and other persons with whom TRUSTCLOUD has a legal or contractual duty of confidentiality.
- Transaction records, including complete records and audit trails of transactions.
- All information classified as "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL".

However, the following materials, among others, shall be considered as non-confidential public documents:

- TRUSTCLOUD's Qualified Electronic Signature and Seal Retention Practice Statement
- All information that is considered "Public".

13 PROTECTION OF PERSONAL DATA

TRUSTCLOUD will process the personal data necessary for the development of its activity by obtaining the guarantee from the DPO of the correct obtaining of the express consent of the signatories. This processing will be carried out in accordance with the provisions of the GDPR [3].

The personal data provided by Users will be processed by TRUSTCLOUD in its capacity as Data Processor for third parties under the terms and conditions set out in article 28 of the RGPD [3]. In this regard, TRUSTCLOUD undertakes to comply with the following conditions:

- The data processing that TRUSTCLOUD will carry out will be limited to the actions that are necessary to provide the Data Controller with the contracted Services.
- Specifically, TRUSTCLOUD undertakes to process the Personal Data in accordance with the instructions given by the DATA CONTROLLER from time to time, as well as with the provisions of the applicable legislation on personal data protection.
- TRUSTCLOUD also undertakes not to carry out any other processing of the Personal Data, nor to apply or use the data for any purpose other than the provision of the Service.
- TRUSTCLOUD declares that it complies with the security measures defined in the present DPD, these being those that are necessary to guarantee the security of the personal data processed in the service provided, for the purposes of guaranteeing confidentiality and integrity according to the nature of the data, in accordance with the provisions of the RGPD [3].

For the purposes of the provisions of this section, TRUSTCLOUD shall inform its employees of the obligation of secrecy and confidentiality, as well as the consequences of non-compliance, with respect to the processing of personal data.

TRUSTCLOUD undertakes to keep under its control and custody the personal data provided by the FILE RESPONSIBLE to which it has access in order to provide the Service and not to disclose, transfer or otherwise communicate them, not even for storage to other persons.

Upon completion of the service that is the object of the Contract, TRUSTCLOUD undertakes to destroy or return any information containing personal data that has been transmitted by the FILE RESPONSIBLE to TRUSTCLOUD for the purpose of providing the Service.

In the event that the data subjects, whose data is held in files owned by the FILE CONTROLLER, exercise their rights before TRUSTCLOUD, the latter shall immediately forward the request to the FILE CONTROLLER and, at the latest, within 3 working days of receipt thereof, so that the FILE CONTROLLER may duly resolve the request.

This CPS is considered as a reference document for the implementation of technical and organisational security measures, taking into account Trustcloud's proactive responsibility to ensure compliance with the GDPR [3].

TRUSTCLOUD guarantees compliance with the obligations corresponding to it by virtue of the regulations applicable to it in terms of personal data protection.

In the event of a breach of security or loss of integrity that has a significant impact on the service provided or on the personal data processed, TRUSTCLOUD shall notify the supervisory body and, if necessary, the Spanish Data Protection Agency within 24 hours of becoming aware of the incident, in accordance with article 19.2 of the eIDAS [1].

14 TERMS AND CONDITIONS OF SERVICE

14.1 SERVICE DELIVERY MODEL (SUPPORT, AVAILABILITY)

TRUSTCLOUD has implemented a service delivery model as described in this CPS. This model will be accompanied by a service level agreement to measure its performance, as well as a support service, which will incorporate in general terms:
In case of receiving a request for an export-import package it would be handled at contractual level. The export-import packages will be prepared according to ETSI 119 512.

TRUSTCLOUD provides a preservation with storage service. The data to be stored is preserved by TRUSTCLOUD, while the evidence and preserved data is delivered by TRUSTCLOUD to the client upon request.

When TRUSTCLOUD is unable to collect and verify all validation data, a notification of the failure would be sent and

it would be filed as an unqualified file.

The preservation objective assumed by TRUSTCLOUD is the Preservation of Digital Signatures (PDS).

TRUSTCLOUD uses Excel as a test log, within which the use case test cycles associated with the maintenance service provided by TRUSTCLOUD are specified.
Tests are performed within TrustCloud, stored in the database and in the log tool, evidence is kept in the storage tool.
Evidence is validated using the Digital Signature Service (DSS). Increased proof of preservation is achieved by resealing.
TRUSTCLOUD has a time-stamping provider and a certificate provider.
TRUSTCLOUD in case the preservation sender plays a role in the preservation process, this will be negotiated on a case by case contractual level.

THE CRITERIA TO BE USED IN DEALING WITH PETITIONS

- The level of functional support to be provided and its availability
- The level of technical support to be provided and its availability
- The escalation process to be followed when notifying the occurrence of an occurrence of an incident
- The request management system for the resolution of incidents to be used
- The communication mechanisms that will be used to provide the support
- Available languages in which support will be provided
- The Service Level Agreement (SLA) associated with the service will contain:
  - SLAs relating to response and resolution times in resolving incidents
  - SLAs relating to the overall quality of service delivery
  - SLAs relating to the availability of services
  - SLAs relating to provisioning time for new and/or scalable services
  - SLAs relating to the performance of volumes of information
- Scorecard for the management, control and governance of the service.
- Statistical, operational and NSA compliance reports.

TRUSTCLOUD will, as far as possible, endeavour to ensure that its services are accessible to all those who wish to subscribe to them, provided that they agree to comply with their obligations as set out in these terms and conditions. TRUSTCLOUD, in the provision of the services described in these TOS, warrants that it will not operate in a manner that discriminates in any way.

14.2 OBLIGATIONS OF SUBSCRIBERS

The rates and economic conditions of the different services are available in the document "TRUSTCLOUD General Terms and Conditions".
However, TRUSTCLOUD may establish contractual frameworks with specific Users that particularise these conditions for the collaboration scenario established between both parties.
The rates established by TRUSTCLOUD for payment for the provision of the service will be maintained on the basis of

The following concepts:

- Monthly fee for the use of the Service
- Cost per certification transaction managed by the Platform: the amount of each transaction request to the Platform.
- Cost per communication operation managed by the Platform.

This updated financial information can be accessed at the time of contracting, as well as before or at any other time that may be required, if TRUSTCLOUD is requested to provide this information.

14.3 LIMITATIONS ON THE USE OF THE SERVICE

The Services provided by TRUSTCLOUD have no territorial limits.

14.4 PROVISIONS IN THE EVENT OF TERMINATION OF SERVICE

TRUSTCLOUD undertakes to adopt all necessary measures to minimise the impact that a User or third parties involved in the service of these CPS may suffer as a result of the paralysis or termination of the service. In particular, periodic and continuous maintenance of the information required to verify the effective provision of the services provided by TRUSTCLOUD will be carried out.

In particular, TRUSTCLOUD has an updated service termination plan procedure, which sets out the process that TRUSTCLOUD will carry out prior to service termination, specifically in terms of portability and cessation of activity.

TRUSTCLOUD has arrangements in place that will allow it to cover the costs associated with these minimum requirements in the event that it does not have sufficient funds or for other reasons that it is unable to cover these costs itself, taking into account current insolvency law.

14.4.1 PORTABILITY

TRUSTCLOUD will transmit the documentation evidencing all the registration and other material in its possession that may be necessary to whoever it deems necessary to demonstrate the correct operation of the service for a reasonable period of time in accordance with the provisions of the applicable legislation in force.

The specific material destruction or handover processes of each service, if any, would be defined in their specific policy definitions.

14.4.2 CESSATION OF ACTIVITY

In the event of termination of its activity as Certification Service Provider, TRUSTCLOUD shall, with at least two months' notice, take the following actions:

- Inform all subscribers to its services of the cessation of activity.
- Inform all third parties with whom you have signed a contract concerning this service.
- Notify the Ministry responsible for the Information Society of the cessation of its activity and the destination it is going to give to the electronic signatures and seals kept, as well as any other relevant circumstance related to the cessation of activity.

14.5 RESOLUTION

Without prejudice to the causes described in the Spanish regulations, TRUSTCLOUD will consider the following as causes for early termination of the provision of services:

- In the event of breach by the parties of any of the obligations set out in these General Conditions of Use, the defaulting party shall be required to remedy the breach within a period of 30 days.
- By judicial or administrative decision, which implies the impossibility for any of the parties to execute the agreed conditions of the service.
- The simple non-compliance and/or delay in the payment of any of the payment obligations listed in the contracting conditions shall be understood as sufficient grounds for TRUSTCLOUD to unilaterally terminate the service contract, without prejudice to claiming the outstanding payment obligations, if any.

TRUSTCLOUD reserves the right to terminate the contract in the event of supervening circumstances arising from a change in market conditions, vices or deficiencies in the data or information received for the preparation of the economic proposal, or any other circumstance beyond its control, including the production of a mismatch between the agreed prices and the cost of execution of the Service, derived from market circumstances, resulting in an economic deficit for the execution of the Service and in general for any cause beyond the control of TRUSTCLOUD, which produces a break in the economic balance of the same.

14.6 SUBCONTRACTING

TRUSTCLOUD may subcontract the services it deems necessary for the provisioning and operation of the Service in accordance with the needs that may arise, and will formalise this relationship by means of a written agreement that will determine the conditions of the service provided by means of this subcontracting.

14.7 NULLITY

If any of the General Conditions of Use is declared wholly or partially null and void or ineffective, such nullity or invalidity shall not affect the validity or enforceability of the General Conditions of Use.

ineffectiveness shall affect only that provision or part of it which is ineffective or void, and the rest of the clauses shall continue in force, such provision or part of it being deemed not to be in force.

14.8 NOTIFICATIONS

Any notification, demand, request or any other communication required under the practices described in this Declaration of Certification Practices shall be made by means of a digitally signed document or electronic message or in writing by certified mail addressed to any of the addresses contained in the point relating to Contact details. The electronic communications shall become effective once they are received by the addressee to whom they are addressed. In the event of a change of address, the parties shall be obliged to notify the other party of the change in the manner set out in the first paragraph.

14.9 APPROVAL AND REVIEW OF TRUST SERVICE PRACTICES

14.9.1 APPROVAL AND IMPLEMENTATION

These CPS shall be approved by the Director of TRUSTCLOUD, the highest level and authority of responsibility within TRUSTCLOUD, who shall also have the responsibility and capacity to prepare and manage them. A management team has been established and is responsible for the implementation of the security and organisational practices required to ensure confidentiality, integrity and all that is established in these CPS. TRUSTCLOUD has defined a team made up of the heads of the different areas involved in each of the steps of the signature and electronic seal preservation service.

14.9.2 MODIFICATIONS

TRUSTCLOUD reserves the right to unilaterally modify this document provided that:

- The modification is technically and legally justified.
- Users are notified of all changes resulting from these modifications and accept them before using the service.
- A mechanism for change and edit control is provided.

In this regard, a procedure has been established for this purpose, which regulates the mechanisms to be followed in the event of the need to modify the CPD. Once it has been decided that a revision is advisable, the person responsible for drawing up the document will make the appropriate modifications, which will be identified in the new edition by shading the modified text. This method may coexist with or be replaced by a change control list listing the changes introduced in each of the editions or versions of the document.

If the changes made to the document result in an alteration that affects the service provided to users, they will be considered a major release. Otherwise they will be considered a minor release.

Users will be informed in the event of a major release and the list will be modified.
contractual agreement between TRUSTCLOUD and them. Users must therefore adhere to the new terms and conditions.

of use after the provision of new services or the initiation of a de-registration process.

14.9.3 VERSIONS

These CPDs are subject to change over time. When a major release change occurs, it will increase the versions of the document by one. However, when a minor release change occurs it will change its version number.

14.9.4 PUBLICATION

It is TRUSTCLOUD's obligation to publish information regarding its practices, its certificates and the status of these certificates. The entire history of this documentation must be kept and accessible on request via the contact email address on the website (point 6) for at least 15 years.

Any publication shall be made on the TRUSTCLOUD website or on websites under the control of TRUSTCLOUD and with a direct or indirect link to TRUSTCLOUD's corporate name and/or brand. It shall also be published by sending certified e-mail and on the website of the Competent Authority. The publication shall be made at the time of its creation.

14.9.5 APPLICABLE LAW AND JURISDICTION

These general terms and conditions shall be governed by Spanish law.

The parties, expressly waiving any other jurisdiction that may correspond to them, submit to the Jurisdiction and Jurisdiction of the Courts and Tribunals of Madrid for any matter relating to the interpretation, compliance or execution of this declaration.

15 CONSERVATION PROFILE

TRUSTCLOUD only provides the service of preservation with storage. At the end of the transition period agreed with the client, the period of blocking of the data obtained begins, which are deleted at the end of this period in accordance with the legislation in force.

The preservation profile is identified by the following OID: 1.3.6.1.4.1.5 2582.1.1.1. The
operations supported by the preservation protocol are the following:

Call 1) Send. Send the information. Described in section 7.2 MAIN FEATURES OF TRUSTCLOUD SERVICES

Call 2) retrieve the file. File recovery method via the API Call 3) Delete P0. Method of deletion through the API.

The period of validity of the preservation profile shall start after completion of the process described in point 7.3 PRESERVATION SERVICE FOR QUALIFIED SIGNATURES AND ELECTRONIC SEALS

The storage with preservation model provided by TRUSTCLOUD is a preservation with storage model.

TRUSTCLOUD refers to the statutory retention periods for blocked data:

- In compliance with article 9.3.a) Law 6/2020 of 11 November, regarding the obligations applicable to qualified providers, "the period of time during which they must retain the information relating to the services provided in accordance with article 24.2.h) of Regulation (EU) 910/2014, shall be 15 years from the expiry of the certificate or the termination of the service provided". Therefore, TrustCloud will retain the information relating to the signature and seal preservation service for 15 years from the termination of the service provided.

Preservation objectives are a combination of Preservation of digital signatures and enhancement of preservation evidence through resealing.

16 PRESERVATION EVIDENCE POLICY

Tests are performed within Trustcloud and stored in the database and in the log tool, evidence is kept in the storage tool.

SHA-256 algorithms are used for document hashes and SHA-512 for timestamps.

Preservation evidences are validated through the Digital Signature Service (DSS). The PDF evidences are PAdES. This same validation could be done by a third party. Increased preservation evidence is achieved by resealing.

We use PAdES, when downloading the evidence they have no information about our service, only the time stamp.

TRUSTCLOUD has a qualified timestamp provider and a qualified certificate provider.

TRUSTCLOUD, when unable to collect and verify all validation data, will send a failure notification and archive as an unqualified file.

17 SUBSCRIBER AGREEMENT

The following policy applies to access rights:

- Reading: authorised users.
- Modification: administrators, and only on request for good cause.
- Deletion: administrators. and only on request for good cause.

All evidences generated during the custody process are recorded in an evidence certificate generated by TRUSTCLOUD. These evidences will be delivered at the end of the service or delivered to the subscriber upon request.