STATEMENT OF PRACTICES FOR THE PRESERVATION OF ELECTRONIC SIGNATURES AND SEALS

TrustCloud

TYPE OF DOCUMENT				
				Secret Documentation
			x	Public Documentation
				Internal Documentation
				Confidential Documentation
QUALIFICATION			STATEMENT OF PRACTICES OF CONSERVATIONOF SIGNATURES AND ELECTRONIC STAMPS	
ENTITY			TRUSTCLOUD TECH SL	
FORMAT			Electronic - PDF	
PAGES			35	
VERSION	DATE OF EMISSION	OID	AUTHOR	
04	10/24/2024	1.3.6.1.4.1.62143.1.1.1	TRUSTCLOUD	
Revised by: Alberto Angon (CISO-RSI) Firmado electrónicamente por ALBERTO ANGON ROBLES el 2024-11-15 14:03:25 CET			Date:	
Approved by: Committee of Address TRUSTCLOUD Firmado electrónicamente por ALBERTO ANGON ROBLES el 2024-11-15 14:03:26 CET			Date:	

RECORD OF CHANGES

Version	Date	Description of the action	Pages
01	09/01/2024	First version of the document.	
02	05/22/2024	Correction of STAGE 1 audit findings. Modification of sections 4 and 9.2.	
03	10/17/2024	Align the documentation in accordance with the provisions of Article 24.2.a of Regulation (EU) No 910/2014	
04	10/24/2024	Qualified trust service providers should inform the supervisory body at least three months in advance if they intend to cease such activities.	

Index

1 INTRODUCTION

The present document is a Statement of Internships of the Service of Conservation of signatures and stampselectronic, through which TRUSTCLOUD TECH SL, as a trusted service provider, exposes and describes the shape in that lends the service of conservation of signatures electronic qualified and stampselectronic qualified and ensures compliance of the obligations legally enforceable, reportingto the public about the correct mode of utilization of these services.

This Declaration of Practices are directed to All natural and legal persons requesting, subscribers and in general users of the services of custody, of accordance with it established inLaw 6/2020, of November 11, regulating certain aspects of electronic trust services and Regulation 910/2014 of the Parliament European and Council resolutions of 23 July 2014 on electronic identification and electronic identification services trust for the transactions electronic in the market inside and for the that HE repeals the Directive1999/93/EC.

To this end, TRUSTCLOUD 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 provider comprehensive trust services, obtaining its ISO/IEC 27001 certification, with the objective of developing and implanting effectively their services

In addition, for the custody service of electronic signatures and electronic seals, TRUSTCLOUD continuesthe indications of the standards of the European Telecommunications Standards Institute -ETSI-guided by the technical specifications of the ETSI TS 119 511 and EN 319 401 standards (general requirements for trust service providers), EN 319-102-1 (procedurecreation and validation of AdES digital signature), TS 101 533-1 (European standard for the system of conservation) and ISO 14641-1 (specifications for the design and operation of a system of information for the preservation of the information digital). NOM-151 (Requirements that must be observed for the conservation of messages of data and digitalization of documents)

To this end, TRUSTCLOUD has carried out the design and development of a technological infrastructurethat, of shape integrated, puts to provision of their Users a tool to thorough of them that canretain qualified electronic signatures and seals for a long time, and reseal them periodically, mode that HE guarantees the effectiveness legal probationary enough during all the validity of the custody.

2 DOCUMENT IDENTIFICATION

In order to identify each type of service performed by TRUSTCLOUD, I agree with this Declaration of Practices for the Conservation of Electronic Signatures and Seals qualified, HE assigns to each guy an identifier of object (OID).

This Certification Practice Statement describes the services related to the conservation of signatures and stamps electronic qualified borrowed to through of the platform ownershipof TRUSTCLOUD, including among other aspects of the description and functionality of the services borrowed the following:

- The characteristics of each service.
- The flows of treatment and operation.
- The identification of all those involved, from those providing documentation to be kept in custodyqualified manner, up to the certification service providers responsible for generating stamps of time and electronic signatures.
- The obligations assumed in the provision of the services.

- The measures security techniques and organizational implanted.
- The conditions generally of use and hiring of the services.

3 ACRONYMS AND DEFINITIONS

Acronyms

ACRONYM	DEFINITION
LSC	Law 6/2020, of November 11, 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 the Directive 1999/93/EC
GDPR	Regulation 2016/679 of 27 April 2016 on the protection of natural personal data about the processing of personal data and the free movement of these data and by he that is repealed the Directive 95/46/EC
LSSI	Law 34/2002, of 11 of July, of services of the society of information and e-commerce
PCSC	Providers of Services of Certification
TSA	Time Stamp Authority – Authority of Sealed of Time
CPD	Center of Prosecution of Data
NTP	Network Time Protocol – Protocol of Internet for synchronize the watches ofthe computer systems.
PKI	Public Key Infrastructure – Infrastructure of Clue Public
WF	Workflow – Flows of work of each process
CRL	Certificate Revocation List
OID	Object Identifier - Worth, of nature hierarchical and comprehensive of a sequence of components variables, although always constituted by integers,non-negative numbers separated by a dot, which can be assigned to objects registered and that they have the property of be unique between the rest of OID

Definitions

CONCEPT	DEFINITION
DPC	**Certification Practices Statement:** Trustcloud Statement putting to provision of the public by via electronics and of shape freeperformed in quality of Lender of Services of Trust in complianceof it willing by the Law.
LENDER OFSERVICES OF TRUST	Person physics either legal that lend one either further service of trust, of accordance with it established in he eIDAS
LENDER QUALIFIED BYSERVICES OF TRUST	Trusted service provider that provides one or more services qualified and to whom the supervisory body has granted the qualification.
AUTHORITY OF SEALED OF TIME	person physics either legal that, of accordance with the regulations about Sealedof Time issues Stamps of time electronic.

STAMP OF TIME ELECTRONIC	Data in an electronic format that links other data in electronic formatwith a specific moment, providing proof that these latest data existed in that instant.
STAMP OF TIME ELECTRONIC SKILLED	Seal of time electronic that fulfils the established requirements in Article 42 of the eIDAS.
USER	Natural or legal person who uses the services of qualified custody of signatures either stamps electronic qualified, previous acceptance of the conditionsassociated with the service and the DPC.
DOCUMENTATION	Set of digital evidence received by Trustcloud from the User, that they comply with the requirements established in the presents DPC.
CERTIFICATE	File signed electronically by a lender of services ofcertification that links signature verification data to a signer and confirms his identity.
CLUE PUBLIC	Publicly known mathematical values are used for verification of digital signature or data encryption. Also call verification data signature.
CLUE PRIVATE	Mathematical value known only to the subscriber and used for the creation of a signature digital he decoded of data. Also call dataof creation of signature.
FUNCTION HASH	Operation that HE performs about a set of data of any size, ofso that the result obtained is another set of data of fixed size, regardless of the original size, and which has the property of being associated.

HASH EITHER FINGERPRINT DIGITAL	Fixed-size result obtained after applying a hash function to a message and that fulfils the property of being uniquely associated with the data initials.
PACKAGE OF EXPORT- IMPORT	Information extracted from the preservation service that includes the object of data of presentation (SubDO), the evidence of preservation and the metadatarelated to the preservation, it that allows that other service of preservation matters to continue achieving the preservation goal based on this information

4 APPLICABLE RULES AND STANDARDS

1] Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on the electronic identification and trust services for electronic transactions in the internal market and beyond the one that HE repeals the Directive 1999/93/EC
[2] Law 6/2020, of November 11, regulating certain aspects of electronic trust services
[3] Regulation 2016/679, of April 27, 2016, regarding the protection of natural people with regard to respects to the treatment of data personal and to the free circulation of these data and by he that HE repealsthe Directive 95/46/EC
[4] Law 34/2002, of 11 of July, of services of the society of the information and of trade electronic
[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 signatures.
[6] ETSI IN 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 IN 319 421 v1.0.0 Electronic Signatures and Infrastructures (ESI); Policy and SecurityRequirements for Trust Service Providers issuing Timestamps
[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 standardization of long-term data preservation services, including preservation of/with digital signatures.

5 COMPLIANCE REQUIREMENTS

TRUSTCLOUD guarantees, in line with his statement of applicability and with the legal requirements, that fulfills with:

1) The Policy of security of the information that is aligned with the regulation legally applicable.
2) The Policy of service of conservation of signatures and stamps electronic qualified defined in thisStatement of Internships of Certification.
3) The organizational requirements defined in the spots 8.1.1.
4) The obligation to provide the required information, when necessary, to its business partners, auditors and regulatory authorities, as specified in sections 8.1.2 and 8.1.3. of this document. document, including the requirements organizational.
5) Trustcloud has implemented controls that meet the requirements specified in Annex A of the ETSI TS 119 511 standard [5], guaranteed by the implementation of an ISMS based on the rule ISO/IEC 27001 :2022, as supplier of services of trust.
6) Trustcloud considers the legal requirements necessary for the use of signatures and seals electronic qualified that use devices Insurance of creation of signature.

6 IDENTIFICATION AND CONTACT DATA

- Company Name: TRUSTCLOUD TECH S.L.
- Denomination Commercial: TRUSTCLOUD
- CIF: B67693655
- Address: CALLE BUENOS AIRES, 12. 48001 BILBAO
- Customer Service to the Client (SAC): +34 913 518 558
- Mail: contact@trustcloud.tech
- Web: https://trustcloud.tech/en/
- Other data of contact: +34 913 518 558

7 SERVICE DESCRIPTION

TRUSTCLOUD, as lender of services of trust, offers a service skilled in conservation of signaturesand qualified electronic seals, which preserves the aforementioned electronic signatures and seals qualified through the utilization of procedures and technologies capable of enlarging the reliability of the dataof the electronic signature qualified, beyond the period of validity of electronic certificate

7.1 PARTIES INVOLVED IN TRUSTCLOUD SERVICES

The parts interveners in the services of TRUSTCLOUD are:

Users of the service:

Users of the services are the natural and legal people to whom the services are intended. preservation of electronic signatures and seals, who wish to preserve qualified electronic signatures and seals long term, guaranteeing integrity, authenticity and its legality to the long weather.

Store of Custody:

Store and Base of data SQL where HE stores the Statements signed and sealed, perfectlyclassified.

Lender of Services of Certification Skilled:

Entity is legally constituted, and duly qualified by some of the authorities competent of a countrymember of the EU, whose main activity is the issuance of certificates of qualified signatures and seals for the purpose of triggering signatures and stamps qualified.

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

1) Requirements of Normalized Policy (N), based in advanced electronic signatures
2) Extended Policy Requirements (N+), the use of which provides greater security by expanding the standardized requirements with requirements for signatures electronic qualified, demanding the useof AdES formats issued with secure signature creation devices and based on certificates qualified.

TRUSTCLOUD demands of the Providers of Services of Trust Skilled, in all cases, that use the policyN+ (signatures electronic qualified) in this service.

Authority of Sealed of Time Qualified:

Authority that generates qualified time stamp certificates with the file summary Hash, the date and the hour obtained of a fountain reliable of time, proceeds to his signature electronics and HE provides to TRUSTCLOUD, guaranteeing his existence and his integrity in the time from the moment of the realization of the sealed.

Of the same mode, the Authority of Sealed of Time Qualified will perform the processes of resealed of time of the signatures and stamps electronic preserved, being carried out before of its expiration, a new sealed electronic oftime, with the sole purpose of guaranteeing the longevity of this, and therefore the reliability of the electronic signature throughout the time.

Other providers of services:

TRUSTCLOUD accounts for the services of providers of service of storage Cloud for the conservation.

The description of the intervention in the different processes, in which the service providers intervene previously cited, is reflected in the present DPC.

7.2 KEY FEATURES OF TRUSTCLOUD SERVICES

Through the service borrowed by TRUSTCLOUD, HE guarantees the following aspects

1) That the files that HE receives by part of the User HE finds, in all cases, in format PARENTS.

2) That the electronic signatures and seals kept are qualified, in such a way that they comply with the following requirements:

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

✓ That has been generated, in all cases, in a device sure of creation of signatures.

3) That the signatures and qualified stamps that preserved comply with the requirements of longevity, expandingthe reliability of the data of the qualified electronic signature or seal, used beyond the period of validity of the certificate electronic with which HE performs the signature.

7.3 SERVICE FOR THE PRESERVATION OF QUALIFIED ELECTRONIC SIGNATURES AND SEALS

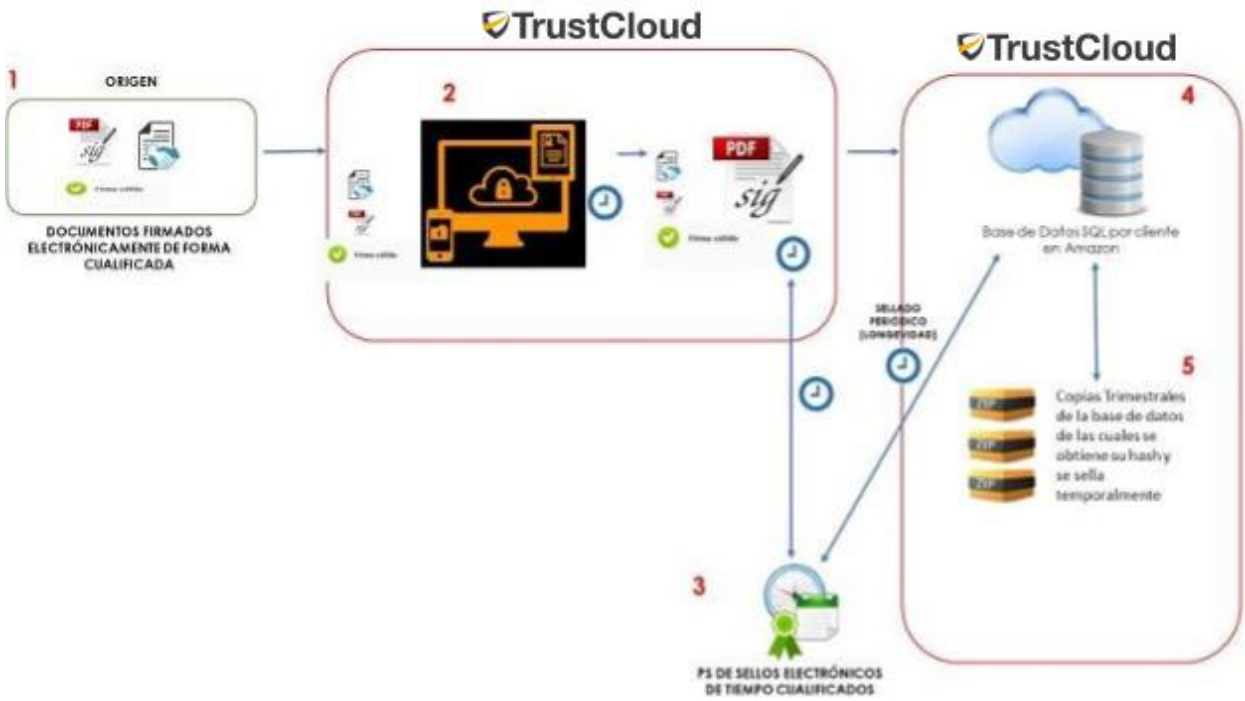
The electronic signature and seal conservation service consists of a solution aimed at guaranteeing the integrity and legal validity of the files incorporated therein. The entire process is carried out in accordance with the guidelines of the service skilled of conservation of qualified electronic signatures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

Through this service, only the electronic signatures and seals of the files are preserved (reception, reviews and recording of the signatures and electronic seals of each file, record of operations for guarantee his integrity, authenticity and Confidentiality to it long of the time), while that he storageand the preservation of the electronic files associated with these signatures and seals is the responsibility ofthe, entity generator of the signatures and stamps qualified.

The procedure for the TRUSTCLOUD electronic qualified signature and seal conservation service is the following: following:

1. He User refers to the platform “TRUSTCLOUD” of TRUSTCLOUD the files electronic in format PAdES, whose integrity and authenticity wishes preserve.
2. He system proceeds to verify that the same HE finds in format PARENTS.
3. The system verifies that the files are electronically signed or sealed and if the signature or seal of these is qualified.
4. If confirmed, the system proceeds to add a qualified time stamp issued by a lender of qualified services for this service and the corresponding signature electronics.
5. The files resulting, duly signed and sealed temporarily of shape qualified HE guard inthe warehouses and at the Base of SQL data of the supplier.
6. From then on, TRUSTCLOUD incorporates electronic time re-stamping. about the files in format PAdES-LTV preserved, before of that expiration, the certificate of the stampsof the time of the signature initially made, thus guaranteeing the integrity of the electronic signature archived.
7. Additionally, TRUSTCLOUD makes quarterly incremental copies of the Database, from which gets its hash, and HE seal with a stamp of time skilled.

He schemes complete of the process HE can notice in the following diagram:



To continue, HE proceeds to detail the processes that they perform are activities.

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 that must be kept for the provision of the electronic signature conservation service, and after acceptance of the this Certification Practices Statement, TRUSTCLOUD will provide the User with passwords to be able to Incorporate the associated documentation and/ or digital objects into the TRUSTCLOUD conservation platform ("TRUSTCLOUD"), being checked by TRUSTCLOUD that the signatures and the stamps received are qualified.

The service of conservation HE integrates with the systems of management of their Users to through of an application web(API. The "TRUSTCLOUD" platform must verify that the signature or seal is qualified when receiving the transferof the file in the system of information.

7.3.2 QUALIFIED ELECTRONIC TIME STAMPING

TRUSTCLOUD requests the Time Stamping Authority (TSA) to issue you a qualified time stamp, in accordance with the ETSI EN 319 421 recommendation [10], by means of a summary of the information to be stamped. This TSA generates a timestamp that is composed of the summary or hash, the date and the time that have been obtained from a fountain reliable of time, and his signature electronics.

TRUSTCLOUD incorporates this seal into the file to guarantee that it exists at that time and its integrity in the future. time.

7.3.3 SQL DATABASE PER CLIENT HOSTED AT SERVICE PROVIDER

Once the process is complete, the qualified signatures and seals are stored by TRUSTCLOUD in a database of SQL data of a lender of services whose servers HE finds housed in the Union European.

TRUSTCLOUD has ensured that said provider establishes the appropriate security measures for guaranteeing the availability, integrity and confidentiality of the database and that it has the certifications of quality required to securely store qualified electronic signatures and seals. The providermust have implemented the technical specifications, in accordance with European legislation, in accordance with these two rules:

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

This documentation HE maintains stored during time indefinite in sayings servers.

Notwithstanding this, a service continuity plan has been provided in the event of service interruption due to part of TRUSTCLOUD (point 10 of the present DPC).

TRUSTCLOUD provides a unique service of conservation with storage. The data that must be stored are preserved by TRUSTCLOUD, while that the evidence and the data preserved are delivered by TRUSTCLOUD to client, prior application

TRUSTCLOUD provides a unique storage preservation service. The data that needs to be stored is preserved by TRUSTCLOUD, while the evidence and the data preserved are delivered by TRUSTCLOUD at customer, previous application

7.3.4 QUARTERLY COPIES AND TIME STAMPING OF THE DATABASE

With the aim of increasing the security of the conservation of the statements, quarterly HE performs an incremental backup of the database data via a CSV file, on which the generates a hash through the application of the algorithm SHA 256, and incorporates a seal of time by TRUSTCLOUD

8 OBLIGATIONS AND RESPONSIBILITIES

8.1 TRUSTCLOUD OBLIGATIONS

TRUSTCLOUD as PCSC HE compromises to achieve a series of detailed obligations in this DPC, in theframe of the eIDAS [1], its provisions of development and other legislations that be of application.

8.1.1 TRUSTCLOUD ORGANIZATIONAL REQUIREMENTS

- Operate their infrastructures of services partners to the signature digital according to it exposed in this STATEMENT PRACTICES OF CERTIFICATION.
- Lend the service of conservation of signatures and stamps electronic of shape impartial and objective.
- Guarantee the adequacy of their processes and services to the standards that HE adheres to.
- Inform the service applicant of the characteristics of the service provision, the obligations that assumes and the limits of responsibility
- Protect of manner reliable all the data of their Users, so as the records of activity and auditwith the means it considers most appropriate for this purpose and during the period of time contemplated according to nature of the data registered.
- Attempt the benefit of the service of conservation of signatures electronic of shape diligently and uninterrupted
- Communicate to their Users with the enough in advance the No availability of the system in case of carry outprocesses of modification, improvement or maintenance that involve a standstill of the service.
- Notify the parties involved as soon as possible whenever any incident is detected in thesystem with impact on the same.
- Ensure that digital signature systems operate in synchrony with reliable time sources, using for this purpose an Authority of Sealing of Time qualified.
- Publish the most recent versions of this document and other definitions of practices of other services of manners previous to the application of the conditions that HE contemplates in them.
- Have a communication channel with Users and third parties for requests, queries, complaints and claims.
- Attend the applications, queries, Complaints and claims of Users and third parties in a term reasonable
- In the event of receiving an application for a package of export-imports HE would manage to level contractual whereHE will elaborate a plan detailed on how to perform the associated process
- Depending on the method of production of the package or package, HE you will apply the measures of securitynecessary. By example: encryption, password, double factor etc.
- The data obtained once the transition period agreed with the client has ended, begins the blocking period corresponding and is deleted to the ending of this according to as indicated in the legislation in vigor

8.1.2 INFORMATION FOR BUSINESS PARTNERS

The partners commercials that they trust in the objects digital archived by TRUSTCLOUD and do use of their services must be performed the following actions

- Verify the validity, suspension or revocation of the certificates used using the information on the revocation status (OCSP or CRL's of the Certification Service Provider that issued the certificate), incorporated inside of one's own file PAdES-LTA.
- Respect the measures of security that indicate TRUSTCLOUD for access to the service of Preservation of electronic signatures and qualified seals

8.1.3 INFORMATION FOR AUDITORS AND REGULATORY AUTHORITIES

TRUSTCLOUD is committed to communicating to the Authority Public competent that information confidential eithercontaining personal data when it has been requested by the same and in the cases provided for legally:

- Notify to the authority of supervision and control accredited (SETSI of the MINETAD) any modificationin the present Statement of Internships of conservation of signatures electronic.

- Notify the competent authority and the parties involved the change in the infrastructure that canaffect the benefit of the service.

Specifically, TRUSTCLOUD is obliged to reveal the identity of the signatories when requested by the governing bodies. judicial in the exercise of the functions assigned to them, and in the rest of the cases provided for in the GDPR / Current data protection legislation [3].

TRUSTCLOUD will inform auditors, authorities Regulatory and prosecutors that they trust in the service of conservationof signatures and electronic stamps, which must:

- Verify the validity, suspension or revocation of the certificates used using the information on the revocation status (OCSP or CRL's of the Certification Service Provider that issued the certificate), incorporated within one's own file PAdES-LTA.

Respect the security measures indicated by TRUSTCLOUD to access the conservation service of signatures and stamps electronic qualified

8.2 RESPONSIBILITY

TRUSTCLOUD as a Trust Service Provider is subject to the liability regime as set out in Article 13 of eIDAS [1] and will therefore assume liability for any damage caused by deliberate either by negligence or any person physics legal in the terms planned in the current legislation.

TRUSTCLOUD will not respond to the damage and damage caused by his improper use of the service of conservation of

signatures and stamps of qualified electronics.

TRUSTCLOUD remains exempted from responsibility by the damages and damage caused in case of force elderly, case fortuitous unpredictable either that, being predictable No HE has could avoid according to the state of the technique.

All cases contemplated by law as Limitations to the liability are excluded. responsibility of the PCSC.

TRUSTCLOUD No will be responsible of the acts or omissions carried out by the Users, being this who will assumeall damages and losses, direct and indirect, that may be caused to any person, property, company, public or private service, specifically due to loss of profits, loss of information and data, or the corresponding damages, as a consequence of the acts, omissions or negligence of the Users as wellas of third parties tied to him, by improper use, being of exclusive risk of Users.

For these purposes, TRUSTCLOUD has taken out civil liability insurance of €3,000,000 (three million euros). euros) to meet the risk of liability for damages that may occur due to of the breach by his part of the obligations that imposes her Regulation eIDAS [1]

8.3 SUBSCRIBER OBLIGATIONS

On his part, he is a subscriber of the Service of Preservation of Signatures and Stamps qualified They must achieve with thefollowing obligations:

- The objects sent must achieve with the requirements established in the rule ETSI 119 511
- Must ensure compliance legal and the accuracy of the objects to preserve.
- You must send the objects in the form precise and complete, such as how HE establishes in theparagraph 7.3 of this DPC.
- You must assume any other caution prescribed in the contract whether either agreement is reached.

9 SECURITY CONTROLS

TRUSTCLOUD has developed and implemented an information security management system consisting of Policies, Norms, Standards, Guides and internal Procedures through which the framework of performance of security in the systems, services and processes of the company, with the purpose of guaranteeing thatin all the areas of the entity HE reached the highest level of security.

9.1 PHYSICAL SECURITY

TRUSTCLOUD guarantees that it complies with the applicable regulations and the main standards and good practices in the subject of physical security, according to HE describes in it this section.

Different security perimeters with barriers have been established at TRUSTCLOUD facilities. security and entry controls appropriate to the activities carried out in each of them. All of thiswith the end of reducing the risk of access not authorized or of damage to the computer resources.

TRUSTCLOUD information systems are located in areas with restricted access that have been adequately protected through appropriate physical access control mechanisms. Furthermore, these systems have been protected against other types of environmental threats such as fires, floods orpower outages.

Bliss protection HE extends to those systems whose securitization physics this delegate in some supplier. ForTherefore, the appropriate clauses have been signed in the contracts and the monitoring mechanisms have been established. necessary by TRUSTCLOUD. The processing of information outside of TRUSTCLOUD systems is duly authorized, at a time that HE guarantees her compliance with the level of security requested.

TRUSTCLOUD has also implemented an asset management policy based on inventory and classification, storage and records of entrance and exit. In the slope technique, HE adopts proceduresthat guarantee that the information contained therein is adequately secured, as well as allowing thereuse of these without those present risks for information.

Some of the measures adopted by TRUSTCLOUD are the following:

• Authentication and Access Control. Building access control
• Access control to data processing centers (Datacenter) based on biometric fingerprint identification and centralized authorization with access records, both in and out.
• Temperature conditions are guaranteed by autonomous cooling equipment located within the Datacenter that maintains its temperature within the established margins
• Redundant power supply, providing two power supply lines to the racks intended to house the equipment.
• The cabling used in the Data Center is category 6.7 and fiber optic.
• Uninterruptible power supply systems. • Fire detection, based on smoke and aspiration detectors.
• Continuous and adequate air conditioning of the CPD areas with n+1 redundancy in each area. • Humidity detectors in the CPD areas and electrical rooms.
• There is an agreement with a specialized service provider for the safekeeping of magnetic media, with an earthquake-proof armored room for this purpose.
• Access of outsiders (visitors) to the CPD
• Exposure to water
• Information recovery

9.2 LOGICAL SECURITY

TRUSTCLOUD uses measures of security logic common to all the systems. The systems specifically used for the provision of the service subject to this CPS have been provided with a second level of security measures.

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

An incident management procedure has been established and defined in order to minimize the impact caused due to security incidents or failures in the operation of the systems, which allows a fast reaction in view of the possible incidents produced, so as the establishment of measures corrective thatavoid its repetition.

HE has established likewise an adequate segregation of functions in the assignment of responsibilities withthe objective of preventing inappropriate use of information systems, establishing, in cases where such segregation is not feasible, other appropriate control mechanisms that allow for its monitoring and control.

Procedures and controls have been established to adequately prevent the introduction of software maliciously, guaranteeing the integrity of the software and of the information of TRUSTCLOUD.

Safeguard measures have been established, including the necessary backups, checking periodically its validity by restoring it, together with the permanent monitoring of the systems, which allows to guarantee the continuity of the systems, services and information of TRUSTCLOUD, and the borrowed services.

The information transmitted by communications networks, public or private, is adequately protected. protected through the mechanisms timely that guarantee his Confidentiality and integrity. They have established the necessary controls to prevent the impersonation of the issuer, 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 relies on in the provision of its services as part intervening in them.

Procedures have been established that regulate TRUSTCLOUD's information encryption strategy, describing the measures organizational and techniques that guarantee the Confidentiality and integrity of the information.

Procedures are also established that regulate in detail the storage, handling, transportation and destruction of sensitive information both on computers, laptops, mobile devices, etc.), such as residually, in medium paper, all it with the purpose of mitigating the risk of access No authorized, loss otheft.

9.2.1 ACCESS TO SYSTEMS

Access by both internal and external personnel to TRUSTCLOUD information systems, as well as for the information they process and store, it is regulated based on the information needs and operation of each user, granting exclusively to those functions and information that HE requires for the correct performance of his activity labor, chord with his function I profile operational.

Those responsible for the processing of information assets will be responsible for defining the levels of access to resources and authorizing any extraordinary access, all in accordance with the guidelines of the owners of the information, either, in its case, of the owners of the process either business.

Without prejudice specifying an elderly detail in his application, neither of the delegation formal functions, HE understandas owners of the process or business Those responsible of the following positions:

- Responsible for Security of the Information (RSI-CISO)
- Responsible Systems (RS)

All the accesses carried out to the information systems of TRUSTCLOUD by the users will carry associated anidentification, authentication and authorization process, establishing the appropriate controls so that such processes are perform of shape safely.

To this end, mechanisms for registration, monitoring of access and use of the systems that allow us to know the effectiveness of the measures installed and detect possible incidents of security.

9.2.2 REFERENCE TO SYSTEM EVENTS

In relation to possible system events, considering the category of services provided, TRUSTCLOUD has designed a system of records and controls that allow the inspection reactive between others ofthe following events about their systems:

- Attempts successful either failure of start or end of session.
- Attempts successful failure of create, modify either delete accounts of the system.
- Attempts successful or failed of create, modify either delete users of the system authorized.
- Attempts are successful failure of creation, modification cancellation of requests inside of the different components of the system.
- Attempts successful failure of signature of files.
- Attempts successful failure of files of certification.
- Successful attempts failure of tired of shipment of communications.
- Changes in the configuration of the system.

9.2.3 RECORDS MANAGEMENT

The integrity and availability of audit records will be maintained at all times, saving the synchronization of time sources with all systems that generate such records, centralizing, whenever technologically possible, the control and monitoring of records by means of some tool of management.

Audit logs generated by the systems that deal with confidential information must be stored as required by law, for the rest of the systems this time will be regulated by the procedures timely.

The systems of information must have enough ability for the storage of the records ofaudit do not degrade the level of service.

Any changes that are strictly necessary to carry out in relation to the generation of audit records must be duly authorized by the security responsible.

The elimination of the records HE shall of carry out by mechanisms that No degrade the Confidentiality of these.

9.2.3.1 PROTECTION OF RECORDS

Access to TRUSTCLOUD's archiving and document custody systems is restricted exclusively to authorized personnel. Thus, an access control, identification and security system has been set upauthentication of such manner that HE finds protected against accesses, modification, erased or Others unauthorized manipulations.

The systems, support and media that contain the documentation and information susceptible to archiving and custody, as well as the applications necessary to process and treat the data in custody are maintained and may be accessed by the period of time established in the present DPC.

9.2.3.2 RECORD RETENTION PERIOD

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

9.2.3.3 REQUIREMENTS FOR TIME SOURCES

The certificates, CRLs, and other entries of bases of data of revocation They must contain information of dateand time.

The systems of TRUSTCLOUD perform the record of the instant of time exact in he that they perform the records,using for this purpose a time stamp issued by a TSA qualified for the case of being part of the processes members of the services of conservation of electronic signatures qualified borrowed by TRUSTCLOUD.

All TRUSTCLOUD systems synchronize their time instant with reliable time sources based onthe protocol NTP (Network Time Protocol), self-calibrating by different media.

9.2.3.4 BACKUP OF RECORDS

They perform copies of security of the files that contain the object of records of retention, that arestored in the cloud.

Are copies of security HE they perform about all the components of the service.

9.3 VULNERABILITY ANALYSIS

Given the growing risk of insertion of malicious code in programs, it will be mandatory to adopt some criteria for collaboration in the protection of the Systems of Information against this type of attacks.

The department of computing will establish all the measures of nature technique and organizational to its scope to avoid the entrance and spread of malicious code in their systems computer scientists.

Between are measures HE find, with character enunciative, but no limitative, the following:

The Systems of Information of TRUSTCLOUD must have installed antivirus, firewall, antispyware and filtered of mail, DLP all they of update automated, always that technologically the systems support controls of these guys. We have Defend corporate, internal SonicWall firewall and Movistar managed firewall for office network connection and the measures of YES of AWS.

- TRUSTCLOUD's antivirus and mail filtering systems must check all messages incoming and outgoing email, as well as all internal messages from your networks communications
- When an email does not meet the security criteria defined in antivirus applications and filters of contents, the mail No will be delivered to his addressee and will be erased automatically. This action will be carried out in accordance with the appropriate legal guarantees and respect for privacy.
- The state of any portable device, regardless of the way in which it has been obtained, shall be checked through the tools of detection of malicious code.

TRUSTCLOUD, or an external auditor with sufficient certification and knowledge, will carry out at least one annual analysis of vulnerabilities.

It is the responsibility of the coordinators of the analysis teams to inform those responsible for the service of TRUSTCLOUD, through the Security Manager, of the results of the analyses carried out of any problem that prevents the realization of audits, the delivery of the documentation resulting.

Security scans involve initiating the tasks required to correct the detected vulnerabilities and the emission of a counter-report.

The vulnerabilities found will be detailed in a resulting document labeled: "Vulnerability Analysis." vulnerabilities about platform TRUSTCLOUD ". Yeah, out found some vulnerability, the equipment ofTRUSTCLOUD will analyze them and categorize and weigh them according to the degree of affectation, proceeding to create a proposal with countermeasures.

Countermeasures will be applied in the shortest possible time, notifying the parties involved if there were harmed entities by the vulnerabilities found.

9.4 PERSONNEL SAFETY

TRUSTCLOUD will determine the human and technical team necessary to provide the services, ensuring the conditions of quality and operation required and guaranteeing the level of service agreed.

TRUSTCLOUD will use all technical and human resources necessary for the execution of the services, with the ability, qualification and experience adequate for the provision of these.

TRUSTCLOUD reserves the right to make any technical and human changes it deems appropriate to maintain the quality of the service provided, without prejudice to which, we will try to ensure that changes in the provision of the Service be minors possible.

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

Likewise, it will be to account of TRUSTCLOUD the training that will result necessary for that the staff of the Userthat use the service contracted. The duration and the number of attendants will be agreed with the USER.

10 CONTINUITY AND CONTINGENCY PLAN

TRUSTCLOUD has established business continuity and availability management processes to minimize the impact on the functions and processes critics in case of disaster, of shape that HE reduces the time of unavailability to levelspreviously established. These processes have the appropriate combination of character controls, organizational, technological and procedural both Preventive such as recovery.

These processes HE supports in a Plan of Continuity and availability of Business that is tired of shape periodically, keeping up updated in all moments. For it HE evaluates the risk in view of threats and the impact associatedcaused by the lack of continuity of the information assets that support or are involved inthe processes of business of TRUSTCLOUD.

10.1 BUSINESS CONTINUITY AND AVAILABILITY PLAN

The Continuity of Business is the ability tactic and strategic that has TRUSTCLOUD for planning and replyto incidents and business interruptions in order to continue critical business operations withinof a level of acceptable service and acceptable by TRUSTCLOUD.

The scope for the Plan of Continuity and Availability of business is the same that HE has definite for the implantation of the System Information Security Management (IS). It includes the services and processes of TRUSTCLOUD, the headquarters that HE places in Madrid, so as the systems of information and assets in the support information and data, software, equipment, communications, items auxiliaries, supports of information, staff and local.

In a disaster situation, the protection of people has the highest priority. This aspect is not contemplated in this plan, since it is only oriented from the technological point of view. No activity will be considered until the security and the welfare of people do not are insured.

The personnel forming the recovery team will be familiar with the responsibilities and content contemplated in this Plan.

In the event of a disaster situation TRUSTCLOUD will contact the corresponding provider of material supply. If replenishment time cannot be assured, purchases of spare parts may be necessary. equipment and his storage in a location alternative to the main facilities.

At the time that the Procedure of Recovery was established, his maintenance was mandatory. The processof recovery is viable only if this document is updated and complete.

TRUSTCLOUD has provided a financial plan that allows it to have sufficient financial stability and resources to operate off in accordance with the present DPC and give an answer to situations of contingency.

10.2 CONTINGENCY PLAN

TRUSTCLOUD has established a contingency response plan, which determines the strategy and treatment to give to the same.

The services and processes of the IT department are most critical to the business. In case of serious contingencies, the service will be suspended while we are last, notifying the elderlyas soon as possible to the users of the system.

The contingencies contemplated that could suppose some risks for the quality of the service are:

- Time of answer so high that supposed a clear rape of the policy of quality of service.
- Loss of synchronism with the sources of primary and secondary.

The contingencies that they can suppose a risk for the benefit of the service are:

- Errors in the systems of exploitation partners to the benefit of the service.
- Errors in the systems of communication partners to the benefit of the service.
- Errors that affect the benefit of the service are detected in the software of some of the services.

Besides, HE defines the procedures for the teams to reconstitute the operations of TRUSTCLOUD usingdata of backing and the copies of back of the keys.

11 COMPLIANCE AUDITS

11.1 AUDITOR PROFILE

The auditor's external equipment of auditors external will be selected at the moment of the planning of eachaudit.

Any company or person hired to perform a security audit on TRUSTCLOUD or any otherof its services in concrete should comply with the following requirements:

- Adequate and accredited training and experience in security and processes of audit of systemsof information.
- Independence to level organizational of the authority of TRUSTCLOUD, for the case of auditsexternal.

He auditor external either equipment of auditors external besides No They must have no relationship, current either planned, financial, legal, or any other kind that may result in a conflict of interest with TRUSTCLOUD. In order to comply with current regulations regarding data processing, and if the process of audit would imply, he accesses the data of character staff, the auditor will have the consideration of in chargeof Treatment, by virtue of it provided for in article 28th of GDPR [3].

11.2 AUDIT CRITERIA

Without damage of seeing expanded by documents of the individuals offered by TRUSTCLOUD, in thisin this section we will define the set of minimum checks on the suitability of the services offered. With regard to it definite in this DPC. The aspects covered by an audit will include, but no will be limited to:

- Policy of security.
- Security physics of the facilities of the audited service.
- Security logic of the systems and services of TRUSTCLOUD
- Assessment of technological components of the service.
- Administration of the services as well as security in the same.
- The present DPC and policies of services current.
- Compliance of the demands legally applicable

11.3 FREQUENCY

Compliance and compliance audits are carried out at least biannually, unless otherwise specified. produce relevant or essential changes in the TRUSTCLOUD systems and services, where audits of extraordinary character will be executed.

11.4 PLAN OF ACTION

The identification of deficiencies in the audit will immediately lead to the adoption of corrective measures. The authorities competent in the subject according to it definite by the legislation current in collaboration with the auditor will be the responsible of the determination of are

11.5 COMMUNICATION OF RESULTS

The external auditor or auditors will communicate the results of the audit to the Security Officer.of TRUSTCLOUD, as well as those responsible for the different areas in which non-conformities are detected, as wellas in his case to the competent authority according to the certain in current legislation.

12 PRIVACY POLICY

There is his duty generic of Confidentiality regard to the information that the employees of TRUSTCLOUD know by reason of his position of job. The information considered as confidential facilitated to TRUSTCLOUD will not be disclosed to third parties under any circumstances unless it is covered by the following assumptions: request of collaboration with the competent institutions

The Parties shall not be subject to the obligation of confidentiality regulated in this Clause when the Confidential information must be disclosed by legal imperative or to comply with an order of judicial or administrative nature, provided that they notify such circumstance to the Party to whom the dispute belongs information confidential in question.

In this sense, HE will consider information of the guy "confidential" (without damage of that other guy of information can be so also):

- Plans for continuity of business and of emergencies.
- Information relating to the operational operations and maintenance of the service.
- All information relating to the operations that are carried out to cape TRUSTCLOUD.
- All information is related to the parameters of security, control and procedures of audit.
- All the information about character staff provided to TRUSTCLOUD during the process of recording certificate subscribers, except as specified in the Certification Policy applicable and the contract of certification.
- The information of business supplied by their Suppliers and Other people with the that TRUSTCLOUD hashe duty of keep secret legally established or conventionally.
- Transaction records, including full records and audit records of transactions.
- All the information is classified as "CONFIDENTIAL" or "STRICTLY CONFIDENTIAL"

Without embargo, will be considered as public documents No Confidential among others the following materials:

- Statement of Internships for Conservation of Signatures and Stamps Electronics Qualified of TRUSTCLOUD
- All that information that sea considered as “Public”

13 PERSONAL DATA PROTECTION

TRUSTCLOUD will treat those data of the personal nature necessary for the development of its activity obtaining the guarantee by the DPO of the correct obtaining of the express consent of the signatories. This treatment HE will be carried out in accordance with the GDPR [3].

The personal data provided by the Users will be processed by TRUSTCLOUD as Data Processing Manager responsibility of third parties under the terms and conditions provided in, he articles 28 of the GDPR [3]. In this sense, TRUSTCLOUD is committed to achieve the following conditions:

- The treatment of data that TRUSTCLOUD will perform HE will limit to the performances that result necessaryto lend to the RESPONSIBLE OF THE Treatment of the Services hired.
- In concrete, TRUSTCLOUD i s compromises to carry out the treatment of the Data Personal adjusting to the instructions that, at any time, the FILE MANAGER gives you, as well as to the will in the regulations that you result applicable in subject of protection of data personal.
- In addition, TRUSTCLOUD is committed to carry out no other treatment about Data Personal, nor to apply either use the data with a purpose different to the benefit of the Service.
- TRUSTCLOUD declares that it complies with the security measures defined in these DPD, being are the that result necessary for guarantee the security of the data of character staff treatiesin the service provided, in order to guarantee confidentiality and integrity based on the nature of the data, of accordance with it established in the GDPR [3].

For the purposes of the provisions of this section, TRUSTCLOUD must inform its employees of the obligation of secret and confidentiality, So as the consequences of his breach, regard of thetreatment of data of personal character.

TRUSTCLOUD undertakes to keep under its control and custody the personal data provided by the PERSON RESPONSIBLE FOR FILE that is accessed in connection with the provision of the Service and not to disclose them, transfer them, either of any another way communicate them, neither even for your conservation to other people.

Once the provision of the service subject to the Contract has been completed, TRUSTCLOUD undertakes to destroy or return that information that contain data of character staff that is been transmitted by theRESPONSIBLE FOR THE FILE to TRUSTCLOUD on the occasion of the benefit of the Service

In the event that the affected parties, whose data are in files owned by the CONTROLLER OF THE DATA FILE, exercised their rights in view of TRUSTCLOUD, this shall give transfer of the shape application immediateto the FILE MANAGER and, at the latest, within 3 working days from its reception, so that he RESPONSIBLE FOR THE FILE duly resolve said request.

This CPD is considered a reference document for the implementation of measures technical and organizational security, considering TrustCloud's proactive responsibility to ensure thecompliance of the GDPR [3].

TRUSTCLOUD guarantees compliance with the obligations that you correspond in virtue of the regulations that youresult of application in matter of protection of data personal.

In case of rape of the security either loss of the integrity that suppose an impact significant in the serviceborrowed either in the data of character staff treaties, TRUSTCLOUD it will notify in the term maximum of 24 hoursfrom that HE had knowledge of such incident to the body of supervision and in case necessary to the AgencySpanish of Protection of data

in compliance from the 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 in accordance with the provisions of the present DPC. This model will be accompanied by a service level agreement to measure its implementation, as well as by a service of support, which will generally incorporate:
In the event of receiving an application for a package of export- import HE would manage to level contractual. The packages of export-imports will elaborate according to the indicated in the ETSI 119 512

TRUSTCLOUD provides a service of conservation with storage. The data that must be storedis preserved by TRUSTCLOUD, while the Evidence and preserved data are delivered by TRUSTCLOUD to the client, prior application

When TRUSTCLOUD is unable to collect and verify all validation data, a notification of the failure would be sent. failed and HE would file as a record unqualified.

The aim of preservation taken by TRUSTCLOUD is the Preservation of signatures digital (PDS)

TRUSTCLOUD uses as record of evidence Excel, inside of which HE specifies the cycles of evidence according to the case of use partners to the service of conservation provided by TRUSTCLOUD
The evidence HE they perform inside of TrustCloud, stored in base of data and in the tool of logs, theevidence is preserved in the tool of storage.
The evidence HE validates using the Digital Signature Service (DSS). He increases the evidence of preservation HEgets with resealing.
TRUSTCLOUD account with a supplier of sealed of time and a supplier of certificates.
TRUSTCLOUD in case of that the sender of the preservation perform a paper in the process of preservation,HE will negotiate case by case level contractual

THE CRITERIA TO BE USED FOR HANDLING REQUESTS

- He level of medium functional that HE goes to provide and availability of the same
- He level of medium technical that HE goes to provide and availability of the same
- The process of scaling that is leaving to continue to the hour of notify the occurrence of an incidence
- He system management of requests for the resolution of incidents that HE goes to use
- The mechanisms of communication that HE is going to use to provide the medium
- The languages available in those who HE goes to provide the medium
- He Agreement of Level of Service (ANS) associated to the service will contain:
  - ANS relative to time of attention and resolution to the hour of solving the incidents
  - ANS relative to the general quality with which HE lends the services
  - ANS relative to the availability of the services
  - ANS relative to the time of provisioning of services new and/or scalable
  - ANS relative to the performance of volumes of information

- Chart of Command for the management, control and government of the service.
- Information statisticians, operatives and of compliance of ANS.

TRUSTCLOUD will, to the extent possible, try 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 stated established in these terms and conditions. TRUSTCLOUD providing the services described in these CPS guarantees that it will not operate in a manner that produces some risk of discrimination.

14.2 SUBSCRIBERS' OBLIGATIONS

The rates and conditions economic of the different services HE find available in the document of"General Conditions of Hiring of TRUSTCLOUD ".
No However, TRUSTCLOUD may establish frames contractual with Users punctual that particularizeThese conditions for the stage of collaboration established between both parties.
The rates established by TRUSTCLOUD for payment for the provision of the service will be maintained based on thefollowing concepts:

- Share monthly by the utilization of the Service
- Cost by operation of Certification managed by the Platform: the amount of each application of operation to the Platform.
- Cost by operation of communication managed by the Platform.

In the moment of the hiring, so as previously in any other moment that HE precise, Yeah, HErequests to TRUSTCLOUD this data, can access to this information economic updated.

14.3 LIMITATIONS ON THE USE OF THE SERVICE

The Services borrowed by TRUSTCLOUD do not have limit territorial.

14.4 PROVISIONS IN CASE OF TERMINATION OF SERVICE

TRUSTCLOUD is committed to adopting all the measures necessary to minimize the impact that could suffer froma User, or third parties involved in the service of these DPC, such as consequence of the stoppage or termination of the service. In particular, periodic and continuous maintenance will be carried out on the information required to verify the effective benefit of the services provided by TRUSTCLOUD.

In concrete TRUSTCLOUD has a procedure of plan of termination of the service updated, in he thatHE collects he process that will carry to cape TRUSTCLOUD before of the termination of the service, in concrete in how muchto portability and cessation of activity

TRUSTCLOUD has agreements that will allow the costs associated with these minimum requirements to be covered in the event that it did not have sufficient funds or there were other reasons that prevented it from covering such costs

by itself, having into account the current regulations on the subject of bankruptcy.

14.4.1 PORTABILITY

TRUSTCLOUD will carry out the transmission of the documentation that evidences all the registration and other material in its power that may be necessary for the person considered, in order to demonstrate the correct operation of the service for a reasonable period of time as required by applicable law.

The processes of destruction of material or specific transfers of each service, if these existed, would be defined in their definitions of specific policies.

14.4.2 CESSATION OF ACTIVITY

In the event of the cessation of his activity as Lender of Services of Certification, TRUSTCLOUD will perform,in advance of three months, the following actions:

- Inform all the subscribers of their services of the cessation of the activity.
- Inform all third parties with whom you have signed a contract regarding this service.
- Communicate to the Ministry competent in subject of Society of the Information he cessation his activity anddestiny that goes to give to the signatures and stamps electronic preserved, So as any other circumstance relevant related to the cessation of activity.

14.5 RESOLUTION

Without damage of the causes described in the regulations Spanish, TRUSTCLOUD will consider as cause of resolutionearly of the provision of the services, the following:

- Failure by the parties to comply with any obligation provided for in these Conditions General of Use, required the Part non-compliant, this No proceeds to the correction of the breachin a deadline 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 that are related in the conditions of hiring, HE will understand as reason enough for that TRUSTCLOUD by resolved from manner unilateral the contract of benefit of service, without damage ofclaim the obligations earrings of pass payment Yeah, the three were.

TRUSTCLOUD HE booking the faculty of resolution of the contract in case of that existed circumstances supervening, resulting from a change in market conditions, due to defects or deficiencies in the data or information received for the elaboration of the Proposal Economic, either any other circumstance alien to his will, including the production of a mismatch between the agreed prices and the cost of execution of the Service, derivative of circumstances of the market will result a deficit economic by the execution of the Service and in

generalfor any reason beyond the control of TRUSTCLOUD, which causes the economic balance of the same.

14.6 SUBCONTRACTING

TRUSTCLOUD may subcontract the services that estimate necessary for the provisioning and exploitation of theService according to the needs that arise and will formalize this relationship through a written agreement that will determine the conditions of the service provided through this outsourcing.

14.7 NULLITY

Yeah, any of the Conditions General of Use was declared total either partially null or ineffective, such nullity either inefficiency will affect only to bliss provision either part of the same that result ineffective either null, and the rest ofthe clauses will continue in force, having such condition or the part thereof that is affected by not putting.

14.8 NOTIFICATIONS

Any notice, demand, request or other communication required under the practices described in This Certification Practices Statement shall be made through a signed document or electronic message digitally or in writing by certified mail addressed to any of the addresses contained in the spot relative to Data of contact. Electronic communications HE will do effective a time that the receive headdressee to the that they go directed
For these purposes, the parties will expressly designate the addresses for the practice of communications. In the event of modification of the home, the parts HE will force to notify to the other the modification in the shape established in the first paragraph.

14.9 APPROVAL AND REVIEW OF TRUST SERVICE PRACTICES

14.9.1 APPROVAL AND IMPLEMENTATION

The present DPC will be approved by the Director of TRUSTCLOUD, the maximum level and authority of responsibility within TRUSTCLOUD, which will also be endowed with the responsibility and capacity to prepare and manage the same. HE has established equipment of management responsible for the implantation of the practices of security and organizational requirements to ensure confidentiality, integrity and everything established in these CPS. TRUSTCLOUD has defined a team made up of those responsible for the different areas involved in each one of the steps of the service of conservation of signatures and electronic stamps.

14.9.2 MODIFICATIONS

TRUSTCLOUD is booking the right to modify this document always and when:

- The modification of this is justified from the spot of view technical and legal.

• HE notifies the users of all the derivatives of our modifications, and theseaccept the same previous use of the service.

• HE offers a mechanism of control of changes and of editions.

In this regard, a procedure has been established for this purpose in which the mechanisms to be followed are regulated. case of need to modify the CPS. Once it has been decided that it is appropriate to carry out a review, the person responsible for preparing the document will make the appropriate changes, identifying them in the new edition through shading the text modified. This method can coexist and be replaced bya change control list listing the changes introduced in each of the edition's version of the document.

Yeah, the modifications carried out to the document produce a disturbance that affects the service borrowed to the users will be considered a "major release". Of other mode will be considered a "minor release".

Users will be informed in the event of a "major" event. release" modifying the relationship contractual between TRUSTCLOUD and these. In this way, Users must adhere to the new conditions of prior use provision of new services or open a process of low in the service

14.9.3 VERSIONS

These DPCs may change over time. When a "major" change occurs release" will mean increasing the document versions by one. However, when a "minor" change occurs release" will modify the number of your version.

14.9.4 PUBLICATION

TRUSTCLOUD is obliged to publish information regarding its practices, its certificates and the status of said certificates. All the history of this documentation must be kept and accessible. low demand through e-mail of contact of the web (spot 6) to the less by a period of 15 years.

All publications HE will carry to camp in the place web of TRUSTCLOUD or in sites web lower the control of TRUSTCLOUD and with a direct or indirect link to the TRUSTCLOUD company name and/or brand. It will also be published through the shipment of an electronic mail certificate and on the page of the Authority competent. The publication HEwill be carried out at the time of its creation

14.9.5 APPLICABLE LEGISLATION AND JURISDICTION

The presents conditions general of hiring HE will govern by the regulations Spanish.

The parts, with express resignation to any jurisdiction that could correspond to them, submit to the Jurisdiction and Competence of the Courts and Courts of Madrid for any question related to the interpretation, compliance either execution of the present statement

15 CONSERVATION PROFILE

TRUSTCLOUD only provides the preservation service with storage. Once the storage period has ended,transition agreed with the customer, HE starts her period of blockade of the data obtained, which are deleted at the end of this as indicated in the legislation in force

The profile of preservation HE identifies to through the next OID: 1.3.6.1.4.1.5 2582.1.1.1.
The operations supported by the protocol of preservation are the following:

Call 1) Send. Send the information. Described in the spot 7.2 CHARACTERISTICS MAIN OF THESERVICES FROM TRUSTCLOUD

Call 2) recover the file. Method of recovery of files to through of the APICall 3) Delete P0. Method of erased to through

of the API.

He period of validity from the profile of preservation HE will start a time finished on process described in he points 7.3 SERVICE OF CONSERVATION OF SIGNATURES AND STAMPS ELECTRONICS QUALIFIED

The model of storage with preservation that lend TRUSTCLOUD i s a model of preservation withstorage.

Regarding the retention periods for blocked data, TRUSTCLOUD refers to the legal deadlines:

- In compliance with article 9.3.a) of Law 6/2020 of November 11, 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, will be 15 years from the expiration of the certificate or the end of the service provided". Therefore, TrustCloud will retain the information relating to the signature and seal preservation service for 15 years from the end of the service provided.

The goals of preservation are a combination of Preservation of signatures digital and increase of the evidence of preservation to through resealing.

16 EVIDENCE PRESERVATION POLICY

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

They use Algorithms SHA-256 for hashes of documents and SHA-512 for stamps of time.

The evidence of conservation HE validates the through of the service Digital Signature Service (DSS). The evidence PDF are PAdES. This same validation could be done by a third party. The increase in preservation tests is get with resealing.

We use PAdES when downloading the evidence, they do not have information about our service, only the time stamp.

TRUSTCLOUD has a supplier skilled in terms of time and a supplier skilled in certificates.

TRUSTCLOUD, when no one can collect and verify all the data of validation, will send a notification of the failure andwill be filed as a non-record skilled.

17 SUBSCRIBER AGREEMENT

For the rights of access, HE applies the following policy:

- Reading: users authorized.
- Modification: administrators, and only low request by cause justified
- Erased: administrators. and only low request by cause justified

All the evidence generated during the process of custody remains registered in a certificate of evidence generated by TRUSTCLOUD. This evidence will be delivered at the end of the service or delivered to the subscriber of previous application.