STATEMENT OF PRACTICES AND POLICIES IDENTITY VERIFICATION SERVICE (DPyP)

TrustCloud

TYPE OF DOCUMENT		**Secret Documentation**
	x	**Public Documentation**
		Internal Documentation
		Confidential documentation

TITLE			STATEMENT OF PRACTICES AND POLICIES IDENTITY VERIFICATION SERVICE
ENTITY			TRUSTCLOUD SOLUTIONS
FORMAT			Electronic - PDF
PAGES			
VERSION	**DATE DA TE OF ISSUANCE**	**OID**	**AUTHOR**
1.1	07/11/2023	1.3.6.1.4.1.52582.1.1.1	TRUSTCLOUD SOLUTIONS
Reviewed by: Alberto Angón (CISO-RSI) Signed by ALBERTO ANGON on 2023-12-05 14:24:19 CET			Date:
Approved Signed by Saioa Echebarria on 2023-12-05 14:35:58 CET By the Management Committee TRUSTCLOUD SOLUTIONS S.L.			Date:

CHANGE HISTORY

Version	Date	Description of the action	Pages
1.0	10/04/2023	Initial edition	
1.1	08/11/2023	Updating references to the regulatory framework (sections 3 and 4).	

INDEX

1. INTRODUCTION

This document is a Statement of Identity Verification Service Practices and Policies, by means of which TRUSTCLOUD SOLUTIONS, as a non-qualified trust service provider, exposes and describes the way in which it provides the Identity Verification Service 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 applicants, subscribers and in general users of Identity Verification services, in accordance with the provisions of Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting minimum technical specifications and procedures for security levels of electronic identification means 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 Identity Verification Service, TRUSTCLOUD SOLUTIONS follows the indications of the standards of the European Telecommunications Standards Institute -ETSI- guided by the technical specifications of the standards, EN 319 401 (general requirements for trust service providers), EN 119 461 (Policy and security requirements for trust service components accreditation of the identity of the subjects of trust services) ISO 30107 Biometrics. To this end, TRUSTCLOUD SOLUTIONS has carried out the design and development of a technological infrastructure that, in an integrated manner, provides its Users with a tool through which they can check the correspondence between their identification data and their biometric parameters with those contained in their authentication document, as well as corroborate the authenticity, validity and integrity of the latter.

2. DOCUMENT IDENTIFICATION

In order to individually identify each type of service performed by TRUSTCLOUD, in accordance with this Statement of Identity Verification Service Practices and Policies, each type is assigned an Object Identifier (OID).

This Statement of Practice describes the services related to identity verification provided through the TRUSTCLOUD owned platform, including among other aspects of the description and functionality of the services provided the following:

- The characteristics of each service.
- Treatment and operation flows.
- Identification of all participants
- The obligations assumed in the provision of services.
- The technical and organizational security measures implemented.
- The general conditions of use and contracting of services.

3. ACRONYMS AND DEFINITIONS

Acronyms

ACRONYM	DEFINITION
LSC	Law 6/2020, of November 11, 2020, regulating certain aspects of the services provided by reliable electronics
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.
RGPD	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 July 11, 2002, on information society services and electronic commerce.
PCSC	Certification Service Providers
TSA	Time Stamp Authority - Time Stamp Authority
CPD	Data Processing Center
PKI	Public Key Infrastructure - Infraestructura de Clave Pública - Public Key Infrastructure
PBC&FT	Prevention of Money Laundering (AML) and the Financing of Terrorism (FT)
WF	Work Flow - Workflows of each process
CRL	Certificate Revocation List
OID	Object Identifier - 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
DPyP	**Statement of Identity Verification Service Practices and Policies**: TRUSTCLOUD's 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 Act.
TRUSTED SERVICE PROVIDER	Natural or legal person that provides one or more trust services, in accordance with the provisions of the eIDAS.
QUALIFIED PROVIDER OF TRUSTWORTHY SERVICES	Trust service provider that provides one or more qualified trust services and has been granted qualification by the supervisory body.
USER	Natural or legal person using identity verification services.
DOCUMENTATION	Set of digital evidences received by TRUSTCLOUD from the User, which comply with the requirements set forth in these T&Cs

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 November 11, 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 July 11, 2002, on information society services and electronic commerce.
5) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, and amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ("DPBAC").
6) ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
7) [ETSI EN 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects.
8) ISO/IEC 30107-1 Biometric
9) ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection - Information security management systems
10) ISO/IEC 27002;2022 Information security, cybersecurity, and privacy protection - Information security controls

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 regulations.
2) The Identity Verification Service Policy in this Statement of Practice and Policy.
3) The organizational requirements defined in point 8.1.1.
4) The obligation to provide the required information, when necessary, to its business partners, auditors and regulatory authorities, as specified in points 8.1.2 and 8.1.3 of this document, including organizational requirements.
5) That TRUSTCLOUD has implemented controls that comply with the requirements specified in the ETSI TS 119 461 standard, guaranteed by the implementation of an ISMS based on the ISO/IEC 27001 standard.
6) That TRUSTCLOUD takes into account the necessary legal requirements.

6. IDENTIFICATION AND CONTACT INFORMATION

- Company Name: TRUSTCLOUD S.L.
- Trade Name: TRUSTCLOUD
- VAT NUMBER: B87142618
- Registered Office: Paseo Club Deportivo 1, 28223 Pozuelo de Alarcón, Madrid
- Customer Service Center (SAC): +34 913 518 558
- E-mail: soporte@trustcloud.tech
- Web: https://www.trustcloud.tech/
- Other contact information: +34 913 518 558

7. DESCRIPTION OF THE SERVICE

Through the "VideoID" solution, TRUSTCLOUD, provides its customers with a video-identification system that allows authenticating the user by checking the correspondence between their identification data and their biometric parameters - facial features - with those contained in their reliable document (depending on the country, but generally ID card format, with photograph, and MRZ. Residence permits that also comply with the format, and passports), as well as to corroborate the authenticity, validity and integrity of the latter.

Throughout the process, a series of electronic evidences are generated and recorded, which can be used as evidence in a later judicial process to prove the content of the video-identification carried out.

All of this evidence is collected in a document, called a "certificate of completion", which is issued under TRUSTCLOUD's qualified electronic signature at the moment any of the termination events of the video-identification process occurs. To wit:

I. The correct identification of the user.

II. The lack of correspondence between the data provided by the user and the data contained in the reliable document or the existence of signs of falsity or manipulation in the aforementioned document.

III. The impossibility of completing the identification process due to technical causes that prevent or make it difficult to verify the correspondence between the holder of the document and the customer being identified.

Likewise, once the video-identification has been completed, TRUSTCLOUD's qualified electronic signature and a SHA-256 algorithm are applied to the electronic document containing the recording, guaranteeing that the recording has been issued by TRUSTCLOUD and that it has remained intact and unalterable.

One of the main characteristics of the service is its versatility and the possibility of integrating it with the obligated client's contracting platforms and adapting it to its business model and risk criteria. However, in general terms, the video-identification process is structured in the following steps:

A. User access to video-identification platform

Due to the aforementioned features, the end user can access the video-identification platform:

1. In an integrated way with the digital platform of the obligated client: embedding in this process - generally, once the end user has provided his basic identification data- a button with the option "Access to video-identification" or of analogous meaning in the web or mobile application.
2. Independently from the digital platform of the obligated client: sending the user an e-mail or SMS informing him/her of the existence of a video-identification process pending completion and providing a link to it.

In both cases, the effective access to the platform can be linked to the previous validation of the user through one of the identification methods available to TRUSTCLOUD, providing a higher level of security. However, we do not consider that this point is essential for the legal validity of the process, since the identification required for the purposes of the PBC&FT regulations is the one that takes place during the development of the video-identification and not the one that occurs prior to it.

In this regard, we draw attention to the fact that, according to the SEPBLAC Resolution of May 11, 2017, it is understood that the use of pre-recorded files by the client or other persons outside the obliged subject will not be admissible. The Solution as it is proposed does not correspond to any of these situations, so it would also comply with this requirement.

In any case, it should be noted that simultaneously with the access to the video-identification platform, a connection is established between the user's device and the destination server through the TLS 1.2 protocol, which allows an encrypted and secure communication according to the highest standards currently existing in the market.

B. Development of the video-identification process. user authentication and document validity verification.

B.1 Assisted identification process

The assisted identification process is characterized by the fact that, once the user has accessed the video-identification platform, a video-agent will be in charge of guiding him/her through the whole process. The basic lines of the flowchart are as follows:

1. The user must state his/her name, surname(s) and identification document number in order to check that they match those entered in the client's platform -or those provided by the client in the event that both platforms are not integrated- and those shown in the identification document that will later be shown to the camera.

2. The video agent remotely takes control of the camera of the device used - with prior consent.

The user is asked to show the front and back of the identification document, moving it slightly so that the different physical security elements incorporated in it (CLI, kinegram, OVI ink, among others) can be engraved.

3. The video agent takes pictures of the front and back of the ID card and the user's face and returns control of the camera to the user.
4. The video agent checks that the snapshots meet the necessary quality and sharpness conditions and, if necessary, sends them to the validation and matching system.
5. The video agent informs the user of the conclusion of the video-identification process and refers the user to the platform of the obligated client.
6. The obligated client, through its digital platform or by the means it deems most appropriate, informs the user of the result of the video-identification and:

I. If correct, of the next steps to be taken to complete the requested contracting.

II. In case of failure, of the alternative methods of formal identification made available by the obligated customer, such as the repetition of the video-identification process in case it has been terminated for technical reasons.

The process can only be carried out from a device and the communication is developed, in any case live, in digital format, continuously and without interruption, proceeding to its immediate recording, unless there are technical or physical incidents that prevent it from having the necessary level of quality. In these circumstances, an attempt will be made to remedy these deficiencies and, if it is not possible or feasible within a reasonable time, the user will be informed of the impossibility of completing the video-identification process, requesting, if it is a temporary incident, to try again later or, otherwise, to opt for any of the alternative methods of formal identification.

B.2 Unassisted identification process

The unassisted identification process is characterized by the fact that the customer only interacts with the video identification platform. There is, therefore, no video agent (physical person) in charge of guiding the customer during the video identification process, but this task is carried out automatically by the platform itself. The basic lines of the flowchart are as follows:

1. The platform asks the user to show the front and back of the identification document and to place it in a specific box to take photographs of both sides.
2. Once the photographs of the identification document have been taken, the platform asks the user to place his or her face in a certain space, perform certain movements as "proof of life" and then takes a photograph of his or her face.
3. After the photographs, the process - from the client's perspective - ends.
4. The platform automatically checks that:
    a. The information contained in the identification document matches the information provided by the customer on the obligated customer's platform.
    b. There is no evidence of forgery on the identification document.
    c. There is a correspondence between the facial features of the client being identified and the photograph contained in the identification document that has been displayed and photographed.

5. In cases of positive identification, an agent reviews the recording and verifies that the following have been met

all requirements.

For both processes (assisted and unassisted), the Solution has implemented the following measures:

- √ Recording is immediate and can be configured to start automatically in all sessions or be manually initiated by the agent.
- √ The communication is developed in digital format and without alteration.
- √ The protection of user data and the overall security of your cloud platform is ensured.
- √ All communications, including signaling and audiovisual media, are secured through an encrypted tunnel.
- √ The software installed by the client is digitally signed to prevent modification or code injection attacks.

C. User authentication and document validity check

C.1 Assisted identification process

Once the video-identification process is completed, the video-agent, with the help of the automatic validation and matching system, verifies that none of the impeditive circumstances are present. Namely:

I. **Indications of falsification or manipulation of the identification document;**

II. **Indications of mismatch between the document holder and the customer being identified;**

III. **Poor communication conditions that impede or hinder the verification tasks to be performed.**

The result of the process is positive as long as none of the above circumstances are present and, consequently, the correspondence between the user and the valid identification document exhibited by him/her is accredited.

C.2 Unassisted identification process

On the other hand, as detailed in point B.2, in the unassisted identification process, the platform itself automatically verifies the authenticity of the document and the correspondence between the holder and the customer being video-identified. Additionally, an agent reviews the recording and verifies that all requirements have been met.

D. Communication of the result of the process and issuance of the termination file.

Once the video-identification process has been analyzed, TRUSTCLOUD communicates the result to the customer, detailing, if applicable, the reasons for the denial.

In addition, if requested, it makes available to the obligated customer the "certificate of completion" which - if the customer requests it, it makes available to the obligated customer the "certificate of completion" that as detailed in section 7 - is issued automatically once one of the milestones has been reached.

that lead to the termination of the process.

E. Requirements to be met during the development of the video-identification process.

1. Be managed by specifically trained personnel

In order to comply with this specification, all TRUSTCLOUD personnel directly or indirectly related to the provision of the video-identification service must have received the appropriate training on PBC&FT and electronic identification. Likewise, the video agents will be trained in the use and use of the tool, as well as in the flow charts and the response to possible incidents that may occur.

2. Record the video-identification process and record its date and time.

The developed solution proceeds to record each and every one of the video-identification processes, leaving a record of the date and time at which it takes place and of its beginning and end. Likewise, once the process has been completed, a single summary of the recording is calculated and recorded in the "completion file" together with the dates and times mentioned above in order to be able to subsequently prove its completion.

It should be noted that:

I. Each of the video-identification processes has its own unique and independent recording and its associated hash (identification number) because, otherwise (i.e., if several video-identification processes are included in the same file), the possible alteration or deterioration of one of the processes would affect all the others with which it shares a file.

II. The video-identification process is recorded in its entirety, which allows its sequential playback without time jumps and allows to credit its content, as well as the date and time in which it has been recorded.

3. Ensuring conversation and customer privacy, transmission security, and recording authenticity and integrity

TRUSTCLOUD has implemented technical and physical measures to ensure the privacy of the conversation held with the user, as well as the customer and the video-identification process itself according to the state of the art at the date of issuance of this report. In addition, these measures guarantee the security of the transmission.

In terms of technical measures, communication with users is based on the TLS 1.2 protocol, which establishes an encrypted connection with the destination server. This protocol meets the highest market standards, replacing the old SSL protocol. This provides a secure communication that prevents surreptitious interception of its content, since it travels encrypted and can only be deduced by using the keys previously exchanged between the participants. This key exchange mechanism is executed through the ECDHE_RSA system, which currently guarantees "perfect forward secrecy", with a trusted service provider - other than TRUSTCLOUD - issuing a certificate attesting to the authenticity of the platform on which the recording takes place and the identity of its owner. Finally, it should be noted that these solutions make use of encryption through algorithms such as

AES_256_GCM and the authentication code used is HMAC-SHA2.

With respect to physical measures for assisted identification procedures, the video-agents' stations are separated by screens and during the video-identification, headphones are used in order to ensure the necessary privacy and prevent the video-identification from being seen and heard by a worker other than the person in charge. Likewise, video agents must comply with the "Don't Stop. Don't Look. Don't Talk (NOPMH)" protocol when they get up from their workstation and pass behind the conversation that another video agent is carrying out during that moment.

Regarding the authenticity of the recording, the fact that at the very moment of its completion the recording is signed by a qualified electronic signature of TRUSTCLOUD provides solid evidence to ensure that the recording has been made and issued by TRUSTCLOUD and not by any other third party.

Finally, with regard to the integrity of the recording, the TRUSTCLOUD solution has a mechanism that applies the SHA-256 algorithm to the electronic document containing the recording, which makes it possible to obtain for each electronic document a single fixed-length value (known as a unique summary or hash). The hash is kept in custody and is reflected in each of the certificates of completion issued.

The solvency of the system used is based on the following premises:

1. Irreplicability of the result: If the same algorithm is applied to two identical documents, the same hash will always be obtained. However, if these documents differ - even by a single comma - the summary will be different.
2. Unidirectionality of the function: This function makes it possible to obtain from an electronic document its unique summary, but the inverse result is not technically possible, i.e. applying the algorithm to the hash does not extract the original document. Thus, its use makes it possible to guarantee the integrity of the electronic document without creating a series of copies that could compromise its confidentiality.
3. International recognition: The SHA-2 algorithm used is a FIPS standard designed by the NSA27.

In this way, the mechanism implemented by TRUSTCLOUD offers guarantees that the electronic document containing the recording and, therefore, the recording itself, has remained intact and unalterable, since, if one of the parties were to report that the document has been altered, its hash would be obtained and compared with the hash that was issued and deposited in TRUSTCLOUD's systems.

4. Display the front and back of the identification document and obtain and retain a photograph or snapshot.

The video-agent asks the user to show his identification document and takes control of the camera in order to be the one who takes the pictures and prevent the user from sending pictures previously stored in his device. Likewise, before considering the video-identification finished, the video-agent checks that they have the necessary quality and sharpness guarantees and may proceed to take them again in case, for example, they are shaky or the lighting conditions are not suitable.

5. To certify the authenticity, validity and completeness of the documents and their correspondence with the user.

In addition to the training received detailing the security measures linked to the documents

Currently analyzed, the service may include an automatic matching and validation system that will proceed to OCR reading and check the match between the user's facial features and those contained in the photograph of the ID document through a series of critical points. It is also important to highlight the possibility of adding complementary security layers such as, where appropriate, electronic validation of the DNIe 3.0. in the event that the user has a device with accessible NFC technology.

The sum of these elements allows us to declare that, formally and according to the information provided, the proposed system, in an optimal operating situation, accredits the authenticity, validity and integrity of the documents and their correspondence with the user within the margin of risk inherent to any remote activity.

6. Ensure that the process is carried out from a single device, that the communication is in digital format, unaltered and live, and that it is immediately recorded.

According to the functional description of the service provided, the implementation of the measures that guarantee the obligations related to the execution of the process, the establishment of the communication and the recording of the same would mean that the "VideoID" service formally complies with the aforementioned requirements.

F. Post-development requirements of the video-identification process

1. Negative results for certain scenarios

As stated in the functional description of the service, the result of the video-identification will always be negative when the impeditive circumstances described in the Specification are met:

1. Indications of forgery or manipulation in the identification document.
2. Indications of mismatch between the document holder and the customer being identified.
3. Deficient conditions of the communication prevent or make it difficult to verify the authenticity and integrity of the document and the correspondence between the holder and the client being identified.

2. Retain the recording of the process and the documents used in the process for a period of 10 years.

TRUSTCLOUD archives in electronic support, as a minimum, the following documentation:

1. The "certificate of completion".
2. Recording of the video-identification process.
3. Snapshots taken of the front and back of the identification document and the face of the identified user.

This electronic documentation, including the recording of the video-identification, is kept and duly guarded by TRUSTCLOUD for a minimum period of 10 years, with a mechanism that offers guarantees of its authenticity and integrity in accordance with the above. Likewise, it will be delivered to the obligated client at any time during the contractual relationship or at the

The company will be able to comply with its obligations in terms of PBC&FT.

Additionally, it should be noted that TRUSTCLOUD is considered a Qualified Trust Service Provider for the service of preservation of qualified electronic signatures and seals.

3. **Submit the video-identification procedure to an annual review by an external expert.**

In relation to this requirement, it should be emphasized, for the sake of impartiality, that we consider that it should be the regulated entity who appoints the expert in charge of annually analyzing the video-identification process as one more of the procedures established by the regulated entity in the area of PBC&FT.

4. **Subject the video-identification procedure to a specific and individual review prior to the execution of any operations.**

Finally, and in relation to unassisted video-identification procedures only, a specific and individual review of the recording of the process will be required prior to the execution of any obligations.

8. OBLIGATIONS AND RESPONSIBILITIES ABILITIES

8.1 TRUSTCLOUD OBLIGATIONS

TRUSTCLOUD as an unqualified Trusted Service Provider undertakes to comply with a number of obligations detailed in this R&DP, within the framework of eIDAS [1], its implementing provisions and other applicable legislation.

8.1.1 TRUSTCLOUD ORGANIZATIONAL REQUIREMENTS

- Operate its Identity Verification service infrastructures a s set forth in this Statement of Practice and Policy.
- To provide the Identity Verification Service in an impartial and objective manner.
- To guarantee the adequacy of its processes and services to the standards to which they adhere.
- Inform 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 with the means it deems most appropriate and for the period of time contemplated according to the nature of the data recorded.
- To provide the Identity Verification Service in a diligent and uninterrupted manner.
- Communicate to its Users sufficiently in advance the unavailability of the system in case of modification, improvement or maintenance processes that imply a paralyzation of the service.
- Notify the parties involved as soon as possible whenever an incident is detected in the system that affects them.
- Publish the most recent versions of this document and other definitions of practices of other services prior to the application of the conditions contemplated therein.
- To have a communication channel with Users and third parties for requests, queries, complaints and claims.
- Respond to requests, inquiries, complaints and claims from Users and third parties within a reasonable period of time.

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 validity, suspension or revocation of identity verification
- Respect the security measures indicated by TRUSTCLOUD to access the Identity Verification 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 modification to this Statement of Practices and policies.

- Notify the competent authority and the parties involved of any change in the infrastructure that might

affect the provision of the service.

8.2 RESPONSIBILITY

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

TRUSTCLOUD shall not be liable for any damages resulting from the misuse of the Identity Verification Service.

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

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

TRUSTCLOUD shall not be liable for the acts or omissions made by the Users, 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 Users as well as third parties linked to them, due to improper use, being the exclusive risk of the Users.

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

The subscriber of the Identity Verification Service must comply with the following obligations:

- Objects shipped must comply with the requirements of ETSI 119 461.
- It shall ensure legal compliance and the accuracy of the objects to be preserved.
- 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, in order to ensure that the highest level of security is achieved in all areas of the company.

9.1 PHYSICAL SECURITY

TRUSTCLOUD warrants that it complies with applicable regulations and leading physical security standards and best practices 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 of them. All this in order to reduce the risk of unauthorized access or damage to computer resources.

TRUSTCLOUD's information systems are located in restricted access areas that have been designed to be used by the company's customers.

have been adequately protected by appropriate physical access control mechanisms. Likewise, these systems have been protected against other types of environmental threats such as fire, floods or power outages.

This protection extends to those systems whose physical security is delegated to a supplier. For this purpose, 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 authorized, once compliance with the required security level 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 are adopted to ensure that the information contained therein is adequately secured, as well as to allow the reuse of these without presenting risks to the information.

Some of the measures adopted by TRUSTCLOUD are as follows:

- Authentication and Access Control. Building access control
- Access control to data processing centers (DataCenter) based on biometric fingerprint identification and centralized authorization with access registration, both incoming and outgoing.
- The temperature conditions are guaranteed by autonomous cooling equipment located inside the DataCenter that maintains 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 Center is category 6, 7 and fiber optic.
- Uninterruptible power supply systems.
- Fire detection, based on smoke detectors and vacuum 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.
- There is an agreement with a specialized service provider for the safekeeping of magnetic media, with an earthquake-proof vault for this purpose.
- Access by outsiders (visitors) to the DPC
- Water exposure
- Information retrieval

9.2 LOGICAL SAFETY

TRUSTCLOUD uses logical security measures common to all systems. The specific systems used for the provision of the service covered by this P&ID 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 minimize the impact caused by security incidents or failures in the operation of the systems, which allows a quick reaction to possible incidents, as well as the establishment of corrective measures to avoid their repetition.

Adequate segregation of duties has also been established in the assignment of responsibilities in order to prevent inappropriate use of the information systems, establishing, in those 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 by public or private communications networks is adequately protected by means of the appropriate mechanisms that 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, as well as with other external systems, such as those entities with which TRUSTCLOUD has 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 organizational 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 (laptops, mobile devices and telephones, etc.), as well as, residually, on paper, in order to mitigate the risk of unauthorized access, loss or theft.

9.2.1 SYSTEM ACCESS

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 required for the correct performance of their work activity, in accordance with their function and/or operational profile.

Those responsible for the treatment of information assets shall 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, or, where appropriate, of the owners of the process or business.

Without prejudice to further detail in its application, or the formal delegation of functions, the owners of the process or business are understood to be those responsible for the following positions:

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

All accesses made to TRUSTCLOUD information systems by users will be associated with a process of identification, authentication and authorization, establishing the appropriate controls to ensure that such 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 events in the system, taking into account the category of services provided,

TRUSTCLOUD has designed a system of records and controls that allow the reactive inspection of the following events on your systems, among others:

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

9.2.3 RECORDS MANAGEMENT

The integrity and availability of audit records shall be maintained at all times, keeping 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 a management tool.

Audit records generated by systems that treat confidential information must be stored according to the law, for the rest of the systems this time will be regulated by the appropriate procedures.

Information systems should have sufficient capacity so that the storage of audit trails does not degrade the level of service.

Any changes that are strictly necessary in relation to the generation of audit logs must be duly authorized by the security manager.

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

9.2.3.1 PROTECTION ON RECORDS

Access to TRUSTCLOUD's filing and documentation custody systems is restricted to authorized personnel only. Thus, an access control, identification and authentication system has been configured in such a way that it is protected against unauthorized access, modification, deletion or other manipulations.

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 COP and COP. (Retain the recording of the process and the documents used in the process for a period of 10 years).

9.2.3.2 RECORD RETENTION PERIOD

The aforementioned 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 those pertaining to daily audits, two (2) years for monthly audits and four (4) years for those pertaining to annual audits.

9.3.2.3 REQUIREMENTS FOR TIME SOURCES

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

TRUSTCLOUD systems record the exact time instant at which the records are made, using for this purpose 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 synchronize their instantaneous time with reliable time sources based on the Network Time Protocol (NTP), self-calibrating by various means.

9.3.2.4 BACKUP OF RECORDS

Backup copies of the files containing the records subject to retention are made and stored in the cloud.

These backups are performed on all service components.

9.3 VULNERABILITY ANALYSIS

Given the growing risk of malicious code insertion in programs, it will be mandatory to adopt criteria to collaborate in the protection of information systems against this type of attack.

The IT department will put in place all technical and organizational measures available to it to prevent the entry and propagation of malicious code on its computer systems.

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

- TRUSTCLOUD Information Systems must have installed antivirus, firewall, antispyware, mail filtering and DLP, all of them with automated updates, provided that the systems technologically support these types of controls. We have Defender for business, internal firewall Sonicwall and firewall managed by Movistar for office network connection and AWS IS measures. With prior authorization, the use of Avast (Android) and Firewall (iOS) is also allowed.
  Also a SIEM (Wazhu) and a proactive vulnerability management tool (Tenable).
- 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 e-mail does not meet the security criteria defined in the antivirus and content filtering applications, the e-mail 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 an annual 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 performed, of any problems that prevent the performance of the audits, or the delivery of the resulting documentation.

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

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

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

9.4 PERSONNEL SECURITY

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

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

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 keep the changes in the provision of the Service as minor as possible.

TRUSTCLOUD guarantees to make available to its staff the training courses that may be necessary for the provision of services to be performed 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 personnel using the contracted service. The duration and number of attendees shall be agreed with the USER.

10. CONTINUITY AND CONTINGENCY PLAN

TRUSTCLOUD has established business continuity and availability management processes to minimize 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 organizational, technological and procedural controls, both preventive and recovery.

These processes are supported by a Business Continuity and Availability Plan that is periodically tested and kept up to date at all times. For this purpose, 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 evaluated.

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 are assured.

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 appropriate material supply provider. If replenishment time cannot be assured, equipment purchases and storage at an alternative location to the main facility may be necessary.

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 provided for a financial plan that will enable it to have sufficient financial stability and resources to operate in accordance with these T&PP 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 them.

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

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

- Response times that were so long that they were 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 include:

- 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 key backups.

11. COMPLIANCE AUDITS

11.1 PERFIL AUDITOR

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 on TRUSTCLOUD or any of its services in particular must comply with the following requirements:

- Adequate and accredited training and experience in security and information systems auditing processes.
- Organizational independence from TRUSTCLOUD authority, in the 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 may result in a conflict of interest with TRUSTCLOUD. In order to comply with current data processing regulations, and if the audit process involves access to personal data, the auditor shall be considered a Data Processor, pursuant to the provisions of Article 28 of the GDPR [4].

11.2 AUDIT CRITERIA

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

- Security policy.
- Physical security of the facilities of the audited service.
- Logical security of TRUSTCLOUD systems and services
- Technological evaluation of the service components.
- Administration of the services, as well as security in the same.

- The present MYPD 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 will result as an immediate measure in the adoption of corrective measures. The competent authorities in the matter as defined by the legislation in force in collaboration with the auditor will be responsible for the determination of the same.

11.5 COMMUNICATION OF RESULTS

The external auditor or external auditors 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 respect to the information that TRUSTCLOUD employees know because of their job. The information considered confidential provided to TRUSTCLOUD will in no case be disclosed to third parties unless it is covered in the cases of request for cooperation with the competent institutions.

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

In this sense, it will be considered as "confidential" information (without prejudice that other types of information may also be confidential):

- Business continuity and emergency plans.
- Information related to the operations and maintenance of the service.
- Any information relating to the operations carried out by TRUSTCLOUD.
- All information related to security parameters, control and audit procedures.
- All personal information provided to TRUSTCLOUD during the registration process of certificate subscribers, 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, will be considered non-confidential public documents:

- TRUSTCLOUD Statement of Practice and Policy (SPP)
- All information that is considered "Public".

13. PROTECTION OF PERSONAL DATA

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

The personal data provided by Users will be processed by TRUSTCLOUD as Data Processor under the terms and conditions provided for in Article 28 of the GDPR [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 CONTROLLER of the processing at any given time, as well as with the provisions of the applicable regulations on personal data protection.
- Furthermore, TRUSTCLOUD 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 or the fulfillment of legal or contractual obligations.
- TRUSTCLOUD declares that it complies with the security measures defined in the present DPD, these being those that are necessary to ensure the security of personal data processed in the service provided, for the purpose of ensuring confidentiality and integrity depending on the nature of the data, in accordance with the provisions of the RGPD [3].

For the purposes of the provisions of this paragraph, 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 RESPONSIBLE to which it has access due to the provision of the Service and not to disclose, transfer, or otherwise communicate them, not even for preservation to other persons except in compliance with legal obligations.

Upon completion of the provision of the service covered by the Contract, TRUSTCLOUD undertakes to destroy or return any information containing personal data that has been transmitted by the RESPONSIBLE to TRUSTCLOUD in connection with the provision of the Service.

In the event that the affected parties, whose data are in files owned by the RESPONSIBLE, exercise their rights before TRUSTCLOUD, the latter must immediately transfer the request to the RESPONSIBLE and, at the latest, within 3 working days of receipt, so that the RESPONSIBLE duly resolves the request.

The present DPyP has the consideration of reference document for the implementation of technical and organizational security measures, attending to the proactive responsibility of TRUSTCLOUD to ensure compliance with the RGPD [3].

TRUSTCLOUD guarantees compliance with its obligations under the applicable regulations on the protection of personal data.

In the event of a breach of security or loss of integrity that has a significant impact on the service provided or 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 compliance with Article 19.2 of 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 SPD. 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:

THE CRITERIA TO BE USED FOR THE ATTENTION OF THE PETITIONS

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

TRUSTCLOUD will, to the extent possible, try to ensure that its services are accessible to all those who would like to subscribe to them, provided that they agree to comply with their obligations as set forth in these terms and conditions.
TRUSTCLOUD, in the provision of the services described in these T&OP, guarantees that it will not operate in a way that will result in any type of discrimination.

14.2 OBLIGATIONS OF SUBSCRIBERS

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

- Periodic fee for the use of the Service

- Cost per certification operation managed by the Platform: the amount of each operation request to the Platform.
- Cost per communication operation managed by the Platform.

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

14.3 LIMITATIONS ON THE USE OF THE SERVICE

The Services provided by TRUSTCLOUD have no territorial limits. The Customer shall be responsible for ensuring that the use of the Services is in accordance with the regulations of the country in which the Customer wishes to operate.

14.4 PROVISIONS IN THE EVENT OF TERMINATION OF SERVICE

TRUSTCLOUD undertakes to take all necessary measures to minimize the impact that could be suffered by a User or third parties involved in the service of these T&PP, as a result of the stoppage 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.

Specifically, TRUSTCLOUD has an updated service termination plan procedure, which outlines 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 prevent it from covering such costs itself, taking into account current insolvency regulations.

14.4.1 PORTABILITY

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

The processes for the destruction of material or specific transfers of each service, if they exist, would be defined in their specific policy definitions.

14.4.2 TERMINATION OF ACTIVITY

In case of termination of its activity as Certification Service Provider, TRUSTCLOUD will perform, with a minimum of two months, the following actions:

- Inform all subscribers of its services of the termination of the activity.
- Inform all third parties with whom you have signed a contract regarding this service.
- Communicate to the Ministry responsible for the Information Society the cessation of its activity and the destination to be given 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:

- The breach by the parties of any of the obligations provided for in these General Conditions of Use, the defaulting party is requested to remedy the breach, the latter does not proceed to remedy the

breach.

within 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 reason 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, derived from a change in market conditions, due to 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 the rupture of 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 according to the needs that may arise, and will formalize this relationship through a written agreement that will determine the conditions of the service provided through this subcontracting.

14.7 NULLITY

If any of the General Conditions of Use is declared totally or partially null or ineffective, such nullity or ineffectiveness shall only affect such provision or part thereof that is ineffective or null, and the rest of the clauses shall continue in force, and such condition or part thereof that is affected shall be deemed not to be in force.

14.8 NOTIFICATIONS

Any notice, demand, request or any other communication required under the practices described in this Statement of Privacy Practices and Policies shall be made by means of a digitally signed document or electronic message or in writing by certified mail to any of the addresses contained in the section on Contact Information. Electronic communications will be effective upon receipt by the addressee to whom they are addressed.
For this purpose, the parties shall expressly designate the addresses for the practice of communications. In case of modification of the domicile, the parties shall be obliged to notify the other party of the modification in the manner established in the first paragraph.

14.9 APPROVAL AND REVIEW OF TRUST SERVICE PRACTICES

14.9.1 APPROVAL AND IMPLEMENTATION

The present MOP will be approved by the Director of TRUSTCLOUD, the highest level and authority of responsibility within TRUSTCLOUD, who will also be endowed with the responsibility and capacity to elaborate and manage them.
A management team responsible for the implementation of the security and organizational practices required to ensure confidentiality, integrity and all that is established in these COP and COP has been established. TRUSTCLOUD has defined a team made up of the heads of the different areas involved in each of the steps of the Identity Verification Service.

14.9.2 MODIFICATIONS

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

- The modification is justified from a technical and legal point of view.
- Users are notified of all the effects derived 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 P&PD. Once it has been decided that a revision is advisable, the person responsible for preparing the document will make the appropriate modifications, which will be identified in the new edition by shading the modified text. This method can coexist or be replaced by a change control list listing the changes introduced in each edition or version of the document.

If the modifications made to the document produce 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 contractual relationship between TRUSTCLOUD and them will be modified. Thus, Users must adhere to the new conditions of use prior to the provision of new services or open a process to unsubscribe from the service.

14.9.3 VERSIONS

These MOPDs 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 demand via email contact on the website (point 6) for a period of at least 15 years.

Any publication will 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 will also be published by sending certified e-mail and on the page of the Competent Authority. The publication will 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 Competence of the Courts and Tribunals of Madrid for any matter related to the interpretation, compliance or execution of this declaration.

15. SUBSCRIBER AGREEMENT

The following policy applies to access rights:

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

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