SECURITYDATA
TU IDENTIDAD DIGITAL, EN UNA FIRMA.

TIME-STAMPING CERTIFICATION PRACTICE STATEMENT

marzo 4

2026

VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
1	INITIAL EDITION	12/18/2025	SUPERVISOR LEGAL	CHIEF TECHNOLOGY OFFICER (CTO)	GENERAL MANAGER
2	In the section 3.2.1., the method to prove possession of the private key in the event of purchase is added. Section 4.1.2. is modified, adding that the provision of the service will be subject to a contract. The application processing time is placed. The grace period for the request for revocation is added. The requirements for checking for the revocation of CRL are added. Section 5.5.2. and it is added as a guarantee of Legal Security and Non-Repudiation in the long term. The procedure for confirmed or suspected compromise of the private key is specifically placed. Certificate interoperability is added. The whole of section 6.1.6. Paragraph 6.2.7 is added. Section 6.8.3. and the guarantee of synchronization accuracy is added. All the sections are listed.	02/13/2026	LEGAL SUPERVISOR	CHIEF TECHNOLOGY OFFICER (CTO)	GENERAL MANAGER

Contents

1. Introduction.

1.1. GENERAL DESCRIPTION.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A, here in after SECURITY DATA is a certifying entity that was born in order to meet the needs of the Ecuadorian market of electronic signatures and digital certificates.

SECURITY DATA is a company incorporated in accordance with Ecuadorian law, registered in the commercial registry under number 2246 on July 13, 2010 with legal existence until July 13, 2060.

The Information Certification Services and Related Electronic Services offered by SECURITY DATA are aimed at individuals, Public and Private Corporations (such as companies, public entities) and their objective is to accredit the digital identity of corporations and natural persons acting through the network.

This document declares the certification practices for SECURITY DATA's electronic timestamp issuance service, through the exploitation of public key infrastructure (PKI).

The structure of this document is based on the specification of the "RFC3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework," created by the IETF's PKIX working group. In addition to the General Conditions established in this CPS, each type of certificate issued by SECURITY DATA is governed by specific conditions of issuance set out in a document called "Certification Policy" (PC or Certificate Policy).

1.2. NAME AND IDENTIFICATION OF THE DOCUMENT.

Name:	Time-Stamping (CPS) Certification Practice Statement
Document Code:	SD-ID-PE-14
Version:	2
Description:	Security Data Seguridad en Datos y Firma Digital S.A. Certification Practices Statement
Date of issue:	February 12, 2026
Address:	Alonso de Torres and Av. Del Parque, El Bosque Shopping Center Administrative Offices C8
Phone Number:	023922169
Website:	www.securitydata.net.ec

1.3. PARTICIPANTS IN CERTIFICATION SERVICES.

1.3.1. Certificate Authority (CA).

The Security Data Seguridad en Datos y Firma Digital S.A certification system is composed of various Certificate Authorities (CAs) organized under a Certification Hierarchy.

1.3.2. Registration authorities (RAs).

Security Data Security and Digital Signature as the registration authority, is responsible for verifying the identity of applicants for digital certificates, as well as validating, approving or rejecting requests for issuance, renewal, revocation or suspension of such certificates.

1.3.3. Certification service provider.

The Electronic Certification Service Provider (CSP) is the natural or legal person who provides one or more certification services. Security Data is a CSP in compliance with its Certification Practices Statement (CPS) that issues certificates recognized under the Electronic Commerce, Electronic Signatures and Data Messaging Act.

1.3.4. Subscribers.

The subscribers of the certification service are the end users of the electronic time stamps issued by SECURITY DATA. Subscribers can be natural or legal persons.

1.3.5. Third parties who trust.

They are the natural or legal persons who voluntarily trust and make use of the time stamps issued by SECURITY DATA.

The time stamps issued by SECURITY DATA are universal and are accepted by the public bodies of the Ecuadorian state, such as Ministries, Secretariats, etc.

1.4. USES OF THE TIME STAMPING SERVICE.

1.4.1. Appropriate uses.

The time-stamping service provided by SECURITY DATA as the Time-Stamping Authority may be used exclusively to generate reliable electronic evidence that proves the existence of electronic data on a certain date and time, in accordance with the applicable technical regulations and the legislation in force in the Republic of Ecuador.

The time-stamping service is intended to support the integrity and authenticity of electronic documents, data messages, digital transactions, computer records and any other set of electronic information, as set forth in the Electronic Commerce, Electronic Signatures and Data Messages Act.

1.4.2. Prohibited Uses.

The time-stamping service provided by SECURITY DATA may not be used for purposes other than those expressly permitted in this Statement of Certification Practices or in contravention of the legal regulations in force in the Republic of Ecuador.

The following uses are considered unauthorized:

- The use of the service for illicit, fraudulent purposes or purposes contrary to the Ecuadorian legal system, including those that violate the Law on Electronic Commerce, Electronic Signatures and Data Messages, its regulations, the Organic Law on the Protection of Personal Data and other applicable regulations.

- The generation or attempted generation of time stamps for the purpose of creating, altering, concealing, or validating false, deceptive, or manipulated electronic evidence.

- The use of the service to support content, transactions or activities that violate fundamental rights, the rights of third parties or rules of public order.

- The use of the service in order to circumvent legal, regulatory, contractual or judicial controls, or to obstruct audit, audit or investigation processes.

- The use of the time-stamping service on systems, applications or processes that are not declared or not compatible with the technical and security policies established by the TSA.

- The request for time stamps that imply the processing of personal data without a legal basis, without a legitimate purpose or in breach of the principles established in the Organic Law on the Protection of Personal Data.

1.5. ADADMINISTRATION OF POLICIES.

1.5.1. Organization that administers the document.

SECURITY DATA is responsible for the administration of this CPS and the Time Stamping Certification Policies.

1.5.2. Contact person.

Name:	Lenin Alberto Vásquez González
Address:	Alonso de Torres and Edmundo Carvajal "El Bosque" Shopping Center Administrative Offices 1st floor.
Address:	Quito - Ecuador
Email:	cto@securitydata.net.ec
Phone:	(02) 3922169
Website:	www.securitydata.net.ec

1.5.3. Person who determines the appropriateness of the policy.

The suitability of this policy is determined by the Legal Supervisor and the Chief Technology Officer (CTO) who are responsible for evaluating and approving that its content is adequate,

sufficient and consistent with the services provided, the requirements established in RFC 3647, as well as with the applicable legal and regulatory regulations.

1.5.4. Approval Procedure.

The publication of the revisions of this CPS and the Time Stamping PCs must be approved by the Senior Management of Security Data, after verifying compliance with the requirements expressed in them.

1.6. DEFINITIONS AND ACRONYMS.

1.6.1. Definitions.

Electronic Certificate: It is a document electronically signed by a certification service provider that links signature verification data to a signatory and confirms their identity.

Public Key and Private Key: The asymmetric cryptography on which PKI is based employs a pair of (it could be two pairs of keys), what is encrypted with one of them can only be decipher with the other and vice versa. One of these keys is called public and is included in the electronic certificate, while the other is called private and is only known by the holder of the certificate.

Electronic Signature: It is the set of data in electronic form, consigned together with other or associated with them, which can be used as a means of personal identification.

Advanced Electronic Signature: It is the electronic signature that allows identity to be established personal of the subscriber with respect to the signed data and verify the integrity of the same, as it is exclusively linked to both the subscriber and the data to which it is subjected. refers to, and because it was created by means that it keeps under its exclusive control.

Hash Function: It is an operation that is performed on a set of data of any size, so 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 with unequivocally to the initial data.

Lists of Revoked Certificates (CRLs): list of certificate lists revoked or suspended.

Hardware Cryptographic Module (HSM): Hardware module used to perform functions cryptographic and store keys in secure mode.

Time-stamping: Electronic annotation electronically signed and added to a message of data stating at least the date, time and identity of the person who makes the annotation.

Time-Stamping Authority (TSA): A trusted entity that issues time-stamps.

Validation Authority (VA): A trusted entity that provides information about the validity of digital certificates and electronic signatures.

Linked Third Party: A trusted entity that provides and/or manages the services of certification.

1.6.2. Acronyms.

AC:	Certificate Authority
AC Sub:	Subordinate Certificate Authority
PC:	Certification Policy
CPS:	Certification Practices Statement
CRL:	Certificate Revocation List
HSM:	Hardware Security Module
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Public Key Infrastructure
CSP:	Certification Service Provider
TSA:	Time Stamp Authority
VA:	Validation Authority
ECI:	Information Certification Authority
OID:	Unique Object Identifier
DN:	Dinstinguished Name
C:	Country
CN:	Common Name
Or:	Organization
OU:	Organizational Unit
SN:	SurName
ISO:	International Organizational for Standardization
PKCS:	Public Key Cryptography Standards, PKI Standards
UTF8:	Unique Transformation Format – 8-bit.
TSU:	Time Stamping Unit.

2. Repositories and Publication of Information.

2.1. REPOSITORIES.

Security Data repositories are referenced by the URL: https://www.securitydata.net.ec/ayuda-security-data-ecuador/#tabs_firma|3
Any changes to URLs will be notified to all entities that may be affected.

The IP addresses corresponding to each URL may be multiple and dynamic, and may be modified without prior notice.

2.2. PUBLICATION OF INFORMATION

2.2.1. Certification Policies and Practices.

Both the current CPS and the Time Stamping Certification Policies will be available in electronic format on the Security Data website.

Previous versions will be removed from your on-line consultation, but may be requested by interested parties at the Security Data contact address.

2.3. FREQUENCY OF PUBLICATION.

SECURITY DATA will immediately publish any modifications to the Time-Stamping Certification Statement of Practices and Policies.

2.4. CONTROL OF ACCESS TO REPOSITORIES.

This CPS and the Time-Stamping Certification Policies must be published in publicly accessible repositories without access control.

3. Identification and Authentication.

3.1. DENOMINATION.

3.1.1. Types of names.

The electronic certificates used for the issuance of the Time Stamp service require a distinguished name (DN) in accordance with the X.500 standard. In addition, all the names of the recognized certificates are consistent with the provisions of the standards:

- ETSI TS 101 862 known as "European profile for Qualified Certificates"
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- RFC 3739 "Qualified Certificates Profile".
- RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

3.1.2. Need for names to have meaning.

The DN fields in the electronic certificates used for the issuance of the Time Stamping service referring to the correct data of the natural person, Public or Private Legal Entity that acquired the services.

In the event that the data entered in the DN are fictitious or their invalidity (e.g. "PROOF" or "INVALID"), the certificate without legal validity will be considered, only valid for technical interoperability tests.

3.1.3. Anonymity or pseudonym of subscribers.

Not applicable.

3.1.4. Rules for the interpretation of the different forms of names.

Security Data complies in any case with the X.500 reference standard in ISO/IEC 9594.

3.1.5. Uniqueness of names.

The distinguished name (DN) of the certificates issued used for the issuance of the Time Stamping service will be unique for each Public or Private Legal Entity. The CIF or NIF attribute is used to distinguish between two identities when there is a problem of duplication of names.

3.1.6. Recognition, authentication and function of trademarks.

Not applicable.

3.2. INITIAL IDENTITY VALIDATION.

Security Data does not perform the validation of the identity of the subscribers as a requirement for the issuance of the certificate or Time Stamp service for natural or legal persons.

When the application is made by a legal person, theinitial validation is limited to the verification of the legal existence of the applicant legal person, as well as the verification that the application is made by its duly accredited legal representative or by an authorized member of the organization.

3.2.1. Method to prove possession of the private key.

The demonstration of the possession of the private key by users or subscribers does not apply, since the time-stamping service is automatically provided by Security Data as TSA, which is the only entity that owns and controls the cryptographic keys used for the issuance of the timestamps.

In cases where the subscriber requests a Time Stamp certificate to be operated externally, possession of the private key will be demonstrated by the delivery of a signed certification request generated on a secure device.

3.2.2. Authentication of the organization's identity.

Authentication of an organisation's identity is limited to verifying the legal existence of the applicant legal person, as well as verifying that the application is made by its duly accredited legal representative or by an authorised company member of the organisation.

3.2.3. Authentication of individual identity.

The time-stamping service does not contemplate the authentication of the identity of natural persons.

3.2.4. Unverified subscriber information.

Not applicable.

3.2.5. Authority validation.

Security Data validates its authority to provide the time-stamping service by verifying its legal existence, legal capacity and current accreditation, granted by the Telecommunications Regulation and Control Agency (ARCOTEL), in accordance with the provisions of the Law on Electronic Commerce, Electronic Signatures and Data Messages, its complementary regulations and the technical resolutions issued by the regulatory authority.

3.2.6. Interoperability criteria.

The time stamps issued by Security Data are generated in accordance with internationally recognized technical standards, guaranteeing their interoperability and the possibility of validation by systems, applications and third parties that trust and have the root certificate and suborconfigured

3.3. IDENTIFICATION AND AUTHENTICATION IN THE RENEWAL OF CERTIFICATES.

Security Data does not validate the identity of subscribers as a requirement for the renewal of the Time Stamp certificate or service for natural or legal persons.

When the renewal application is made by a legal person, the initial validation is limited to the verification of the legal existence of the applicant legal person, as well as the verification that the application is made by its duly accredited legal representative or by an authorized member of the organization.

3.3.1. Identification and authentication for routine key renewal.

Not applicable.

3.3.2. Identification and authentication for key renewal after revocation.

Not applicable.

3.4. IDENTIFICATION AND AUTHENTICATION IN THE REVOCATION OF CERTIFICATES.

The identification of subscribers in the certificate revocation process may be
Made by:

- Sending the identity document by email.
- The presentation of the applicant's identity document at the offices of Security Data.

4. Requirements Operations for the Life Cycle of Certificates.

4.1. REQUESTFOR CERTIFICATES.

4.1.1. Who can apply for a Certificate.

The Time Stamping service is available to natural or legal persons, public or private.

4.1.2. Enrollment Process and Responsibilities.

The applicant must contact Security Data to manage the request of the service Time Stamping, either by means of of the mail electronic soporte@securitydata.net.ec or in person at the offices of Security Data or of any of the associated Linked Third Parties.
If the applicant requires the time-stamping service for an organization, he or she must submit the necessary documentation to verify the legal existence of the legal entity, that is:

- Identity document of the legal representative.
- Deed or incorporation.
- RUC
- Appointment of the legal representative and its registration in the Mercantile Registry.
- Letter of authorization signed by the legal representative in the case of company members.

The provision of the service will be subject to the subscription of a service subscriber contract approved by the competent authority or the acceptance of the general terms and conditions of use by the subscriber

4.2. CERTIFICATE REQUEST PROCESSES.

4.2.1. Performing identification and authentication functions.

It is the responsibility of Security Data, or the duly authorized Linked Third Party, to reliably verify the legal existence of the requesting legal entity, as well as to verify that the person acting on its behalf has the status of legal representative, attorney-in-fact or authorized member of the organization, in accordance with the corresponding enabling documentation.

4.2.2. Approval or rejection of certificate requests.

Once the certificate request has been made, the Security Data registry operator You will need to verify the information provided by the applicant.

In addition, the Applicant must also accept the conditions of use and privacy policy . After obtaining the evidence, it will be checked with the evidence generated by the system to accept or reject the validity of the application.

If the information is not correct, the request will be denied, informing the applicant of the reason.

4.2.3. Processing time for certificate applications.

The average time to process applications for time-stamped certificates is 24 to 48 working hours from the complete validation of the documentation.

4.3. ISSUANCE OF THE TIME STAMP.

4.3.1. Actions of the CA during the issuance of the certificate.

Time stamp certificates will be issued on the Security Data Secure Cryptographic Appliance (HSM).

Time stamps are generated in response to valid requests, in accordance with the established technical and security mechanisms, guaranteeing the integrity of the stamped information and the accuracy of the date and time recorded. The issuance of the time stamp is carried out without manual intervention, ensuring the continuity, availability and consistency of the service.

The electronic certificates used for the issuance of the time stamps are an integral part of the service and are used exclusively for the generation, signature and verification of the time stamps, in accordance with the policies and practices defined in this Statement of Certification Practices.

4.3.2. Notification to the subscriber by the CA of the issuance of the certificate.

Once the time-stamp certificate has been issued, the applicant will receive an email from Security Data with the URL, username, password and the numberof available stamps.

4.4. ACCEPTANCE OF THE CERTIFICATE.

4.4.1. Conduct that constitutes acceptance of the certificate.

The certificate will be accepted at the time the binding legal instrument between the subscriber and Security Data has been signed. Consequently, the acceptance of the time-stamping service

will be understood to have been made when the subscriber makes effective use of the certificate for the generation of a time-stamp in the signing of an electronic document.

4.4.2. Publication of the certificate by the CA.

Not applicable.

4.4.3. Notification of the issuance of certificates by the CA to other entities.

Not applicable.

4.5. USING KEY PAIRS AND THE CERTIFICATE.

4.5.1. Use of the subscriber's private key and certificate.

The private key associated with the certificate used for the provision of the time-stamping service is for the exclusive use of Security Data and is used only for the generation and signing of time-stamps, in accordance with the procedures established in this CPS.

4.5.2. Use of public key and certificate of the relying party.

The trusting parties use the public key contained in the certificate solely to verify the authenticity, integrity, and validity of the issued time stamps, and are responsible for checking the validity and status of the certificate.

4.6. CERTIFICATE RENEWAL.

4.6.1. Circumstances for the renewal of the certificate.

The electronic certificates used in the provision of the Time Stamping service will be renewed close to the expiration date of the certificate.

4.6.2. Who can apply for renewal.

The renewal of the Time Stamping service can be carried out by any natural or legal person, public or private.

4.6.3. Processing of applications for renewal of certificates.

Security Data Receiveá Applications for renewal of the electronic certificates used in the provision of the Time Stamping service by means of Email soporte@securitydata.net.ec or in person at the offices of Security Data or any of the associated Linked Third Parties.

4.6.4. Notification of the issuance of a new certificate to the subscriber.

Once the time-stamping certificate has been renewed, the applicant will receive an email from Security Data with the URL, username, password and the number of stamps available.

4.6.5. Conduct that constitutes acceptance of a renewal certificate.

The certificate will be accepted at the time the binding legal instrument between the subscriber and Security Data has been signed. Consequently, the acceptance of the time-stamping service will be understood to have been made when the subscriber makes effective use of the certificate for the generation of a time-stamp in the signing of an electronic document.

4.6.6. Publication of the renewal certificate by the CA.

The publication of the time-stamp certificate will be carried out as specified in the regulations, by consulting the web series.

4.6.7. Notification of the issuance of certificates by the CA to other entities.

Not applicable.

4.7. MODIFICATION OF CERTIFICATES.

4.7.1. Circumstances for the modification of the certificate.

In the event of any erroneous data in the electronic certificate used in the provision of the Time Stamping service, it must be revoked and a new certificate with the modified data must be issued.

4.7.2. Who can request the modification of the certificate.

The modification of the certificate used for the Time Stamping service must be made by the certificate holder.

4.7.3. Processing of certificate modification requests.

Security Data Receiveá requests for Modification of the electronic certificates used in the provision of the Time Stamping service by means of Email soporte@securitydata.net.ec or in person at the offices of Security Data or any of the associated Linked Third Parties.

4.7.4. Notification of the issuance of a new certificate to the subscriber.

Once the time-stamping certificate has been issued, the applicant will receive an email from Security Data with the URL, username, password and the number of stamps available.

4.7.5. Conduct that constitutes acceptance of the modified certificate.

The certificate will be accepted at the time the binding legal instrument between the subscriber and Security Data has been signed. Consequently, the acceptance of the time-stamping service will be understood to have been made when the subscriber makes effective use of the certificate for the generation of a time-stamp in the signing of an electronic document.

4.7.6. Publication of the certificate modified by the CA.

The publication of the time-stamp certificate will be carried out as specified in the regulations, by consulting the web series.

4.7.7. Notification of the issuance of certificates by the CA to other entities.

Not applicable.

4.8. REVOCATION AND SUSPENSION OF CERTIFICATES.

The revocation of an electronic certificate used in the provision of the Time Stamping service entails the loss of validity of the same, and is irreversible. The suspension will not be applicable for this type of certificate.

Revocations take effect from the moment they are published in the CRL.

4.8.1. Circumstances of revocation.

An electronic certificate used in the provision of the Time Stamping service may be revoked due to the following causes:

a) Circumstances affecting the information contained in the certificate:
- Modification of any of the data contained in the certificate.
- Discovery that some of the data contained in the certificate request is incorrect.
- Loss or change of the signatory's relationship with the Corporation.

b) Circumstances affecting the security of the private key or certificate:
- Compromise of the private key or TSA infrastructure or systems, as long as it affects the reliability of the certificates issued from that incident.
- Infringement by the TSA of the requirements set out in the certificate management procedures set out in the CPS.
- Compromise or suspected compromise of the security of the subscriber's key or certificate.
- Unauthorized access or use, by a third party, of the subscriber's private key.
- Irregular use of the certificate by the subscriber or signatory.

- Failure by the subscriber or signatory to comply with the rules of use of the certificate set out in the CPS or in the legal instrument binding between Security Data and the subscriber.

c) Circumstances affecting the security of the cryptographic device:
- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disabling due to damage of the cryptographic device.
- Unauthorized access, by a third party, to the subscriber's activation data.
- Failure by the subscriber or signatory to comply with the rules of use of the certificate set out in the CPS or in the legal instrument binding between Security Data and the subscriber.

d) Circumstances affecting the subscriber:
- Termination of the legal relationship between Security Data and Subscriber.
- Modification or termination of the underlying legal relationship or cause that allowed the issuance of the certificate to the signatory.
- Infringement by the applicant of the certificate of the pre-established requirements for the application of the same.
- Infringement by the subscriber of its obligations, liability and guarantees, established in the corresponding legal instrument or in the CPS.

e) Other circumstances:
- The suspension of the digital certificate for a period longer than that established in the CPS.
- By judicial or administrative resolution that orders it.
- Due to the concurrence of any other cause specified in the CPS.

4.8.2. Who Can Request Revocation.

The following may request the revocation of an electronic certificate used in the provision of the Time Stamping service:
- The subscriber himself, who must request the revocation of the certificate if he becomes aware of any of the circumstances indicated above.
- Any person may request the revocation of a certificate if they become aware of any of the circumstances indicated above.

The following may process the revocation of the certificate:
- The authorized operators of the Linked Third Party to which the subscriber of the certificate belongs.
- TSA authorized operators.

4.8.3. Procedures for the Request for Revocation.

There are different alternatives for the subscriber when requesting the revocation of the electronic certificate used in the provision of the Time Stamping service.

In any case, at the time of suspension or revocation of the certificate, a communication will be sent to the
subscriber.

4.8.4. Grace period for the request for revocation.

A maximum grace period of 24 hours is established for the subscriber to notify a key commitment. Once the applicant's identity has been verified, the revocation will be processed immediately

4.8.5. Revocation during Office Hours.

The subscriber or signatory must contact Security Data or the associated Linked Third Party either via email or personally.

If the subscriber or signatory attends in person, their identity will be authenticated by presenting their identity card or passport. In the event of proceeding with the revocation of the certificate, it will be carried out immediately, once the revocation request has been completed and signed and delivered to the Security Data operator.

If you do so via email to soporte@securitydata.net.ec, the revocation request must be electronically signed and the definitive revocation will proceed.

Revocations take effect from the moment they are published in the CRLs.

4.8.6. Revocation Outside of Office Hours.

The customer will request the revocation by email to soporte@securitydata.net.ec, the It will be processed the next business day from 8:00 a.m.

4.8.7. Period within which the CA must process the Request for Revocation.

Once the subscriber's identity has been authenticated as set forth above, and the revocation duly processed by Security Data, the revocation will be effective immediately.

4.8.8. Revocation check requirement for relying parties.

Verification of the status of electronic certificates used in the provision of the Time Stamping service is mandatory, either by consulting the revocation list (CRL) or the OCSP service.

4.8.9. CRL Emission Frequency.

The CRL of end-entity certificates is issued every 24 hours or when a revocation and for quick reference the CA issues a delta CRL every 4 hours.

The CRL for certificates of authority (ARLs) is issued every 6 months or when a revocation.

4.8.10. Maximum latency for CRL.

Since the publication of the CRLs is made at the time of their generation, considers the elapsed time to be zero or null.

4.8.11. Online health check/revocation availability.

Information regarding the status of the certificates will be available online 24 hours a day. day, 7 days a week.
In the event of a system failure, or any other factor not under Security Data's control, Security Data will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 24 hours.

4.8.12. Online revocation check requirements.

Not applicable.

4.8.13. CRL Revocation Check Requirements

For the use of the CRLs service, which is freely accessible, the following must be considered:

- In any case, the last CRL issued must be checked, which can be downloaded from the URL address contained in the certificate itself in the "CRL Distribution Point" extension.
- The user must additionally check the relevant CRL(s) of the hierarchy certification chain.
- The user must ensure that the revocation list is signed by the authority that has issued the certificate they want to validate.
- Expired revoked certificates will be removed from the CRL.

4.8.14. Other forms of revocation notices available.

Not applicable.

4.8.15. Special key compromise requirements.

- Compromise of the private key or the infrastructure or systems of the CA, whenever it affects the reliability of the certificates issued from that incident.
- Infringement by the CA or the Related Third Party of the requirements set out in the certificate management procedures set out in this CPS.
- Compromise or suspected compromise of the security of the subscriber's key or certificate.
- Unauthorized access or use by a third party of the subscriber's private key.
- Irregular use of the certificate by the subscriber or signatory.

- Failure by the subscriber or signatory to comply with the rules for the use of the certificate set out in this CPS or in the legal instrument binding between Security Data Data Seguridad en Datos y Firma Digital and the subscriber.

4.8.16. Circumstances of suspension.

Not applicable.

4.8.17. Who can request the suspension.

Not applicable.

4.8.18. Procedure for requesting suspension.

Not applicable.

4.8.19. Limits on the suspension period.

Not applicable.

4.9. CERTIFICATE STATUS INFORMATION SERVICE.

4.9.1. Operational characteristics.

Security Data offers a free service of publishing on the website the Revoked Certificate Lists (CRLs) without access restrictions which contain the list of revocations since their creation and are signed by the Root CA.

4.9.2. Service Availability.

Download links can be found at the following addresses:

CRLS SUBCA-2:

http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl ,
http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl

Security Data has all revocation lists published.

In addition, Security Data offers the certificate validation service using the OCSP (Online Certificate Status Protocol) protocol. Information on this can be found in the OSCP DCP published at the following link:

https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/Ocsp_DPC.pdf

4.9.3. Optional features.

Not applicable.

4.10. TERMINATION OF SUBSCRIPTION.

The subscription will end at the time of expiration or revocation of the electronic certificate used in the provision of the Time Stamping service.

4.11. CUSTODY AND RECOVERY OF KEYS.

4.11.1. Key Deposit and Recovery Policy and Practices.

Not applicable.

4.11.2. Session key encapsulation and retrieval policy and practices.

Not applicable.

5. Facilities management and operational controls.

5.1. PHYSICAL SECURITY CHECKS.

Security Data has physical and environmental security controls in place to protect the resources of the facilities where the systems and equipment used for operations are located.

The physical and environmental security policy applicable to electronic certification services provides protection against:

- Unauthorized physical access
- Natural disasters
- Fires
- Failure of support systems (e-power, telecommunications, etc.)
- Collapse of the structure
- Flooding
- Theft
- Unauthorized departure of equipment, information, supports and applications related to components used for the services of the Accredited Entity

The facilities have preventive and corrective maintenance systems with assistance 24 hours a day, 365 days a year, with assistance within 24 hours of the notification. The location of the facilities guarantees the presence of security forces within a period of no more than 30 minutes.

5.1.1. Physical Location and Construction.

Security Data's facilities are built with materials that guarantee protection against brute force attacks, and are located in an area of low disaster risk and allows quick access.

Specifically, the room where cryptographic operations are carried out is a cage with protection from external radiation, double flooring, fire detection and extinguishing, anti-humidity systems, double cooling system and double electricity supply system.

5.1.2. Physical Access.

Physical access to Security Data premises where time-stamping certification certification processes are performed is limited and protected by a combination of physical and procedural measures.

It is limited to expressly authorized personnel, with identification at the time of access and registration, including CCTV filming and archiving.

The facilities have presence detectors at all vulnerable points, as well as alarm systems for intrusion detection with warning through alternative channels.

Access to the rooms is made with identification card and fingerprint readers, managed by a computer system that maintains an automatic log of entrances and exits.

5.1.3. Electric Power and Air Conditioning.

Security Data's facilities have current stabilizing equipment and a duplicated electrical supply system for equipment by means of a redundant generator set with fuel tanks that can be refilled from the outside.

The rooms that house computer equipment have temperature control systems with duplicate air conditioning equipment.

5.1.4. Water Exposure.

The rooms where computer equipment is housed have a humidity detection system.

5.1.5. Fire Protection and Prevention .

The rooms where computer equipment is housed have automatic fire detection and extinguishing systems.

5.1.6. Storage System.

Each detachable storage medium (tapes, cartridges, floppy disks, etc.), containing classified information, is labeled with the highest level of classification of the information it contains and

remains within the reach of authorized personnel only.

Information classified as Confidential, regardless of the storage device, is kept in fireproof cabinets or locked up permanently, requiring express authorization for its removal.

5.1.7. Elimination of Information Carriers.

When it is no longer useful, sensitive information is destroyed in the most appropriate way for the medium that contains it:

- Printed matter and paper: by shredders or in bins provided for this purpose to be subsequently destroyed, under control.
- Storage media: before being discarded or reused, they must be processed for deletion physically destroyed or make the information contained illegible.

5.1.8. Information Backup

Daily backups of the information are established.

5.2. PROCEDURAL CONTROLS.

5.2.1. Roles of those responsible.

Trust roles are those described in the respective Certification Policies of the hierarchy in a way that guarantees a segregation of duties that disseminates control and limits internal fraud, not allowing a single person to control from start to finish all certification functions. The minimum roles established are:

- Security Officer: Maintains overall responsibility for the administration and implementation of security policies and procedures.
- System Administrators: Authorized to make changes to system configuration, but without access to system data.
- System Operators: Responsible for the day-to-day management of the system (Monitoring, backup, recovery)
- Internal Auditor (System Auditor): Authorized to access the logs of the system and verify the procedures that are carried out on it.
- TSA Operator - Certification Operator: Responsible for activating TSA keys in the Online environment, or for the certificate and CRL signing processes in the Root Offline environment.
- Registration Officer: Responsible for approving, issuing, suspending, and revoking End-Entity certificates.

5.2.2. Number of People Required per Task.

Security Data ensures at least two people to perform the tasks that require multi-person control

and are detailed below:

- The generation of the TSA key.
- The recovery and backup of the TSA private key.
- The issuance of TSA certificates.
- Activation of the TSA private key.
- Any activity performed on the hardware and software resources that support the TSA root.

5.2.3. Identification and Authentication by Role.

The people assigned to each role are identified by the internal auditor who will ensure that each person performs the operations for which he or she is assigned.

Each person only controls the assets necessary for their role, thus ensuring that no one person has access to unallocated resources.

Access to resources is done depending on the asset through login/password, digital certificates, physical access cards and keys.

5.2.4. Roles That Require Segregation of Duties.

The Auditor tasks are incompatible in time with the Certification tasks and incompatible with Systems. These functions will be subordinate to the head of operations, reporting both to it and to the technical management.

Persons involved in Systems Administration may not carry out any activity in the tasks of Auditing or Certification.

5.3. PERSONNEL CONTROL.

5.3.1. Requirements Relating to Professional Qualification, Knowledge and Experience.

All personnel who perform tasks classified as reliable without supervision have been working at the production site for at least six months and have a permanent employment contract.

All personnel are qualified and have been properly instructed to perform the operations assigned to them.

Security Data ensures that the registration staff is trusted by theCorporation to perform registration tasks. To this end, a declaration to this effect is required by the Entity that assumes the functions of the Related Third Party.

The registry operator will have completed a preparation course to carry out the tasks of registration and

validation of the requests. At the end of this course, your knowledge of the process will be assessed.

Security Data will remove an employee from their trust duties when it becomes aware of the existence of the commission of a criminal act that could affect the performance of these functions.

5.3.2. Background Check Procedures.

Security Data conducts the relevant investigations prior to the hiring of any person.

Related Third Parties may establish different criteria, being responsible for the actions of the persons they authorize.

5.3.3. Training Requirements.

Security Data carries out the necessary courses to ensure that the certification tasks are carried out correctly, especially when substantial modifications are made to them and based on the personal knowledge of each operator.

5.3.4. Requirements and Frequency of Training Updates.

CurityData will conduct ongoing training for all staff at least once a year on information security.

5.3.5. Frequency and sequence of job rotation.

Not applicable.

5.3.6. Independent Contractor Requirements.

Employees hired to perform reliable tasks must first sign the
confidentiality clauses and operational requirements employed by Security Data.

Any action that compromises the safety of accepted critical processes may result in the termination of the employment contract.

5.3.7. Penalties for unauthorized actions.

Security Data will take disciplinary action when it finds that any unauthorized action has been taken.

Upon detection of an unauthorized action, Security Data will initiate an investigation process to determine the veracity and impact of the action and the collaborators involved. After this, disciplinary measures will be taken according to the seriousness and intention of the action.

5.3.8. Requirements for hiring personnel.

The requirements for hiring new personnel at Security Data are verified in the profile and description of each position. Among these requirements are mainly the academic training, experience and knowledge necessary for the position.

In addition, new personnel must undergo a medical evaluation to verify that they are fit to perform their duties.

5.3.9. Documentation provided to staff.

All personnel incorporated within Security Data are provided with the following documentation:

- Internal Regulations on Occupational Safety and Health
- Internal Regulations

5.4. AUDIT TRAIL PROCEDURES.

5.4.1. Types of events logged.

Security Data records and records all events related to the TSA security system.
These include the following events:

- Switching the system on and off.
- Login and logout attempts.
- Attempts to gain unauthorized access to the TSA system over the network.
- Attempts to gain unauthorized access to the internal network.
- Unauthorized access attempts to the file system.
- System configuration and maintenance changes.
- Turning the TSA app on and off.

In addition, Security Data retains, either manually or electronically, the following information:

- Physical access logs.
- System maintenance and configuration changes.
- Changes in the personnel who perform trust tasks.
- Reports of commitments and discrepancies.
- Records of the destruction of material containing key information, activation data, or subscriber personal information, if that information is managed.

5.4.2. Frequency of Audit Log Processing.

The audit logs will be reviewed every week and in any case when there is a system alert due to the existence of an incident, in search of suspicious or unusual activity.

5.4.3. Audit Log Retention Period.

Security Data will store the information in the audit logs for as long as it is considered necessary to guarantee the security of the system depending on the importance of each specific log.

5.4.4. Protection of Audit Trails.

System logs are protected from manipulation by signing the files that contain them.

They are stored in fireproof devices. Its availability is protected by storing it in facilities outside the centre where the Certification Authority is located.

The devices are operated at all times by authorized personnel.

5.4.5. Procedures for Supporting Audit Trails.

Security Data has an appropriate backup procedure in place so that in the event of loss or destruction of relevant files, the corresponding backup copies of the logs are available within a short period of time.

Security Data has implemented a secure backup procedure for audit logs, making a weekly copy of all logs on an external medium. The external medium is stored in a fireproof cabinet under security measures that guarantee that access is only allowed to authorized personnel. Daily, incremental, and full weekly copies are made.

Additionally, a copy of the audit logs is kept in the external custody center.

5.4.6. Audit Information Collection System.

Event audit information is collected internally and automatically by the operating system and certification software.

5.4.7. Notification to the subject causing the event.

In the event of a critical event that affects the validity or security of the time-stamping service, Security Data will formally notify the causative subject, detailing the nature of the event and the necessary corrective actions if warranted. Notification must be formal and documented, ensuring that corrective action is taken within a reasonable timeframe.

5.4.8. Vulnerability Analysis.

Security Data conducts an annual review of discrepancies in log information and suspicious activity.

5.5. LOG FILES.

5.5.1. Type of Archived Events.

Events that take place during the life cycle of the time-stamping certificate, including the renewal of the time-stamping certificate, will be retained. It will be stored by Security Data or, by delegation thereof to the Linked Third Party:

- All audit data
- Certificate Issuance and Revocation Requests
- All certificates issued or published
- CRL's issued or status records of the certificates generated
- Documentation required by auditors
- Communications between PKI elements

Security Data is responsible for the proper archiving of all such material and documentation.

5.5.2. Record Retention Period.

All system data relating to the lifecycle of certificates must be retained for the duration of the the period established by current legislation when applicable. The certificates are They will keep published in the repository for at least one year after their expiration.

The Subscriber contracts and any information regarding identification and authentication of the subscriber will be kept for at least 15 years or the period established by current legislation.

In order to ensure long-term Legal Certainty and Non-Repudiation, Security Data will keep historical revocation lists (CRLs) and audit trails available even after the expiration of the TSA certificate. This allows relying third parties to perform Long-Term Validation (LTV) of the sealed documents during the validity period of the certificate, ensuring that the proof of existence is valid in future administrative or judicial processes.

5.5.3. Protection of the Archive.

Security Data ensures the correct protection of files by assigning qualified personnel for their processing and storing them in fireproof safe deposit boxes and external facilities where required.

Security Data has technical and configuration documents detailing all the actions taken to ensure file protection.

5.5.4. File Backup Procedures.

Security Data has an external storage center to ensure the availability of copies of the electronic file archive. Physical documents are stored in secure locations with access restricted only to authorized personnel.

5.5.5. Requirements for the Time Stamping of Records.

The records are dated with a reliable source.

The processes of generating time stamps are governed and strictly comply with the provisions of the Ecuadorian Technical Regulations in its Chapter VI, article 22, paragraph D.

5.5.6. Audit Information Filing System.

Not stipulated.

5.5.7. Procedures for Obtaining and Verifying Archival Information

During the required audit, the auditor will verify the integrity of the information on file.
Access to archived information is made only by authorized personnel.

Security Data will provide the information and means to the auditor to be able to verify the archived information.

5.6. TSA PASSWORD CHANGE.

Before the Security Data certificate expires, a key change (rekeying) will be carried out and, where appropriate, changes will be made to the content of the TSU certificate that better comply with current legislation and the reality of Security Data Data Security and Digital Signature and the market. A new TSA will be generated with a new private key.

5.6.1. Procedure for action in the event of a TSA's private key vulnerability.

The compromise or suspicion of your private key is considered an incident and will be treated as a major incident of the provision of digital certification services.

In the event of confirmed compromise or well-founded suspicion of the TSA private key, Security Data will execute a crisis communication plan that includes:

1. Immediate notification to the regulatory authority;
2. Posting an alert notice on the main website within one (1) hour at the latest; y,
3. Sending electronic notifications to active subscribers. The notice will indicate the exact date and time of the commitment so that users can identify time stamps that have lost their presumption of integrity

5.7. COMPROMISE AND DISASTER RECOVERY.

5.7.1. Incident and Vulnerability Management Procedures.

Security Data , based on its infrastructure, can recover all systems in less than 48 hours, although

it ensures the revocation and publication of certificate status information in less than 24 hours.

5.7.2. Alteration of Hardware, Software and/or Data Resources.

In the event of an incident that alters or corrupts hardware, software and data resources, Security Data will proceed as stipulated in the "Security Policy" document.

5.7.3. Procedure for Action in the Face of the Vulnerability of the Private Key of a Certification Authority.

In the event of a Security Data private key compromise:

- Inform all subscribers, users, and other TSAs with whom it has agreements or other relationships of the commitment, at a minimum, by posting a notice on the Security Data website.
- It will indicate that certificates and revocation status information signed using this key are invalid.

5.7.4. Business Continuity after a disaster.

- Security Data will restore critical services (Revocation and Publication of Revoked Certificates) in accordance with this CPS within 24 hours of an unforeseen disaster or emergency.
- An alternative centre is available, if necessary, for the implementation of the certification systems.
- The restoration is done logically.
- Backups run on a daily basis at a logical level with a 7-day hold.

5.8. CESSATION OF ACTIVITY.

5.8.1. Certificate Authority

Before the cessation of its activity, the TSA will carry out the following actions:

- It will provide the necessary funds to continue the completion of the revocation activities until the definitive cessation of the activity, if applicable.
- It will inform all subscribers, applicants, users, other TSA's or entities with which it has agreements or other types of relationship of the termination with a minimum of 2 months' notice, or the period established by current legislation.
- Revoke all authorization to subcontracted entities that use the TSA.
- It shall inform the competent administration, in advance of the notice indicated, of the cessation of its activity and the destination to be given to the certificates, specifying, where appropriate, whether the management is to be transferred and to whom.
- TSA records will be archived and transferred to a specific custodian.

6. Technical safety controls.

6.1. KEY PAIR GENERATION AND INSTALLATION.

6.1.1. Key Pair Generation.

Two cases will be distinguished in the generation of keys for recognized certificates:

a) On HSM hardware (physical media)

Access

Access to the Time Stamping Authority (TSA) service is in accordance with the documented key ceremony process, within the Accredited Entity's security room, using hardware cryptographic devices (HSMs). Such access is granted only to duly authorized personnel, in accordance with the defined trust roles, under a dual control scheme, and with the participation of witnesses from SECURITY DATA, the organization that owns the TSA and the external auditor, ensuring that no person can access or perform critical operations individually.

Certificate Generation

Accredited Information and Related Services Certification Bodies or Related Third Parties shall issue time-stamping certificates on secure cryptographic devices HSMs (Hardware Security Modules) designed to provide a secure and reliable environment for cryptographic operations, securely protecting against unauthorized access, as defined in the RFC 3161 standard. ensuring interoperability and uniformity in the implementation of time stamping in different systems and applications.

b) TSA Service

The subscriber will receive the access credentials to the SECURITY DATA time-stamping service, consisting of an access URL, username and password, through a previously defined secure channel.

Access to the service will allow the subscriber to use the number of contracted time stamps, within the established period of validity, without the subscriber participating in the generation or custody of cryptographic keys, which are managed exclusively by the Time Stamping Authority (TSA) in its secure infrastructure.

Security Data's time-stamping service is fully interoperable and compliant with international standards and supports advanced e-signature profiles. This ensures that the generated timestamps are recognized by third-party applications, standard PDF readers, and government platforms

6.1.2. Delivery of the Private Key to the Subscriber.

a) On hardware (physical media)

The private key will be delivered along with the certificate to the signature creation device. The Linked Third Party will be responsible for ensuring the delivery of the device to the subscriber, thus ensuring that the latter is in possession of the signature creation data corresponding to the verification data contained in the certificate.

6.1.3. Delivery of the public key to the certificate issuer.

The public key is sent to the CA for certificate generation by means of a standard format preferably in self-signed PKCS#10 or X.509 format, using a secure channel for transmission.

6.1.4. Delivery of the Public Key to the Third Parties Relying on the Certificates.

The TSA certificate in the certification chain and your fingerprint will be available in the available to users on the Security Data Data Data Security and Digital Signature website.

6.1.5. Key Size

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits.

6.1.6. Generation of public key parameters and quality control.

Generation

The generation of the key pair is carried out within the associated HSM, using the PKCS#11 interface.

The generation operation is executed under double control (System Administrator + System Operator) and is recorded in:

- HSM Staff(when applicable),
- Auditoría/logs de EJBCA,

Quality Control

For quality control, at least the following are verified:

- Size and parameter verification
- RSA module length ≥ 2048 bits
- Confirmation that the key was created correctly.
- Cryptographic validation of the pair (e.g. proof of signature and verification with the newly generated key, or equivalent validation provided by the HSM).

- HSM health check (self-tests/operational status)
- HSM version/firmware registration

6.1.7. Supported Key Applications (X.509v3 KeyUsage field).

All TSA certificates include the Key Usage and Extended Key Usage extension, indicating the enabled uses of the keys.

DigitalSignature is used under OID 2.5.29.15.

6.1.8. Extended Key Usage (EKU).

The EKUs that are included in Security Data's TSA Certificates S.A. is:

Timestamping 1.3.6.1.5.5.7.3.8

6.2. PRIVATE KEY PROTECTION AND ENGINEERING CONTROLS OF CRYPTOGRAPHIC MODULES.

6.2.1. Standards for Cryptographic Modules.

The cryptographic modules used to generate and store the keys of the Certificate Authorities are certified to the FIPS-140-2 level 3 standard.

The keys of DSCF-recognized certificate subscribers and operators and administrators are securely generated by the data subject using a CC EAL4+, FIPS 140-1 Level 3, ITSEC E4 High or other equivalent level cryptographic device.

Cryptographic devices that safeguard the private key of the DSCF-recognized certificate subscriber and the operator or administrator provide a level of security.

6.2.2. Multi-person control (k of n) of the Private Key.

Access to Security Data's private keys requires the simultaneous concurrence of three different cryptographic devices out of five possible, protected by an access key.

6.2.3. Private Key Deposit.

The private keys of Security Data certificates are held by a cryptographic device, hardware certified with the FIPS 140-2 level 3 standard, ensuring that the private key is never clear outside the cryptographic device. Activation and use of the private key requires the multi-person control detailed above. After the operation is carried out, the session is closed, and the private key is deactivated.

The private keys of TSU certificates are held on secure cryptographic devices certified to FIPS 140-2 Level 3.

6.2.4. Private Key Backup.

The private keys of Security Data certificates have backups that allow them to be restored in the event of disaster, loss or damage. The generation and recovery of these copies is carried out under a dual control scheme, and the recovery files are stored in fireproof cabinets and in an external custody center.

6.2.5. Subscriber's Private Key File.

Security Data will not archive the certificate signing private key after the expiration of the certificate signing private key.

The private keys of the internal certificates used by the various components of the system Security Data to communicate with each other, sign and encrypt the information will be archived for a period of at least 10 years, after the issuance of the last certificate.

6.2.6. Transfer of the Private Key to or from the Cryptographic Module.

There is a Security Data key ceremony document that describes the processes of generating the private key and the use of cryptographic hardware.

In other cases, a file in PKCS12 format can be used to transfer the private key to the cryptographic module. In any case, the file will be protected by an activation code.

6.2.7. Private key storage in the cryptographic module.

Through the application of the TSA, the freeflow of thecryptographic module is validated, sThe CSR is generated and the certificate is subsequently issued to the cryptographic device.

6.2.8. Private Key Activation Method.

The keys of TSA certificates are activated by a process that requires the simultaneous use of cryptographic devices (cards).

6.2.9. Private Key Deactivation Method.

The TSA private key for certificates will be deactivated once the key pair is removed from the HSM module.

6.2.10. Private Key Destruction Method.

The method of destruction must be governed in accordance with the Procedure for Archiving, Accessing, and Destroying archived Security Data private keys.

6.2.11. Classification of Cryptographic module.

Prior to the destruction of the keys, a certificate revocation of the public keys associated with them will be issued.

Devices that have any part of the private keys stored in them will be physically destroyed or rebooted at a low level. For the restart, the steps described in the procedure for Deletion and Destruction of keys will be followed. Finally, the backups will be securely destroyed.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.

6.3.1. Public Key File.

Security Data will retain all public keys for the period required by applicable law, where applicable, or for as long as the certification service is active and at least 6 more months, otherwise.

6.3.2. Certificate Operating Periods and Key Pair Usage Period.

The period of use of a certificate will be determined by its temporary validity.

A time-stamped certificate should not be used after the validity period of the certificate, even if the relying party may use it to verify historical data considering that there will be no valid online verification service for that certificate.

6.4. ACTIVATION DATA.

6.4.1. Generation and Installation of Activation Data.

Activation data is generated at the time of initialization of the cryptographic device.

If the initialization occurs in an external entity, the activation data will be delivered to the subscriber through a process that ensures the confidentiality of the same before third parties.

6.4.2. Protection of Activation Data.

Only authorized personnel are aware of the activation data of the Security Data private keys.

6.5. COMPUTER SECURITY CONTROLS.

Security Data uses reliable systems and commercial products to offer its certification services.

The equipment used is initially configured with the appropriate security profiles by Security Data's systems personnel in the following aspects:

- Operating system security settings.
- Application security settings.
- User and Permissions Settings.
- Log Event Configuration.
- Backup and recovery plan.
- Antivirus settings.

The Security Data technical and configuration documentation details the architecture of the equipment that offers the certification service in both its physical and logical security.

6.5.1. Specific Technical Safety Requirements.

Each Security Data server includes the following capabilities:

- Control of access to TSA services and privilege management.
- Enforcing separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Archiving of subscriber and TSA history and audit data.
- Audit of security-related events.

The exposed functionalities are provided through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security classification.

Security Data maintains an inventory of assets and documentation and a procedure for managing information to ensure its use.

The security policy details the procedures for managing the information where it is classified according to its level of confidentiality.

The documents are catalogued in three levels: PUBLIC, INTERNAL and CONFIDENTIAL.

6.6. LIFECYCLE SECURITY CONTROLS.

6.6.1. Systems Development Controls.

Security Data has a procedure for controlling changes in versions and applications that imply an improvement in its security functions or that correct any detected vulnerabilities.

6.6.2. Security Management Controls.

a) Security Management.

The necessary activities are developed for the training and awareness of employees in terms of safety. Training materials and process descriptive documents are updated after approval by a security management forum.

The equivalent security measures are required by contract for any external supplier involved in the certification work.

b) Management Operations.

There is an adequate procedure for managing and responding to incidents, through the implementation of an alert system and the generation of periodic reports.

Security Data has fireproof safes for the storage of physical media.

Security Data has documented the entire procedure related to the roles and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

c) Treatment of Supports and Security.

All media will be treated securely in accordance with the requirements of the information classification. Media containing sensitive data is securely destroyed if it is not to be required again.

d) System Planning.

Security Data's technical department keeps track of the capabilities of the equipment. Together with the application of resource control of each system, a possible resizing can be foreseen.

e) Operational Procedures and Responsibilities.

Security Data defines activities assigned to people with a trusted role other than people in charge of performing day-to-day operations that are not confidential.

6.6.3. Lifecycle security controls.

Access System Management.

Security Data makes every reasonable effort to confirm that access to the system is limited to authorized persons. In particular:

a) Certificate Generation:

- TSA facilities are provided with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an attempt to access its resources without authorization and/or irregularity.
- The authentication to carry out the issuance process is carried out by a system of n operators for the activation of the TSA private key.

b) Revocation management:

- The revocation refers to the loss of effectiveness of a digital certificate permanently, a certificate on which the TSA is based. The revocation will be done by strong card authentication to the applications of an authorized administrator. The log systems will generate the evidence that guarantees the non-repudiation of the action carried out by the TSA operator.

c) Revocation status

- The revocation status application has access control based on certificate authentication to prevent attempts to modify the revocation status information.

Cryptographic Hardware Life Cycle Management.

- It ensures that cryptographic hardware used for certificate signing is not tampered with during transport.
- Cryptographic hardware is built on supports prepared to prevent any manipulation.
- The TSA records all pertinent device information to add to the SECURITY DATA asset catalog.
- The use of cryptographic certificate signing hardware requires the use of at least two trusted employees.
- SECURITY DATA performs test tests at least once a year to ensure the correct operation of the device.
- The cryptographic device is only tampered with by trusted personnel.
- The TSA certificate private key stored on the cryptographic hardware will be deleted once the device has been removed.
- Security Data has a maintenance contract for the device for its correct maintenance.

6.7. NETWORK SECURITY CONTROLS.

Security Data protects physical access to network management devices and has an architecture that orders the traffic generated based on its security characteristics by creating clearly defined network sections. This division is done through the use of firewall.

Sensitive information that is transferred over unsecured networks is done in encrypted form.

6.8. TIME STAMPING.

Security Data's time-stamping service provides irrefutable proof of the exact moment when electronic documents are generated or digital signatures are issued. This service makes it possible to legally prove that a document existed at a specific time and that it has not been altered subsequently, even when the signatory's certificate has expired or been revoked.

Technically, a hash function is applied to the document, which is sent to the TSA (Time Stamping Authority). The TSA stamps the hash with the server's official date and time and generates a time-stamping certificate, in accordance with the RFC 3161 standard, which can be attached to the digital signature.

6.8.1. Legal framework in Ecuador.

In accordance with the Law on Electronic Commerce, Electronic Signatures and Data Messages, accredited certification bodies may provide time-stamping services, provided that these are technically accredited by ARCOTEL.

The Regulations of the Law establish that the time stamp certifies, for legal purposes, the exact date and time in which a data message is received and delivered, taking as a reference the time zone of the Ecuadorian continental territory. The provision of this service is governed by a scheme of free competition and contracting.

6.8.2. Minimum content of the time stamp.

According to the regulations, the time stamping must include:

- Date, expressed in year, month and day format.
- Hour, expressed in hours, minutes and seconds according to the International System of Measurements.
- Identity, determined by the electronic signature of the entity that performs the sealing.

6.8.3. Legal reference time.

The time-stamping service exclusively uses UTC time on all of its servers and service. Consequently, time-stamping constitutes unequivocal proof of the exact moment in which an electronic document is created, sent or received.

Security Data ensures a TSA time synchronization accuracy with respect to the UTC source of at least **+/- 1 second**. To ensure this accuracy, the system uses multiple NTP Stratum 1 time sources. In the event of a *clock drift* above the established threshold is detected, the time-stamping service will be automatically suspended to prevent the issuance of stamps with inaccurate time information, resuming only after a successful and verified synchronization

7. TSA Certificate Profiles

7.1. PROFILE OF THE CERTIFICATES.

The certificates are aligned with the X.509 version 3 standard.

The technical details, extensions, required fields and other specifications of the certificate profile are described in the corresponding Certification Policies (PC).

7.1.1. Version number.

Security Data issues certificates aligned to the X.509 version 3 standard.

7.1.2. Certificate extensions.

The details of the extensions can be found in the profile of the certificates in the corresponding Certification Policies (PCs).

7.1.3. Algorithm object identifiers.

The object indicator of the signature algorithm is: 1.2.840.113549.1.1.11 SHA-256 with RSA Signature.

7.1.4. Forms of names.

The format of the names is specified in the corresponding Certification Policy.

7.1.5. Name restrictions.

The names contained in the certificates are unique and unambiguous.

7.1.6. Certificate Policy Object Identifier.

Not applicable.

7.1.7. Using the Policy Restrictions extension.

Not applicable.

7.1.8. Syntax and semantics of policy qualifiers.

Not applicable.

7.1.9. Processing semantics for the extension of critical certificate policies.

Not applicable.

7.2. CRL PROFILE.

7.2.1. Version number(s).

The CRLs issued by Security Data are version 2.

7.2.2. CRLs and CRL input extensions.

The entry extensions of CRLs are specified in the Security Data Statement of Certification Practices.

7.3. OCSP PROFILE .

7.3.1. Version number(s).

The OSCP profile is aligned with the X.509 version 3 standard.

7.3.2. OCSP extensions.

Extensions are specified in the Security Data Statement of Certification Practices.

8. Compliance audits and other controls.

The Security Data Certificate issuance system is subject to annual audits to ensure proper operation, operability and security.

8.1. FREQUENCY OF AUDITS.

Internal audit plans will be carried out with reporting, in order to have control over the life cycle of the certification authority and external authorship will be carried out as long as it is requested by the regulatory authority.

Webtrust seal maintenance audits are conducted annually.

8.2. AUDITOR QUALIFICATION.

Audits can be internal or external. In this second case, they are carried out by companies of recognised prestige in the field of audits.

8.3. RELATIONSHIP BETWEEN THE AUDITOR AND THE AUDITED AUTHORITY

The companies that carry out external audits never represent any conflict of interest that could

distort their performance in their relationship with Security Data.

However, Security Data will carry out planned internal audits with monthly reports to ensure at all times that it is in line with the requirements set by the hierarchy's certification policies.

8.4. ASPECTS COVERED BY THE CONTROLS

The audit verifies the following principles:

a) Publication of Information: That Security Data publishes the Business and Certificate Management Practices, as well as the information privacy and personal data protection policy and provides its services in accordance with such statements.

b) Service Integrity. That Security Data maintains effective controls to reasonably ensure that:
   - Subscriber information is properly authenticated (for registration activities performed), and

c) General controls. That Security Data maintains effective controls to reasonably ensure that:
   - Subscriber and user information is restricted to authorized personnel and protected from uses not specified in TSA's published business practices.
   - Continuity of operations related to key and certificate lifecycle management is maintained .
   - The tasks of operation, development and maintenance of Security Data's systems are properly authorised and carried out to maintain their integrity.

8.5. ACTIONS TO BE TAKEN AS A RESULT OF THE DETECTION OF INCIDENTS.

In the event that incidents or non-conformities are detected, the appropriate measures will be enabled to resolve them in the shortest possible time. Security Data undertakes to resolve it within a maximum period of sixty days.

In any case, a resolution committee will be formed made up of staff from the affected areas and another monitoring committee will be formed by those responsible for the affected areas and the General Management.

8.6. COMMUNICATION OF RESULTS.

The auditor shall communicate the results to senior management and the management system.

9. Other legal and activity issues.

9.1. TARIFAS.

9.1.1. Certificate issuance or renewal fee.

The fee corresponding to the issuance or renewal of Time Stamps is linked to the prices established for electronic signatures, which can be consulted at the following official link: https://www.securitydata.net.ec/firma-electronica-en-ecuador/#planes_fe

At the time of issuance of the certificate, a personalized quote will be made, according to the specific needs of the client and the current conditions.

The rate is subject to revision or modification without prior notice, by management or the commercial department of SECURITY DATA, in the same way the prices may be variable taking into account promotions or legal regulations in force in the country.

9.1.2. Access Fees to Time Stamp Certificates.

Access to the public key of the issued time-stamp certificates is free of charge, however, Security Data reserves the right to impose any fee due to legal changes or any other circumstance that in the opinion of Security Data should be taxed.

9.1.3. Status Information Access or Revocation Fees.

Security Data provides access to information regarding the status of time-stamping certificates free of charge, through the publication of the corresponding CRLs.

Security Data offers other commercial certificate validation services (such as OCSP).

9.1.4. Other Services Fees.

Rates applicable to other services will be negotiated between Security Data and the customers of the services offered.

9.1.5. Refund Policy.

Certificate subscribers may request reimbursement under the following guidelines:

- When an excess deposit has been made
- When the service has not been provided and the customer does not wish to continue with the procedure

In these cases, the customer must demonstrate the evidence of the payment made, once the circumstances have been analyzed to make the refund, the financial department will proceed with the respective refund.

In these cases, the customer must send an email indicating the reason for the refund to devoluciones@securitydata.net.ec, Once it has been analysed whether or not to apply the refund, the customer is notified.

The value of the refund will be that of the service requested, and the value deposited in excess.

9.2. FINANCIAL RESPONSIBILITIES.

9.2.1. Insurance Coverage.

The insurance covers all contractual and non-contractual damages of Security Data' s customers, exempt from fault arising from errors and omissions, or acts of bad faith by the administrators, legal representatives or employees of the SECURITY DATA Certification authority in the development of the activities for which it is authorized.

9.2.2. Other Assets.

No stipulation

9.2.3. Insurance or Guarantee of Coverage for Final Entities.

Security Data has acquired insurance issued by an insurance company authorized to operate in Ecuador, which covers all contractual and non-contractual damages of the owners and third parties who trust Security Data, free of fault, derived from errors and omissions, or acts of bad faith of the administrators, legal representatives or employees of Security Data in the development of the activities for which it is authorized.

9.3. CONFIDENTIALITY OF INFORMATION.

Security Data has an appropriate information processing policy and agreement models that must be signed by all persons who have access to confidential information, whether commercial, technical, operational, human resources, etc.

9.3.1. Scope of Confidential Information.

All non-public information is considered confidential and therefore of restricted access:

Confidentiality of the Certification Authority's private key.

- Confidentiality of the holder's private key.
- Confidentiality of the information provided by the owner.
- Records of transactions.
- Audit trail logs.
- Security policies.
- Contingency Plan.

- Business continuity plans.
- Any other subscriber-related information or Security Data that may be confidential in nature.

9.3.2. Non-Confidential Information.

The following information will be considered as non-confidential:

- That contained in this CPS.
- All information contained in issued certificates and certificate revocation lists (CRLs), including all such information that can be obtained.
- Certificate information (as authorized by the subscriber in the subscriber's agreement) and certificate status information.
- Any information whose publicity is required by law.
- All information expressly classified as "PUBLIC".

9.3.3. Responsibility to protect confidential information.

Security Data's employees, agents, and contractors are contractually obligated to protect confidential information.

Certificate subscribers are responsible for protecting their own private key and all activation information (i.e., passwords or PINs) required to access or use the private key.

9.4. PRIVACY OF PERSONAL INFORMATION.

9.4.1. Privacy Policy.

Security Data's privacy policy is the provisions of the right to habeas data: "Private information will be that which, because it deals with personal information or not, and that, becauseit is in a private sphere, can only be obtained or offered by order of a judicial authority in the performance of its functions."

9.4.2. Information treated as Private.

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

In compliance with the Organic Law on the Protection of Personal Data (LOPDP), Security Data guarantees data holders the exercise of their rights of access, rectification and opposition. Once the legal retention period of 15 years required by the Electronic Commerce Law for testing purposes has expired, Security Data will proceed to securely delete the personal data from its operational databases, or to anonymise them irreversibly, keeping only the technical statistical information that does not allow the identification of the owner.

9.4.3. Information Not Classified as Private.

The contents of the certificate and the status information of the certificate are not considered private.

9.4.4. Responsibility for the Protection of Personal Data.

Security Data is responsible for and has the appropriate security and control mechanisms to ensure the protection, confidentiality and proper use of the information provided by the owner.

9.4.5. Notice and Consent to Use Personal Data.

Personal data may not be communicated or used by third parties without due notification and consent fromthe owner.

9.4.6. Disclosure in the framework of an administrative or judicial process.

Security Data may disclose private information without notice to requestors or subscribers when such disclosure is required by law or regulation.

9.4.7. Other circumstances of disclosure of information.

Not applicable.

9.5. INTELLECTUAL PROPERTY RIGHTS.

Security Data, has intellectual property rights in all its regulatory documents, plans, processes, patents, trademarks, commercial material and certificates that it issues unless explicitly agreed otherwise, and may not be modified or attributed to another entity in an unauthorized manner.

9.6. REPRESENTATIONSAND WARRANTIES.

9.6.1. CA's Representations and Warranties.

Security Data represents, to the extent specified in your PC/CPS, complies, in all material respects, with all applicable laws and regulations.

Security Data assures that:

- You have taken reasonable steps to verify that the information contained in any Certificate is accurate at the time of issuance and is verified in accordance with this document.
- Certificates will be revoked if Security Data believes or is notified that the contents of the certificate are no longer accurate, or that the key associated with a certificate has been compromised in any way.

Security Data makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the fullest extent permitted by applicable law, including, but not limited to, all warranties as to merchantability or fitness for a particular purpose.

9.6.2. RA Representations and Warranties.

Security Data ensures that:

- It carries out the issuance process in accordance with this document.
- The information provided does not contain any false or misleading information.
- All requested time-stamping certificates comply with all the material requirements of this document.

9.6.3. Subscriber's Representation and Warranties.

Subscribers represent and warrant to Security Data, relying third parties, and other parties that, for each certificate, Subscriber must:

- Securely generate your private keys and protect your private key.
- Provide accurate and complete information when you contact Security Data.
- Confirm the accuracy of the certificate data before usingit.
- Immediately request the revocation of a Certificate and notify Security Data if there is any real or suspected compromise of the Private Key associated with the Public Key included in the certificate.
- Immediately request revocation of the Certificate and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
- Use the Certificate only for authorized and lawful purposes, in accordance with the purpose of the certificate, this CPS, any applicable PC, and the relevant Subscriber Agreement.
- To use the Certificate and the related Private Key immediately after the expiration date of the Certificate.

9.6.4. Representation and Warranties of the Relying Third Party.

The trusting third party is solely responsible for making the decision to trust a Security Data certificate.

9.6.5. Representation and Warranties of Other Parties.

Not applicable.

9.7. DISCLAIMERS OF WARRANTIES.

The time-stamping service is provided without additional implied warranties, limited to what is expressly set forth in this CPS and applicable regulations.

9.8. LIMITATIONS OF LIABILITY.

To the extent that Security Data, has issued and managed the time-stamping certificate in accordance with the CPS, it shall have no liability to Subscriber, the relying third party, or any Third Party for any loss or damage suffered as a result of the use of or reliance on such certificate.

Security Data assumes no responsibility with regard to the monitoring of the content, type and/or format of documents where the time-stamping service is used.

9.9. COMPENSATION.

The cases of compensation are defined in the contracts of the holders.

9.10. TERM AND TERMINATION.

9.10.1. Validity.

This Time-Stamping Certification Practice Statement document, and any amendments thereto, shall enter into force upon its publication on the Security Data website and shall remain in effect until it is replaced by a new version.

9.10.2. Termination.

This Time-Stamping Certification Practice Statement document and any amendments will remain in effect until modified or replaced by a new version.

9.10.3. Effect of Termination and Survival.

Upon completion of this Time-Stamping Certification Practice Statement, SECURITY DATA participants are bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. At a minimum, all liabilities related to the protection of confidential information will survive termination.

9.11. INDIVIDUAL NOTIFICATION AND COMMUNICATION.

In general, the SECURITY DATA website will be used to make any type of notification and communication. In the event of security problems or loss of integrity that may affect a natural or legal person, SECURITY DATA will notify them of this incident.

9.12. AMENDMENTS.

Amendments and changes will be communicated to ARCOTEL and after their approval they will be published on the website and notified to the holders and subscribers, in accordance with the means specified in their contracts.

9.12.1. Modification procedure.

Not applicable.

9.12.2. Mechanism and deadline for notification.

Not applicable.

9.12.3. Circumstances in which the OID should be changed.

Not applicable.

9.13. DISPUTE RESOLUTION PROCEDURE.

The dispute resolution procedure will be defined in the contracts of the holders.

9.14. COMPLIANCE WITH APPLICABLE LAW.

Law on Electronic Commerce, Electronic Signatures and Data Messages, its Regulations; Organic Law on Consumer Protection, Organic Law on Transparency of Information and Accreditation of ARCOTEL.

9.15. COMPLIANCE WITH APPLICABLE LAW.

Certificates issued under SECURITY DATA will be used by subscribers and relying third parties only in accordance with the laws and regulations of the jurisdiction in which they are used or based.

9.16. MISCELLANEOUS PROVISIONS.

9.16.1. Entire Agreement.

No stipulation.

9.16.2. Assignment.

Issuing TSAs, underwriters, relying third parties, Registration Entities, or any other entity operating under this Certification Practices Statement have no right to assign any of their rights or obligations under this Certification Practices Statement.

9.16.3. Severability.

If any provision of this Certification Practices Statement is held to be invalid by a competent authority in the applicable jurisdiction, the remainder of the Statement of Practices and Certification Policy shall remain valid and enforceable.

9.16.4. Execution.

No stipulation.

9.16.5. Force majeure.

Security Data accepts no liability for any delay or failure to perform an obligation under its Certification Practices Statement to the extent that such delay or failure is caused by events beyond its reasonable control.

9.17. OTHER PROVISIONS.

No stipulation.

10. Approval control

PREPARED BY	LEGAL SUPERVISOR	
REVIEWED BY	CHIEF TECHNOLOGY OFFICER (CTO)	
APPROVED BY	GENERAL MANAGER	