TIME STAMP CERTIFICATION POLICY

marzo 5

2026

VERSION HISTORY

VERSION	DESCRIPTION	DATE	PREPARED BY	REVIEWED BY	APPROVED BY
1	INITIAL EDITION	12/22/2025	LEGAL SUPERVISOR	CHIEF TECHNOLOGY OFFICER (CTO)	GENERAL MANAGER
2	General update of the PC in accordance with the Technical Regulations and RFC 3647.	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. 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 Seguridad en Datos y Firma Digital S.A. is a company incorporated in accordance with Ecuadorian legislation, 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 Seguridad en Datos y Firma Digital S.A. are aimed at individuals, Public and Private Corporations (such as companies, public entities) whose objective is to accredit the digital identity of corporations and natural persons acting through the network.

This document declares the Certification Policy for the Time Stamping service of Security Data Seguridad en Datos y Firma Digital S.A., here in after Security Data, in compliance with the rules and decrees applicable to the provision of digital certification services.

The Certification Policy is mandatory for the CA, its personnel, suppliers and other parties involved in the provision of the time-stamping service, and constitutes a public document, except for those sections that, for security reasons, must be classified.

This Certification Policy (PC), together with the EC Security Data Seguridad en Datos y Firma Digital S.A., are aimed at anyone who relies on this type of certificate.

1.2. NAME AND IDENTIFICATION OF THE DOCUMENT.

Name:	Time Stamp Certification Policy
Document Code:	SD-ID-PE-12
Version:	2
Description:	Security Data Seguridad en Datos y Firma Digital S.A. Time Stamp Certification Policy
Publication date:	February 12, 2026
Document Type:	Public
OID:	1.3.6.1.4.1.37746.102.2.5.1

1.3. PKI PARTICIPANTS.

1.3.1. Certification Authority.

The Certification Authority, hereinafter "AC", is the person authorised and empowered to issue certificates in relation to the electronic signatures of individuals, to offer or facilitate the services of registration and chronological stamping of the transmission and reception of data messages, as well as to perform other functions related to communications based on electronic signatures.

1.3.2. Certification Service Provider.

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

1.3.3. Time Stamping Authority.

Security Data is the Certification Service Provider that acts as the Time Stamping Authority (TSA) for the issuance of electronic time stamps and time stamp certificates.

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. Parties that 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. USE OF THE CERTIFICATE.

1.4.1. Appropriate Uses of the Certificate.

These certificates must be used in accordance with the legal regulations in force, which govern certain aspects of electronic trust services. The subscriber's use of the keys and certificate presupposes acceptance of the terms of use set out in the Security Data Timestamp CPS.

A certificate will be considered to be misused when it is used to carry out unauthorized operations according to this Certification Policy (PC) applicable to the certificate and the

contracts with its subscribers, as a result of this, Security Data may revoke the certificate and terminate the contract unilaterally.

If the subscriber's certificate in the validity period is compromised, that is, its private key, it must initiate the revocation procedure as mentioned in this PC and CPS.

1.4.2. Prohibited Uses of Certificates.

Use that is contrary to Ecuadorian and Community regulations, international conventions ratified by the Ecuadorian State, customs, morals and public order is not permitted. Nor is use other than that established in this Certification Policy and in the established CPS allowed.

The certificates have not been designed, cannot be used for and are not authorized for use or resale as hazardous situation control equipment or for uses that require fail-safe actions, such as the operation of nuclear facilities, air navigation or communications systems, or weapons control systems, where a failure could directly lead to death, personal injury or severe environmental damage.

End-user certificates cannot be used to sign public key certificates of any kind, or to sign certificate revocation lists.

1.5. POLICY MANAGEMENT.

1.5.1. Organization that administers the Document.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. is the entity that manages and is the author of this Certification Policy and other regulatory documents.

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 suitability of the CPS for the Policy.

This document is digitally signed by the Head of the Security Data AC before being published, and its versions are controlled, in order to avoid unauthorized modifications and impersonations.

1.5.4. CPS approval procedures.

The publication of the revisions of this PC and CPS must be approved and signed by the Security Data AC manager before publication.

Updated and approved versions of the PCs as well as other regulatory documents will be forwarded to the Supervisory Authority and subsequently published on the Security Data website.

Each document will maintain a version history, in which the changes made will be recorded, in order to prevent unauthorized alterations or impersonations.

1.6. DEFINITIONS AND ACRONYMS.

1.6.1. Definitions.

ARCOTEL: Telecommunications Regulation and Control Agency.

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 decrypted 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 others or associated with them, which can be used as a means of personal identification.

TSA Systems: Information technology systems that support the provision of time-stamping services. Hardware and software components that are managed as a unit to provide time stamps from a time source.

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 uniquely associated with the initial data.

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

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

Time stamping: An electronic annotation signed electronically and added to a data message stating at least the date, time and identity of the person making the annotation.

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

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

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

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
PSC:	Certification Service Provider
TSA:	Time Stamp Authority
VA:	Validation Authority
ECI:	Information Certification Entity
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. Publishing and Repository Responsibilities.

2.1. REPOSITORIES.

Time-stamp Certification Practice Statement:
https://www.securitydata.net.ec/wp-content/downloads/Normativas/p_certificacion/cps_ts.pdf

Certification Policy:
https://www.securitydata.net.ec/normativas/pc_ts.pdf

CA Root Certificate:
https://www.securitydata.net.ec/wp-content/downloads/descargas/certificados/Sistema_Windows/SECDATA-CA-2.cer

Subordinate CA Certificate:
http://subca2.securitydata.net.ec/subca2sd/subca2.crt

CRL:

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

2.2. PUBLICATION OF CERTIFICATION INFORMATION.

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

2.3. TIME OR FREQUENCY OF PUBLICATION.

This Time Stamping PC will be reviewed and, if appropriate, updated, annually or when any changes are presented or required.

Any substantial change that affects confidence or operability will be notified to the supervisory authority (ARCOTEL) at least 15 days prior to its publication.

2.4. ACCESS CONTROLS TO REPOSITORIES.

The repositories available on the aforementioned Security Data website are freely accessible to the public.

3. Identification and Authentication.

3.1. NAME.

3.1.1. Types of Names.

All certificates 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 EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

3.1.2. Need for names to have meaning.

Security Data must ensure that the names assigned to the digital certificates, both of the holder (Subject) and the issuer (Issuer), are meaningful, clear, precise and unambiguous, in accordance with the Technical Standard.

The names used must explicitly identify the legal person or entity that owns it and ensure that the use of the time stamp can be objectively attributed to the corresponding entity.

3.1.3. Anonymity or pseudonym of subscribers.

Alias may not be used in the Owner fields, Security Data does not issue pseudonymous certificates.

3.1.4. Rules for the Interpretation of the Different Forms of Names.

The name of the certificate holder must correspond exactly to the legal or institutional name that appears in the official documents presented during the validation process.

The names included in the identification fields of the certificate must allow the unequivocal identification of the holder of the time-stamp certificate, without ambiguities or elements that may mislead as to their identity, legal nature or scope of action.

3.1.5. Uniqueness of names.

The DN of the certificates issued is unique for each subscriber and/or signatory. However, for the same person who has several certificates and types of certificates, there is a unique serial for each one.

3.1.6. Recognition, authentication and function of trademarks.

The AC is not required to collect or request evidence in relation to the possession or ownership of trademarks or other distinctive signs prior to the issuance of the certificates. Security Data does not assume any obligation in the issuance of certificates regarding the use of trademarks or other distinctive signs.

3.2. INITIAL IDENTITY VALIDATION.

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

When the application is made by a legal person, the initial validation is limited to the verification of the legal existence of the requesting 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.

As defined in the Timestamp CPS.

3.2.2. Organization Identity Authentication.

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. Authenticationof Individual Identity.

Not applicable.

3.2.4. Unverified subscriber information.

Under no circumstances will Security Data omit the verification tasks that lead to the identification of the Subscriber and that results in the request for the disclosure of the aforementioned documents for legal entities.

3.2.5. Authority Validation.

The AC verifies that the applicant for the certificate has the authority, faculty or legal representation necessary to act on behalf of the legal entity, position or function to which the requested certificate will be associated.

The AC validates that the applicant has a current appointment, power of attorney or authorization, granted in accordance with the applicable legal regulations, which empowers him or her to request and use the certificate on behalf of the entity, in accordance with the provisions of the section Authentication of the Identity of a Legal Entity.

3.2.6. Interoperability Criteria.

Security Data issues time-stamp certificates in accordance with internationally recognized technical standards, guaranteeing their interoperability and the possibility of validation by systems, applications and third parties that trust, also have the root and subordinate certificate configured.

3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS.

Security Data does not perform identity validation of subscribers as a requirement for the renewal of the Time Stamp certificate or service. 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 the renewal of keys after revocation.

Not applicable.

3.4. IDENTIFICATION AND AUTHENTICATION FOR THE REVOCATION REQUEST.

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. Certificate Life Cycle Operational Requirements.

4.1. APPLICATION FOR THE CERTIFICATE.

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

4.2. REGISTRATION PROCESS AND RESPONSIBILITIES.

The processing process will be carried out as defined in the Security Data Timestamp CPS.

4.3. ISSUANCE OF THE CERTIFICATE.

The issuance process will be performed as defined in the Security Data Timestamp CPS.

4.4. ACCEPTANCE OF THE CERTIFICATE.

The acceptance process will be performed as defined in the Security Data Timestamp CPS.

4.5. USE OF KEY PAIRS AND CERTIFICATES.

The process will be performed as defined in the Security Data Timestamp CPS.

4.6. RENEWAL OF THE CERTIFICATE.

The renewal process will be performed as defined in the Security Data Timestamp CPS.

4.7. CHANGE OF CERTIFICATE KEY.

Not applicable

4.8. MODIFICATION OF THE CERTIFICATE.

The application process will be performed as defined in the Security Data Timestamp CPS.

4.9. REVOCATION AND SUSPENSION OF THE CERTIFICATE.

The application process will be performed as defined in the Security Data Timestamp CPS.

4.10. CERTIFICATE STATUS SERVICES.

The process will be performed as defined in the Security Data Timestamp CPS.

4.11. END 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.

4.12. CUSTODY AND RECOVERY OF PASSWORDS.

This option is not contemplated.

5. Facilities, Management and Operation Controls.

5.1. PHYSICAL CONTROLS.

As defined in the Security Data Timestamp CPS.

5.2. PROCEDURAL CONTROLS.

5.2.1. Roles of Trust.

Trust roles are those described in the respective Certification Practice Statements, so that a segregation of duties is guaranteed that disseminates control and limits internal fraud, not allowing a single person to control all certification functions from start to finish.

5.3. PERSONNEL CONTROLS.

5.3.1. Qualifications, Experience and Requirements.

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

Security Data ensures that registry operators are trusted individuals to perform registration tasks. In addition, registration operators will receive an induction to prepare them to carry out the tasks of registration and validation of the requests. At the end of this induction, you will proceed to evaluate your knowledge.

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.

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

Security Data periodically checks the criminal and police records of employees, as defined in internal procedures.

5.3.3. Training requirements.

Security Data personnel who manage the systems for the request for issuance, revocation, modification or suspension, must receive continuous training regarding:

- Digital certificates.
- Electronic signature.
- Regulations.
- Security and privacy policies.
- CPS and PC.
- Contingency plan.
- Functions with respect to their role.
- Information Security.

5.3.4. Frequency and retraining requirement.

The frequency of training should be at least once before operating in Security Data and then annually.

5.3.5. Frequency and retraining requirement.

Not stipulated.

5.3.6. 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.

5.3.7. Independent Contractor Requirements.

Employees hired to perform reliable tasks must previously sign the confidentiality agreement, contract and operational requirements used by Security Data Seguridad en Datos y Firma Digital S.A.

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

5.3.8. Documentation provided to the Staff.

Security Data will make available to all personnel documentation detailing the functions entrusted, the policies and practices that govern such processes, and the security documentation.

In addition, the documentation required by the staff at all times will be provided, so that they can competently carry out their functions.

5.4. AUDIT TRAIL PROCEDURES.

5.4.1. Types of Events Recorded.

SECURITY DATA records and saves the logs of all events related to the AC security system. These include the following events:

- Switching the system on and off.
- Attempts to create, delete, set passwords, or change privileges.
- Login and logout attempts.
- Attempts to gain unauthorized access to the SECURITY DATA system through the network.
- Attempts to gain unauthorized access to SECURITY DATA's internal network.
- Unauthorized access attempts to the file system.
- Physical access to logs.
- System configuration and maintenance changes.
- Logs of SECURITY DATA applications.
- Turning the SECURITY DATA application on and off.

- Changes to SECURITY DATA details and/or your passwords.
- Changes to certificate profiling.
- Generation of own keys.
- Certificate lifecycle events.
- Events associated with the use of the SECURITY DATA cryptographic module.
- Records of the destruction of the media containing the keys, activation data.

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

- System maintenance and configuration changes.
- Changes in the personnel who perform trust tasks in the CA.
- 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.
- Possession of activation data, for operations with the private key of the CA.

5.4.2. Frequency of Audit Log Processing.

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

5.4.3. Audit Log Retention Period.

The information in the audit logs will be stored 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 Records.

The logs of the systems 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, 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.

In addition, a copy of the audit logs is kept in an external custody center of SECURITY DATA.

5.4.6. Audit Information Collection System.

SECURITY DATA's event audit information is collected internally and automatically by the operating system and by the certification software.

5.4.7. Event Notification.

SECURITY DATA establishes that the possibility of allowing notification to a holder is taken into consideration in cases where it is established that the event is of an accidental nature and it is likely that it may occur again.

5.4.8. Vulnerability Analysis.

SECURITY DATA performs an annual review of discrepancies in log information and suspicious activities.

5.5. LOG FILE.

5.5.1. Type of Archived Records.

Events that take place during the life cycle of the certificate, including the renewal of the certificate, will be retained. The following shall be stored by the CA or, by delegation thereof to the Related 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

The CA is responsible for the correct filing of all this material and documentation.

5.5.2. Data retention period.

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

5.5.3. Protection of the Archive.

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

The CA has technical and configuration documents detailing all the actions taken to ensure the protection of the files.

5.5.4. File Backup Procedures.

The TSA has an external storage center to ensure the availability of copies of the electronic file file. 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.

5.6. CHANGE OF PASSWORD.

As stipulated in the Security Data Timestamp CPS.

5.7. DISASTER ENGAGEMENT AND RECOVERY.

5.7.1. Incident and Compromise Management Procedures.

The procedure is detailed in the Security Data Timestamp CPS.

5.7.2. Computer resources, software and/or data.

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

5.7.3. Procedure for the commitment of the entity's Private Key.

The procedure is detailed in the Security Data Timestamp CPS.

5.7.4. Business Continuity Capabilities after a Disaster.

The actions are detailed in the Security Data Timestamp CPS.

5.8. TERMINATION OR CESSATION.

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

- Protecting audit trails.
- Notify subscribers, holders and trusted third parties of the cessation of operations at least thirty (30) days in advance.
- Inform ARCOTEL at least sixty (60) days in advance.

Security Data takes steps to transfer audit logs to the Competent Authority for a period of 10 years after the log is generated.

All existing applications and contracts of subscribers and holders will be transferred to the Competent Authority or to another PSC designated by it, in compliance with the previously established guarantees and responsibilities.

All subscribers, holders and trusted third parties will be warned of the changes and any type of condition associated with the continuity of the use of the certificates issued by a CA that terminates or transfers its operations, through a communication published on the Security Data website.

6. Technical Security Controls.

6.1. KEY PAIR GENERATION AND INSTALLATION.

The build and install process will be performed as defined in the Security Data Timestamp CPS.

The generation of the private key of the digital certificate with which the time stamps are signed is carried out in a secure physical environment (in accordance with section 7.4.4 of RFC 3628), by trusted personnel (section 7.4.3 of RFC 3628) under the authorization of at least two persons.

The generation of the private key is carried out in a security hardware module – HSM with FIPS 140-2 level 3 or Common Criteria EAL 4+ certifications and its administration is protected by at least two people.

6.2. PROTECTION OF PRIVATE KEYS AND ENGINEERING OF CRYPTOGRAPHIC MODULES.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

The private key of each timestamp's signing certificate is safeguarded during use within a FIPS 140-2 Level 3 certified cryptographic hardware module. Backups are stored in a cryptographic module of the same level of security.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

6.4. ACTIVATION DATA.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

6.5. COMPUTER SECURITY CONTROLS.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

6.6. TECHNICAL CONTROLS OF THE LIFE CYCLE.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

6.7. NETWORK SECURITY CONTROLS.

The controls are stipulated as defined in the Security Data Time Stamp CPS.

6.8. TIME STAMPING.

6.8.1. Types and Uses of Time Stamps.

Time stamps issued by the Security Data CA comply with the following:

- Timestamps conform to RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
- The timestamp includes a timestamp policy identifier, in accordance with the TSA and Security Data TSU. (see section Validating Time Stamps).
- The timestamp includes the summary of the signed data (HASH) included in the corresponding timestamp request.
- The timestamp is signed by a key generated for this purpose, corresponding to the TSA Security Data TSU.
- The signature hashing algorithm of timestamps is SHA-256.
- A synchronization service is used to the reliable time source.
- The time included in the timestamp is synchronized with the UTC time of the reliable time source within the accuracy of +/- 1 second, which is included in the timestamp (the value of the accuracy field in the timestamp is 1 second).
- If the time stamp provider's clock is detected to be out of the stated accuracy, the time stamps are not issued.

Customers who receive this time-stamping service are obliged to comply with the provisions of current regulations, to respect the provisions of the contracts signed with this Sealing Authority, to verify the correctness of the time-stamp signature, the validity of the TSU certificate, as well as to verify that the hash of the time-stamp matches the one that was sent.

6.8.2. Validation of Time Stamps.

Third parties should check the status of the electronic timestamps they wish to rely on by checking the status of the TSU Certificate. One method by which the status of TSU certificates can be checked is by consulting the most recent Certificate Revocation List issued by Security Data as the Certificate Authority, responsible for the issuance of these.

Certificate Revocation Lists or CRLs are published on the Security Data website, as well as at the following web addresses, indicated within the certificates:

- CRLs can be downloaded from:
  - http://crl1.securitydata.net.ec/subca2crl1/crlfile.crl
  - http://crl2.securitydata.net.ec/subca2crl2/crlfile.crl

The validity status of certificates can also be checked using the OCSP 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

6.8.3. Time Accuracy on the Time Stamp.

The time included in the timestamp is synchronized with the UTC time of the reliable time source within the accuracy of +/- 1 second, which is included in the timestamp (the value of the accuracy field in the timestamp is 1 second)

6.8.4. Certificate Usage Limits.

Electronic time stamps limit their use in the applications and/or systems of customers (natural or legal persons) who have contracted these services.

Time stamps will not be used for purposes other than those specified above.

7. Certificate, CRL and OCSP profiles.

7.1. CERTIFICATE PROFILE.

Each time stamp issued by SECURITY DATA S.A. contains all the documentation required by the regulations, as shown in the following table:

Field Cert. Time Stamping	Authentication and Signing	Oblig.	Crit.	Observations OID 1.3.6.1.4.1.oid_AC.2.5.1
1. Basic structure				
1.1. Version	"2"	YES		Item "2" corresponds to version 3. X.509 v3
1.2. Serial Number	Automatically set by the CA Unique Identification Number of the certificate.	YES		It cannot be a negative number or 0.
1.3. Signature Algorithm		YES		
1.3.1. Algorithm	SHA-256 with RSA Signature	YES		1.2.840.113549.1.1.11
1.4. Issuer		YES		
1.4.1. Country Name (C)	Country Code "EC" (ISO 3166)	YES		OID 2.5.4.6
1.4.3. Organization Name(O)	Name of the Subordinate CA "Organization"	YES		OID 2.5.4.10
1.4.5. Common Name (CN)	Name of the Subordinate CA	YES		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Name of the Organizational Unit of the Subordinate CA Ej. ELECTRONIC SIGNATURE UNIT	No		OID 2.5.4.11
1.5. Validity	Recommended (maximum 5 years)	YES		
1.5.1. Not Before	Validity Start Date	YES		YYMMDDHHMMSSZ
1.5.2. Not After	Expiration Date	YES		YYMMDDHHMMSSZ
1.6. Subject		YES		
1.6.1. Country Name (C)	Country where the Legal Person (Public or Private) Holder of the Signature "EC" (ISO 3166) is located	YES		OID 2.5.4.6
1.6.2. Organization Name (O)	Name of the Legal Person (Public or Private) Holder of the Firm requesting the time stamp e.g. "NOTARY"	YES		OID 2.5.4.10
1.6.3. Locality Name (L)	Locality of the Legal Entity (Public or Private), City) ej QUITO	YES		OID 2.5.4.7
1.6.4. Organization Identifier	Unique Taxpayer Registration Number of the legal entity (Public or Private) to which the Time Stamp "VAT(CÓDIGO_PAIS)-RUC is linked, e.g. VATEC-1716151413001	No		OID 2.5.4.97coding according to ETSI EN 319 412-1RFC 5280 establishes as non-mandatory
1.6.5. Serial Number	Unique Taxpayer Registration Number of the Legal Entity (Public or Private) Ej "1716151413001"	YES		OID 2.5.4.5
1.6.6. Common Name (CN)	Name of the Service "Time stamping of the Legal Person (Public or Private)"	YES		OID 2.5.4.3
1.6.7. Organization Unit Name (OU)	Name of the Organizational Unit of the Legal Entity (Public or Private) Ej. NOTARY TIME STAMPING UNIT	YES		OID 2.5.4.11
1.7. Subject Public Key Info		YES		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	YES		OID 1.2.840.113549.1.1.1
1.7.2. SubjectPublicKey	Encoded public key of aceurdo with 2048-bit cryptographic algorithm	YES		ETSITS 119312 Accord
2. Extensions				
2.1. Authority Key Identifier	Issuer Key Identifier	No	NO	OID 2.5.29.35(Marked as NOT critical according to EN 319412-2) Not Mandatory as long as the public key of the CA is distributed in "SELF-SIGNED" certificate format

2.1.1. KeyIdentifier		No		Derived from the public key
2.2. Subject Key Identifier	Subject key identifier	YES	NO	OID 2.5.29.14(Marked as NOT critical according to EN 319412-2)
2.2.1. KeyIdentifier		YES		Derived from the public key
2.3. Key Usage		YES	YES	OID 2.5.29.15
2.3.1. Digital Signature	Selected "1"	YES		
2.3.2. Content commintment	Not selected. “0”			
2.3.3. Key Encipherment	Not selected. “0”			
2.3.4. Data Encipherment	Not selected. “0”			
2.3.5. Key Agreement	Not selected. “0”			
2.3.6. Key Certificate Signature	Not selected. “0”			
2.3.7. CRL Signature	Not selected. “0”			
2.3.8. Encipher Only	Not selected. “0”			
2.3.9. Decipher Only	Not selected. “0”			
2.4. Certificate Policies		YES	NO	OID 2.5.29.32(Marked as NOT critical according to EN 319412-2)
2.4.1. Policy Information		YES		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.5.1	YES		CA Policy ID
2.4.1.2. Policy Qualifiers		YES		
2.4.1.1.1 CPS URI	(https://www.repo_example.com/dpc/)	YES		OID 1.3.6.1.5.5.7.2.1 URL of the Certificate Policy of the Accredited Entity
2.4.1.1.2. User Notice/Explicit text	“TIME-STAMP CERTIFICATE”	YES		OID 1.3.6.1.5.5.7.2.2 Indicative text
2.5. Subject Alternative Names		YES	NO	OID 2.5.29.17(Marked as NOT critical according to EN 319412-2)
2.5.1. rfc822Name	Email from the Accredited Entity "info@example.com.ec"	YES		
2.6. Extended Key Usage		YES	YES	OID 2.5.29.37(Marked as critical per RFC 3161)
2.6.1. TimeStamping	Present (1.3.6.1.5.5.7.3.8)	YES		
2.7. cRLDistributionPoint		YES	NO	OID 2.5.29.31 (Marked as NOT critical according to EN 319412-2)
2.7.1. distributionPoint	(http://crl1.example.com/example1subordinada.crl)	YES		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme
2.7.2. distributionPoint	(http://crl2.example.com/example2subordinada.crl)	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETFRFC 4516 [4] scheme
2.8. Authority Information Access		YES	NO	OID 1.3.6.1.5.5.7.1.1(Marked as NOT critical according to EN 319412-2)
2.8.1. Access Description		YES		
2.8.1.1. Access Method	id-ad-ocsp	Yes		OID 1.3.6.1.5.5.7.48.1

2.8.1.1.1 Access Location	(http://ocsp1.example.com/ocsp/)	Yes		OCSP(http://) access URL IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Access Location	(http://ocsp2.example.com/ocsp/)	No		OCSP Access URL (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		No		Not Required as long as you include the OCSP access location
2.8.2.1. Access Method	id-ad-calssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	(http://www.example.com/subordinate1.crt)	No		URL Access to AC(http://) IETF RFC 7230-7235 [3] or (https://) IETF RFC 2818 [5] certificate
2.9. Basic Constraints		YES	YES	OID 2.5.29.19
2.9.1. cA	FALSE	YES		

7.1.1. Version Number.

Specified in the Certificate Profile.

7.1.2. Certificate Extensions.

Specified in the Certificate Profile.

7.1.3. Algorithm Object Identifiers.

Specified in the Certificate Profile.

7.1.4. Forms of names.

Specified in the Certificate Profile.

7.1.5. Name Restrictions.

The X.509 "Name Constraints" extension is not used in the certificates in this policy, i.e. no technical restrictions are included using OID 2.5.29.30. As a result, there are no "permittedSubtrees/excludedSubtrees" expressed in the certificate.

Name limitation is done by issuance profile, subject template, and allowed fields, so certificates issued under this policy must: Contain a Subject DN aimed at identifying the Time-Stamping Service (TSA) that includes C, L, O, CN, OU, Serial Number, and Organization Identifier fields..

7.1.6. Certificate Policy object identifier.

The OID for this Policy is 1.3.6.1.4.1.37746.102.2.5.1

7.1.7. Use of the Policy Restrictions extension.

The X.509 "Policy Constraints" extension under OID 2.5.29.36 is not used in the certificates in this policy. Therefore: No technical restrictions of "requireExplicitPolicy" or "inhibitPolicyMapping" are applied within the final certificate.

7.1.8. Syntax and Semantics of the Qualifiers of Politics.

The CA declares the applicable policies in the Certificate Policies extension with OID 2.5.29.32, the CA includesPolicy Qualifiers of the types:

- CPS URI with OID 1.3.6.1.5.5.7.2.1: Link to the current PC document applicable to the TSA service.
- User Notice with OID 1.3.6.1.5.5.7.2.2: short text describing the type/scope of the certificate as "TIME-STAMPING CERTIFICATE"

Semantics:

- The CPS URI is informational: it points to the normative document that describes controls, responsibilities, and limits of use.
- The User Notice is informative: it summarizes the purpose of the certificate and can warn about restrictions on use.

7.1.9. Processing Semantics for Critical Certificate Policy Extension.

In this policy, the Certificate Policies extension with OID 2.5.29.32 is issued as NOT critical.

Applications that validate the string should process the Certificate Policies extension when the use case requires verifying purpose/policy.

7.2. CRL PROFILE.

The profile of the CRLs corresponds to the one proposed in the corresponding certification policies, and to the X.509 standard of the 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". CRLs are signed by the certificate authority that issued the certificates.

7.2.1. Version Number.

The CRLs issued by the CA are version 2.

7.2.2. CRLs and CRL input extensions.

CRLs and extensions are defined in the Security Data CPS.

7.3. OCSP PROFILE.

Certificates issued for the OCSP validation service follow an X.509 v3 certificate profile intended exclusively for OCSP response signing. The certificate does NOT act as a CA where CA=FALSE and its use is restricted by EKU to the OCSPSigning purpose.

Characteristic elements of the profile:

- Subject DN identifies OCSP Responder
- Basic Constraints: CA=FALSE.
- EKU: OCSPSigning with OID 1.3.6.1.5.5.7.3.9
- Contains the OCSP No Check extension to allow relying parties not to require additional revocation verification of this certificate during OCSP validation.
- Publishes CRL Distribution Points and Authority Information Access for string and issuer fetching.

7.3.1. Version Number.

The OCSP certificate is issued as X.509 Version 3, to allow the use of critical and non-critical extensions necessary for OCSP service operation.

7.3.2. OCSP extensions.

The following are the extensions present in the OCSP certificate and their semantics of use within this profile:

- Critical Extensions
    - Key Usage with OID 2.5.29.15 – CRITICAL
        - digitalSignature = TRUE OCSP response signature.
        - contentCommitment / nonRepudiation = TRUE
        - All other KeyUsage bits are kept at FALSE, no encryption, certificate signing, or CRL signing is allowed.
    - Basic Constraints with OID 2.5.29.19 – REVIEW
        - CA = FALSE.
        - No pathLenConstraint.
        - Confirms that the certificate is an end-entity certificate and cannot issue certificates.
- Non-Critical Extensions
    - Extended Key Usage with OID 2.5.29.37 – NON-CRITICAL
        - Includes id-kp-OCSPSigning with OID 1.3.6.1.5.5.7.3.9.
        - Restricts the use of the certificate to OCSP response signing.
    - OCSP No Check with OID 1.3.6.1.5.5.7.48.1.5 – NON-CRITICAL

- Indicates that relying parties can bypass the CRL/OCSP revocation check of this OCSP certificate when validating OCSP responses, according to common practices for OCSP responder certificates.

- Certificate Policies with OID 2.5.29.32 – NON-CRITICAL
  - Includes the policy OID applicable to the OCSP certificate: 1.3.6.1.4.1.37746.2.6.1
  - In addition, the documentary reference of policy is published:
    - CPS: https://www.securitydata.net.ec/normativas/dpcocsp.pdf
    - User Notice: "OCSP VALIDATION CERTIFICATE"
- Subject Alternative Name with OID 2.5.29.17 – NON-CRITICAL
  - Includes rfc822Name with service contact email:
- CRL Distribution Points with OID 2.5.29.31 – NON-CRITICAL
  - Publish issuer CRL distribution points
- Authority Information Access with OID 1.3.6.1.5.5.7.1.1 – NON-CRITICAL
  - Publish caIssuers for download of the issuer certificate (issuer HTTP URL).
- Subject Key Identifier with OID 2.5.29.14 – NON-CRITICAL
  - Subject key identifier to facilitate string construction and validation.
- Authority Key Identifier with OID 2.5.29.35 – NON-CRITICAL
  - Key identifier of the issuing CA for easy string construction and validation.

8. Compliance audits and other controls.

The SECURITY DATA Certificate issuance system is audited to keep the Webtrust Seal active.

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. QUALIFICATION OF THE AUDITOR.

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 the TSA of the hierarchy to ensure at all times that they comply 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 the CA makes public the Business and Certificate Management Practices in the CPS, as well as the information privacy and personal data protection policy and provides its services in accordance with said statements.
b) Service Integrity: That the CA maintains effective controls to reasonably ensure that:
    - Subscriber information is properly authenticated (for registration activities performed by the CA), and
c) General controls. That the CA maintains effective controls to reasonably ensure that:
    - Subscriber and user information is restricted to authorized personnel and protected from uses not specified in the CA's published business practices.
    - Continuity of operations related to the management of the life cycle of keys and certificates is maintained.
    - The tasks of operation, development and maintenance of the AC systems are properly authorized and carried out to maintain their integrity.

8.5. ACTIONS TAKEN AS A RESULT.

The deficiencies detected during the audit process must be corrected through a Corrective Action Plan that contains the actions, procedures or implementation of the controls required to minimize risks.

In the event that incidents or non-conformities are detected, the appropriate measures will be taken to resolve them in the shortest possible time, according to the procedures established by Security Data.

8.6. COMMUNICATION OF RESULTS.

The auditor will communicate the results to Senior Management, and if necessary, to the owners of each process, in the event that the analysis and resolution of any deviation from compliance is required, Security Data will be in charge of drawing up a subsequent corrective action plan.

9. Other Business and Legal Matters.

9.1. RATES.

9.1.1. Certificate Issuance or Renewal Fees.

Issuance fees are stipulated in the Security Data Time Stamp CPS.

9.1.2. Certificate access fees.

Access fees are stipulated in the Security Data Timestamp CPS.

9.1.3. Revocation or status Information Access Fees.

Access fees are stipulated in the Security Data Timestamp CPS.

9.1.4. Fee for Other Services.

Rates are stipulated in the Security Data Time Stamp CPS.

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 info@securitydata.net.ec, once it has been analyzed whether or not the refund is applied, 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 RESPONSIBILITY.

9.2.1. Insurance Coverage.

The insurance covers all contractual and non-contractual damages of SECURITY DATA's client holders, who trust SECURITY DATA to be free of 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 authorised.

9.2.2. Other Assets.

No stipulation

9.2.3. Insurance or Guarantee of Coverage for Final Entities.

SECURITY DATA has acquired an insurance policy 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 to be free of fault derived from errors and omissions, or acts of bad faith by the administrators, legal representatives or employees of SECURITY DATA in the development of the activities for which it is authorized.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION.

Security Data personnel must sign contracts that include confidentiality clauses regarding the protection of privacy and confidentiality of all information submitted by customers, as well as a confidentiality agreement. Any action that compromises the safety of the accepted critical processes may lead to the termination of the employment contract.

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 information relating to the subscriber or SECURITY DATA, which may be confidential in nature.

9.3.2. Non-Confidential Information.

The CA will keep the following as non-private information:

- That contained in this PC and 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.
- All information expressly classified as "PUBLIC".
- Information regarding the revocation of a certificate.
- Any other information whose publicity is required by law

9.3.3. Duty 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 that established in current regulations, in the terms and conditions published. With regard to the protection of personal data, the applicable regulations in this area will apply , especially the Organic Law on the Protection of Personal Data (LOPDP), its regulations and other provisions issued by the competent authority.

Security Data will also implement appropriate technical and organisational measures to ensure the security of the personal data processed.

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.

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 to third parties without the due notification and consent of its 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 stipulated

9.5. INTELLECTUAL PROPERTY RIGHTS.

SECURITY DATA, has intellectual property rights over 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. REPRESENTATIONS AND WARRANTIES.

9.6.1. CA Representations and Warranties.

It is guaranteed that it complies with all the requirements established in the Certification Policy, Statement of Certification Practices, being responsible for compliance with the procedures described, in accordance with the indications contained in this document.

Security Data provides Digital Certification services in accordance with this Certification Policy, Time-Stamping Certification Practice Statement, and applicable standards. Likewise, it issues time stamps according to the information in its possession and free of data entry errors, delivering the services with the reliability and accuracy established in the respective contracts and in this document. The time-stamp service will be provided as a service either with the TSA certificate issued for the CA or with a TSA issued for the customer and governed by the technical standard.

Security Data informs the subscriber of the terms and conditions relating to the use of the seal, its price and its limitations of use.

Security Data links subscribers, key holders, and third parties who rely on certificates, in written and understandable language, with the following minimum contents:

- Requirements to comply with the provisions of this document.
- Limits on the use of time stamps.
- Information on how to validate a timestamp, including the requirement to verify the status of the timestamp, and the conditions under which it can reasonably be relied upon, which is applicable when the subscriber is acting as a relying third party on the certificate.

9.6.2. RA Representations and Warranties.

The responsibilities of the registry entity are as follows:

- Verify the identity of certificate applicants, as well as the veracity of the information and documents provided.
- Respect the provisions of the CPS and PC.
- Provide the minimum information necessary for the use of the certificates to the applicant, whose information must be transmitted free of charge, in writing or electronically.
- Take measures against certificate forgery and ensure the confidentiality of signature creation data during the generation process, as well as its delivery by a secure procedure to the subscriber.
- Do not copy or store subscriber signature creation data.
- Protect the personal data of applicants and users of digital or electronic certificates.

9.6.3. Subscriber Representations and Warranties.

The Subscriber shall be obliged to comply with the provisions of the regulations in force and also to:

- Integrate, configure and use the CA's chronological stamping service, in accordance with the instructions sent by the CA to the Applicant.
- Use client systems that submit requests to the CA Time-Stamping Service and interpret their responses in accordance with the format set forth in RFC 3161, and perform TSA certificate status checks.
- Respect the provisions of the legal instruments binding on the CA.
- The Subscriber shall be liable for any damages caused by the failure to perform its respective obligations listed in this PC.

9.6.4. Representations and Warranties of the Relying Party.

It will be the obligation of the Third Parties who trust to comply with the provisions of the regulations in force and also:

a) Know and abide by the applicable warranties, limits, and responsibilities in the acceptance and use of the time stamps on which they rely, and agree to be bound by them.
b) Notify Security Data of any irregular situation with respect to the service provided by the CA.

The test will normally be carried out automatically by the verifier's software and, in any case, in accordance with the CPS and this PC.

The relying third party undertakes not to use any type of information on the status of the time stamps or any other type that has been provided by Security Data, in the performance of any transaction prohibited by the law applicable to the aforementioned transaction.

The relying third party undertakes not to inspect, interfere with or reverse engineer the technical implementation of Ecuador's public certification services, without prior written consent.

In addition, the relying third party agrees not to intentionally compromise the security of Security Data's time-stamping services.

The time-stamping services provided by Security Data are not designed and do not permit use or resale, as hazardous situation control equipment or for uses that require error-proof actions, such as the operation of nuclear facilities, air navigation or communication systems, air traffic control systems, or weapons control systems. where a mistake could cause death, physical damage or serious environmental damage.

9.6.5. Representations and Warranties of Other Participants.

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES.

SECURITY DATA hereby disclaims all warranties, including the warranty of merchantability and/or fitness for a particular purpose other than to the extent prohibited by law or expressly stipulated in this PC and CPS.

9.8. LIMITATIONS OF LIABILITY.

To the extent that the SECURITY DATA CA has issued and managed the time-stamping certificate in accordance with the PC/CPS, it shall have no liability to the 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 TSA shall be liable to certificate holders or relying third parties for direct losses arising from any breach of this PC and CPS or for any other liability they may incur in contract, tort or otherwise, including liability for negligence by subscriber or trusted third party or third party by certificate, provided that the subscriber, trusted third party, or third party is in full compliance with such CP and CPS.

The TSA's liability of SECURITY DATA, to any person for damages arising under, out of, or in connection with this PC and CPS, Subscriber Agreement, applicable contract, or any other related agreement, whether in contract, warranty, tort, or otherwise, shall be limited to the actual damages suffered by that person. SECURITY DATA's TSA shall not be liable for any indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise.

9.9. COMPENSATION.

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

9.10. TERM AND TERMINATION.

9.10.1. Term.

This Certification Policy document and any amendments to it will become effective upon publication on the SECURITY DATA website and will remain in force until it is replaced by a newer version.

9.10.2. Termination.

This CPS and Certification Policy document, and any amendments will remain in effect until amended or replaced by a newer version.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.

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 owners and subscribers, in accordance with the means specified in their contracts.

9.13. DISPUTE RESOLUTION PROVISIONS.

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

9.14. GOVERNING 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, Technical Standard for the Provision of Certification Services and Related Services, issued by the Agency for the Regulation and Control of Telecommunications (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 CA, subscribers, relying third parties, Registration Entities, or any other entity operating under this Certification Policy and are not entitled to assign any of their rights or obligations hereunder without the prior written consent of SECURITY DATA.

9.16.3. Severability.

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

9.16.4. Execution.

No stipulation.

9.16.5. Force Majeure.

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

9.17. OTHER PROVISIONS.

No stipulation.

10. Control of Approvals.

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