CERTIFICATE POLICIES (CP)

Certificate of

COMPANY MEMBER

Version 10.1

ECI SECURITY DATA PC

DATA SECURITY AND DIGITAL SIGNATURE SA

Contents

1. LEGAL FRAMEWORK

1.1. Legal base

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

1.2. Validity

This document will come into force from the date of its approval.

1.3. Legal Support

a) Law on Electronic Commerce, Electronic Signatures and Data Messages, published in the Official Gazette No. 577 of April 17, 2002.

b) In accordance with the provisions of Article 37 of the Law on Electronic Commerce, Electronic Signatures and Data Messages, the National Telecommunications Council is the Agency for the authorization, registration and regulation of Accredited Information Certification Entities and Related Services.

c) General Regulations to the Law on Electronic Commerce, Electronic Signatures and Data Messages, issued by Executive Decree No. 3496 published in the Official Gazette 735 of December 31, 2002, and constant reforms in Executive Decree 1356 of September 29, 2008, published in the Official Gazette No. 440 of October 6, 2008.

d) That, the second article listed added by article 4 of Executive Decree No. 1356 after article 17 of the General Regulations to the Law of Electronic Commerce, Electronic Signatures and Data Messages, provides that the accreditation as an information certification entity and related services, will consist of an administrative act issued by CONATEL through a resolution that will be registered in the National Public Registry of

Accredited Information and Related Services Certification Entities and Related Third Parties.

e) Resolution 477-20-CONATEL-2008 of October 8, 2008, approved the resolution model for Accreditation as an Information and Related Services Certification Entity.

f) Resolution No. TEL-640-21-CONATEL-2010 of October 22, 2010, approved the request for Accreditation of the Company SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL SA as Certification Entity of Information and Related Services, for which the SENATEL signed the respective administrative act, according to the model approved by the National Telecommunications Council.

2. INTRODUCTION

2.1. Presentation

This document contemplates the Certification Policy (PC) of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL for Company Member Certificates

This CP specifies and contemplates what is established in the CPS of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, establishing a set of rules that indicate the procedures followed by the Certification Entity in the provision of its services for the request, identification, acceptance, issuance, revocation of digital certificates as well as the limits of use, the scope of application and the technical characteristics of this type of certificate.

This Certification Policy (PC), together with the CPS of the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, are addressed to anyone who trusts this type of certificates.

2.2. Document Name

2.2.1. ID

Name: Certificate Policies (PC)
Version: 10.0
Description: Company Member Certificate Policies
Date of issue: September 09, 2021

2.2.2. Publication

This document can be obtained freely at the electronic address https://www.securitydata.net.ec/

2.3. Definitions and Acronyms

2.3.1. 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.

- **Recognized Certificate:** Certificate issued by an Accredited Entity that meets the requirements established in the Law regarding verification of the identity and other circumstances of the applicants and the reliability and guarantees of the certification services they provide.

- **Public Key and Private Key:** The asymmetric cryptography on which PKI is based uses a pair of keys (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.

- **Signature Creation Data (Private Key):** They are unique data, such as codes or private cryptographic keys, that the subscriber uses to create the electronic signature.

- **Signature Verification Data (Public Key):** It is the data, such as codes or public cryptographic keys, that are used to verify the electronic signature.

- **Secure Signature Creation Device (DSCF):** Instrument used to apply the signature creation data.

- **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.

- **Advanced Electronic Signature:** It is that electronic signature that allows establishing the personal identity of the subscriber with respect to the signed data and verifying the integrity of the same, as it is exclusively linked to both the subscriber and the data to which it refers, and for having been created by means that it maintains under its exclusive control.

- **Hashing function:** It is an operation that is performed on a data set of any size, so that the result obtained is another data set of fixed size, regardless of the original size, and that has the property of being uniquely associated with the initial data.

- **Certificate Revocation Lists (CRL):** List containing the relationships of revoked or suspended certificates.

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

- **Time stamp:** Electronic annotation signed electronically and added to a data message that includes at least the date, time and identity of the person making the annotation.

- **Time Stamping Authority (TSA):** Trusted entity that issues time stamps.

- **Validation Authority (VA):** Trusted entity that provides information on the validity of digital certificates and electronic signatures

2.3.2. acronyms

AC:	Certification Authority
SubCA:	Subordinate Certification Authority
RA:	registration authority
CP:	Certification Policy
CPD:	Certification Practices Statement
CRL:	List of Revoked Certificates (Certificate Revocation List)
HSM:	Cryptographic Security Module (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Public Key Infrastructure
PSC:	Certification Services Provider
TSA:	time stamp authority
VA:	validation authority (Validation Authority)
ECI:	Entity Certification Information
OID:	unique object identifier (Object identifier)
DN:	Name Distinctive (Distinguished Name)
C:	Country (Country), Distinctive Name Attribute
NC:	Common Name (Common Name), Distinctive Name Attribute
O:	Organization (Organization), Distinctive Name Attribute
OU:	Organizational Unit, Name Attribute
SN:	surname (Surname), Distinctive Name Attribute

ISO:	International Standardization form organization
PKCS:	Public Key Cryptography Standards, PKI Standards
UTF8:	Unicode Transformation Format – 8 bits.

3. PARTICIPATING ENTITIES

3.1. Accredited Entity (AE)

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL is an Accredited Entity (EA) that issues recognized certificates according to the Law of Electronic Commerce, Electronic Signatures and Data Messages. SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL is the issuing entity of the certificates and responsible for the life cycle operations of the certificates. The functions of authorization, registration, issuance and revocation with respect to the personal certificates of the final entity, may be carried out by other entities by delegation supported contractually with SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, which will act as intermediaries. SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL also offers electronic signature validation and issuance services; and time stamping, governed by their policies,

3.2. Certification Authority (CA)

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL certification system is made up of various Certification Authorities (in English CA or Certificate Authority) organized under a Certification Hierarchy.

3.2.1. Root Certification Authorities

Root Certification Authority (CA Root) is the entity within the hierarchy that issues certificates to other certification authorities, and whose public key certificate has been self-signed. Its function is to sign the certificate of the other CAs belonging to the Certification Hierarchy.

3.3. Registration Authority (RA)

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL Registration Authority (RA or Registration Authority) is the entity in charge of:

- Process certificate requests.
- Identify the applicant and verify that they meet the necessary requirements for requesting the certificates.
- Validate the personal circumstances of the person who will appear as the signatory of the certificate
- Manage key generation and certificate issuance
- Deliver the certificate to the subscriber.

They may act as RA of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL:

- Any legal entity that is a client of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL and complies with the accreditation process for the issuance of certificates in the name of the legal entity or its members.
- Any trusted entity that reaches an agreement with SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL to act as an intermediary on behalf of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL Security Data itself SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL e directly.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will contractually formalize the relations between it and each of the entities that act as RA of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

The entity that acts as RA of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may authorize one or several persons as Operator of the RA to operate with the SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL certificate issuing computer system on behalf of the RA.

Where the geographical location of the subscribers represents a logistical problem for the identification of the subscriber and in the request and delivery of certificates, the RA may delegate these functions to another trusted entity. Said entity must have a special relationship with the RA and a close relationship with the subscribers of the certificates that justifies the delegation. The trusted entity must sign a collaboration agreement with the RA accepting the delegation of these functions. SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL must know and expressly authorize the agreement.

3.4. Applicant

Applicant is the natural person who, on their own behalf or on behalf of a third party, requests the issuance of a certificate from SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL. The requirements that an applicant must meet will depend on the type of certificate requested and will be included in the "Certification Policy" of each specific type of certificate.

3.5. Subscriber

The Subscriber is the natural or legal person who has contracted the certification services of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL. Therefore, it will be the owner of the certificate. In general, the subscriber of a SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL certificate will be a legal person (private company, public entity, natural person), whose identity will appear on the certificate itself.

3.6. Signatory

The Signatory is the person who has a signature creation device and who acts on their own behalf or on behalf of a legal person they represent.

The Signatory will be responsible for safeguarding the signature creation data, that is, the private key associated with the certificate.

3.7. Custodian of Keys

The custody of the signature creation data associated with each electronic certificate of a natural or legal person will be the responsibility of the requesting natural person, whose identification will be included in the electronic certificate.

3.8. Third party that trusts the Certificates

A third party that trusts the certificates (in English, relaying party) is understood to be any person or organization that voluntarily trusts a certificate issued by SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

The recognized certificates issued by SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL are universal in nature and are accepted by public bodies of the Ecuadorian state, such as Ministries, Secretariats, etc.

The obligations and responsibilities of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL with third parties that voluntarily trust the certificates will be limited to those included in the CPS of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL
Third parties relying on these certificates should be aware of the limitations on their use.

4. CHARACTERISTICS OF THE CERTIFICATES

4.1. Certificate validity period

The Company Member certificates will have the validity chosen by the user in the application form, or by default two years, up to a maximum of five years counted from the date of issue thereof in accordance with the Regulations of the Trade Law Electronic, Electronic Signatures and Data Messages (Decree No.3469).

4.2. Support Types

The Company Member Certificates may be generated both in hardware or Software support.

4.3. Secure Signature Creation Device (DSCF)

The private keys of the certificates issued on hardware support are generated and stored in a "Secure Signature Creation Device (DSCF)", such as a Smart Card or a cryptographic Token. The DSCF provided by SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL SA are FIPS certified.

Therefore, the use of Company Member Certificates with DSCF allows electronic signatures to be carried out with high security.

The certificate keys generated in DSCF cannot be copied in any way, so if the device is lost or damaged, it will be necessary to carry out a new certificate issuance process.

To activate the DSCF it will be necessary to enter the activation code (PIN). If the PIN is entered incorrectly six times in a row, the device will be locked and therefore unusable. To proceed with the unlocking, you must go to the RA where you purchased the certificate with the locked device or send it to it, where the unlocking will take place.

The PIN is secret and personal for the user, an initial PIN will be given to the user, which must be modified later by the user using the corresponding applications.

4.4. Software Support

4.4.1. Certificates, Public and private keys in Software

This service allows the user, after having made the request and that it has been approved by the Certifying Entity, to issue a digital certificate with their public and private keys, storing it in a P12/PFX file or as an EPF file, which

is protected by a password defined by the user, being the use of these certificates to sign and encrypt documents and for encrypted mail.

4.4.2. Certificates, public and private keys for Secure Web Server – SSL

This service allows the user, after having made the request and being approved by the Certifying Entity through the necessary mechanisms for verifying the information, to relate an Internet domain with a Legal Entity or a registered merchant and, once the request has been generated in the Web Server, it will proceed to the generation in a .CER/CRT/DER format.

Being the use of these certificates for the implementation of Secure Web servers.

5. TYPES OF CERTIFICATES

5.1. Legal Entity Certificates

Legal Entity Certificates are recognized electronic signature certificates whose subscriber is a legal entity (either a company, an organization, or a Public Administration):

- Legal Representative Certificates: These are recognized certificates that identify the subscriber as a legal entity and the signer as the legal representative of said corporation.
- Company Member Corporate Certificates: These are recognized certificates that identify the subscriber as a legal entity and the signer as linked to that company as an employee.

5.2. Natural Person Certificates

Natural Person Certificates: These are recognized natural person certificates that identify the subscriber as a natural person that can be used for this certificate for tax, legal and personal matters.

Professional Natural Person Certificates: These are recognized professional natural person certificates that identify the subscriber as a natural person who has a recognized and duly supported profession and that can be used for this certificate for tax, legal and personal matters.

5.3. Secure Server Certificates

Secure Server Certificates: These are certificates that link an Internet domain with a legal entity or a specific registered merchant.

6. COMPANY MEMBERSHIP CERTIFICATES

6.1. General features

6.1.1. Area of application

The certificates issued by the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL under this PC can be used to create electronic signatures and for encryption. Likewise, they can be used as an identification mechanism for computer services and applications.

For this reason, the Ecuadorian legislation referring to electronic signatures will apply.

6.1.2. Data in the Certificate

The information that will be included in the Company Member Certificate issued by the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL will be the following:

Fields included in the certificate		Description
WatchZion	WatchZion	Shows the version within the X.509 standard (v3)
serial number	Serial Number	certificate serial number
Signature Algorithm	signature algorithm	sha256RSA signature algorithm

Signature hash algorithm	signature algorithm for hash	sha256	
Issuer	Transmitter	Organizational Unit (OU)	entity of certification of information (ECI)
		Domain Component (DC)	information of the domain (securitydata.net.ec)
		organization Name (EITHER)	Name certification organization- Security Data Data seguridad en datos y firmas digitales
		Country Name (c)	country of authority certification- Ecuador (ec)
Valid from	Valid From	Certificate issue date	
Valid	Valid Until	Certificate expiration date	
Subject	Signatory	Common Name (CN)	full name subscriber
		Organizational Unit (OU)	entity of certification of information (ECI)
		organization Name (EITHER)	Name certification organization- Security Data Data seguridad en datos y firmas digitales
		Country Name (c)	country of authority certification- Ecuador (ec)
Public Key	public key	Public key of the Subscriber	
Key Usage	key	Identifies the use that will be applicable	
Access to authority information	Access to information of authority	Information indicating that OSCP will be used	
Certify Policy	assets of the Certified	Detailed certificate information including link to certificate pc	
1.3.6.1.4.1.37746.3.1	1.3.6.1.4.1.37746.3.1	Citizenship card or Passport No.	
1.3.6.1.4.1.37746.3.2	1.3.6.1.4.1.37746.3.2	Names	
1.3.6.1.4.1.37746.3.3	1.3.6.1.4.1.37746.3.3	Surname	

1.3.6.1.4.1.37746.3.4	1.3.6.1.4.1.37746.3.4	Second Surname: (if it does not have it, it is left blank)
1.3.6.1.4.1.37746.3.5	1.3.6.1.4.1.37746.3.5	Position
1.3.6.1.4.1.37746.3.7	1.3.6.1.4.1.37746.3.7	Section
1.3.6.1.4.1.37746.3.34	1.3.6.1.4.1.37746.3.34	Postal Code: (if it does not have it is blank)
1.3.6.1.4.1.37746.3.8	1.3.6.1.4.1.37746.3.8	Phone
1.3.6.1.4.1.37746.3.9	1.3.6.1.4.1.37746.3.9	City
1.3.6.1.4.1.37746.3.12	1.3.6.1.4.1.37746.3.12	Country
1.3.6.1.4.1.37746.3.10	1.3.6.1.4.1.37746.3.10	Business name
1.3.6.1.4.1.37746.3.11	1.3.6.1.4.1.37746.3.11	RUC
1.3.6.1.4.1.37746.3.29	1.3.6.1.4.1.37746.3.29	RUP (if it does not have it is blank)
1.3.6.1.4.1.37746.3.32	1.3.6.1.4.1.37746.3.32	Invoice number
1.3.6.1.4.1.37746.3.33	1.3.6.1.4.1.37746.3.33	Token Serial Number
Subject Alternative Name	Alternative Name Signatory	subscriber email
CRL Distribution Points	Distribution Points of the CRL	CRL distribution points. address where the certificate revocation list is published
Private Key Usage	Periods of use of private key	Time in which the private key will be valid
Authority Key Identifier	key identifier of issuing entity	Extension of the X509 standard
Subject Key Identifier	key identifier of subject	Extension of the X509 standard
Basic Constrains	Basic constraints	Determines what the AC is intended for, the route of certification as final entity of ECI
Entrust Version Info	Entrust Information	Information about the PKI platform
t Algorithm	algorithm of identification	signature algorithm used by the CA
Thumbprint	Fingerprint	fingerprint associated with the certificate

6.2. Private use of certificates

6.2.1. Appropriate use of certificates

- The subscriber may make use of the Electronic Signature certificate as established in this certificate policy, in the service provision contract signed with the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, and the CPS.

- It will be considered that a Certificate is misused when it is used to carry out unauthorized operations according to the Certificate Policies applicable to each of the Certificates, and the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL contracts with its subscribers. Because of this, the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may revoke the certificate and terminate the contract.
- The authorized uses of the Certificates issued by the ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may be specified in each type of certificate.
- If the subscriber's certificate is found to be compromised during the validity period, that is, its private key, it must initiate the revocation procedure as mentioned in this CP, and in the DPCs.
- The electronic signature Certificate issued by ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL to the subscriber, must be used as supplied. Any alteration of the certificate by the user is prohibited.
- Electronic signature certificates may not be used for illicit actions, in accordance with the provisions of Ecuadorian legislation.
- The electronic signature certificates present the following guarantees:
    - **Authenticity:** The information on the document and its electronic signature undoubtedly correspond to the person who signed it.
    - **Integrity:** The information contained in the electronic document has not been modified or altered after its signature.
    - **Non-repudiation:** The person who has signed electronically cannot deny their authorship.
    - **Confidentiality:** The information contained has been encrypted and by the will of the issuer, only the receiver is allowed to decrypt it.

6.2.2. Unauthorized use of certificates

Use that is contrary to Ecuadorian and community regulations, international conventions ratified by the Ecuadorian state, customs, morality and public order is not allowed. The use other than what is established in the

Certification Practices Statement and in this corresponding Certification Policy is also not allowed.

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

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

6.2.3. Generation of the keys and the Certificate

The support for the storage of the keys and the certificate will be a cryptographic device or by means of software. Access to the cryptographic device, where the private key is located, will be done through a password (PIN) or in turn through the fingerprint in the biometric devices. Access to the Software certificate in P12/PFX format file is done through a password (defined by the end user). To make an electronic signature it is necessary to enter the PIN/Password that only the Subscriber must know or the scan of the fingerprint,

6.3. Rates

Certificate Issuance or Renewal Fees

The prices of the certification services or any other service will be provided to clients or potential clients by the Commercial Department of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL or through the website https://www.securitydata.net.ec /wp-content/downloads/lists/price_list.pdf

6.31. Change of rates or exceptions

The prices indicated in point6.3, may be subject to revision or modification without prior notice, by the management or commercial department of Security Data, in the same way the prices may be variable considering promotions or legal regulations in force in the country.

6.3.2. Certificate Access Fees

Access to the issued certificates will be according to the price list published according to the rates contemplated in the list of numeral 6.3.

6.3.3. Fees for Access to Status Information or Revocation

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL provides free access to information regarding the status of certificates or revoked certificates, through the publication of the corresponding CRL.

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL offers other commercial certificate validation services (such as OCSP).

6.3.4. Other Services Rates

The rates applicable to others will be considered in the price list published according to the list in numeral 6.3

6.3.5. refunds

Certificate subscribers may request money reimbursement under the following guidelines:
When an excess deposit has been made
When the service has not been provided and the client does not want to continue with the process

For these cases, the client must demonstrate the evidence of the payment made, once the circumstances for making the reimbursement have been analyzed, the financial department will proceed with the respective refund.

In these cases, the client must send an email indicating the reason for the refund to devoluciones@securitydata.net.ec, once analyzed whether or not the refund applies, the client is notified.
The value of the refund will be that of the requested service, and the value deposited in excess.

6.4. Certificate Request

6.4.1. Who can apply for a certificate

Applicant is the natural person who identifies the subscriber as a legal person and the signer as linked to that legal person, whether as an employee, associate, collaborator, client or supplier, requests the issuance of a certificate from SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL. The applicant or subscriber of a Company Member certificate must be in possession of the following documentation:

a) A biometric process will be carried out to validate the identity of the applicant and in the case of foreigners, the passport will be requested; If the validation process is not successful, the request for the identity card will proceed, along with a video of the applicant with a script defined by the certification entity.
b) The certification entity will validate the RUC before the SRI and will store a screenshot of its status, in case the SRI page is not available, the certificate is not granted until the manual validation of the RUC is carried out.

c) Legible copy of the appointment with its due registration when applicable or registration of directives of the company member in the case of Legal Entities.

d) Copy of the constitution, bylaws or creation document, as appropriate, of the requesting Company.
e) Letter of authorization, appointment, or registration of directors when appropriate depending on the case.

6.4.2. Certificate Request Processes

The applicant must contact SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL to manage the request for the certificate, either through the CA's website, in person, or through one of the associated RAs. The RA will provide the applicant with the following information:

- Necessary documentation to present for the processing of your request and to verify the identity of the subscriber.
- Availability to carry out the registration process.
- Information about the issuance and revocation process, the custody of the private key, as well as the responsibilities and conditions of use of the certificate and the device.
- How to access and consult this document and the certification policies.

6.5. Processing of Certificate Requests

6.5.1. Performing identification and authentication functions

It is the responsibility of the RA to reliably carry out the identification and authentication of the subscriber. This process must be carried out prior to the issuance of the certificate.

6.5.2. Approvals or denial of certificate requests

Once the certificate request has been made, the RA must verify the information provided by the applicant, including validation of the subscriber's identity.

If the information is not correct, the AR will deny the request, indicating the reason to the requester. If it is correct, the binding legal instrument will be signed between the subscriber and/or the applicant and SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

6.6. Issuance of Certificates

6.6.1. RA Actions

Once the request is approved, the certificate will be issued, which must be delivered securely to the subscriber.

For the issuance of certificates, the following actions will be carried out:

a) For certificates in hardware support:

- The Linked Third Party will deliver the token.
- Generation of the pair of keys: The generation codes will be generated in the CA.
- The Linked Third Party will deliver one of the generation codes. The second-generation code will be sent to the applicant to the email that has been provided in the application.

b) For Software certificates:

Once the subscriber has received the email notification, they will have to generate their certificate through the indicated portal, filling out the download form with the following information:
ID number
RUC number (only legal person)
Reference number
Password that the subscriber will create at the time of download.

6.6.2. Delivery of the certificate.

When the subscriber has the two generated keys (Authorization Code and Reference Number, for Hardware issue), he will be able to generate the certificate.

a) In Hardware

The two keys must be entered on the web page https://www.securitydata.net.ec and you must follow the procedure described in the Certificate Activation Manual via Hardware. Once the procedure has been carried out, the certificate is issued, the same as You will install the Crypto Device.

b) In Software

Once the subscriber has received the email notification, they will have to generate their certificate through the indicated portal, filling out the download form with the following information:
ID number
RUC number (only legal person)
Reference number
Password that the subscriber will create at the time of download.

6.7. Certificate Acceptance

6.7.1. Form in which the Certificate is accepted

The certificate will be accepted at the time the binding legal instrument between the subscriber and SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL has been signed and the certificate has been delivered in accordance with the procedure selected by the subscriber.

As evidence of acceptance, the contract is signed with the electronic certificate, storing it on the CA's servers and sending a copy to the subscriber by email. The certificate will be considered valid from the date the certificate is issued.

6.7.2. Certificate Publication

Once the certificate has been generated and accepted by the subscriber or signatory, the certificate will be published in the CA's certificate repositories.

6.8. Revocation and Suspension of Certificates

The revocation of a certificate supposes the loss of its validity, and it is irreversible. The suspension supposes the temporary loss of validity of a certificate, and it is reversible.

Revocations and suspensions take effect from the moment they appear published in the CRL.

6.8.1. grounds for revocation

ORA certificate may be revoked due to the following causes:

a) Circumstances that affect 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 relationship of the signatory with the Corporation.

b) Circumstances that affect the security of the private key or certificate:

- Compromise of the private key or of the infrastructure or systems of the CA, if it affects the reliability of the certificates issued from that incident.
- Violation, by the CA or the Linked Third Party of the requirements set forth in the certificate management procedures established 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.
- The 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 forth in this CPS or in the binding legal instrument between SECURITY DATA

SEGURIDAD EN DATOS Y FIRMA DIGITAL and the subscriber.

c) Circumstances that affect the security of the cryptographic device:

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disablement 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 forth in this CPS or in the binding legal instrument between SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL and the subscriber.

d) Circumstances affecting the subscriber:

- Termination of the legal relationship between SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL and the Subscriber.
- Modification or termination of the underlying legal relationship or because that allowed the issuance of the certificate to the signatory.
- Violation by the applicant of the certificate of the pre-established requirements for its application.
- Infringement by the subscriber of his obligations, responsibility and guarantees, established in the corresponding legal instrument or in the CPS.
- The supervening disability, total or partial.
- Due to the death of the subscriber or signatory.

e) other circumstances:

- The suspension of the digital certificate for a period greater 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

6.8.2. Who can Request Revocation

They can request the revocation of a certificate:

- The own subscriber, who must request the revocation of the certificate in case of becoming aware of any of the circumstances before mentioned.
- Any person may request the revocation of a certificate in case of becoming aware of any of the circumstances before mentioned.

They may process the revocation of the certificate:

- The authorized operators of the Linked Third Party to which the subscriber of the certificate belongs.
- The authorized CA operators.
- The are users accessing the administration of your certificate.

6.8.3. Revocation Request Procedures

There are different alternatives for the subscriber when requesting the revocation of the certificate.

In any case, at the time the certificate is suspended or revoked, a communication will be sent to the subscriber, communicating the time of the same.

6.8.3.1 Revocation in office hours

The subscriber or signatory must contact the certifying entity or the Linked Third Party of SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL either via email, in person or by telephone.
If the subscriber or signatory attends personally, it will be authenticated by means of their identity card or passport and the certificate may be immediately revoked, after filling out the revocation request and delivered to the operator of the registration authority, in the event of suspension of the certificate. subscriber can request prior data validation from the AC.
If it is done by telephone at 023922169-026020655-046020655, the certificate will be suspended until the subscriber or signatory appears personally before the Linked Third Party or sends a letter requesting the revocation of the certificate. The certificate will be suspended for a maximum period of 90 days after which it will be revoked. Within these 90 days the applicant or signatory can cancel the suspension and

the revocation procedure.
If you do it via email to soporte@securitydata.net.ec, the certificate will be suspended until the subscriber personally submits to the linked third party or sends a letter requesting the revocation of the certificate, in case the revocation request is signed. Electronically, the definitive revocation is carried out, otherwise the certificate will be suspended for a period of 90 days, after which it will be revoked. Within these 90 days the applicant or signatory can cancel the suspension and the revocation procedure.
Depending on the type of request received, the operator will carry out the respective revocation within the Security Data income portal, which has the revocation option in which it can suspend or revoke the certificate prior to loading the letter delivered by the subscriber, for the different means.
Revocations and suspensions take effect from the moment they appear published in the CRL.

6.8.3.1.1 Suspension criteria

A certificate may be suspended due to the following causes:

a) Circumstances that affect 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 relationship of the signatory with the Corporation.

b) Circumstances that affect the security of the private key or certificate:

- Compromise of the private key or of the infrastructure or systems of the CA, if it affects the reliability of the certificates issued from that incident.
- Violation, by the CA or the Linked Third Party of the requirements set forth in the certificate management procedures established 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.
- The 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 forth in this CPS or in the binding legal instrument between SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL and the subscriber.

c) Circumstances that affect the security of the cryptographic device:

- Compromise or suspected compromise of the security of the cryptographic device.
- Loss or disablement 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 forth in this CPS or in the binding legal instrument between SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL and the subscriber.

d) Circumstances affecting the subscriber:

- Termination of the legal relationship between SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL Digital and the Subscriber.
- Modification or termination of the underlying legal relationship or because that allowed the issuance of the certificate to the signatory.
- Violation by the applicant of the certificate of the pre-established requirements for its application.
- Infringement by the subscriber of his obligations, responsibility and guarantees, established in the corresponding legal instrument or in the CPS.
- The supervening disability, total or partial.
- Due to the death of the subscriber or signatory.

e) other circumstances:

- The suspension of the digital certificate for a period greater 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

6.8.3.1.2. Suspension Lift Criteria

The client will be the only entity authorized to lift the suspension, according to the subscriber's criteria, and it cannot be delegated to a third person, the procedure for suspension or lifting is the same as detailed in point 6.8.3.1 .1

6.8.3.2. Revocation outside of office hours

The customer will request the revocation by email to soporte@securitydata.net.ec, it will be processed the next business day from 9:00 a.m.

6.8.4. The time in which the CA must resolve the Revocation Request

Once the identity of the subscriber has been authenticated as stated above, and the revocation has been duly processed by the Linked Third Party, the revocation will be effective immediately.

6.8.5. Obligation Verification of Revocations by Third Parties

The verification of the status of the certificates is mandatory for each use of the certificates, either by consulting the revocation list (CRL) or the OCSP service.

6.8.6. Issuance sequence of CRLs

The CRL of the end entity certificates are issued at least every 24 hours, or when a revocation occurs.

The CRL of the authority certificates (ARL) is issued every 6 months or when a revocation occurs.

6.8.7. Maximum time between Generation and Publication of CRLs

Since the publication of the CRL is carried out at the moment of its generation, the elapsed time is considered zero or null.

6.8.8. gave Availability of the Online Certificate Status Verification System

Information regarding the status of certificates will be available online 24 hours a day, 7 days a week.

In case of system failure, or any other factor that is not under the control of the AC, it will make every effort to ensure that this information service is not unavailable for longer than the maximum period of 24 hours.

6.8.9. Online Revocation Checking Requirements

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

- I know in any case, you must check the last CRL issued, which can be downloaded from the URL address contained in the certificate itself in the "CRL Distribution Point" extension.
- The user shall additionally check the relevant CRL(s) of the hierarchy's certification chain.
- The user must ensure that the revocation list is signed by the authority that has issued the certificate to be validated.
- The revoked certificates that expire will be removed from the CRL.

6.8.10. Reasons for Suspension

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL may suspend a certificate in the following cases:

- If the compromise of a key is suspected, until this fact is confirmed or denied.
- If the subscriber has incurred in non-payment of his certificate.
- If they do not have all the information necessary to determine the revocation of a certificate.
- Be provided by ARCOTEL, in accordance with the provisions of the Law on Electronic Commerce, electronic signatures and data messages
- I know verify by the information certification entity, falsity in the data consigned by the holder of the certificate.
- I know the breach of the contract between the information certification entity and the owner of the electronic signature occurs.

6.8.11. Who can Request Suspension

They may only carry out the suspension of the certificate:

- The authorized operators of the Linked Third Party to which the subscriber of the certificate belongs.
- The authorized CA operators
- The are users accessing the administration of your certificate.

6.8.12. Limits of the Suspension Period

The limit is established by the client itself or in turn by the validity of the certificate or by what is described in point 6.8.3.1.2.

6.8.12. Circumstances for lifting the suspension

The subscriber is the one who will request the lifting of the suspension prior to 90 days, otherwise the certificate will be revoked.

6.9. Certificate renewal

6.9.1. Renewal of Certificates without Change of Keys

This option is not considered.

6.9.2. Renewal with Change of Keys

Renewal process, which will be carried out in the same way as the issuance of a new certificate, since the subscriber has the public and private key in his possession, for this reason the certification entity does not store said information and a new certificate is issued and therefore, you cannot extend the validity of the certificate without a new issuance of the same.

6.10. Protection of the Private Key and Engineering Controls of the Cryptographic Modules

6.10.1. Standards for Cryptographic Modules

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

The keys of the subscribers of certificates recognized with DSCF and of operators and administrators are generated by the interested party in a secure way using a cryptographic device CC EAL4+, FIPS 140-1 level 3, ITSEC E4 High or another of equivalent level.

The cryptographic devices for the custody of the private key of the subscriber of recognized certificates with DSCF and of the operator or administrator provide a level of security

6.10.2. Multiperson Control (k of n) of the Private Key

Access to the private keys of the CAs requires the simultaneous participation of three different cryptographic devices out of five possible, protected by an access key.

6.10.3. Custody of the Private Key

The root CA's private key is guarded by a FIPS 140-2 level 3 certified hardware cryptographic device, ensuring that the private key is never in the clear outside of the cryptographic device. The activation and use of the private key requires the multi-person control detailed above. After the operation performed, the session is closed, leaving the private key deactivated.

The private keys of the Subordinate CAs are kept in secure cryptographic devices certified with the FIPS 140-2 level 3 standard.

6.10.4. Backup of the Private Key of the CA

There are some devices that allow the CA's private key to be restored, which are stored securely and only accessible by authorized personnel according to trust roles, using at least dual control on a secure physical medium.

The keys of the Root CA can be restored in accordance with what is indicated in the Procedure of Recovery, backup and storage of private keys of the CA.

6.10.5. Subscriber Private Key File

The CA will not file the certificate signing private key after the expiration of its validity period.

The private keys of the internal certificates used by the different components of the CA system 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.

The private keys of the subscribers can be archived by themselves, through the conservation of the signature creation device or other methods, because they may be necessary to decrypt the historical information encrypted with the public key, if the custody device allows the operation.

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

There is a CA key ceremony document that describes the private key generation processes 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.

6.10.7. Private Key Activation Method

The CA Root keys are activated by a process that requires the simultaneous use of 3 out of 5 cryptographic devices (cards). The keys of the Subordinate CAs are activated by a process that requires the use of 1 of 4 cryptographic devices (cards).

Access to the subscriber's private key is done through a PIN or, if applicable, through a fingerprint. The pin device has a protection system against access attempts that block it when an incorrect access code is entered more than six times.

6.10.8. Private Key Deactivation Method

The private key of the certificate subscriber with DSCF will be deactivated once the cryptographic signature creation device is removed from the reading device.

6.10.9. Private Key Destruction Method

The method of destruction must be governed in accordance with what is indicated in the Procedure for Archiving, Access and Destruction of private keys archived by the AC.

6.11. Certificate expiration notification to a subscriber for renewal

Security Data will notify the subscriber of the certificate expiration via email 30 days in advance.

It is up to the subscriber to renew or not the signing certificate.

6.11.1. Notification of the issuance of the certificate by the CA to other entities

Security Data will notify entities, government agencies and private companies of the renewal of a certificate through the Security Data website.

7. REVISIONS

Document: Company Member Certificate Policies								
Revision	**1**	**two**	**3**	**4**	**5**	**6**	**7**	**8**
Publication	01/24/2011	03/31/2011	06/27/2011	09/01/2011	09/26/2011	12/15/2011	02/25/2015	06/25/2019
Author(s)	LV/XC	XC	XC	XC	XC	XC	DC	DC/LV

Review date	02/18/2011	05/16/2011	05/16/2011	09/14/2011			05/03/2011	06/25/2011
Reviewed by	XC	XC	XC	XC	XC	XC	CS	MF
Approved Date	03/02/2011	05/16/2011	08/16/2011	09/15/2011	09/26/2011	12/15/2011	05/03/2015	06/25/2011
Approved by	CS	CS	CS	CS	CS	CS	CS	CS