



CERTIFICATION POLICY ELECTRONIC BILLING

Andes SCD S.A.

2023




	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Table of contents

1. Presentation of the document6

1.1. Name and identification of th document.....6

1.2. References6

1.3. Policy administration7

1.3.1. Organization that manages the document.....7

1.3.2. Contact Person.....7

1.3.3. Policy Approval Procedures.....7

1.3.4. Publication of the document7

1.4. User Community and Applicability7

1.5. Scope of application.....8

1.5.1. Uses of the certificate.....8

1.5.2. Limits on the use of certificates9

1.5.2.1. Limits on the use of certificates in operating systems..... 10

1.5.3. Prohibitions on the use of certificates 10

1.5.4. Minutes and contracts 11

2. Publication and registration of certificates 11

3. Identification and authentication 11

3.1. Names 12

3.1.1. Types of names 12

3.1.2. The need for names to be meaningful..... 13


3.1.3. Anonyms and pseudonyms in names..... 13

3.1.4. Rules for interpreting name formats 13


3.1.5. Singularity of names 13

3.2. Identity Approval..... 13


3.2.1. Method for proving possession of the private key..... 13

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


3.2.2. Authentication of the applicant's identity	13
3.2.3. Unverified Applicant Information.....	16
3.2.4. Response Times.....	16
3.2.5. Identification and authentication for revocation requests.....	16
4. Certificate life cycle and operating procedures	17
4.1. Request for certificates	17
4.1.1. Who can apply for the issuance of a certificate	17
4.1.2. Procedure for requesting a certificate	17
4.1.3 Acceptance of the certificate.....	19
4.1.4. Publication of the certificate by Andes SCD	19
4.1.5. Key pair and use of the certificate.....	19
4.1.5.1. On the part of the subscriber	19
4.1.5.2. By relying users	20
4.2. Renewal of Certificates - Key Pair	20
4.2.1 Renewal of certificate keys.....	20
4.3. Modification of certificates.....	20
4.4 Suspension of Certificates	20
4.5 Revocation of certificates	21
4.6. Replacement of certificates.....	21
4.7. Certificate status services	22
4.8. Validity of certificates	22
5. Security controls	22
6. Technical safety controls	23
6.1. Key generation and installation.....	23
6.1.1. Key Pair Generation	23

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

6.1.2. Delivery of the private key to the subscriber	23
6.1.3. Delivery of the public key to the certificate issuer	23
6.1.4. Subscriber Public Key Distribution	23
6.1.5. Distribution of the Andes SCD Public Key to Users	24
6.1.6. Period of use of the private key	24
6.1.7. Size of keys.....	24
6.2. Private Key Protection Controls	24
6.3. Supported Cryptographic Devices	25
6.3.1. Associated risks	26
6.4. Other key pair management issues	27
6.4.1. Public Key File	27
6.4.2. Certificate operational periods and key pair usage periods.....	27
6.5. Activation data	28
6.5.1. Generation of Activation and Installation Data.....	28
6.5.2. Protection of activation data.....	28
6.6. Informatic security controls	28
6.7 CA and RA Termination.....	28
7. Certificate, CRL and OCSP Profiles	28
7.1. Contents of the certificate	28
7.2. Certificate profiles	30
7.2.1. Version number.....	30
7.2.2. Certificate Extensions	30
7.2.3. Algorithm Object Identifiers	31
7.2.4. Name formats.....	31
7.2.5. Name restrictions.....	31


	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

7.2.6. Identifying object of the certification policy	31
7.2.7. Syntax and semantics of policy qualifiers	31
7.3. Profile CRL	32
7.3.1. Version number	32
7.3.2. CRLs and extensions	32
7.4. Profile OCSP	33
7.4.1. Version Number	33
7.4.2. Extensiones OCSP	33
8. Audit and other valuations	33
9. Business and legal matters	33
9.1. Rates	33
9.2. Financial responsibility	33
9.3. Confidentiality of information	34
9.4. Intellectual property rights	34
9.5. Rights and duties	34
9.5.1. Rights and duties of ANDES SCD	34
9.5.2. Applicant's Rights and Duties	34
9.5.3. Subscriber Rights and Duties	34
9.5.4. Subscriber Prohibitions:	34
9.6. Principle of Impartiality	35
9.7. Limitations of liability	35
9.8. Indemnifications	35
9.9. Term and termination	35
9.10. Specification change procedure	35
9.11. Dispute prevention	35

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

9.12. Applicable Law and Compliance with Applicable Law..... 35

10. Change control..... 35

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Introduction

This Policy for Electronic Billing complements the provisions established in the Certification Practices Statement and specifically expresses the set of rules defined by the Andes SCD Certification Authority for the application of certificates of Electronic Billing to a community, the uses that can be given to this type of certificate and the technical, legal and security requirements for its issuance and revocation.

It is recommended to read this document before requesting a Certificate of electronic billing or make use of it for verification of electronic signatures in order to know the scope and legal effects associated with the use of this type of certificate.

1. Presentation of the document


1.1. Name and identification of th document

Document	CERTIFICATION POLICY ELECTRONIC BILLING
Description	The certificate for electronic billing issuer accredits the identity of the subscriber and his condition as electronic invoicing agent, and allows the subscriber to sign documents digitally in the capacity accredited by his certificate.
OID	1.3.6.1.4.1.31304.1.2.5.5.0
Version	V 5.0
Date of issue	April 14th , 2023
Location	https://www.andesscd.com.co/docs/cp_electronicbilling.pdf

1.2. References

The development of the content of the Certification Policies and the Certification Practices Statement is issued taking into account the recommendations of the (Request for comments) RFC 3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework and the following European standards:

- ETSI EN 319 411-2: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 411-1: Policy Requirements for certification authorities issuing public key certificates.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

1.3. Policy administration

The content of this Certification Policy is managed by the Policy and Security committee in charge of its development, registration, maintenance and updating. Below are the details of the policy and security committee and a contact person available to answer questions regarding this document.

1.3.1. Organization that manages the document

Name : Policy and Security Committee
Address : Calle 26 #69c-03 Torre B oficina 701.
Email : comite.politicas.seguridad@andesscd.com.co
Telephone : PBX 601 745 6884

1.3.2. Contact Person

company's business name: Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Name : Sandra Cecilia Restrepo Martínez – Gerente General
Address : Calle 26 #69c-03 Torre B oficina 701.
Email : info@andesscd.com.co
Teèlphone : PBX 601 745 6884

1.3.3. Policy Approval Procedures


Policy is managed by the Policy and Security Committee and is approved by Andes SCD's General Management, following the documented information procedure.

1.3.4. Publication of the document

The electronic billing Certification Policies and the Certification Practices Statement are public documents available on the Andes SCD website. Any modification to these documents is published immediately and a version history is maintained.

1.4. User Community and Applicability

Electronic billing certificates are issued to natural persons or legal entities, accrediting the identity of the holder and its status as Electronic Biller in the signing of electronic documents, guaranteeing the authenticity of the issuer of the communication, the non-repudiation of the origin and the integrity of the content.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Certificación authority (CA)

Andes SCD Certification Authority is the entity that acts as a trusted third party between the subscriber and users in the electronic environment and is responsible for issuing and managing digital certificates for electronic billing in accordance with this Certification Policy. The Certification Practices Statement details the hierarchy of the Certification Authorities that make up Andes SCD.

Registration authority (RA)

The Registration Authorities are the entities delegated by the Andes SCD Certification Authority to manage requests for issuance, corroborate the identity of applicants and perform complete registration of applicants wishing to acquire a digital certificate in accordance with this Certification Policy.

Subscribers

The subscriber is the Natural Person or Legal legal person that has acquired an electronic invoice issuer certificate issued by the Andes SCD Certification Authority to operate in the electronic environment as an electronic biller. It is considered a subscriber if such certificate is in force.

Applicants

The applicant is the Natural Person or Legal Entity that wishes to access digital certification services by acquiring a certificate for electronic invoice issuer issued by Andes SCD.


Users:

The user is any person who voluntarily places his trust in the Electronic Billing certificates issued by the Andes SCD Certification Authority and uses the certification service to certify the authenticity and integrity of a document signed by a third party.

1.5. Scope of application

1.5.1. Uses of the certificate

The Certificate of Electronic Billing issued under this policy may be used for the following purposes:

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Identity authentication

The certificate can be used to identify the electronic biller in the scope of its activity, only with the digital signature of the electronic invoices that it issues, in compliance with its obligations established in Decree 2242 of 2015, which regulates the conditions of issuance and interoperability of electronic invoices for purposes of massification and fiscal control.

Digital signature

Digital signatures made with legal person certificates provide the means of support by guaranteeing the authenticity of the origin, the integrity of the signed data and non-repudiation.


- **Authenticity of origin:** In an electronic communication, the subscriber can validly prove his identity to another person by demonstrating possession of the private key associated with the respective public key contained in the certificate
- **Document integrity:** There is a guarantee that the document was not altered or modified after it was signed by the subscriber since the summary of the document is encrypted with the private key of the issuer who is the only one in possession of it.
- **No repudiation:** It prevents the issuer of the signed document from denying at any given time the authorship or integrity of the document, since the signature through the digital certificate can prove the identity of the issuer without the latter being able to repudiate it.

Encryption of information

It is the process of transforming information to make it incomprehensible to all but the intended recipient.

1.5.2. Limits on the use of certificates

The certificates for Electronic Billing issuer can only be used for the digital signature of electronic invoices (XML), their graphic representation (PDF) and the electronic payroll payment supports and the adjustment notes of the electronic payroll payment support document issued by the subscriber.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

1.5.2.1. Limits on the use of certificates in operating systems

For the use of the certificate, please note the following delivery methods:

- Virtual Token:

To use the virtual token you must have Windows XP service pack 2 and above; for MacOs it is required to use the online signature service provided by Andes SCD through our website.


- Physical Token:

For the use of the physical token it is indispensable to have the Windows seven service pack 2 operating system or higher; for MacOs operating system you must have the Monterrey 12.0.1 version and higher, as well as an Intel processor, to guarantee its operation.

1.5.3. Prohibitions on the use of certificates

The performance of unauthorized operations according to this Certification Policy, by third parties or subscribers of the service will exempt the Andes SCD Certification Authority from any liability for this prohibited use.

- The use of the Electronic Billing certificate to sign other certificates or revocation lists (CRL) is not allowed.
- It is forbidden to use the certificate for uses other than those stipulated in the section "Permitted uses of the certificate" and "Limits of use of certificates" of this Certification Policy.
- Alterations to certificates are not allowed and the certificate must be used as supplied by the Andes SCD Certification Authority.
- The use of certificates in control systems or systems intolerant to failures that may cause personal or environmental damage is prohibited.
- Any action that violates the provisions, obligations and requirements stipulated in this Certification Policy is considered prohibited.
- It is not possible for Andes SCD to issue any assessment on the content of the documents signed by the subscriber, therefore, the responsibility for the content of the message is the sole responsibility of the signatory.
- It is not possible for Andes SCD to recover the encrypted data in case of loss of the Subscriber's private key because the CA for security reasons does not keep a copy of the Subscriber's private key, therefore, it is the responsibility of the Subscriber to use data encryption.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

1.5.4. Minutes and contracts

By registering the certificate issuance request, the subscriber declares that he/she is aware of and accepts the terms and conditions of the service described on the Website.

No explicit confirmation by the subscriber is required to accept the terms and conditions of service. It is considered that the terms and conditions of service are accepted at the moment the request is registered.

Once the digital signature certificate is issued, ANDES SCD will deliver by e-mail to the subscriber a notification with the information of interest to manage the life cycle of the certificate. This notification contains at least the following information:


- a) Type of certificate
- b) PC OID reference
- c) Certificate Serial
- d) Beginning of validity
- e) End of validity
- f) Certificate holder
- g) Entity
- h) Certificate delivery form
- i) Revocation Code

2. Publication and registration of certificates

All system data related to the life cycle of the certificates are kept in digital form for the period established by current legislation when applicable. Current and expired certificates are kept published in LDAP in accordance with RFC 4523.

3. Identification and authentication

The following describes the procedures and criteria applied to verify the identity of the applicant and approve the issuance of a certificate Electronic Billing.


	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

3.1. Names

3.1.1. Types of names

The Electronic Billing certificates have a section called Subject whose purpose is to identify the certificate holder or subscriber. This section contains a DN or distinguished name characterized by a set of attributes that make up an unequivocal and unique name for each subscriber of the certificates issued by Andes SCD.

Abrev	Name	Legal Person Electronic Billing	Natural Person Electronic Billing
CN	<u>Name</u>	Company name of the legal person	Company name of the natural person
S	<u>Serial</u>	identification number + dv	identification number + dv
E	<u>Email</u>	email address	email address
C	<u>Country</u>	Abbreviation for the country	Abbreviation for the country
ST	<u>Department</u>	Name of the department	Name of the department
L	<u>City</u>	Name of the municipality	Name of the municipality
STREET	<u>Address</u>	Address where the legal person resides	Address where products or services are offered
T	<u>Title</u>	Electronic billing Issuer - Legal Person	Electronic billing Issuer - Natural Person
O	<u>Organization</u>	Name of branch or unit using the certificate	Name of organization in charge of the natural person offering products or services
<u>OU</u>	<u>Organizational Unit</u>	Issued by Andes SCD Calle 26 #69c-03 Torre B office 701.	Issued by Andes SCD Calle 26 #69c-03 Torre B office 701.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

3.1.2. The need for names to be meaningful

The main characteristic of every certificate of electronic billing issued by Andes SCD is the full identification of the subscriber and the assignment of a meaningful name to the certificate.

3.1.3. Anonyms and pseudonyms in names

This Certificate Policy does not allow anonymous or pseudonyms to identify the name of a electronic billing.

The name of the Electronic Billing must be the corporate name that appears in the RUT, legal personality or equivalent document, abbreviated names or acronyms are not accepted. The name of the natural person must be made up of the first and last names as they appear on the citizenship card or equivalent identification document.

3.1.4. Rules for interpreting name formats

The rules for interpreting name formats follow the X.500 reference standard in ISO/IEC 9594.

3.1.5. Singularity of names

It is guaranteed that the distinguished names of the electronic billing certificates are unique for each subscriber because they contain serial and email attributes that allow distinguishing between 2 identities when there are problems of duplicity of names.

3.2. Identity Approval


3.2.1. Method for proving possession of the private key

The Andes SCD Certification Practices Statement details the procedure used by the Certification Authority to demonstrate that the applicant holds the private key corresponding to the public key to be bound to the Electronic billing certificate.

3.2.2. Authentication of the applicant's identity

The applicant can process his request for the issuance of electronic billing certificate in one of the following ways:

1. **In person:** The applicant makes the application in person before the Andes SCD Registration Authority.


	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

2. **Remote:** The applicant makes the application from the Andes SCD WEB site.
3. **Outsourcing:** Requests for issuance of certificates through agreements are processed by a coordinator designated by the entity or company, according to the internal procedures defined by the registration authority.

Requirements
Digital evidence provided by the applicant or by an authorized third party to verify the identity of the electronic biller (Invoice Issuer).

In all applications the ECD will perform identity validation using the mechanisms at its disposal. The following is a description of the documentary requirements:

Requirement	In-person application	Remote request	Outsourcing request	Natural person	Legal person
Citizenship card or document that proves the identity (Enlarged to 150% and legible)	Present original and photocopy of document	Scanned document required	Scanned document required	X	X
RUT or equivalent document evidencing identification of the entity (Complete and legible document, it is optional if you present a chamber of commerce.)	Present original and photocopy of document	Digital PDF document required	Digital PDF document required	X	X
Chamber of Commerce document evidencing	Present photocopy of document	Digital PDF document required			

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

legal representation of the entity (Complete and legible document)			Not applicable	Not applicable	X
--	--	--	----------------	----------------	---

Note: The above documents may be optional if ANDES SCD can rectify the integrity and reliability of the information, otherwise the Registration Authority is empowered to request the corresponding documentary supports.


Face-to-face requests will be registered through the Andes SCD website by the Customer Service area.

In the case of applications processed by outsourcing, other documents or digital evidence may be accepted to verify the identity of the persons and prove their relationship as a public official.

Additionally, the applicant must provide the following information that will allow Andes SCD to contact him/her when necessary

Requirement	Additional information
1	Country, department and city of residence
2	Address and telephone number
3	Personal e-mail

The information provided in the request for issuance of legal person certificate is studied by the supervisor who is responsible for verifying that the information is original, sufficient, and adequate according to the internal procedures defined by Andes SCD.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

If the applicant claims the modification of personal data with respect to those contained in the identification document presented, he/she must show the corresponding civil registry certificate where the variation appears.

The CPS also specifies the aspects relevant to the authentication of applicants and subscribers in the section on Identity Authentication.

3.2.3. Unverified Applicant Information

The registration authority verifies all the applicant's information that is backed up with supporting documents or digital evidence. Residence address and e-mail address are not verified, presuming the good faith of the information provided by the applicant.

3.2.4. Response Times


The deadline for processing an application by the ANDES SCD RA is from one to two business days from the moment of receiving the documentation, complete information, and confirmation from the entity where the applicant is linked. In case of inconsistencies with the documentation provided or identity validation, the RA agents will send an email with a link for the applicant to update the required information or documentation, if after 3 business days from the sending of the notification the update has not been generated and if it is impossible to contact the applicant, the application may be rejected and the applicant must register a new application attaching the corresponding documentation.

When the delivery format is a physical token, the delivery time of the digital certificate after issuance depends on the destination, for major cities the delivery time will be 1 to 2 business days, for other national destinations the delivery time will be 2 to 3 business days, for special destinations or if it is impossible to contact the subscriber the delivery time may take up to 5 business days.

3.2.5. Identification and authentication for revocation requests

The following persons are allowed to request the revocation of a certificate:

- To the subscriber himself, in which case he must use the revocation code given to him at the time of acquiring the certificate.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

- To the authorized representative of the entity to which the subscriber is linked, in which case he/she must formally notify Andes SCD in writing the reason for requesting the revocation of the Legal Representative certificate issued to the subscriber.

- The authorized operators of Andes SCD or the certification hierarchy may revoke any certificate in those cases in which the circumstances established in the Certification Practices Statement are incurred

4. Certificate life cycle and operating procedures

The electronic billing certificates issued by Andes SCD have an explicit validity period in the "valid from" and "valid until" attributes of the certificate itself. The period of validity of the certificate may not exceed 730 calendar days.

At the end of the validity period, the certificate becomes invalid and permanently ceases to operate and the certification service between Andes SCD and the subscriber is terminated.

4.1. Request for certificates

The Andes SCD Certification Authority ensures that the subscribers have been fully identified and that the certificate request is complete.

4.1.1. Who can apply for the issuance of a certificate


The request for the issuance of a digital certificate can be made by a natural person of legal age who is in full capacity to assume the obligations and responsibilities inherent to the possession and use of the certificate and who demonstrates any of the following situations:

- a. It is the legal representative of a Legal person
- b. It is the owner of a commercial establishment
- c. It is the representative of an organization that offers services


4.1.2. Procedure for requesting a certificate

The procedure to be followed by the applicant to acquire a digital certificate is described as follows.

#	Activity	Detail	Responsible
1	Generate key pair	Generate the key pair and obtain the CSR containing the public key	Applicants

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		and implicitly signed by the associated private key.	
2	Process application	<p>enter platform or web service provided by Andes:</p> <ol style="list-style-type: none"> 1 Define the type of certificate "Electronic Invoice Issuer". 2 Provide the required documentation or evidence. 3 Register the electronic biller information. 4 Establish the effective date of the certificate and the period of validity, 5 Supply CSR containing the public key and implicitly signed by the associated private key 6 Accept terms and conditions 7 Register the application and receive email with instructions 	Applicants
3	Study application	<p>Verify the application information and determine whether to recommend issuance of the certificate or reject the application</p> <ul style="list-style-type: none"> - If the application is rejected, an e-mail is sent to the applicant indicating the reasons for the rejection of the application and the process ends - If the application is recommended, the next step of this procedure continues. 	RA Supervisor Andes SCD
4	Issue the certificate	<p>Verify the approved certificate issuance request and give the order to generate the certificate - ANDES SCD verifies that the private key is in the subscriber's possession by verifying the SIGNATURE using the</p>	Andes SCD CA Operator

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		public key sent in the PKCS10 certificate request. - Generate the digital certificate - Notify certificate issuance to the subscriber	
--	--	---	--

4.1.3 Acceptance of the certificate.

The procedure for certificate acceptance is described in the Certification Practices Statement, see certificate acceptance section.

4.1.4. Publication of the certificate by Andes SCD

Once the certificate has been issued by Andes SCD, it is published in the certificate directory.

4.1.5. Key pair and use of the certificate

4.1.5.1. On the part of the subscriber

The subscriber has a public key and a private key legally valid during the period of validity of the Certificate of Electronic Billing that legitimizes them. The private key is for the exclusive use of the subscriber for the purposes stipulated in this Certification Policy and must be protected to prevent unauthorized use by third parties.


The subscriber can only use the certificate and the key pair after accepting the conditions of use established in the CPS and in the present CP and only for what they establish.

Once the certificate has expired or is revoked, the subscriber is obliged not to use the private key again

The subscriber can only use the private key and the certificate for the authorized uses on the PC and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate.

The key pair associated with the end-entity certificates issued by Andes SCD has the following enabled uses:

- Digital signature
- Certificate signature
- CRL signatura

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

The key pair associated with Andes SCD's subordinate CA certificates has the following enabled uses:

- Digital signature
- Certificate signature
- CRL signature

4.1.5.2. By relying users

Users relying on Andes SCD's certification service must verify the uses established in the 'Key usage' field of the certificate or in this Certification Policy to know the scope of application of the Electronic Billing certificate.

Users who trust Andes SCD's certification service must assume the responsibility of verifying the status of the certificate before placing their trust in it.

4.2. Renewal of Certificates - Key Pair

Andes SCD does not have a certificate renewal process. If the subscriber wishes to obtain a new certificate, he/she must request the issuance of a certificate when his/her original certificate has expired.

4.2.1 Renewal of certificate keys


The subscriber may renew the certificate with a new key pair by requesting the issuance of the certificate when it has expired or has been revoked.

4.3. Modification of certificates

Digital certificates issued by Andes SCD cannot be modified. Any modification to the content of the certificates implies the revocation and issuance of a new certificate, which will be subject to an application and verification process, complying with the requirements established in this certification policy.

4.4 Suspension of Certificates

Digital certificates issued by ANDES SCD cannot be suspended. Any suspension on the status of the certificate implies the revocation and issuance of a new certificate which will be subject to application and verification process complying with the requirements established in this certification policy.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

4.5 Revocation of certificates

Revocation consists of the loss of reliability of the certificate and the permanent cessation of its operability, preventing its use by the subscriber; once the certificate is revoked, the Certification Authority includes it in the CRL in order to notify third parties that a certificate has been revoked at the time verification of the certificate is requested.

ANDES SCD, publishes the CRL every 24 hours, the last CRL issued for each CA contains all the certificates issued by the respective CA that are revoked as of the CRL generation date. The user is recommended to check the date of the CRL to verify that it is the most recently issued CRL.

Certificates that are revoked will not be able to return to active status under any circumstances, as this is a definitive action.


Revocation of an Electronic Billing certificate may be requested by the Subscriber who holds the certificate through the means of revocation provided by Andes SCD in the "means to revoke certificates" section of the CPS and by following the revocation procedure specified in the "Procedure to revoke certificates" section of the CPS. Additionally, Andes SCD or any of its component authorities may request the revocation of a Electronic Billing certificate if it becomes aware of or suspects the compromise of the Subscriber's private key or any other determining fact that requires it to proceed to revoke the certificate.

The Certification Practices Statement details the circumstances under which a digital certificate is revoked, the means available to perform the revocation, the procedure to revoke a certificate, the time it takes Andes SCD to process the revocation request and to publish the revoked certificates in the CRL.

4.6. Replacement of certificates

The replacement of a certificate is the procedure where a digital signature certificate is replaced at the request of the entity/subscriber who has acquired it for any of the following reasons:

- Loss of Token device
- Loss or exposure of certificate PIN

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

- Change of certificate holder's information, except for the identification number

Andes SCD has established the following conditions for the replacement of a certificate:

- The certificate must have an initial validity equal to or greater than 1 year.
- The certificate must have a remaining validity of more than 6 months.
- The certificate must not have been previously replaced
- Communicate the reason for the replacement
- The replacement applies to request the same type of certificate initially purchased.

The procedure to request the replacement of a certificate consists of the following procedures.

- Certificate revocation.
- Certificate issuance request.

The subscriber must follow the two procedures mentioned above, complying with the conditions established by Andes SCD and informing the reason for the replacement formally in the application.

4.7. Certificate status services

The Certification Practices Statement provides information on the means to publish the status of issued certificates, the availability of the service and the end of subscription to the certification service.


4.8. Validity of certificates

The validity period of the digital certificates of Electronic Billing is explicit in the certificate itself in the attributes "Valid From" and "Valid To" and will not be greater than 730 calendar days.

The key pair has the same validity period of the digital certificate that endorses them.

5. Security controls

The systems and equipment used by ANDES SCD to offer the certification service are physically located in a Data Center designed with specifications with the strictest construction standards and following rigorous operating standards to ensure that the

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

equipment and information housed therein have the highest level of security and availability. In the event of an incident with its main Data Center, ANDES SCD has an alternate data center with optimal security mechanisms to ensure continuity in the provision of services.

The technological infrastructure that supports the certification services is continuously monitored through a NOC/SOC to identify any type of alert or incident that may compromise the security or availability in the provision of services.

Other procedural, physical security and personal security controls are specified in the Andes SCD Certification Practices Statement.

6. Technical safety controls

6.1. Key generation and installation

The public and private keys of certificate holders of Electronic Billing issuer certificates are generated by the subscriber himself. For the issuance of the certificate, the respective CSR must be provided to Andes SCD.

6.1.1. Key Pair Generation

Not applicable because the private key is never known by ANDES SCD. The private key is generated by the subscriber himself.

6.1.2. Delivery of the private key to the subscriber


The delivery of the subscriber's public key to ANDES SCD is done by registering the certificate issuance request with delivery form "PKCS10" from the platform or web service, where the subscriber binds the CSR that contains the public key and is implicitly signed by the associated private key.

6.1.3. Delivery of the public key to the certificate issuer

The mechanism of delivery of the public key to holders of the Electronic Billing certificates is described in the CPS in the section "delivery of the public key to the issuer of the certificate.

6.1.4. Subscriber Public Key Distribution

The public key of any Electronic Billing Certificate subscriber is permanently available for download in the Andes SCD certificate directory if the certificate is not revoked.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

6.1.5. Distribution of the Andes SCD Public Key to Users

The public key of the Andes Root CA, the CA issuing Class II or end-entity certificates and the CA issuing Class III or end-entity certificates are permanently available for download on the Andes SCD website.

6.1.6. Period of use of the private key

The period of use of the private key is the same as the period of validity of the Electronic Billing certificate or less if the certificate is revoked before expiration. The Andes SCD CPS details the period of use of the private key of the root CA and the subordinate CAs issuing end-entity certificates.

6.1.7. Size of keys


The minimum size of keys the Electronic Billing certificates is 2048 bits based on the RSA algorithm.

The size of the certified keys of the issuing CA of the natural person certificates is 4096 bits long based on the RSA algorithm.

6.2. Private Key Protection Controls

The Andes SCD Certification Practices Statement specifies the controls and standards for the cryptographic modules, control, backup, storage, activation, deactivation and destruction of the Certification Authority's private keys.

The subscriber's private key protection controls are specified below.


	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Protection control	Private key generated by subscriber from CSR device
<u>Private key backup</u>	Andes SCD does not back up subscribers' private keys when the certificate is generated from CSR. Andes SCD is never in possession of these keys and they only remain in the subscriber's custody..
<u>Private key storage</u>	Subscribers' private keys are not stored by Andes SCD. The private key must be stored by the subscriber himself because they may be needed to decrypt the historical information encrypted with the public key.
<u>Private key transfer</u>	The private key generated by the user who delivers the CSR for certificate generation is kept by the subscriber and is never sent to Andes SCD.
<u>Private key activation</u>	The protection of the activation data is the responsibility of the subscriber
<u>disabling of the private key</u>	Deactivation of the private key is the responsibility of the subscriber.
<u>Private key destruction</u>	Destruction of the subscriber's private key can be performed by the subscriber himself by deleting the private key corresponding to the CSR sent to Andes SCD.

6.3. Supported Cryptographic Devices

The cryptographic devices supported by ANDES SCD must comply with the following characteristics:

- Generates RSA key pairs up to 2048 bits.
- Algorithms for RSA, DES, 3DES, MD5 and SHA-256 generation implemented by hardware.
- Random number generator hardware.
- Digital signature generator hardware.
- Minimum available space of 64 Kb..
- FIPS 140-2 Level 3 certification
- CE and FCC certification.
- Full support for PKI applications.
- Compatible with CAPI and PKCS#11 interfaces
- Support for multiple key storage.
- Support for X.509 V3 standard certificate format.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

6.3.1. Associated risks

Cryptographic devices supported by ANDES SCD may present risks such as:

- Loss of the device
- Compromise of the key
- Damage due to improper handling or environmental conditions.
- Damage due to voltage variations.

To mitigate the associated risks, safety standards must be taken into account:

- The PIN is confidential, personal and non-transferable.
- It is recommended to change the PIN periodically.
- Cryptographic devices should be kept in appropriate environmental conditions away from humidity.
- In case of compromise or loss of the private key, revocation of the certificate should be requested.

6.3.1.1. Risks associated with certificates issued in cryptographic device

Cryptographic devices supported by ANDES SCD may present risks such as


- Device loss
- Key compromise
- Damage due to improper handling or environmental conditions.
- Damage due to voltage variations.

To mitigate the associated risks, security standards must be taken into account:

- The PIN is confidential, personal and non-transferable.
- It is recommended to change the PIN periodically.
- Cryptographic devices should be kept in appropriate environmental conditions away from humidity.
- In case of compromise or loss of the private key, revocation of the certificate should be requested.

6.3.1.2. Risks associated with software-issued certificates (PKSC10)

Risk	Description	Recommendation
Improper use of the certificate by the subscriber	In case of using the signature in a certificate of a different nature, it will lose its legal	The use of the certificate must be exclusive for the nature and scope for which it is requested;

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

	validity and the right to non-repudiation.	which is specified in the certificate's CP.
Inadequate safekeeping of the private key of certificates issued from a PKCS10 request.	Loss of certificate reliability (by copying or risk of impersonation).	Store in a secure location for subscriber access only
Private key compromise	Access to the private key by malicious third parties	Use of ANDES SCD recommended software (CSR Generator Software AND PFX Generator Software). Store in a secure location for exclusive subscriber access. Protect your key with a password that only you have access Use a secure Keystore for safekeeping of your private key.

Note: Remember that once the certificate is generated and delivered, the applicant will verify with the appropriate mechanisms to determine that it corresponds to the request made in the PKCS# 10 format.


6.4. Other key pair management issues

6.4.1. Public Key File

Andes SCD keeps on file all digital certificates of Electronic Billing, which include the public key for the period stipulated in the "public key file" section of the CPS.

6.4.2. Certificate operational periods and key pair usage periods

The life time of the certificate of Electronic Billing is governed by the validity of the certificate or as long as its revocation is not explicitly stated in a CRL or in the

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

online verification system. If any of these events occur, the certificate's validity is terminated and it can only be used for historical verification purposes.

The key pair is valid if there is a valid Electronic Billing certificate to support it. Once the certificate is no longer valid the keys lose all legal validity and their use is limited to personal purposes only.

6.5. Activation data

6.5.1. Generation of Activation and Installation Data

The PIN or activation data for the use of the private key must be generated by the subscriber.

6.5.2. Protection of activation data

The PIN or activation data of the TOKEN must be personalized by the applicant before generating the key pair or if there is a suspicion that a third party knows this data.

To change the PIN it is necessary to download the software application offered by the TOKEN manufacturer and available on the Andes SCD website.

6.6. Informatic security controls

The Certification Practices Statement describes Andes SCD's controls for the proper safeguarding of IT resources.


6.7 CA and RA Termination

The Certification Practice Statement describes the procedures for notification and termination of the CA or RA


7. Certificate, CRL and OCSP Profiles

7.1. Contents of the certificate

Electronic Billing Certificate Form		
Field	Description	Value
Version	Certificate version	V3
Serial number	Number identifying the certificate	Subscriber's certificate serial number

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Signature algorithm	Algorithm used by Andes SCD to sign the certificate	SHA256WithRSA
Signature hash algorithm	Algorithm used to obtain the data summary	Sha256
(issuer)	Data of the end-entity subordinate CA that issued the certificate.	See in the certificate the data of the Class II CA or the Subordinate CA of the Class III CA.
Valid from	Date and time UTC start validity	Start date of validity of the certificate
Valid until	Date and time UTC end of validity	End date of certificate validity
Subject	CN	See section 3.1.1 of this document for the value of each attribute of the subject, which may vary if the issuer of the electronic invoice is a Legal Entity or a Natural Person.
	T	
	Serial Number	
	E	
	C	
	ST	
	L	
	STREET	
Public key	Certificate holder's public key	RSA (2048 Bits)
Extensions	Extensions used in certificates	See "Certificate Extensions" section of this document for more details.
Identification algorithm	Algorithm used to obtain the fingerprint of the certificate	Sha1
Digital fingerprint	The synthesis or fingerprinting of the certificate data	Digital fingerprint
Use of the key	Purposes for which the certificate is to be used.	Digital Signature Non-repudiation Encryption of information

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

7.2. Certificate profiles


7.2.1. Version number

Electronic Billing certificates issued under this policy are compliant with the X.509 V3 standard and in accordance with RFC 5280 for certificate profiles and CRLs.

7.2.2. Certificate Extensions

Electronic Billing certificates issued by Andes SCD use a series of extensions that are intended to establish the uses of the certificate, reference the applicable Certification Policies and additional restrictions. The following are the extensions included in the digital certificates of Electronic Billing.

Extensions Certificates Electronic Billing according to standard X.509V3	
Name	Value
Access to the issuing entity's information	Access method = Online certificate status protocol URL address =http://ocsp.andesscd.com.co
Holder's key identifier	Holder's key identifier
Issuing entity key identifier	Andes SCD CA key identifier that issued the certificate
CRL distribution points	CRL publishing URL of the CA that issued the certificate.
Use of the key	Digital Signature Non-repudiation Encryption of information
Improved use of the key	Customer authentication Secure Mail
Alternate Name of Holder	Subscriber's email RFC 822 Name (e-mail address)
Basic Restrictions	Type of case = Final entity Route length restriction = None
Certificate Directive	[1] Certificate Directive: Policy Identifier =1.3.6.1.4.1.31304.1.2.5.7.0 [1,1] Policy certifier information: Id. of directive certifier =User notice Certifier:

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

	<p>Warning text = The use of this certificate is subject to the Certificate of Electronic Billing Policies (PC) and Certification Practices (CPS) established by Andes SCD.</p> <p>[1,2] Policy certifier information: Id. of directive certifier =CPS Certifier: Current CPS URL</p>
--	--

7.2.3. Algorithm Object Identifiers

The digital certificates of Electronic Billing issued under this policy use the following algorithms and their corresponding identifiers (OID)

- OID of the signature algorithm SHA256withRSAEncryption 1.2.840.113549.1.1.11
- OID of the public key algorithm RSAEncryption 1.2.840.113549.1.1.1

7.2.4. Name formats

Digital Certificates of ac issued by Andes SCD are restricted to X.500 'Distinguished names' (DN) which are unique and unambiguous, the certificates contain the DN of the issuer and subscriber of the certificate in the issuer name and subject name fields respectively.

7.2.5. Name restrictions

Digital certificates issued under this policy have DNs in accordance with X.500 recommendations that are unique and unambiguous.


7.2.6. Identifying object of the certification policy

Certification policies and practices are identified by a unique number called an OID, the OID assigned to this policy is 1.3.6.1.4.1.31304.1.2.5.5.0.

More information on this subject can be found in the Certification Practices Statement in the object identifier section of the certification policy.

7.2.7. Syntax and semantics of policy qualifiers

The certificate extension referring to the qualifiers of the Certification Policy contains the following information:

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

- **Policy identifier:** Contains the Certificate Policy identifier Electronic Billing
- **CPS:** Indicates the URL where the Certification Practice Statement (CPD) is published for consultation by users
- **User Notice:** contains the text "The use of this certificate is subject to the CPS Academic Community CPS established by Andes SCD". Accreditation Code 16 -ECD-004.

7.3. Profile CRL


7.3.1. Version number

The CRLs issued by Andes SCD correspond to the X.509 version 2 standard.

7.3.2. CRLs and extensions

The CRL revocation list is issued according to RFC 2459

CRL profile according to standard X.509V2 – CRL		
Name	Description	Value
Version	CRL version	V2
CRL Number	Unique number of CRL	Identified CRL
Issuer	Data of the end-entity subordinate CA that issued the CRL	View in the CRL the data of the CA that issued the CRL
Signature algorithm	Algorithm used for CRL signature	SHA256withRSA
Effective date of issue	Validity period after issuance of the CRL	Date of issuance of the CRL in CUT time
Next update	Date on which the next CRL will be issued	Date of issue of the next CRL in UTC time
Issue distribution points	URL where CRLs issued by Andes SCD are published.	View the publication URL in the CRL
Revoked certificates	List of revoked certificates specifying the serial number, date of revocation and reason for revocation	

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

7.4. Profile OCSP

7.4.1. Version Number

The OCSP certificate is issued in accordance with the standard X,509 V3

7.4.2. Extensiones OCSP

OCSP extensions according to standard X.509V3	
Name	Value
Basic Constraints, critical	CA false
Key Usage critical	Digital signature
Extended Key Usage	OCSPSigner
Subject Key Identifier	key identifier

8. Audit and other valuations

Information about the audit and other assessments is specified in the Andes SCD Certification Practices Statement.

9. Business and legal matters

9.1. Rates


The rates indicated here are reference values and may vary according to special commercial agreements signed with clients, entities or applicants, or in the development of promotional campaigns carried out by ANDES SCD.

Delivery format	3 months	6 months	1 months	2 months
Virtual Token	\$ 57,857	\$ 92,571	\$ 135,000	\$ 200,000
Physical token	N/A	\$ 96,639	\$ 150,000	\$ 220,000

The above prices are per unit and include VAT (19%).

9.2. Financial responsibility

Andes SCD's Certification Practices Statement specifies the value of the coverage to indemnify for damages that may be caused using certificates issued by Andes SCD.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

9.3. Confidentiality of information

As stipulated in the Andes SCD Certification Practices Statement

9.4. Intellectual property rights

As stipulated in the Andes SCD Certification Practices Statement

9.5. Rights and duties

The Certification Practices Statement lists the rights and duties of the Andes SCD Certification Authority, the Registration Authorities, the applicants, subscribers and users of the certification service.

9.5.1. Rights and duties of ANDES SCD.

The Certification Practices Statement lists the rights and duties of the Andes SCD Certification Authority

9.5.2. Applicant's Rights and Duties

The Certification Practices Statement lists the rights and duties of the applicants.


9.5.3. Subscriber Rights and Duties.

The Certification Practices Statement lists the rights and duties of the subscribers.

9.5.4. Subscriber Prohibitions:

The subscriber, in the consumption of ANDES certification services, shall refrain from:

1. Alter or modify, in whole or in part, the digital certificate or software delivered by ANDES SCD, or allow third parties do
2. Copy or reproduce in any form the digital certificate, or allow its copying or reproduction.
3. Reverse engineer, decode, disassemble or perform any action aimed at knowing or deciphering the source code, object code or other relevant information regarding the digital certificate or software related to the provision of the ANDES SCD service.
4. Transfer, assign or negotiate the rights granted by virtue of ANDES services.

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

5. Allow third parties to benefit from or use, directly or indirectly, the rights derived from the provision of digital certification services, under the conditions of this document.
6. Give the digital certificate a use other than that which is derived from the Declaration of Certification Practices.

9.6. Principle of Impartiality

In relations with customers, whatever their nature, size, quality, as well as in the provision of ANDES' services, we shall act in accordance with the principles defined in the policy of Impartiality, Integrity and Independence.

9.7. Limitations of liability

As stipulated in the Andes SCD Certification Practices Statement

9.8. Indemnifications

As stipulated in the Andes SCD Certification Practices Statement

9.9. Term and termination

As stipulated in the Andes SCD Certification Practices Statement

9.10. Specification change procedure

As stipulated in the Andes SCD Certification Practices Statement

9.11. Dispute prevention


As stipulated in the Andes SCD Certification Practices Statement

9.12. Applicable Law and Compliance with Applicable Law


As stipulated in the Andes SCD Certification Practices Statement

10. Change control


Version	Date	Detail	Responsible
1.1	24/02/2011	Initial version authorized by the SIC according to resolution 14349 of March 2011	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


1.2	02/11/2011	<p>a) - 3.1.1 and 7.1.1 - Certificate distinguish name is updated.</p> <p>b) - 6.1.7 and 7.1.1 - increased key size to 2048 keys</p> <p>c) - 6 - Reference is made to the PKCS12 certificate delivery method.</p> <p>d) - 4.6 - Certificates of different validity periods are offered. The validity is explicitly stated in the certificate itself.</p>	Policy and Security Committee
2.0	09/10/2014	<ul style="list-style-type: none"> • - 1.3 - Andes SCD address and PBX are updated. • - 3.1.1 and 7.1 - OU attribute of DN is updated to Certificate of Company Membership Issued by Andes SCD Av. 72nd Street # 9 - 55 • - 3.2.2 - Documents required for issuance of digital signature certificate are updated. • - All the document - Update term p12 to PKCS12 • - 6.1.7 - In the key size section, the term minimum is eliminated to refer to the size of the keys generated by Andes SCD. • - 3.1.1 and 7.1 - On January 27, 2015 OU attribute of DN is abbreviated to Company Membership Issued by Andes SCD Av CII 72 9 55 Of 501 	Policy and Security Committee
2.1	24/11/2015	<ul style="list-style-type: none"> - 1.1 - PC document version and date of issuance are updated. - 1.3 - Contact details and organization that administers the document are updated. - 1.5.2 - Reference to OID document with limitations of use of agreement certificates - 3.1.1 and 7.1 - OU attribute of the DN is updated to: Belonging Company Issued by Andes SCD Cra 27 86 43 	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


		- 7.2.2 - Updated OID PC and URL DPC Certificate Directive	
2.2	26/09/2016	<ul style="list-style-type: none"> - 1.3.2 - Contact person's email address is updated. - 4 - Maximum validity of the certificate is limited to 730 days. - 4.5 - Certificate replacement is included. - 4.7 - Maximum validity of the certificate is limited to 730 days. - 7.2.1 - RFC 3280 is updated to 5280. 	Policy and Security Committee
2.3	06/01/2017	<ul style="list-style-type: none"> - 4, 4.7 - It is specified that the maximum validity of the certificate is 730 calendar days. - 6.1, 6.2, 6.3, 6.4 PKCS12 delivery form deleted - 7.2 URL and version 2.3 of DPC and PC 	Policy and Security Committee
2.4	14/02/2017	<ul style="list-style-type: none"> - 3.2.2 A fragment is included regarding the requirements for issuing a company membership certificate to applicants with service contracts or those linked through temporary companies. 	Policy and Security Committee
2.5	01/07/2017	<ul style="list-style-type: none"> - 3.2.4 the term revocation code is replaced by the term revocation code. - 4. The term subscription contract has been deleted. - 4.5 Condition for replacement of certificates is included. - 7.2 URL and DPC 2.5 and PC 2.5 version 	Policy and Security Committee
2.6	26/10/2017	<ul style="list-style-type: none"> - 3.2.2 The minimum requirements that the document proving the applicant's relationship with the entity must have are detailed 	Policy and Security Committee
2.7	20/03/2018	<ul style="list-style-type: none"> - 1.5.4 The minutes and contracts section is included. - Reference to RFC 4523 related to LDAP is included. - 3.2.2 Other mechanisms are included to validate the identity of the subscriber. 	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


		<ul style="list-style-type: none"> - 3.2.3 Reference is made to the registration authority in charge of collecting the required evidence. - 6.1.2 Reference is made to FIPS 140-2 Level 3 cryptographic devices for the delivery of the subscriber's private key. - 6.3 Cryptographic devices are referenced. - 6.3.1 Reference is made to cryptographic device risks and security recommendations. - 7.2.2 The link to the CPD V.2.7 is updated in the certificate policy. - 9.1 Certificate tariffs are included according to their validity. - 9.5.1 ANDES SCD obligations and responsibilities are described. - 9.5.2 Subscriber's obligations are described. - 9.5.3 Prohibitions for the subscriber are described. - 9.6 Reference is made to the principle of impartiality. 	
2.8	16/07/2018	<ul style="list-style-type: none"> - 7.2.2 reference is made to current CPD URLs 	Policy and Security Committee
2.9	14/09/2018	<ul style="list-style-type: none"> - 1.1 Issue date and PC download url are updated. - 1.3.2 Name and email of the general manager is updated. - 7.2.2 PC OID identifier is updated. - 7.2.6 OID is updated 	Policy and Security Committee
3.0	25/11/2019	<ul style="list-style-type: none"> - 1.3.1, 1.3.2, 3.1.1 Updated ECD address and telephone number. - 3.2.4 Response times are added. - 4.4 Updated publication periods of the CRL - 5. Added sites covered in scope of accreditation (Noc, Triara, IFX) - 9.1 Updated 2019 fees. 	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


		- - References corresponding to agreement procedures in section 6 are eliminated.	
3.1	04/11/2020	<ul style="list-style-type: none"> - Document Name and Identification (1.1): Update location and version - - Policy Approval Procedures (1.3.3): Update of reviewers and approvers (1.3.4): Update of policy approval procedures (1.3.4) - - Security Controls (5): Update of datacenter address and location of SOC and NOC monitoring infrastructure 	Policy and Security Committee
3.2	1/02/2021	<ul style="list-style-type: none"> -- Updating of ETSI TS 101 456 and ETSI TS 102 042 to ETSI EN 319 411-2 and ETSI EN 319 411-1, respectively. -- Update of tariffs. -- The OID of the PC is updated. 	Policy and Security Committee
3.3	28/04/2021	<ul style="list-style-type: none"> - - The date of issue and registration of face-to-face applications is added to section 3.2.2. Authentication of the applicant's identity. The paragraph referring to the documents required for applications processed by agreement has been deleted. - - The response times in section 3.2.4 have been updated. - - The OID of the PC is updated. - - The name of the position of the Director of Projects and Operations is updated. 	Policy and Security Committee
4.0	15/06/2022	<p>The PC OID is updated.</p> <p>-The position "Director of Projects and Operations" is updated to "Operations Manager" responsible for preparing the document.</p> <p>-Update of numeral 1.1 information according</p>	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<p>to the new version of the document.</p> <ul style="list-style-type: none"> -Numereral 4.1 updated the definition of "issue" to "request". -Numereral 4.1.3 Acceptance of the certificate is included. -Number 4.2 "Key pair" is added to the definition of numeral 4.2. -4.2.1 Renewal of certificate keys is included. -4.4 Certificate Suspension is included. -Section 4.6 "Replacement of certificates" includes the procedure for the replacement of certificates. -Section 6.7 "Termination of the CA and RA" is included. -The latest version of the OID identifier is updated in numeral 7.2.6. -The certificate extension code is included in 7.2.7 User Notice section. -Clarifying note is included in section 9.1 regarding the cost of revoking certificates. 	
5.0	12/10/2022	<p>The OID identifier, date of issue, version and date of the document are updated.</p> <p>The name of the legal representative and the contact email address have been updated in section 1.3.2.</p> <p>Section 1.5.2.1 Limit of use of certificates in operating systems is included.</p> <p>In numeral 4.1.5 the use of certificates is included.</p> <p>Section 4.3 modification of the certificate in accordance with the requirements of the CEA is modified.</p> <p>Item 4.4 certificate suspension is modified in accordance with the requirements of the CEA.</p> <p>Item 5, security controls, is updated.</p> <p>Item 9.1 Fees is updated and the fees for the</p>	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<p>virtual token are included. The title of item 9.5, rights and duties, has been updated. The title and content of item 9.5.1 Rights and Duties of Andes SCD is modified.</p>	
6.0	05/12/2022	<ul style="list-style-type: none"> - - The OID, Version and date of issuance of the document are updated. - - Section 3.2.2.2. includes the types of mechanism with the description of validation of the applicant's identity (onboarding or notarized letter). - - In section 3.2.2.1, the e-mail for confirmation is included. - - The validity of the RUT document is modified to 90 days. 	Policy and Security Committee
7.0	14/04/2023	<ul style="list-style-type: none"> - The OID, Version and date of issue are updated in the Document Name and Identification section - The position of Operations Manager is modified to Operations Director - Updated "Identity Authentication" section including identity validation and note for document requirements - Updated the limits of use of certificates in the virtual token delivery format - Updated Andes logo and font. - Updated colors of the format according to the 2023 brand manual 	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.5.0
		Effective date:	14/04/2023
		Version:	5.0
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

SANDRA CECILIA RESTREPO MARTINEZ

General Manager