



ELECTRONIC INVOICING CERTIFICATION POLICY

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Table of Contents

Introduction	7
1. Presentation of the document	7
1.1. Document Name and Identification	7
1.2. References	7
1.3. Policy management	8
1.3.1. Organization that manages the document	8
1.3.2. Contact Person	8
1.3.3. Policy Approval Procedures	8
1.3.4. Publication of the document	8
1.4. User community and applicability	9
1.5. Scope of application	10
1.5.1. Applications of the certificate	10
1.5.2. Certificate usage limits	11
1.5.2.1. Certificate usage limit on operating systems	11
1.5.3. Prohibitions on the use of certificates	11
1.5.4. Minutes and contracts	12
2. Certificate Publication and Registration	12
3. Identification and authentication	12
3.1. Names	13
3.1.1. Types of names	13
3.1.2. Need for names to be meaningful	14
3.1.3. Anonymous and pseudonyms in names	14
3.1.4. Rules for interpreting name formats	14
3.1.5. Uniqueness of the names	14

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

3.2.	Identity Approval	14
3.2.1.	Method to prove possession of the private key	15
3.2.2.	Authenticating the Applicant's Identity	15
3.2.3.	Unverified information about the applicant	16
3.2.4.	Response Times.....	17
3.2.5.	Identification and authentication to request revocation.....	17
4.	Certificate lifecycle and operating procedures.....	17
4.1.	Request for certificates	18
4.1.1.	Who can request the issuance of a certificate	18
4.1.2.	Procedure for requesting and issuing a certificate.....	18
4.1.3.	Acceptance of the certificate.	19
4.1.4.	Publication of the certificate by Andes SCD	20
4.1.5.	Pair of keys and use of the certificate	20
4.1.5.1.	On the part of the subscriber	20
4.1.5.2.	From trusted users	20
4.2.	Certificate Renewal-Pair of Keys	21
4.2.1.	Certificate Key Renewal.....	21
4.3.	Modifying certificates	21
4.4.	Suspension of certification.....	21
4.5.	Decline of the request.....	21
4.6.	Revocation of certificates	21
4.7.	Replacement of certificates.....	22
4.8.	Certificate Status Services	23
4.9.	Validity of certificates	23
5.	Security Controls.....	24
6.	Technical security controls	24

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

6.1.	Key generation and installation	24
6.1.2.	Delivery of the private key to the subscriber	24
6.1.3.	Delivery of the public key to the certificate issuer	24
6.1.4.	Subscriber Public Key Distribution	25
6.1.5.	Distribution of the Andes SCD public key to users	25
6.1.6.	Private Key Usage Period	25
6.1.7.	Size of the keys	25
6.2.	Private Key Protection Controls	25
6.3.	Supported Cryptographic Devices	26
6.3.1.	Associated risks	27
6.3.1.1.	Risks associated with certificates issued on cryptographic devices	27
6.3.1.2.	Risks associated with certificates issued in software (PKSC10)	27
6.4.	Other aspects of key pair management	28
6.4.1.	Public Key File	28
6.4.2.	Certificate Operational Periods and Key Pair Usage Periods	29
6.5.	Activation Data	29
6.5.1.	Activation and installation data generation	29
6.5.2.	Activation Data Protection	29
6.6.	Computer Security Controls	29
6.7.	Cessation of ECD activities	29
7.	Certificate, CRL, and OCSP profiles	29
7.1.	Certificate Content	29
7.2.	Certificate Profiles	31
7.2.1.	Version number	31
7.2.2.	Certificate Extensions	31
7.2.3.	Algorithm object identifiers	32

 andes Servicio de Certificación Digital	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

7.2.4.	Name formats	32
7.2.5.	Name restrictions	32
7.2.6.	Certification Policy Identifier Object.....	32
7.2.7.	Syntax and semantics of policy qualifiers.....	33
7.3.	CRL Profile	33
7.3.1.	Version number.....	33
7.3.2.	CRLs and extensions.....	33
7.4.	OCSP Profile.....	34
7.4.1.	Version number.....	35
7.4.2.	OCSP Extensions	35
8.	Audit and other assessments.....	35
9.	Business & Legal Matters.....	35
9.1.	Rates	35
9.2.	Financial Responsibility	36
9.3.	Confidentiality of information	36
9.4.	Intellectual Property Rights.....	36
9.5.	Rights and Duties	36
9.5.1.	Rights and Duties of ANDES SCD	36
9.5.2.	Rights and Duties of the Applicant.....	37
9.5.3.	Rights and Duties of the Subscriber	37
9.5.4.	Prohibitions for the subscriber.....	37
9.6.	Principle of Impartiality and Non-Discrimination	37
9.7.	Limitations of Liability	37
9.8.	Compensation	38
9.9.	Term and Termination.....	38
9.10.	Specification Change Procedure.....	38

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

9.11.

Dispute Prevention

38

9.12.

Applicable Law and Compliance with Applicable Law

38

10.

Change Control

39

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Introduction

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

It is recommended to read this document before applying for a Certificate for Electronic Invoicing Issuer or making use of it for verification of electronic signatures in order to know the scope of application and the legal effects associated with the use of this type of certificate

1. Presentation of the document

1.1. Document Name and Identification

Document	CERTIFICATION POLICY FOR E-BILLERS
Description	The certificate for electronic invoice issuer certifies the identity of the subscriber and its status as an electronic biller, and allows the subscriber to digitally sign documents in the quality that their certificate accredits.
OID Identifier	1.3.6.1.4.1.31304.1.2.6.11
Version	V11
Date of issue	January 30, 2026
Location	https://www.andesscd.com.co/docs//pc_facturacionelectronica.pdf

1.2. References

The development of the content of the Certification Policies and the Statement of Certification Practices is issued taking into account the recommendations of 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

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

qualified certificates.

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

1.3. Policy management

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

1.3.1. Organization that manages the document

Name : Policy & Safety Committee
Address : Calle 26 #69c-03 Torre B oficina 701.
Email : comite.politicas.seguridad@andesscd.com.co
Phone : PBX (601)2415539

1.3.2. Contact Person

Company name : Andes Servicio de Certificación Digital S.A ACRONYM ANDES SCD SA.
Name : Sandra Cecilia Restrepo Martínez – General Manager
Address : Calle 26 #69c-03 Torre B oficina 701.
Email : info@andesscd.com.co
Phone : PBX (601)2415539

1.3.3. Policy Approval Procedures

The ANDES SCD Electronic Invoicing Certification Policy is administered by the Policy and Security Committee and is approved by the ANDES SCD Management, following the documented information procedure.

1.3.4. Publication of the document

The Certification Policy for electronic invoice issuers and the Statement of Certification Practices are documents for public use that are available on the Andes SCD website. Any modifications to these documents are published

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

immediately maintaining a version history

1.4. User community and applicability

The certificates for the issuer of electronic invoices are issued to natural persons or legal entities, they accredit the identity of the holder and their condition 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.

Certificate Authority (CA)

The Andes SCD Certification Authority is the entity that acts as a trusted third party between the subscriber and the users in the electronic medium and is responsible for issuing and managing the digital certificates for the issuer of electronic invoices in accordance with this Certification Policy. The Statement of Certification Practices 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 face-to-face applications, corroborate the identity of applicants and carry out a complete registration of applicants who wish to acquire a digital certificate in accordance with this Certification Policy.

Subscribers

The subscriber is that Natural Person or Legal Person who has acquired a certificate for an electronic invoice issuer issued by the Andes SCD Certification Authority to act in the electronic environment as an electronic biller. A subscriber is considered as long as said certificate is valid.

Applicants

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

Users

The user is any person who voluntarily places their trust in the certificates for the issuer of electronic invoices issued by the Andes SCD Certification Authority and who uses

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

the certification service as a means of accrediting the authenticity and integrity of a document signed by a third party.

1.5. Scope of application

1.5.1. Applications of the certificate

The e-biller certificate issued under this policy may be used for the following purposes:

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 for the issuance and interoperability of electronic invoices for the purposes of massification and fiscal control

Digital signature

Digital signatures made with a certificate for electronic invoice issuer offer the means of support by guaranteeing the authenticity of the origin, the integrity of the signed data and the non-repudiation.

- **Authenticity of origin:** In an electronic communication, the subscriber may validly prove his or her identity to another person by demonstrating possession of the private key associated with the respective public key contained in the certificate
- **Integrity of the document:** There is a guarantee that the document was not altered or modified after being 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.
- **Non-repudiation:** It prevents the issuer of the signed document from denying at a certain time the authorship or integrity of the document, since the signature through the digital certificate can prove the identity of the issuer without the issuer being able to repudiate it.

Information encryption

It is the process of transforming information to make it incomprehensible to everyone except the recipient to whom it is addressed.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

1.5.2. Certificate usage limits

Electronic Biller Issuer Certificates can only be used for the digital signature of electronic invoices (XML), their graphical representation (PDF), and electronic payroll support supports and adjustment notes of the electronic payroll support document issued by the subscriber.

1.5.2.1. Certificate usage limit on operating systems

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

- **PKCS#10:**

The delivery of certificates from a PKCS10 request, implies the generation of the pair of keys by the requestor, he sent a request attaching the CSR and its respective custody of the private key. This format applies to the issuance of certificates intended for use on unattended signing platforms, the limit of use of the certificates is defined in the respective certification policy.

1.5.3. Prohibitions on the use of certificates

The performance of unauthorized operations according to this Certification Policy and according to the Statement of Certification Practices, 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 elInvoicer certificate to sign other certificates or revocation lists (CRLs) is not permitted
- It is prohibited to use the certificate for uses other than those stipulated in the "Permitted Uses of the Certificate" and "Limits on Use of Certificates" section of this Certification Policy.
- Alterations to certificates are not allowed and the certificate must be used as provided by the Andes SCD Certificate 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.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

- 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 does not keep a copy of the subscribers' private key, therefore, it is the subscriber's responsibility to use data encryption.

1.5.4. Minutes and contracts

By registering the request for the issuance of certificates, the subscriber declares that he/she is aware of and accepts the [terms and conditions of provision of the service](#) described on the website.

No explicit confirmation by the subscriber is required to accept the terms and conditions of the service. The terms and conditions of service provision are considered to be accepted at the time the request is registered.

Once the digital signature certificate has been issued, ANDES SCD will deliver a notification by email to the subscriber with the information of interest to manage the life cycle of their certificate. Such notification contains at least the following information:

- Type of certificate
- PC OID Reference
- Certificate serial
- Effective start
- End of validity
- Certificate holder
- Entity
- Certificate delivery form
- Revocation Code
- PIN

2. Certificate Publication and Registration

The Andes SCD Certification Practices Statement (CPP) details information on the certificate directory, the means of publication, the frequency of publication and the control of access to the certificate directory. Current and expired certificates are retained published in LDAP in accordance with RFC 4523.

3. Identification and authentication

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

The procedures and criteria used to verify the identity of the applicant and approve the issuance of an e-biller certificate are described below.

3.1. Names

3.1.1. Types of names

The certificates for electronic invoice issuers have a section called Subject whose objective is to identify the holder or subscriber of the certificate, 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.

Abbreviate	Name	Legal Entity Electronic Invoicing	Natural Person Electronic Invoicing
CN	<u>Name</u>	Corporate name legal person	Full name of natural person
S	<u>Serial</u>	ID number + DV	ID number + DV
And	<u>Email</u>	Email	Email
C	<u>Country</u>	Country abbreviation	Country abbreviation
ST	<u>Department</u>	Department Name	Department Name
L	<u>City</u>	Name of the municipality	Name of the municipality
STREET	<u>Address</u>	Legal entity address	Address where It is offers products or services
T	<u>Title</u>	Issuer invoice Electronics - Legal person	Issuer invoice Electronics - Natural person

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Or	<u>Organization</u>	Branch name or dependency that uses the certificate	Name of organization in charge of the natural person offering products or services
OU	<u>Organizational Unit</u>	Issued by Andes SCD Calle 26 #69c-03 Torre B oficina 701.	Issued by Andes SCD Calle 26 #69c-03 Torre B oficina 701.

3.1.2. Need for names to be meaningful

All certificates for electronic invoice issuers issued by Andes SCD have as their main characteristic the full identification of the subscriber and the assignment of a meaningful name to their certificate

3.1.3. Anonymous and pseudonyms in names

This Certificate Policy does not allow anonymity or pseudonyms to identify the name of a Legal Entity or the name of a Natural Person.

The name of the legal entity must be the corporate name that appears in the RUT, legal personality or equivalent document, acronyms or abbreviated names are not accepted.

The name of the natural person must be made up of the names and surnames as it appears 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. Uniqueness of the names

The distinguished names of the e-biller certificates are guaranteed to be unique for each subscriber because they contain serial, email, and organization attributes that allow distinguishing between 2 identities when there are duplicate name issues.

3.2. Identity Approval

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

3.2.1. Method to prove possession of the private key

The Andes SCD Statement of Certification Practices details the procedure used by the Certification Authority to demonstrate that the applicant has the private key corresponding to the public key that is intended to be linked to the certificate for the issuer of electronic invoices.

3.2.2. Authenticating the Applicant's Identity

The applicant can process their request for the issuance of a certificate for an electronic invoice issuer in the following ways:

1. **Face-to-face:** The applicant makes an application in person at the Andes SCD facilities.
2. **Remote:** The applicant makes the request from the Andes SCD website.
3. **Agreements:** Applications for the issuance of certificates by agreements are processed by a coordinator designated by the entity or company, in accordance with the internal procedures defined by the registration authority.

Requirements
Digital evidence provided by the applicant or by an authorized third party that allows the identity of the electronic biller (Biller) to be verified.

In all applications for a digital signature certificate, the ECD will carry out identity validation using the mechanisms available for this purpose.

The documentary requirements are described below:

Requirement	Face-to-face application	Remote Request or Agreement	Person Natural	Person Legal
Citizenship card or document proving the identity of the legal representative (readable)	Submit original and photocopy Document	Digital PDF document required	X	X

 andes Servicio de Certificación Digital	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Chamber of commerce or document that accredits legal representation of the entity (Complete, legible document)	Submit Photocopy Document	Digital PDF document required	N/A	X
--	---------------------------	-------------------------------	-----	---

The documentation indicated in the table above will be used as additional support. However, our external sources that ensure and validate the veracity of the information will be our main reference and the basis for decision-making in the process of studying and issuing the certificate. In the event that any novelty or inconsistency is detected in the information from these sources, the registration authority may request additional documentation from the user to support and argue the condition to be validated.

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

In the case of applications processed by agreement, other documents or digital evidence may be accepted that allow their legal representative to be verified.

In addition, the applicant must provide the following information that will allow Andes SCD to contact him or her when necessary:

Requirement	Additional information
1	Country, department and city where you live
2	Address and phone number
3	Contact Email

The information provided in the request for the issuance of a certificate for an electronic invoice issuer is studied by the RA agent, who is responsible for verifying that the information is original, sufficient and adequate in accordance with the internal procedures defined by Andes SCD.

3.2.3. Unverified information about the applicant

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

The registration authority verifies all the applicant's information that is supported by documents or digital evidence as support. Residence address and email are not verified, presuming the good faith of the information provided by the applicant.

3.2.4. Response Times

The ANDES SCD RA processes applications one to two business days after the application is registered along with complete documentation and information and a successful result in identity validation.

In the event 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 given the impossibility of contacting the applicant, The application may be rejected and the applicant must register a new application attaching the corresponding documentation.

3.2.5. Identification and authentication to request revocation

The following persons may apply for the revocation of a certificate:

- The subscriber to whom the certificate was issued for electronic invoice issuer, in which case they must provide the revocation code that was given to them at the time of acquiring the certificate.
- To the authorized representative of the entity to which the subscriber is linked, in which case it must formally notify Andes SCD in writing of the reason for requesting the revocation of the certificate of Legal Representative 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 Statement of Certification Practices are incurred.

4. Certificate lifecycle and operating procedures

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

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

At the end of the period of validity, the certificate becomes invalid and permanently ceases its operation and the provision of 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 request 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 fully capable of assuming the obligations and responsibilities inherent to the possession and use of the certificate and who demonstrates any of the following situations:

- Is the legal representative of a Legal Entity
- You are the owner of a business establishment
- Is the representative of the organization that provides services

4.1.2. Procedure for requesting and issuing a certificate

The procedure that the applicant must carry out to acquire a digital certificate is described below:

Activity		Detail	Responsible
1	Generate the pair of keys	Generate the key pair and get the CSR that contains the public key and is implicitly signed by the associated private key	Applicant
2	Make request	Enter platform or web service provided by Andes 1. Select Certificate Type 2. Accept terms and conditions and authorize the processing of personal data. Select the delivery format and validity of the certificate. 3. Fill in the certificate and billing data, provide CSR that contains the public key and is implicitly signed by the associated private key	Applicant

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

		4. Attach the required documentation according to current and applicable PC. 5. Make the payment for the service by the different means available on the platform 6. Carry out the identity validation process by one of the mechanisms enabled for this purpose. Finally, the platform will indicate to the applicant their file number and the status of the application to follow up	
3	Application Review	Verify the information and documentation of the application; ensure validation of the applicant's identity and determine whether to recommend the issuance of the certificate or reject the request. • In case of rejection of the application, it will send an email to the applicant indicating the reasons why the application was rejected and the process ends • If recommended, the application continues with the next step of this procedure.	Andes SCD Supervisor RA
4	Decision Making Issuance of the Certificate	Verify the RA recommended certificate issuance request and give the command to generate the certificate • ANDES SCD verifies that the private key is in the subscriber's possession by verifying the SIGNATURE using the public key that is sent in the PKCS10 certificate request. • Generate the digital certificate • Notify the subscriber of certificate issuance	Andes SCD Issuance Agent

4.1.3. Acceptance of the certificate.

The procedure for accepting the certificate is described in the DPC Certification Practice Statement. "Certificate Acceptance" section.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

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. Pair of keys 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 that are legally valid during the period of validity of the certificate for the electronic invoice issuer 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 may only use the certificate and key pair after accepting the terms of use set forth in the DPC and this 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 may only use the Private Key and Certificate for 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 have the following uses enabled:

- Digital Signature
- No repudiation
- Information encryption

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

The key pair associated with the certificates of the subordinate CAs of Andes SCD has the following uses enabled:

- Digital signature
- Signing certificates
- CRL Company

4.1.5.2. From trusted users

Users who rely on the Andes SCD certification service must verify the uses

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

established in the 'Key usage' field of the certificate or in this Certification Policy to know the scope of application of the certificate for electronic invoice issuer.

Users who rely on the Andes SCD certification service must take responsibility for verifying the status of the certificate before placing their trust.

4.2. Certificate Renewal-Pair of Keys

Andes SCD does not contemplate the certificate renewal process, if the subscriber wishes to obtain a new certificate he must request the issuance of the certificate when his original certificate has expired

4.2.1. Certificate Key Renewal

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

4.3. Modifying certificates

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 the application and verification process, complying with the requirements established in this certification policy.

4.4. Suspension of certification

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

4.5. Decline of the request.

As stipulated in the Andes SCD Statement of Certification Practices in the declination section of the application

4.6. Revocation of certificates

The revocation consists of the loss of reliability of the certificate and the permanent cessation of its operation, preventing its use by the subscriber; once the certificate has been revoked, the Certificate Authority includes it in the CRL in order to notify

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

third parties that a certificate has been revoked at the time its verification 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 date of generation of the CRL. The user is advised to check the date of the CRL to verify that it is the one recently issued.

The certificates that are revoked may not for any circumstance return to the active state, this being a definitive action.

The subscriber of the certificate in the case of a natural person or the legal representative in the case of a legal person can request the revocation of a certificate for an electronic invoice issuer, based on the revocation means offered by Andes SCD in the "means to revoke certificates" section of the DPC and following the revocation procedure specified in the "procedure for revoking certificates" section of the DPC. Additionally, Andes SCD or any of its constituent authorities may request the revocation of a certificate for an electronic invoice issuer if it has knowledge or suspicion of the compromise of the subscriber's private key or any other determining fact that requires the revocation of the certificate.

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

Issued CRLs, including those that have been replaced by newer versions or that have expired, are stored and retained for a minimum period of seven (7) years, counted from the date of issuance.

4.7. 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 that has acquired it for any of the following reasons:

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

- Loss or exposure of certificate PIN Change of certificate holder information:
 - ✓ For a natural person, it is feasible to modify the information of the certificate holder, except for the identification number.
 - ✓ For legal entities, it is possible to change the information of the owner and/or entity, as long as it belongs to the same NIT

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

- To make the replacement request, the certificate to be replaced must be valid.
- The certificate to be replaced must have an initial validity equal to or greater than 6 months
- The certificate to be replaced must have a remaining validity of more than 60 days.
- Communicate the reason for the cancellation of the certificate to be replaced
- The replacement applies to request the same type of certificate initially acquired

The conditions of replacement may vary according to the specific agreements with users managed through a coordinator or through agreements.

4.8. Certificate Status Services

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

4.9. Validity of certificates

The validity period of the digital certificates issued by ANDES SCD S.A. is explicitly defined in each certificate through the validity fields notBefore and notAfter, which are generated and coded in accordance with the ISO 9594 / X.509 and ISO 15782-1 standards.

For all types of certificates issued by ANDES SCD S.A., the maximum validity shall not exceed seven hundred and thirty (730) calendar days, counted from the date of

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

issuance of the certificate.

The pair of keys has the same period of validity as 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 monitoring rigorous operating standards to ensure that the equipment and information housed there 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 that has optimal security mechanisms to guarantee continuity in the provision of services. The technological infrastructure that supports the certification services that are continuously monitored through a NOC/SOC to identify any type of alert or incident that may compromise the security or availability of the provision of services.

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

6. Technical security controls

6.1. Key generation and installation

6.1.1. Key pair generation

The public and private keys of e-biller certificate holders are generated by the subscriber himself. For the issuance of the certificate, the respective CSR must be provided to Andes SCD.

6.1.2. Delivery of the private key to the subscriber

It does not proceed because the private key is at no time known to ANDES SCD. The private key is generated by the subscriber himself.

6.1.3. Delivery of the public key to the certificate issuer

The delivery of the subscriber's public key to ANDES SCD is made by registering the certificate issuance request with delivery form "PKCS10" from the platform or web service, where the subscriber links the CSR that contains the public key

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

and is implicitly signed by the associated private key.

6.1.4. Subscriber Public Key Distribution

The public key of any certificate subscriber for electronic biller is permanently available for download in the Andes SCD certificate directory as long as the certificate is not revoked.

6.1.5. Distribution of the Andes SCD public key to users

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

When the SubCA public key is renewed, the Certificate Authority makes the prior notification to the interested parties in accordance with the provisions of this DPC and the communications matrix.

This notification is made through the defined institutional channels, sufficiently in advance to allow the updating of the certification chains, dependent certificates and associated configurations, guaranteeing the continuity of the CA's services and avoiding operational interruptions.

6.1.6. Private Key Usage Period

The period of use of the private key is the same time as the validity of the certificate for the electronic biller issuer or less if the certificate is revoked before expiring.

The Andes SCD DPC 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 the keys

The size of the certificate keys for the e-biller is 2048 bits based on the RSA algorithm.

The size of the certified keys of the CA issuing the certificates for the electronic invoice issuer has a length of 4096 bits based on the RSA algorithm.

6.2. Private Key Protection Controls

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

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

The following are the Subscriber Private Key Protection Controls

Protection Control	CSR Subscriber-Generated Private Key
<u>Private Key Backup</u>	Andes SCD does not perform backup, nor is any recovery mechanism implemented on the private keys of the subscribers when the certificate is generated from CSR. Andes SCD is never in possession of such keys and they only remain in the custody of the subscriber himself
<u>Key Storage Private</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 user-generated private key that CSR delivers for certificate generation is held by the subscriber and is never sent to Andes SCD.
<u>Private Key Activation</u>	The protection of activation data is the responsibility of the subscriber
<u>Deactivating The Private Key</u>	Deactivation of the private key is the responsibility of the subscriber
<u>Private Key Destruction</u>	The 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

Cryptographic devices supported by ANDES SCD must meet the following characteristics:

- Generates RSA key pairs up to 2048 bits.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

- Algorithms for RSA 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 certified.
- Full support for PKI applications.
- Compatible with CAPI and PKCS#11 interfaces.
- Support for multi-key storage.
- Support for X.509 V3 standard certificate format.

6.3.1. Associated risks

6.3.1.1. Risks associated with certificates issued on cryptographic devices

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

- Loss of the device
- Key Compromise
- Damage from improper handling or environmental conditions.
- Damage from voltage variations.

To mitigate the associated risks, some safety regulations 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 proper environmental conditions away from moisture.
- In case of compromise or loss of the private key, the revocation of the certificate must be requested.

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

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

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

	and the right to non-repudiation.	which is specified on the certificate PC.
Improper custody of the private key of certificates issued from a PKCS10 request	Loss of certificate reliability (due to copying or impersonation risks)	Store in a secure location for exclusive subscriber access
Private Key Compromise	Access to the private key by malicious third parties	• Use of software recommended by ANDES SCD (CSR Generator Software and PFX Generator Software). • Store in a secure location for exclusive subscriber access. • Protect your key by using your password that only you have access to. • Use a secure Keystore for the custody of your private key

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

6.4. Other aspects of key pair management

6.4.1. Public Key File

Andes SCD keeps archived all certificates generated for the issuer of electronic invoices, which include the public key during the period stipulated in the "public key archive" section of the DPC.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

6.4.2. Certificate Operational Periods and Key Pair Usage Periods

The life time of the certificate for the issuer of electronic invoicing is governed by its validity or as long as its revocation is not explicitly stated in a CRL or in the online verification system. If any of these events occur, the validity of the certificate is terminated and the certificate can only be used for historical verification purposes.

The pair of keys is valid as long as there is a valid certificate for the issuer of electronic invoices that supports them. Once the certificate is no longer valid, the keys lose all legal validity and their use is limited to exclusively personal purposes.

6.5. Activation Data

6.5.1. Activation and installation data generation

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

6.5.2. Activation Data Protection

The protection of PIN or activation data for the use of the private key must be safeguarded by the subscriber

6.6. Computer Security Controls

The Statement of Certification Practices describes Andes SCD's controls to ensure adequate safeguarding of IT resources.

6.7. Cessation of ECD activities

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

7. Certificate, CRL, and OCSP profiles

7.1. Certificate Content

Certificate format for e-invoicing issuer		
Field	Description	Value

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Version	Certificate Version	V3
Serial number	Number that identifies the certificate	Subscriber certificate serial number
Signature algorithm	Algorithm used by Andes SCD to sign the certificate	SHA256WithRSA
Signature hashing algorithm	Algorithm used to obtain the summary of the data	Sha256
Emisor (issuer)	Data from the end-entity subordinate CA that issued the certificate.	View Class II CA data on certificate
Valid from	Date and Time UTC Start Validity	Certificate Validity Start Date
Valid until	UTC Date and Time End Validity	Certificate Validity End Date
Subject	CN	See section 3.1.1 of this document to know the value of each attribute of the matter, which may vary if the issuer of the electronic invoice is a Legal Person or a Natural Person
	S	
	And	
	C	
	ST	
	L	
	STREET	
	T	
	Or	
	OU	
Public Key	Public key of the certificate holder	RSA (2048 Bits)
Extensions	Extensions used in certificates for electronic invoice issuer	See the "Certificate Extensions" section of this document for more details.
Identification algorithm	Algorithm used to obtain the fingerprint of the certificate	Sha1
Fingerprint	The synthesis or fingerprinting of the data of the Certificate	fingerprint
Using the Key	Purposes for which the certificate should be used.	Digital Signature Non-repudiation Information encryption

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

7.2. Certificate Profiles

7.2.1. Version number

Electronic Invoicer Certificates issued under this policy are in compliance with the X.509 V3 standard and in compliance with RFC 5280 for certificate profiles and CRLs.

7.2.2. Certificate Extensions

The certificates for electronic invoice issuers issued by Andes SCD use a series of extensions that aim to establish the uses of the certificate, reference the applicable Certification Policies and additional restrictions. Below are the extensions included in the certificates for electronic invoice issuers

Extensions Certificates for electronic invoice issuer according to X.509V3 standard	
Name	Value
Access to issuer information	Access Method=Online Certificate Status Protocol URL=http://ocsp.andesscd.com.co
Holder key identifier	Holder's key identifier
Issuer Key Identifier	Identifier of the Andes SCD CA Key That Issued the Certificate
Distribution Points of the CRL	CRL publication URL of the CA that issued the certificate.
Using the Key	Digital Signature Non-repudiation Information encryption
Improved key usage	Secure Mail Client Authentication
Alternative name of the holder	Email del suscriptor RFC 822 Name (e-mail address)
Basic Restrictions	Subject Type=End Entity Path Length Constraint=None

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Certificate policy	[1]Certificate policy: Policy ID=1.3.6.1.4.1.31304.1.2.6.11 [1,1]Policy certifier information: Policy Certifier ID=Certifier User Prompt: Notice text=The use of this certificate is subject to the Certificate Policies for electronic invoice issuer (PC) and Certification Practices (DPC) established by Andes SCD. [1,2]Policy Certifier Information: Policy Certifier ID=CPS Certifier: Current DPC URL
--------------------	--

7.2.3. Algorithm object identifiers

Electronic invoicer certificates issued under this policy use the following algorithms and their corresponding identifiers (OIDs)

- SHA256withRSAEncryption Signature Algorithm OID 1.2.840.113549.1.1.11
- RSAEncryption Public Key Algorithm OID 1.2.840.113549.1.1.1

7.2.4. Name formats

The Certificates for electronic invoice issuer issued by Andes SCD are restricted to 'Distinguished names' (DN) X.500 which are unique and unambiguous, the certificates contain the DN of the issuer and the 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. Certification Policy Identifier Object

Certification policies and practices are identified by a unique number called OID, the OID assigned to this policy is 1.3.6.1.4.1.31304.1.2.6.10

More information on this topic can be found in the Statement of Certification Practices in the Identifier Object section of the certification policy

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

7.2.7. Syntax and semantics of policy qualifiers

The extension of the certificates referring to the ratifiers of the Certification Policy contains the following information:

- **Policy identifier:** Contains the Certificate Policy ID for Electronic Invoice Issuer
- **CPS:** Indicates the URL where the Statement of Certification Practices (CPD) is published to be consulted by users
- **User Notice:** contains the text "The use of this certificate is subject to the electronic invoice and DPC PCs established by Andes SCD". Accreditation code: 16-ECD-004.

7.3. CRL Profile

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 as stipulated in RFC 5280

CRL profile according to X.509V2 standard – CRL		
Name	Description	Value
Version	CRL version	V2
CRL Number	CRL Unique Number	Identified from the CRL
Issuer	Data from the end-entity subordinate CA that issued the CRL	View the CRL for CA data issued by the CRL
Signature algorithm	Algorithm used for CRL signature	SHA256withRSA
Effective Date of Issue	Validity Period After CRL Issued	CRL issue date in UTC time
Next update	Date on which the following CRL will be issued	Date of issue of the next CRL in UTC time
Issuing points Distribution	URL where the CRLs issued by Andes SCD are published	View the CRL for the publication URL

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager
Revoked certificates	List of revoked certificates specifying the serial number, date of revocation and reason for revocation		

7.4. OCSP Profile

OCSP Service and Response Certificate Profile

The Certificate Authority (CA) operates an Online Certificate Status Protocol (OCSP) service, in accordance with the provisions of RFC 6960, in order to provide timely and reliable information on the status of issued digital certificates.

The OCSP service is used by trusted third parties, applications, and systems that require verification of the revocation status of certificates issued by the CA.

OCSP responses are digitally signed by the CA or by an authorized OCSP Responder, using an OCSP response certificate whose profile, extensions, and restrictions are defined in this paragraph.

The consumption of the OCSP service is done through the access points published by the CA, using OCSP requests that conform to the applicable standards. The service responds, at a minimum, with the states good, revoked, or unknown, according to the information available in the CA revocation repositories.

OCSP responses include the thisUpdate and nextUpdate temporal fields, which determine the validity period of the response and allow trusted third parties to evaluate its validity.

The CA implements technical and operational controls to guarantee the availability, integrity and authenticity of the OCSP service, as well as mechanisms for monitoring and recording events associated with its operation.

Note: The following example is illustrative and does not limit the use of other OCSP-compliant tools.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

openssl ocspl -issuer ca_emisora.pem -cert certificado_consultar.pem -url <http://ocsp.andesscd.com.co> -CAfile ca_emisora.pem -resp_text -noverify Example overview:

- issuer: Certificate of the CA issuing the certificate queried.
- cert: Certificate whose status is to be verified.
- url: Access point of the OCSP service published by the CA.
- CAfile: CA certificate for response validation (if applicable).
- resp_text: Displays the readable contents of the OCSP response.

The OCSP response will allow you to determine the status of the certificate consulted (good, revoked or unknown) and evaluate the validity of the information using the temporary fields included in the response.

7.4.1. Version number

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

7.4.2. OCSP Extensions

OCSP extensions according to X.509V3 standard	
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 assessments

Information on the audit and other valuations is specified in the Andes SCD Statement of Certification Practices.

9. Business & Legal Matters

9.1. Rates

The rates indicated herein are reference values and may vary according to

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

special commercial agreements signed with clients, entities or applicants, or in the development of promotional campaigns carried out by ANDES SCD.

Type	1 year	2 years	Replacement Value
Person Natural	\$ 326,700	\$588,060	\$86,500
Legal Entity	\$ 326,700	\$ 588,060	\$86,500

- All the rates presented above are values before VAT
- The replacement value applies for the remaining validity of the certificate to be replaced provided that the following conditions are met:

9.2. Financial Responsibility

The Andes SCD Certification Practices Statement specifies the value of the coverage to compensate for damages that may be caused by the use of the certificates issued by Andes SCD.

9.3. Confidentiality of information

As stipulated in the Andes SCD Statement of Certification Practices

9.4. Intellectual Property Rights

As stipulated in the Andes SCD Statement of Certification Practices

9.5. Rights and Duties

The Statement of Certification Practices lists the obligations and guarantees 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 Statement of Certification Practices lists the obligations and guarantees of the Andes SCD Certification Authority

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

9.5.2. Rights and Duties of the Applicant

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

9.5.3. Rights and Duties of the Subscriber

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

9.5.4. Prohibitions for the subscriber

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

1. Alter or modify, in whole or in part, the digital certificate or the software delivered by ANDES SCD, or allow third parties to do so.
2. Copy or reproduce in any form the digital certificate or allow its copying or reproduction.
3. Perform reverse engineering, decoding, disassembly or perform any type of action aimed at knowing or deciphering the source code, object code or other relevant information regarding the digital certificate or software that is related to the provision of the ANDES SCD service.
4. Transfer, assign or negotiate the rights granted under the services of ANDES.
5. Allow third parties to benefit from or use, directly or indirectly, the rights that derive 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 Statement of Certification Practices.

9.6. Principle of Impartiality and Non-Discrimination

In relations with clients, whatever their nature, size, quality, as well as in the provision of ANDES services, we will act in accordance with the principles defined in the Impartiality, Integrity and Independence policy and in the ANDES SCD Statement of Certification Practices.

9.7. Limitations of Liability

As stipulated in the Andes SCD Statement of Certification Practices and additionally:

The Subscriber assumes all risks for damages that may arise from conduct such as providing false information, impersonating third parties, having its employees and contractors sign documents that are not related to electronic invoices, validating documents or incomplete or outdated information.

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

If criminal conduct is committed on the information or digital certificate delivered to the Subscriber for the provision of the electronic invoicing service, the Subscriber will be solely responsible for the damages caused to both ANDES and third parties and in the same way will exclusively assume civil and criminal liability for its conduct.

9.8. Compensation

As stipulated in the Andes SCD Statement of Certification Practices

9.9. Term and Termination

As stipulated in the Andes SCD Statement of Certification Practices

9.10. Specification Change Procedure

As stipulated in the Andes SCD Statement of Certification Practices

9.11. Dispute Prevention

As stipulated in the Andes SCD Statement of Certification Practices

9.12. Applicable Law and Compliance with Applicable Law

As stipulated in the Andes SCD Statement of Certification Practices

SANDRA CECILIA RESTREPO MARTINEZ
General Manager

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

10. Change Control

Version	Date	Detail	Responsible
1.0	26/06/2018	Initial version of the elInvoicer Policy	Policy and Security Committee
1.1	16/07/2018	- 7.2.2 reference to current DPC URLs	Policy Committee and Security
1.2	14/09/2018	- The date of issue and download url of the PC is updated. - 1.3.2 The name and email address of the general manager are updated. - 7.2.2 Updated PC OID Identifier - 7.2.6 Updated OID identifier	Policy and Security Committee
1.3	25/11/2019	- 1.3.1, 1.3.2, 3.1.1 ECD address and telephone number updated - 3.2.4 Added Response Times - 4.4 CRL publication periods are updated - 5. Sites covered in the scope of accreditation are added (Noc, Triara, IFX) - 9.1 Rates for 2019 are updated - References to the convention procedure in paragraph 6 are deleted	Policy and Security Committee
1.4	27/07/2020	- Adjustment in the documents requested from natural persons.	Product Manager Project Manager Operations

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

1.5	04/11/2020	- Document Name and Identification (1.1): Update location and version - Policy Approval Procedures (1.3.3): Updating Review and Approval Officers - Security Controls (5): Datacenter Address Update and Location SOC and NOC Monitoring Infrastructure	Policy and Safety Committee
1.6	01/02/2021	- Updating of ETSI TS 101 456 and ETSI TS 102 042 standards by ETSI EN 319 411-2 and ETSI EN 319 411-1, respectively. - Update RFC 2459 by RFC 5280. - Updating of rates. - Update of the scope of the certificate in accordance with the DIAN resolution, specifically in section 1.5.2. - The PC OID is updated.	Policy and Safety Committee
1.7	28/04/2021	- The column "Request for agreements" is added to the table in section 3.2.2. Authentication of the applicant's identity, the date of issuance and the registration of face-to-face applications are added. - The response times in section 3.2.4 have been updated. - The PC OID is updated. - The title of the Director of Projects and Operations is	Policy & Safety Committee / SGI Senior Analyst

 andes Servicio de Certificación Digital	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

		updated.	
2	15/06/2022	- Item 1.1 Document name and identification are modified, OID Identifier, Version, Date of Issue and Location are updated. - In item 3,2,5 the following is added: "- To the authorized representative of the entity to which the subscriber is linked, in which case he must formally notify Andes SCD in writing of the reason for requesting the revocation of the certificate of Legal Representative issued to the subscriber." - Item 4,1,3, Acceptance of the certificate is included. - Item 4.2.1 is included. Certificate Key Renewal - Item 4.4 suspension of certificates is included - Item 4.6 is modified. Replacement of certificates - Item 6.7 AC and RA termination is included - If you edit item 7.2.6. User Notice	Policy & Safety Committee / SGI Senior Analyst

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

3	12/10/2022	- The IOD identifier, issue date, version, and date of the document are updated. - Numeral 1.3.2 is updated, the name of the legal representative and the contact email. - It is included in numeral 4.1.3 see section acceptance of the certificate - Numeral 4.1.5 includes the use of certificates. - Numeral 4.3 modification of certificates is modified in accordance with the requirements of the CEA. - Numeral 4.4 suspension of certificates is modified in accordance with the requirements of the CEA. - Numeral 5 security controls are updated - The title of numeral 9.5 is updated for rights and duties - The content of numeral 9.5 Rights and duties of Andes SCD is modified - The title and content of numeral 9.5.1 Rights and duties of Andes SCD are modified.	
---	------------	---	--

 andes Servicio de Certificación Digital	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

4	05/12/2022	- The OID, Version and date of issue of the document are updated. - It is included in section 3.2.2. the types of mechanism with the description of validation of the applicant's identity (onboarding or notarized letter). - The validity of RUT is modified to 90 days. - Risks associated with certificates issued in software (PKSC10) are included.	Policy & Safety Committee / SGI Senior Analyst
5	14/04/2023	- Andes logo and font of the letter are updated. - Format colors are updated in accordance with the 2023 brand manual. - The OID, Version, and Issue Date are updated in the Document Name and Identification section. - The position of Operations Manager is changed to Director of Operations. - The item "Identity authentication" is updated to include identity validation and note for documentary requirements.	Policy & Safety Committee / SGI Senior Analyst
6	16/11/2023	- OID and Version Updated - ANDES SCD's phone number is updated. - Title 6.7 is amended from "Termination of CA or RA" to	Policy & Safety Committee / Chief Operating Officer / Senior Analyst SGI

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

		"Cessation of activities of the ECD". - Term decline of applications is included - The response time specifies that you must have successful identity validation. - Conditions for replacement of certificates are modified.	
7	19/02/2024	- OID and Version Updated - Rates are updated and replacement value is included	Policy & Safety Committee / Chief Operating Officer / SGI Professional
8	07/05/2024	- OID and Version Updated - Replacement reasons are updated according to the type of certificate. - Limits on the use of certificates in operating systems are included - RUT document is eliminated as a requirement of the certificate.	Policy & Safety Committee / Chief Operating Officer / SGI Professional
9	06/06/2024	- OID and Version Updated - The item principle of impartiality is updated to include the term Non-Discrimination. - Service rates are updated.	Policy & Safety Committee / Chief Operating Officer / Process Coordinator / SGI Professional
10	24/01/2025	- The logo and header are updated according to the brand manual. - The document name item, ID, OID, version, and date of the document are updated.	Policy & Safety Committee / Director of Operations Operations Coordinator

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

		- Service rates are updated. - The section related to the replacement of certificates is modified. - The "Identity Authentication" numeral is updated to include a note on documentary requirements. - The item 'Response times' is revised and updated, eliminating the option of delivery in physical token format.	
11	30/01/2026	- Updating the OID and the version of the document. - Updating of service rates. - Inclusion of the OCSP Service item and the response certificate profile. - Updating the Private Key Protection Controls item. - Update of the distribution mechanism of the Andes SCD public key to users. - Update of the publication of revoked certificates. - Updating the validity of certificates	Policy & Safety Committee / Chief Technology Officer / Chief Operating Officer / SGI Coordinator/

	ELECTRONIC INVOICING CERTIFICATION POLICY	OID Identifier:	1.3.6.1.4.1.31304.1.2.6.11
		Effective Date:	16/02/2026
		Version:	11
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager