





# **CERTIFICATION POLICY PUBLIC FUNCTION**

**2025**


	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

## Table of contents


<b>1. Presentation of the document</b>	<b>5</b>
1.1. Name of document and identification	5
1.2. References	5
1.3. Policy administration	6
1.3.1. Organization that manages the document	6
1.3.2. Contact Person	6
1.3.3. Policy Approval Procedures	6
1.3.4. Publication of the document	6
1.4. User Community and Applicability	6
1.5. Scope of application	8
1.5.1. Uses of the certificate	8
1.5.2. Limits on the use of certificates	8
1.5.2.1. Limits on the use of certificates in operating systems	9
1.5.3. Prohibitions on the use of certificates	9
1.5.4. Minutes and contracts	10
<b>2. Publication and registration of certificates</b>	<b>10</b>
<b>3. Identificación y autenticación</b>	<b>11</b>
3.1. Names	11
3.1.1. Types of names	11
3.1.2. The need for names to be meaningful	12
3.1.3. Anonyms and pseudonyms in names	12
3.1.4. Rules for interpreting name formats	12
3.1.5. Singularity of names	12
3.2. Identity Approval	12
3.2.1. Method for proving possession of the private key	12
3.2.2. Authentication of the applicant's identity	12
3.2.3. Unverified Applicant Information	14

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

<b>3.2.4. Response Times .....</b>	<b>14</b>
<b>3.2.5. Identification and authentication for revocation requests .....</b>	<b>15</b>
<b>4. Certificate life cycle and operating procedures .....</b>	<b>15</b>
<b>4.1. Request for certificates .....</b>	<b>16</b>
<b>4.1.1. Who can apply for the issuance of a certificate .....</b>	<b>16</b>
<b>4.1.2. Procedure for requesting a certificate .....</b>	<b>16</b>
<b>4.1.3 Acceptance of the certificate. ....</b>	<b>16</b>
<b>4.1.4. Publication of the certificate by Andes SCD .....</b>	<b>16</b>
<b>4.1.5. Key pair and use of the certificate .....</b>	<b>16</b>
<b>4.1.5.1.On the part of the subscriber .....</b>	<b>16</b>
<b>4.1.5.2.By relying users .....</b>	<b>17</b>
<b>4.2. Renewal of Certificates - Key Pair .....</b>	<b>18</b>
<b>4.2.1 Renewal of certificate keys .....</b>	<b>18</b>
<b>4.3. Modification of certificates .....</b>	<b>18</b>
<b>4.4 Suspension of Certificates .....</b>	<b>18</b>
<b>4.5 Declination of Application .....</b>	<b>18</b>
<b>4.6. Revocation of certificates .....</b>	<b>19</b>
<b>4.7. Replacement of certificates .....</b>	<b>20</b>
<b>4.8. Certificate status services .....</b>	<b>20</b>
<b>4.9. Validity of certificates .....</b>	<b>20</b>
<b>5. Security controls .....</b>	<b>20</b>
<b>6. Technical safety controls .....</b>	<b>21</b>
<b>6.1. Key generation and installation .....</b>	<b>21</b>
<b>6.1.1. Key Pair Generation .....</b>	<b>21</b>
<b>6.1.2. Delivery of the private key to the subscriber .....</b>	<b>21</b>
<b>6.1.3. Delivery of the public key to the certificate issuer .....</b>	<b>21</b>
<b>6.1.4. Subscriber Public Key Distribution .....</b>	<b>21</b>
<b>6.1.5. Distribution of the Andes SCD Public Key to Users .....</b>	<b>22</b>

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


<b>6.1.6. Period of use of the private key .....</b>	<b>22</b>
<b>6.1.7. Size of keys .....</b>	<b>22</b>
<b>6.2. Private Key Protection Controls .....</b>	<b>22</b>
<b>6.3. Supported Cryptographic Devices .....</b>	<b>23</b>
<b>6.3.1. Associated risks .....</b>	<b>24</b>
<b>6.4. Other key pair management issues .....</b>	<b>24</b>
<b>6.4.1. Public Key File .....</b>	<b>24</b>
<b>6.4.2. Certificate operational periods and key pair usage periods .....</b>	<b>24</b>
<b>6.5. Activation data .....</b>	<b>25</b>
<b>6.5.1. Generation of Activation and Installation Data .....</b>	<b>25</b>
<b>6.5.2. Protection of activation data .....</b>	<b>25</b>
<b>6.6. Informatic security controls .....</b>	<b>25</b>
<b>6.7 Cessation of DCE activities .....</b>	<b>25</b>
<b>7. Certificate, CRL and OCSP Profiles .....</b>	<b>25</b>
<b>7.1. Contents of the certificate .....</b>	<b>25</b>
<b>7.2. Certificate profiles .....</b>	<b>27</b>
<b>7.2.1. Version number .....</b>	<b>27</b>
<b>7.2.2. Certificate Extensions .....</b>	<b>27</b>
<b>7.2.3. Algorithm Object Identifiers .....</b>	<b>28</b>
<b>7.2.4. Name formats .....</b>	<b>28</b>
<b>7.2.5. Name restrictions .....</b>	<b>28</b>
<b>7.2.6. Identifying object of the certification policy .....</b>	<b>29</b>
<b>7.2.7. Syntax and semantics of policy qualifiers .....</b>	<b>29</b>
<b>7.3. Profile CRL .....</b>	<b>29</b>
<b>7.3.1. Version number .....</b>	<b>29</b>
<b>7.3.2. CRLs and extensions .....</b>	<b>29</b>
<b>7.4. Profile OCSP .....</b>	<b>30</b>
<b>7.4.1. Version Number .....</b>	<b>30</b>

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

<b>7.4.2. Extensiones OCSP .....</b>	<b>30</b>
<b>8. Audit and other valuations .....</b>	<b>30</b>
<b>9. Business and legal matters .....</b>	<b>30</b>
<b>9.1. Rates .....</b>	<b>30</b>
<b>9.2. Financial responsibility .....</b>	<b>31</b>
<b>9.3. Confidentiality of information .....</b>	<b>31</b>
<b>9.4. Intellectual property rights .....</b>	<b>31</b>
<b>9.5. Rights and duties .....</b>	<b>31</b>
<b>9.5.1. Rights and duties of ANDES SCD .....</b>	<b>31</b>
<b>9.5.2. Applicant's Rights and Duties .....</b>	<b>31</b>
<b>9.5.3. Subscriber Rights and Duties .....</b>	<b>31</b>
<b>9.5.4. Subscriber Prohibitions: .....</b>	<b>32</b>
<b>9.6. Principle of Impartiality .....</b>	<b>32</b>
<b>9.7. Limitations of liability .....</b>	<b>32</b>
<b>9.8. Indemnifications .....</b>	<b>32</b>
<b>9.9. Term and termination .....</b>	<b>32</b>
<b>9.10. Specification change procedure .....</b>	<b>32</b>
<b>9.11. Dispute prevention .....</b>	<b>33</b>
<b>9.12. Applicable Law and Compliance with Applicable Law .....</b>	<b>33</b>
<b>10. Change Control .....</b>	<b>33</b>

## Introduction

This Policy for Public Function Certificates complements the provisions established in the Certification Practices provisions established in the Certification Practices Statement and specifically expresses the set of rules defined by the Andes SCD Certification Authority to Andes SCD Certification Authority for the application of Legal Person certificates to a community, the uses that can be given to this type of certificate and

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

the technical, legal and security technical, legal and security requirements for its issuance and revocation.

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

## 1. Presentation of the document


### 1.1. Name and identification of th document

Document	CERTIFICATION POLICY PUBLIC FUNCTION
Description	Public Function certificates are issued in the name of natural person; they accredit the identity of the holder and his or her public official or individual in the exercise of a public function, either by designation or as a result of the execution of a contract that qualifies him/her as such, in the signing of electronic documents, guaranteeing the electronic document signature, guaranteeing the authenticity of the issuer of the of the sender of the communication, the non-repudiation of its of the origin and the integrity of the content. The holder of a Civil Service certificate acts in the capacity accredited in it.
OID	1.3.6.1.4.1.31304.1.2.5.12
Version	V 12
Date of issue	January 24th , 2025
Location	<a href="https://www.andesscd.com.co/docs/cp_publicfunction.pdf">https://www.andesscd.com.co/docs/cp_publicfunction.pdf</a>

### 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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 2415539

#### 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 2415539

#### 1.3.3. Policy Approval Procedures


The Public Function certificate certifies the identity of the subscriber and his/her professional title, and allows the subscriber to sign documents digitally in his/her own name and interest. 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 Public Function Certification Policy 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

Public Function certificates issued to entities, of the holder and his character as a public official or private individual

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

in the exercise of a public function, either by appointment or as a result of the execution of a contract that qualifies him as such 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.

#### 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 public function 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 public function who has acquired a public function certificate issued by the Andes SCD Certification Authority and is considered a subscriber if such certificate is in force.


#### Applicants

The applicant is the public function who wishes to access the digital certification services by acquiring a certificate issued by services by acquiring a public function certificate issued by Andes SCD. Under no circumstances will applications for this type of certificates be accepted in the name of legal entities, devices or third parties representing the person who will appear as the holder of the certificate.

#### Users:

The user is any person who voluntarily places his trust in the public function 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.



	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

## 1.5. Scope of application

### 1.5.1. Uses of the certificate

The Certificate of public function issued under this policy may be used for the following purposes:

#### Identity authentication

The certificate can be used to identify a public function in the field of its activity.

#### Digital signature

Digital signatures made with public function 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 public function certificates cannot be used to act as Registration Authority or Certification Authority, signing other public key certificates of any kind or revoked certificate lists (CRL). Nor can they be used for purposes contrary to current legislation.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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 it is indispensable to have the following operating systems Windows 10 and higher in 64 and 32 bits versions; for MacOS operating system, it is required to use the online signature service is required to use the online signature service provided by Andes SCD through our website. 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.


- Centralized:

The delivery of certificates under the centralized signature model is subject to the development of the integration with the web services exposed by ANDES SCD, allowing signing operations using the certificates stored in its PKI infrastructure.

### 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 public function 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

- 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.

#### 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

### 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 public function.

#### 3.1. Names

##### 3.1.1. Types of names

The public function 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	Description
CN	<u>Name</u>	Company name of the Subscriber's
S	<u>Serial</u>	Subscriber's identification number
E	<u>Email</u>	Subscriber's email address
C	<u>Country</u>	Abbreviation for the country where the entity is located
ST	<u>Department</u>	Name of the department where the entity is located
L	<u>City</u>	Name of the municipality where the entity is located
STREET	<u>Address</u>	Address where the entity is located
T	<u>Title</u>	Area or unit of the subscriber's belong in the entity that makes use of the certificate.
1.3.6.1.4.1.4710.1.3.2		Document number + entity dv
O	<u>Organization</u>	Company name of the entity
OU	<u>Organizational Unit</u>	Name of the organizational unit of the entity to which the subscriber is linked. subscriber is linked to.
OU	<u>Organizational Unit</u>	public function Issued by Andes SCD Calle 26 #69c-03 Tower B office 701

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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 public function 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 public function.

In the case of a natural person with Colombian nationality, the name must be formed by first and last names as it appears in the citizenship card. If the natural person is a foreigner, the name must be formed by first and last names as it appears in the passport or equivalent 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 public function 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 public function certificate.

### 3.2.2. Authentication of the applicant's identity

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

1. **In person:** The applicant makes the application in person before the Andes SCD Registration Authority.
2. **Remote:** The applicant makes the application from the Andes SCD WEB site.


	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

In all applications the ECD will perform identity validation using the mechanisms at its

Requirement	In-person request	Remote request or outsourcing
<b>Citizenship card or document that proves the identity</b>  (Enlarged to 150% and legible)	Present original and photocopy of document	Scanned document required
<b>“RUT” of equivalent document that accredits identification of the the entity</b> (complete, legible document)	Present original and photocopy of document	Digital PDF document required
<b>Documents proving the person's relationship as a public or private individual public function and specifying the position specifies the position held</b> (complete, legible document)	Present original and photocopy of document	Digital PDF document required

disposal. The following is a description of the documentary requirements:

**Note:** The above documents may be optional as long as ANDES SCD can rectify the completeness and reliability of the information, in the case of Face-to-face applications will be registered through the Andes SCD website by the Customer Service area.  
Otherwise, the Registration Authority is entitled to request the corresponding documentary support.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

In the case of applications processed by agreement, 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 Certified Persona Natural 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.

In the event that 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 one to two business days from the moment of receiving the complete documentation and

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

information and having the successful identity validation result. 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 applicant has not generated an update. 3 working days after the notification has been sent, if the update has not been generated the applicant is unable to be contacted, the application may be rejected and the applicant must the request may be rejected and the applicant will have to register a new request 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.
- 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 public function 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.



	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

#### **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 application for a digital certificate of public function can be made by any person of legal age in full capacity to assume the obligations and responsibilities inherent to the possession and use of the certificate.

##### **4.1.2. Procedure for requesting a certificate**

The procedure to be followed by the applicant to acquire a digital certificate is described in the Certification Practices Statement. See section "Procedure to request the issuance of a certificate".

##### **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 possesses a legally valid public key and a legally valid private key during the period of validity of the Legal Entity certificate that legitimizes them. 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. 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 CPD and in the present CP and only for conditions of use established in the CPD and in the present CP and only for what they establish

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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

#### **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 graduate professional 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.


The subscriber has a public key and a private key legally valid during the period of validity of the Certificate of legal person 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 signature

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

## 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.


## 4.5 Declination of Application

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

## 4.6 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 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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

Revocation of public function 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 graduate professional 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.


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

- Loss of Token device
- Loss or exposure of certificate PIN
- 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 6 months.
- The certificate must have a remaining validity of more than 60 days.
- 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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.

#### **4.8. 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.

#### **4.9. Validity of certificates**


The validity period of the digital certificates of public function 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 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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**

#### **6.1.1. Key Pair Generation**

The public and private keys of holders of public function Certificates are generated in accordance with the processes stipulated in the CPS in the section Generation of the subscriber's key pair. The method of subscriber key pair generation varies according to the form of certificate delivery chosen by the subscriber or by agreement.

#### **6.1.2. Delivery of the private key to the subscriber**

When the private keys of the public function certificates are generated by ANDES SCD, they can only be stored in secure cryptographic devices "Token or HSM" that comply with the FIPS 140-2 Level 3 standard. The delivery of the private key is made directly to the subscriber or person in charge or person authorized by the subscriber.

When the delivery format is PKCS10 the key pair is generated by the subscriber, the private key is never known by ANDES SCD.


The mechanism for delivery of the private key to holders of Graduate Professional Certificates is described in the CPS in the section "delivery of the private key to the subscriber".

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

The mechanism of delivery of the public key to holders of the public function 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 public function Certificate subscriber is permanently available for download in the Andes SCD certificate directory if the certificate is not revoked.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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 public function 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 Legal Person certificates is 2048 bits based on the RSA algorithm.

The size of the certified keys of the issuing CA of the public function 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.

 <p><b>andes</b> Servicio de Certificación Digital</p>	<p><b>CERTIFICATION POLICY PUBLIC FUNCTION</b></p>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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 TOKEN and CSR device
<u>Private key backup</u>	Andes SCD does not back up subscribers' private keys generated from TOKEN device or when the certificate is generated from CSR. Andes SCD is never in possession of these keys and they only remain under the subscriber's custody.
<u>Private key storage</u>	Subscribers' private keys generated from TOKEN device are NEVER stored by Andes SCD. The same happens when the certificate is generated from CSR delivered by the subscriber.  The private key must be stored by the subscriber himself by keeping the TOKEN device or other methods, because they may be necessary to decrypt the historical information encrypted with the public key.
<u>Private key transfer</u>	The subscriber's private key generated from the TOKEN never leaves the device. The TOKEN device generates the key pair and protects its use through a PIN that only the subscriber knows. 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 activation of the TOKEN device containing the subscriber's private key is done through a PIN that must be personalized by the subscriber himself at the time of generating the key pair. The protection of the activation data is the responsibility of the subscriber
<u>disabling of the private key</u>	The method to disable the subscriber's private key is to remove the TOKEN device from the computer, immediately any associated content is disabled including the private key.
<u>Private key destruction</u>	The destruction of the private key can be performed by the subscriber using the functions provided by the TOKEN device, taking care not to affect other private keys stored in the device.  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.



	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

- 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.

#### **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.


### **6.4. Other key pair management issues**

#### **6.4.1. Public Key File**

Andes SCD keeps on file all digital certificates of public function, 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 public function is governed by the validity of the certificate 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 certificate's validity is terminated and it can only be used for historical verification purposes.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

The key pair is valid as long as there is a valid natural person 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 subscriber must generate the activation data for his TOKEN by changing the initial PIN that comes with the device by default.

The PIN must be kept by the subscriber so that it is not known by anyone else and exclusive control of the TOKEN is guaranteed.

### 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 Cessation of DCE activities

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

public function Certificate Form		
Field	Description	Value
Version	Certificate versión	V3
Serial number	Number identifying the certificate	Subscriber's certificate serial number
Signature algorithm	Algorithm used by Andes SCD to sign the certificate	SHA256WithRSA

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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	Company name of the legal person
	Serial Number	Company name of the Subscriber's
	E	Subscriber's identification number
	C	Subscriber's email address
	ST	Abbreviation for the country where the entity is located
	L	Name of the department where the entity is located
	STREET	Name of the municipality where the entity is located
	<u>Title</u>	Address where the entity is located
	<u>1.3.6.1.4.1.4710.1.3.2</u>	Document number + entity dv
	O	Company name of the entity
	OU	Name of the organizational unit of the entity to which the subscriber is linked.
	OU	Public Function Issued by Andes SCD Calle 26 #69c-03 Torre B office 701.
Public key	Certificate holder's public key	RSA (2048 Bits)

 <b>andes</b> Servicio de Certificación Digital	<b>CERTIFICATION POLICY</b> <b>PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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

## 7.2. Certificate profiles


### 7.2.1. Version number

Public Function 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

Public Function 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 Public Function .

<b>Extensions Certificates Public Function according to standard X.509V3</b>	
<b>Name</b>	<b>Value</b>
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

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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 =1.3.6.1.4.1.31304.1.2.5.12 [1,1] Policy certifier information: Id. of directive certifier =User notice Certifier: Warning text = The use of this certificate is subject to the Certificate of Public Function Policies (PC) and Certification Practices (CPS) established by Andes SCD. [1,2] Policy certifier information: Id. of directive certifier =CPS Certifier: Current CPS URL

### 7.2.3. Algorithm Object Identifiers

The digital certificates of Public Function 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		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

Certification policies and practices are identified by a unique number called an OID, the OID assigned to this policy is 1.3.6.1.4.1.31304.1.2.5.8.0.

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:

- **Policy identifier:** Contains the Certificate Policy identifier Graduate Professional
- **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

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

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	

## 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.

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

Delivery format	One year	Two years	Replacement value
Virtual Token	\$ 57,857	\$ 92,571	\$ 135,000
Physical token	N/A	\$ 96,639	\$ 150,000

- The above prices are per unit and include VAT (19%).
- The replacement value applies to the remaining validity period of the certificate to be replaced, provided that the conditions stated in the "Replacements" section of this Certification Policy are met.

## 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.

## 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.



	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

#### **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.
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

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

### 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
1.2	02/11/2011	a) - 3.1.1 and 7.1.1 - Certificate distinguish name is updated. b) - 6.1.7 and 7.1.1 - increased key size to 2048 keys c) - 6 - Reference is made to the PKCS12 certificate delivery method. d) - 4.6 - Certificates of different validity periods are offered. The validity is explicitly stated in the certificate itself.	Policy and Security Committee
2.0	09/10/2014	<ul style="list-style-type: none"> <li>- 1.3 - Andes SCD address and PBX are updated.</li> <li>- 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</li> <li>- 3.2.2 - Documents required for issuance of digital signature certificate are updated.</li> <li>- All the document - Update term p12 to PKCS12</li> <li>- 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.</li> <li>- 3.1.1 and 7.1 - On January 27, 2015 OU attribute of DN is abbreviated to Company Membership Issued by Andes SCD Av Cll 72 9 55 Of 501</li> </ul>	Policy and Security Committee

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


2.1	24/11/2015	<ul style="list-style-type: none"> <li>- 1.1 - PC document version and date of issuance are updated.</li> <li>- 1.3 - Contact details and organization that administers the document are updated.</li> <li>- 1.5.2 - Reference to OID document with limitations of use of agreement certificates</li> <li>- 3.1.1 and 7.1 - OU attribute of the DN is updated to: Belonging Company Issued by Andes SCD Cra 27 86 43</li> <li>- 7.2.2 - Updated OID PC and URL DPC Certificate Directive</li> </ul>	Policy and Security Committee
2.2	26/09/2016	<ul style="list-style-type: none"> <li>- 1.3.2 - Contact person's email address is updated.</li> <li>- 4 - Maximum validity of the certificate is limited to 730 days.</li> <li>- 4.5 - Certificate replacement is included.</li> <li>- 4.7 - Maximum validity of the certificate is limited to 730 days.</li> <li>- 7.2.1 - RFC 3280 is updated to 5280.</li> </ul>	Policy and Security Committee
2.3	06/01/2017	<ul style="list-style-type: none"> <li>- 4, 4.7 - It is specified that the maximum validity of the certificate is 730 calendar days.</li> <li>- 6.1, 6.2, 6.3, 6.4 PKCS12 delivery form deleted</li> <li>- 7.2 URL and version 2.3 of DPC and PC</li> </ul>	Policy and Security Committee
2.4	14/02/2017	<ul style="list-style-type: none"> <li>- 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.</li> </ul>	Policy and Security Committee
2.5	01/07/2017	<ul style="list-style-type: none"> <li>- 3.2.4 the term revocation code is replaced by the term revocation code.</li> <li>- 4. The term subscription contract has been deleted.</li> <li>- 4.5 Condition for replacement of certificates is included.</li> </ul>	Policy and Security Committee

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


		- 7.2 URL and DPC 2.5 and PC 2.5 version	
2.6	26/10/2017	- 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"> <li>- 1.5.4 The minutes and contracts section is included.</li> <li>- - Reference to RFC 4523 related to LDAP is included.</li> <li>- - 3.2.2 Other mechanisms are included to validate the identity of the subscriber.</li> <li>- - 3.2.3 Reference is made to the registration authority in charge of collecting the required evidence.</li> <li>- - 6.1.2 Reference is made to FIPS 140-2 Level 3 cryptographic devices for the delivery of the subscriber's private key.</li> <li>- - 6.3 Cryptographic devices are referenced.</li> <li>- - 6.3.1 Reference is made to cryptographic device risks and security recommendations.</li> <li>- - 7.2.2 The link to the CPD V.2.7 is updated in the certificate policy.</li> <li>- - 9.1 Certificate tariffs are included according to their validity.</li> <li>- - 9.5.1 ANDES SCD obligations and responsibilities are described.</li> <li>- - 9.5.2 Subscriber's obligations are described.</li> <li>- - 9.5.3 Prohibitions for the subscriber are described.</li> <li>- - 9.6 Reference is made to the principle of impartiality.</li> </ul>	Policy and Security Committee
2.8	16/07/2018	- 7.2.2 reference is made to current CPD URLs	Policy and Security Committee

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager


2.9	14/09/2018	<ul style="list-style-type: none"> <li>- 1.1 Issue date and PC download url are updated.</li> <li>- 1.3.2 Name and email of the general manager is updated.</li> <li>- 7.2.2 PC OID identifier is updated.</li> <li>- 7.2.6 OID is updated</li> </ul>	Policy and Security Committee
3.0	25/11/2019	<ul style="list-style-type: none"> <li>- 1.3.1, 1.3.2, 3.1.1 Updated ECD address and telephone number.</li> <li>- 3.2.4 Response times are added.</li> <li>- 4.4 Updated publication periods of the CRL</li> <li>- 5. Added sites covered in scope of accreditation (Noc, Triara, IFX)</li> <li>- 9.1 Updated 2019 fees.</li> <li>- References corresponding to agreement procedures in section 6 are eliminated.</li> </ul>	Policy and Security Committee
3.1	04/11/2020	<ul style="list-style-type: none"> <li>- Document Name and Identification (1.1): Update location and version</li> <li>- Policy Approval Procedures (1.3.3): Update of reviewers and approvers (1.3.4): Update of policy approval procedures (1.3.4)</li> <li>- Security Controls (5): Update of datacenter address and location of SOC and NOC monitoring infrastructure</li> </ul>	Policy and Security Committee
3.2	1/02/2021	<ul style="list-style-type: none"> <li>- Updating of ETSI TS 101 456 and ETSI TS 102 042 to ETSI EN 319 411-2 and ETSI EN 319 411-1, respectively.</li> <li>- Update of tariffs.</li> <li>- The OID of the PC is updated.</li> </ul>	Policy and Security Committee
3.3	28/04/2021	<ul style="list-style-type: none"> <li>- 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</li> </ul>	Policy and Security Committee

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<p>applications processed by agreement has been deleted.</p> <ul style="list-style-type: none"> <li>- The response times in section 3.2.4 have been updated.</li> <li>- The OID of the PC is updated.</li> <li>- The name of the position of the Director of Projects and Operations is updated.  </li> </ul>	
4.0	15/06/2022	<p>The PC OID is updated.</p> <ul style="list-style-type: none"> <li>-The position "Director of Projects and Operations" is updated to "Operations Manager" responsible for preparing the document.</li> <li>-Update of numeral 1.1 information according to the new version of the document.</li> <li>-Numereral 4.1 updated the definition of "issue" to "request".</li> <li>-Numereral 4.1.3 Acceptance of the certificate is included.</li> <li>-Number 4.2 "Key pair" is added to the definition of numeral 4.2.</li> <li>-4.2.1 Renewal of certificate keys is included.</li> <li>-4.4 Certificate Suspension is included.</li> <li>-Section 4.6 "Replacement of certificates" includes the procedure for the replacement of certificates.</li> <li>-Section 6.7 "Termination of the CA and RA" is included.</li> <li>-The latest version of the OID identifier is updated in numeral 7.2.6.</li> <li>-The certificate extension code is included in 7.2.7 User Notice section.</li> <li>-Clarifying note is included in section 9.1 regarding the cost of revoking certificates.</li> </ul>	Policy and Security Committee
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</p>	Policy and Security Committee


	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<p>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 virtual token are included.</p> <p>The title of item 9.5, rights and duties, has been updated.</p> <p>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"> <li>- - The OID, Version and date of issuance of the document are updated.</li> <li>- - Section 3.2.2.2. includes the types of mechanism with the description of validation of the applicant's identity (onboarding or notarized letter).</li> <li>- - In section 3.2.2.1, the e-mail for confirmation is included.</li> <li>- - The validity of the RUT document is modified to 90 days.</li> </ul>	Policy and Security Committee
7.0	14/04/20232	<ul style="list-style-type: none"> <li>- The OID, Version and date of issue are updated in the Document Name and Identification section</li> <li>- The position of Operations Manager is modified to Operations Director</li> </ul>	Policy and Security Committee


	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<ul style="list-style-type: none"> <li>- Updated "Identity Authentication" section including identity validation and note for document requirements</li> <li>- Updated the limits of use of certificates in the virtual token delivery format</li> <li>- Updated Andes logo and font. - Updated colors of the format according to the 2023 brand manual</li> </ul>	
8.0	16/11/2023	<ul style="list-style-type: none"> <li>- Updated OID and Version</li> <li>- ANDES phone number is updated</li> <li>- SCD.</li> <li>- Title 6.7 is modified from "Termination of CA or RA" to "Cessation of ECD activities".</li> <li>- The term "Declination of applications" is included.</li> <li>- In the response time it is specified that validation of successful identity validation is successful identity validation.</li> <li>- Conditions for the replacement of certificates are modified.</li> </ul>	Policy and Security Committee
9	19/02/2024	<ul style="list-style-type: none"> <li>- The OID and Version are updated.</li> <li>- The Rates are updated, and the replacement value of the certificates is included.</li> </ul>	Policy and Security Committee
10	07/05/2024	<ul style="list-style-type: none"> <li>- The OID and Version are updated.</li> </ul>	Policy and Security Committee



	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

		<ul style="list-style-type: none"> <li>- The reasons for replacement are updated according to the type of certificate.</li> <li>- The usage limits of the certificates in operating systems are updated.</li> <li>- The RUT document is removed as a certificate requirement.</li> </ul>	
11	6/06/2024	<ul style="list-style-type: none"> <li>- The document's date, version, and OID are updated.</li> <li>- The principle of impartiality item is updated to include the term "Non-Discrimination."</li> <li>- The service rates are updated.</li> <li>- The documentary requirements table for the applicant's authentication and identification item is updated.</li> </ul>	Policy and Security Committee
12	24/01/2025	<ul style="list-style-type: none"> <li>- The logo and cover are updated according to the brand manual.</li> <li>- The document name, identification, OID, version, and date are updated.</li> <li>- The service rates are updated.</li> <li>- The section related to certificate replacement is modified.</li> <li>- The "Identity Authentication" section is updated to include a note on documentary requirements.</li> <li>- The "Response Times" item is reviewed and updated, incorporating the digital signature certificate delivery policy.</li> </ul>	Policy and Security Committee

	<b>CERTIFICATION POLICY PUBLIC FUNCTION</b>	Identificador OID:	1.3.6.1.4.1.31304.1.2.5.12
		Effective date:	24/01/2025
		Version:	12
		Classify of the information::	Public
		Elaborated:	Director of Operations
		Revised::	Policy and Security Committee
		Approved:	General Manager

SANDRA CECILIA RESTREPO MARTINEZ  
**General Manager**