andes
Servicio de Certificación Digital

ACADEMIC COMMUNITY CERTIFICATION POLICY

Andes SCD S.A.

andes Servicio de Certificación Digital	**ACADEMIC COMMUNITY CERTIFICATION POLICY**	OID Identifier:	1.3.6.1.4.1.31304.1.2.2.13
		Effective Date:	16/02/2026
		Version:	13
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Table of Contents

andes Servicio de Certificación Digital	**ACADEMIC COMMUNITY CERTIFICATION POLICY**	OID Identifier:	1.3.6.1.4.1.31304.1.2.2.13
		Effective Date:	16/02/2026
		Version:	13
		Classification of information:	Public
		Elaborated:	Chief Operating Officer
		Reviewed:	Policy and Security Committee
		Approved:	General Manager

Introduction

This Policy for Academic Community Certificates 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 an Academic Community Certificate 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 ACADEMIC COMMUNITY
Description	The Academic Community certificate certifies the identity of the subscriber and his/her quality as a teacher, student, graduate, administrator, associate, parent or member of an academic community, and allows the subscriber to digitally sign documents in his/her own name and interest.
OID Identifier	1.3.6.1.4.1.31304.1.2.2.13
Version	V 13
Date of issue	January 30, 2026
Location	https://www.andesscd.com.co/docs/pc_comunidadacademica.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 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 Martinez – 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 Academic Community Certification Policy is administered by the Policy and Safety Committee and is approved by the General Management of ANDES SCD, following the documented information procedure.

1.3.4. Publication of the document

The Academic Community Certification Policies and the Certification Practices Statement are documents for public use that are available on the Andes SCD website. Any modifications to these documents are published immediately maintaining a version history.

1.4. User community and applicability

The Academic Community certificates are issued to individuals, they accredit the identity of the holder and their quality as a teacher, student, graduate, administrator, associate, parent or member of an academic community in the signing of electronic

documents, guaranteeing the authenticity of the sender of the communication, the non-repudiation of the origin and the integrity of the content. The holder of an Academic Community certificate acts in his or her own name and interest.

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 Academic Community 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 applications, corroborate the identity of applicants in person and carry out a complete registration of applicants who wish to acquire a digital certificate of Academic Community in accordance with this Certification Policy.

Subscribers
The subscriber is the natural person who has acquired an Academic Community certificate issued by the Andes SCD Certification Authority to act in the electronic environment on their own behalf and is considered a subscriber while said certificate is valid.

Applicants
The applicant is the natural person who wishes to access digital certification services by acquiring an Academic Community certificate issued by Andes SCD. Under no circumstances are applications for this type of certificate accepted in the name of people who do not demonstrate that they are linked as a teacher, student, graduate, administrator, associate, parent or member of an academic community.

Users
The user is any person who voluntarily places their trust in the Academic Community certificates issued by the Andes SCD Certification Authority and who uses the certification service as a means to accredit 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 Academic Community certificate issued under this policy may be used for the following purposes:

Identity authentication

The certificate can be used to identify a natural person as a teacher, student, graduate, administrator, associate, parent or member of an academic community in the field of their activity.

Digital signature

Digital signatures made with Academic Community certificates 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

1.5.2. Certificate usage limits

Academic Community certificates may not be used to act as either a Registration Authority or a Certificate Authority, signing other public key certificates of any kind or lists of revoked certificates (CRLs). Nor may they be used for purposes contrary to current legislation.

1.5.2.1. Certificate usage limit on operating systems

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

- **Virtual Token:**

For the use of the virtual token it is essential to have the Windows 10 operating system and higher in 64 and 32-bit versions; for the MacOS operating system it is required to use the online signature service provided by Andes SCD through our website.

- **Physical Token:**

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

- **Centralised:**

The delivery of certificates under the centralized signature model is conditional on the development for the integration of the web services exposed by ANDES SCD, to allow signing operations making use of the certificates escrowed 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 Academic Community 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.

- 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:

a) Type of certificate
b) PC OID Reference
c) Certificate serial
d) Effective start
e) End of validity
f) Certificate holder
g) Entity
h) Certificate delivery form
i) Revocation Code
j) PIN

2. Certificate Publication and Registration

All system data relating to the life cycle of certificates are kept digitally for the period established by current legislation where applicable. Current and expired certificates are retained published in LDAP in accordance with RFC 4523.

3. Identification and authentication

The procedures and criteria applied to verify the identity of the applicant and approve the issuance of an Academic Community certificate are described below.

3.1. Names

3.1.1. Types of names

The Academic Community certificates 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	Description
CN	Name	Full names and surnames of the subscriber
S	Serial	Identification document number
And	Email	Subscriber Email
C	Country	Abbreviation of the country where the subscriber resides
ST	Department	Name of the department where the subscriber resides
L	City	Name municipality where the subscriber resides
STREET	Address	Address where the subscriber resides
T	Title	Indicates the type of relationship of the subscriber with the academic community
1.3.6.1.4.1.4710.1.3.2		Document number + dv of the entity
Or	Organization	Corporate name of the entity or Academic Community.
OU	Unity Organizational	Academic Community Issued by Andes SCD Calle 26 #69c-03 Torre B oficina 701.

3.1.2. Need for names to be meaningful

All Academic Community certificates issued by Andes SCD have as their main characteristic the full identification of the subscriber and the assignment of a significant name to their certificate.

3.1.3. Anonymous and pseudonyms in names

Anonymous or pseudonymous to identify the name of a Natural Person is not permitted in this Certificate Policy.

In the case of a natural person with Colombian nationality, the name must be made up of names and surnames as it appears on the citizenship card. If the natural person is a foreigner, the name must be made up of names and surnames, 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. Uniqueness of the names

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

3.2. Identity Approval

3.2.1. Method to prove possession of the private key

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

3.2.2. Authenticating the Applicant's Identity

The applicant can process their request for the issuance of an Academic Community certificate in the following ways:

1. **Face-to-face**: the applicant makes the 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.

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
Citizenship card or document that proves identity (legible)	Submit original and photocopy Document	Digital PDF document required
Document or digital evidence issued by the educational institution stating the relationship with the applicant (Legible document that meets the requirements specified in item 3.2.2.1)	Submit Photocopy Document	Digital PDF document required

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.

3.2.2.1. Information required in the document that accredits the applicant's link to an entity.

Requirement	Observation

Document with membrete	Header and/or footer with name of the entity, corporate image, address, contact telephone number
Date not exceeding 90 days	The date of issue of the document must not exceed 90 calendar days
Accreditation of the identity of the person who belongs to the entity	It must include full name, type and identification number and explicitly indicate the position held by the person in the entity.
Full name, area and signature of the person issuing the document	It must include the full name, area to which it belongs, and the digital or handwritten signature of the person authorizing the issuance of the certificate by the company.

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 number, landline and cell phone
3	Personal Email
4	Institutional email

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

The information provided in the request for the issuance of the Academic Community certificate is studied by the RA agent who is in charge of verifying that the information is original, sufficient and adequate in accordance with the internal procedures defined by Andes SCD.

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

3.2.3. Unverified information about the applicant

The registration authority verifies all the applicant's information that is supported by documents or digital evidence as support. No Residence Address and Email 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.

When the delivery format is a physical token, the delivery time of the digital certificate after its issuance will depend on the place of destination. For more information, please refer to our certificate delivery policy on our website.

3.2.5. Identification and authentication to request revocation

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

- To the subscriber himself, in which case he must use the revocation code that was given to him at the time of acquiring the certificate.
- To the authorized representative of the academic community 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 academic community certificate issued to the subscriber.

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

4. Certificate lifecycle and operating procedures

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

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 application for a digital certificate can be made by any person linked to an educational institution, an educational institution and who is fully capable of assuming the obligations and responsibilities inherent to the possession and use of the certificate.

4.1.2. Procedure for requesting a certificate

The procedure that the applicant must carry out to acquire a digital certificate is described in the DPC Certification Practice Statement. See section "Procedure for requesting issuance of the certificate" in the DPC.

4.1.3. Acceptance of the certificate.

The procedure for accepting the certificate is described in the DPC Certification Practice Statement. See section "acceptance of the certificate".

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 Academic Community certificate 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 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

The subscriber can only use the certificate and the key pair after accepting the terms of use set out in the DPC and PC and only for what they establish.

4.1.5.2. From trusted users

Users who rely on the Andes SCD certification service should 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 Academic Community certificate.
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

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

4.4. Certificate Suspension

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 Application

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 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 who holds the certificate may request the revocation of an Academic Community certificate from the means of revocation offered by Andes SCD in the section "means to revoke certificates" of the DPC and following the revocation procedure specified in the section "procedure to revoke certificates of the DPC. Additionally, Andes SCD or any of the authorities that compose it may request the revocation of an Academic Community certificate 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:

- Loss of Token Device

- Loss or exposure of the certificate PIN.
- Change of the information of the holder of the digital signature, as long as it belongs to the same NIT of the community

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 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 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 holders of Academic Community Certificates are generated in accordance with the processes stipulated in the DPC section "Generation of the pair of Keys". The method of generating the subscriber's key pair varies according to the form of delivery of the certificate chosen by the subscriber or according to the agreement.

6.1.2. Delivery of the private key to the subscriber

When the private keys of the Academic Community certificates are generated by ANDES SCD, they may only be stored on cryptographic devices that comply with the FIPS 140-2 Level 3 standard.

When the delivery format is PKCS10 the key pair is generated by the subscriber himself, the private key is at no time known by ANDES SCD

The mechanism for handing over the private key to holders of Academic Community Certificates is described in the DPC. 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 for handing over the public key to holders of Academic Community Certificates is described in the DPC. Section "Delivery of the public key to the issuer of the certificate"

6.1.4. Subscriber Public Key Distribution

The public key of any subscriber of Academic Community Certificates 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 Academic Community certificate 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 Class II or Final Entity certificate-issuing CA.

6.1.7. Size of the keys

The minimum size of Academic Community certificate keys is 2048 bits based on the RSA algorithm.

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

6.2. Private Key Protection Controls

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 controls for protecting the subscriber's private key:

Protection Control	Subscriber-generated private key from Device TOKEN and CSR
Private Key Backup	Andes SCD does not perform backup, nor is any recovery mechanism implemented on the private keys of the subscribers generated from the TOKEN device or 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
Private Key Storage	Subscribers' private keys generated from the 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 through the retention of the TOKEN device or other methods, because

	they may be necessary to decrypt the historical information encrypted with the public key
Private Key Transfer	The subscribers' private key generated from the TOKEN never leaves the device. With the TOKEN device, the pair of keys is generated and its use is protected through a PIN that only the subscriber knows. The user-generated private key that CSR delivers for certificate generation is held by the subscriber and is never sent to Andes SCD.
Private Key Activation	The activation of the TOKEN device containing the subscriber's private key is done through a PIN that must be customized by the subscriber himself at the time of generating the pair of keys. The protection of activation data is the responsibility of the subscriber
Deactivating the private key	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
Private Key Destruction	The destruction of the private key can be performed by the subscriber himself using the functions provided by the TOKEN device, taking care not to affect other private keys stored on the device. 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. Private keys of subscribers to the centralized signing service are generated and stored in a protected form within an HSM, using

	key wrapping mechanisms with a non-exportable AES key. The Certificate Authority does not access or process keys in clear text, and their use is strictly controlled through authentication, authorization, and validation of the certificate status. When a certificate expires or is revoked, the associated private key is permanently disabled for use, preventing any further cryptographic operations, even if the protected material remains stored. This scheme guarantees the impossibility of use and non-reuse of private keys, in compliance with WebTrust criteria.

6.3. Supported Cryptographic Devices

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

- Generates RSA key pairs up to 2048 bits.
- 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

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.

6.4. Other aspects of key pair management

6.4.1. Public Key File

Andes SCD keeps all the digital certificates of the Academic Community, which include the public key, on file during the period stipulated in the "public key archive" section of the DPC.

6.4.2. Certificate Operational Periods and Key Pair Usage Periods

The lifetime of the Academic Community certificate 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 from the academic community 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 subscriber must generate the activation data of their TOKEN by changing the initial PIN that the device comes with by default.

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

6.5.2. Activation Data Protection

The PIN or activation data of the TOKEN must be personalized by the applicant before generating their pair of keys 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 manufacturer of the TOKEN and which is available on the Andes SCD website.

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

Academic Community Certificate Format		
Field	**Description**	**Value**
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 or Class III CA Subordinate CA data in the 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	Subscriber's full name
	Serial Number	Subscriber identification document number
	And	Subscriber Email
	C	Abbreviation of the country where the subscriber resides
	ST	Name of the department where the subscriber resides
	L	Name municipality where the subscriber resides
	STREET	Address where the subscriber resides
	T	Indicates the type of relationship of the subscriber with the academic community.
	Or	Name of the university or Academic Community.
	OU	Name of faculty and career to which it is linked
	OU	Academic Community Issued by Andes SCD Off. Calle 26 NO 69C-03

Public Key	Public key of the certificate holder	RSA (2048 Bits)
Extensions	Extensions used in certificates	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 fingerprint of the certificate data	fingerprint
Using the Key	Purposes for which the certificate should be used.	Digital Signature No repudiation Information encryption

7.2. Certificate Profiles

7.2.1. Version number

Academic Community 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 Academic Community 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 extensions included in the Academic Community digital certificates are detailed below.

Extensions Certificates Academic community according to X.509V3 standard	
Name	**Value**
Access to issuer information	Access Method=Online Certificate Status Protocol Dirección 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
CRL Distribution Points	CRL publication URL of the CA that issued the certificate.
Using the Key	Digital Signature No repudiation Information encryption
Improved key usage	Client authentication Secure Email
Alternative name of the holder	Email del suscriptor RFC 822 Name (e-mail address)
Basic Restrictions	Subject Type=End Entity Path Length Constraint=None
Certificate policy	[1]Certificate policy: Policy ID=1.3.6.1.4.1.31304.1.2.2.13 [1,1]Policy certifier information: Policy Certifier ID=User Notice Certifier: Notice Text=The use of this certificate is subject to the Academic Community (PC) Certificate and Certification Practices (DPC) Policies established by Andes SCD. [1,2]Policy certifier information: Policy certifier ID=CPS Certifier: Current DPC URL

7.2.3. Algorithm object identifiers

Academic Community digital 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 Academic Community Digital Certificates 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 1.3.6.1.4.1.31304.1.2.2.13

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

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 identifier of the Academic Community Certificate Policy
- **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 CPs of the academic community and the DPCs 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
Issue distribution points	URL where the CRLs issued by Andes SCD are published	View the CRL for the publication URL
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.

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

Delivery Format	1 year	2 years	Replacement value
Token Virtual	$ 1 176,418	$ 261,360	$86,500
Physical Token	$ 176,418	$ 261,360	$110,000

- All the rates presented above are values before VAT
- The replacement value applies for the remaining validity of the certificate to be replaced, as long as the conditions mentioned in the Replacements item of this Certification policy 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 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 Statement of Certification Practices lists the rights and duties of the Andes SCD Certification Authority.

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 subscribers.

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

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

Firmado por:
Sandra Cecilia Restrepo Martinez
2026/02/16 09:16:52:484

SANDRA CECILIA RESTREPO MARTINEZ
General Manager

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	- 3.1.1 and 7.1.1 – Certificate distinguish name is updated - 6.1.7 and 7.1.1 – Increased size of keys to 2048 - 6 – Reference is made to the form of delivery of PKCS12 certificates - 4.6 – Certificates of different validity are offered. The validity is explicit in the certificate itself	Policy and Security Committee
2.0	09/10/2014	- 1.3 - Andes SCD address and PBX are updated - 3.1.1 and 7.1 - Updated OU attribute of the DN to Academic Community Certificate Issued by Andes SCD Av. Calle 72 # 9 - 55 Office 501 - 3.2.2 - Documents required for issuance of digital signature certificate are updated - Full document - Updated p12 term by PKCS12 - 6.1.7 - In the section size of the keys, the minimum term to refer to the size of the	Policy and Security Committee

		keys generated by Andes SCD is eliminated. - 3.1.1 and 7.1 - On 27 January 2015 the OU attribute of the DN is abbreviated to Academic Community Issued by Andes SCD Av. Cll 72 9 55 Of 501	
2.1	24/11/2015	- 1.1 - PC document version and issue date are updated - 1.3 - Contact details and organization that manages the document is updated - 1.5.2 - Reference to OID document with limitations of use certificates of conventions - 3.1.1 and 7.1 - Updated the OU attribute of the DN to: Academic community Issued by Andes SCD Cra 27 86 43 - 7.2.2 - Updated OID PC and URL DPC Certificate Policy	Policy and Security Committee
2.2	26/09/2016	- 1.3.2 – Contact person email is updated - 4 – The maximum validity of the certificate is limited to 730 days. - 4.5 – Replacement of certificates is included. - 4.7 – The maximum validity of the certificate is limited to 730 days. - 7.2.1 - RFC 3280 is updated by 5280	Policy and Security Committee
2.3	06/01/2017	- 4, 4.7 – It is specified that the maximum validity of the certificate is 730 calendar days - 6.1, 6.2, 6.3, 6.4 PKCS12 Delivery Form Removed - 7.2 DPC and PC URL and Version 2.3	Policy and Security Committee
2.4	22/06/2018	- 1.5.4 The minutes and contracts section is included.	Policy and Security Committee

		- 2. Reference is made to RFC 4523 related to LDAP . - 3.2.3 Reference is made to the registration authority in charge of collecting the required evidence. - 3.2.4 Revocation key term is replaced by revocation code - 4. The term subscription contract is deleted - 4.5 A condition for replacement of certificates was included - 6.1.2 Reference is made to FIPS 140-2 Level 3 cryptographic devices for the delivery of the private key of subscribers. - 6.3 Reference is made to cryptographic devices. - 6.3.1Reference is made to risks of cryptographic devices and security recommendations. - 7.2.2 The link to the DPC is updated in the certificate policy - 7.3.2 Updated SHA256withRSA Signature Algorithm - 9.1 Certificate fees are included according to validity - 9.5.1 Obligations and responsibilities of ANDES SCD are described. - 9.5.2 Subscriber obligations are described. - 9.5.3 Subscriber prohibitions are described. - 9.6 Reference is made to the principle of impartiality	
2.5	16/07/2018	- 7.2.2 reference to current DPC URLs	Policy and Safety Committee

2.6	14/09/2018	- 1.1 Updated issue date and download url from PC. - 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 Safety Committee
2.7	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 Safety Committee
2.8	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
2.9	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. - The PC OID is updated.	Policy and Safety Committee
3.0	28/04/2021	- The description of the name of the document is updated, expanding the subscribers of this certificate. - Section 1.4 is updated. Community of Users and Applicability, expanding the subscribers of this certifying. - Section 1.5.1 is updated. Uses of the	Policy & Safety Committee / SGI Senior Analyst

		Certificate, expanding the subscribers of this certifying. - The DN attributes are updated in section 3.1.1. - Section 3.2.2. Authentication of the applicant's identity, the table of requirements and the table of minimum requirements of the document that proves the person's link to the entity is 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 updated.	
4.0	15/06/2022	- -The OID of the PC is updated. - -The position "Director of Projects and Operations" is updated to "Operations Manager" responsible for preparing the document. - -Update of numeral information 1.1 in accordance with the new version of the document. - -Numeral 4.1 the definition "issuance" is updated to "request". - -Numeral 4.1.3 Acceptance of the certificate is included. - -It is added to the definition of numeral 4.2 "Pair of keys". - -Numeral 4.2.1 Renewal of certificate keys is included. - -Numeral 4.4 Suspension of certificates is included. - -Numeral 4.6 replacement of certificates includes the procedure for the replacement of certificates. - -Numeral 6.7 "Termination of the CA and	Policy and Safety Committee / Senior Analyst SGI.

		RA" is included. - -The latest version of the OID identifier is updated in numeral 7.2.6. - - The code of the certificate extension is included in numeral 7.2.7 User Notice section - - An explanatory note is included in numeral 9.1 regarding the cost of revoking certificates.	
5.0	12/10/2022	- The OID identifier, the date of issue, version, and date of the document are updated. - Updated in numeral 1.3.2 name of legal representative and contact email - Numeral 1.5.2.1 Limit of use of certificates in operating systems is included. - 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 the certificate is modified in accordance with the requirements of the CEA. - Numeral 4.4 suspension of the certificate is modified in accordance with the requirements of the CEA. - Item 5, security controls, is updated. - Numeral 9.1 Fees is updated and the fees for the virtual token are included. - The title of numeral 9.5 is updated for rights and duties. - The title and content of numeral 9.5.1 Rights and duties of Andes SCD are modified.	Policy and Safety Committee / Senior Analyst SGI.

6.0	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).	Policy and Safety Committee / Senior Analyst SGI.
7.0	14/04/2023	- 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 numeral "identity authentication" is updated to include identity validation and note for documentary requirements - The usage limits of certificates in the virtual token delivery format are updated. - Andes logo and font of the letter are updated. - Document colors are updated according to the 2023 brand manual	Policy & Safety Committee / SGI Senior Analyst
8.0	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 "Cessation of activities of the ECD". - Term decline of applications is included - The response time specifies that you must have successful identity validation. - One of the conditions for replacing certificates is modified.	Policy & Safety Committee / Chief Operating Officer / Senior Analyst SGI

9	19/02/2024	- OID and Version Updated - The Rates are updated and the replacement value of the certificates is included.	Policy & Safety Committee / Chief Operating Officer / SGI Professional
10	07/05/2024	- OID and Version Updated - Replacement reasons are updated according to the type of certificate. - Updated limits on the use of certificates in operating systems - RUT document is eliminated as a requirement of the certificate.	Policy & Safety Committee / Chief Operating Officer / SGI Professional
11	06/06/2024	- Date, version, and OID of the document are updated - The item principle of impartiality is updated to include the term Non-Discrimination. - Service rates are updated. - The table of documentary requirements of the item authentication identification of the applicant is updated.	Policy & Safety Committee / Chief Operating Officer / SGI Professional

12	24/01/2025	- The logo and cover are updated according to the brand manual. - The document name, ID, OID, version, and date of the document are updated. - 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 reviewed and updated, incorporating the policy for the delivery of digital signature certificates.	Policy & Safety Committee / Director of Operations / Operations Coordinator
13	30/01/2026	- Updating the OID, version, and date 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