



CERTIFICATION PRACTICES STATEMENT(CPS)

Andes SCD S.A.

2023






	<p align="center">CERTIFICATION PRACTICES STATEMENT</p>	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

TABLE OF CONTENTS


1. Document presentation	10
1.1. Document Name and Identification	10
1.2. Identification of the Digital Certificacton Entity	11
1.3. Identification of Data Center Main.....	11
1.4. Identification of Data Center Alternate	12
1.5. Scope	13
1.6. Activities and services accreditates from ANDES SCD	13
1.7. References	13
1.8. Definitions.....	14
1.9. List of abbreviations and acronyms.....	15
1.10. Participants of PKI or Trust Model	15
1.10.1. Certification Authority (CA)	16
1.10.2. Registration Authority (RA)	19
1.10.3. Subscriber	20
1.10.4. Applicant	20
1.10.5. Accepting user Input.....	20
1.10.5.1. Precautions to be observed by third parties	20
1.11. Scope of application	21
1.11.1. Certificate Uses	21
1.11.2. Limits on the use of certificates	21
1.11.2.1. Limits on the use of certificates in operating systems	21
1.11.3. General Prohibitions.....	22
1.11.4. Prohibitions on the use of certificates	22
1.11.5 Minutes and Contracts.....	23
1.12. Certification services catalog	23

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.12.1.	Certificates for Final Entity	23
1.13.	Policy Administration.....	25
1.13.1.	Organization is administering this document	25
1.13.2.	Contact Person	26
1.13.3.	Policy approval procedures.....	26
1.13.4.	Document publication	26
2.	Publication and registration of certificates.....	26
2.1.	Certificate Directory	26
2.2.	Publication media.....	27
2.3.	Frecuencia de publicación Publication frequency	29
2.4.	Certificate directory access control.....	29
3.	Identification and authentication	30
3.1.	Names	30
3.1.1.	Name Types.....	30
3.1.2.	Need for names to be meaningful	30
3.1.3.	Anonyms and pseudonyms in names.....	30
3.1.4.	Rules for interpreting name formats.....	30
3.1.5.	Singularity of names	30
3.1.6.	Recognition, authentication and function of registered trademarks	31
3.2.	Identity Approval.....	32
3.2.1.	Method for proving possession of the private key	32
3.2.2.	Identity Authentication.....	34
3.2.3.	Unverified Applicant Information.....	35
3.2.4.	Criterion for interpretation	35
3.2.5.	Identification and authentication to request revocation	36
4.	Certificate lifecycle and operating procedures.....	36
4.1.	Request for certificates.....	36

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.1.1. Who can request the issuance of a certificate	36
4.1.2. Procedure for requesting the issuance of certificates	36
4.1.3. Acceptance of the certificate	37
4.1.4. Publication of the certificate by ANDES SCD	38
4.1.5. Key pair and use of the certificate	38
4.1.5.1. On the part of the subscriber.....	38
4.1.5.2. From users who trust	39
4.2. Processing of certificate requests	39
4.2.1. Response Times	39
4.3 Issuance of certificates.....	39
4.3.1 Certificate Issuance Procedure	39
4.4. Certificate Renewal - Key Pair.....	40
4.4.1. Renewal of certificate keys	40
4.5. Modification of certificates.....	40
4.6. Suspension of certificates	40
4.7. Revocation of certificates.....	40
4.7.1. Causes of revocation	40
4.7.2. Who can request the revocation of certificates	42
4.7.3. Means of revoking certificates.....	42
4.7.4. Procedure to revoke certificates	43
4.7.5. Time for processing revocation request.....	45
4.7.6. Requirements for verification of revocations from Users who trust in ANDES SCD 45	
4.7.7. Publication of revoked certificates	45
4.8. Certificate status information services.....	46
4.8.1. Operational characteristics.....	46
4.8.2. Service availability	46

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.8.3. End of subscription.....	47
4.9. Replenishment of certificates	47
4.10. Validity of certificates.....	47
5. Security controls	47
5.1. Conditions required of critical suppliers	47
5.2. Physical security controls	48
5.2.1. Location and Environmental Safety	48
5.2.2. Access system management	50
5.2.3. Security of servers.....	50
5.3. Procedural controls	51
5.3.1. Roles of confidence	52
5.3.2. Number of persons required by task	55
5.3.3. Identification and authentication of each role	55
5.3.4. Roles requiring separation of duties.....	55
5.3.5. Relationship between ANDES SCD and the Registration Authorities	55
5.3.6. Personal security controls	56
5.3.6.1. Qualifications, experience and requirements.....	56
5.3.7. Background check procedures	57
5.3.8. Training requirements	57
5.3.9. Training frequency and requirements	57
5.3.10. Frequency of job rotation	57
5.3.11. Penalties for unauthorized actions.....	57
5.3.12. Recruitment requirements	58
5.3.13. Documentation provided to personnel	58
5.4. Audit Controls	58
5.4.1. Types of audited events.....	58
5.4.2. Frequency of processing of audit records.....	59

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


5.4.3.	Period of storage of audit records	59
5.4.4.	Protection of Audit Records	60
5.4.5.	Procedures for backing up audit records	60
5.4.6.	Audit information collection systems.....	60
5.4.7.	Event review systems	60
5.4.8.	Vulnerability analysis	60
5.5.	Information storage and archiving controls.....	61
5.5.1.	Type of information to be safeguarded	61
5.5.2.	Information storage period.....	61
5.5.3.	Information protection.....	61
5.5.4.	Information backup procedure	61
5.5.5.	Internal and external storage systems	61
5.5.6.	Procedure for obtaining and verifying archived information	62
5.6.	Key change	62
5.7.	Engagement and disaster recovery.....	62
5.7.1.1.	Incident management procedures.....	62
5.7.2.	Informatics resources, software and corrupted data.....	64
5.7.3.	Procedures in the event of private key compromise	64
5.7.4.	Business continuity capabilities in the event of disaster.....	64
5.7.5.	Measures to Correct Detected Vulnerabilities.....	65
5.8.	Termination of CA or RA.....	¡Error! Marcador no definido.
6.	Technical safety controls	66
6.1.	Key generation and installation	66
6.1.1.	Key Pair Generation.....	66
6.1.2.	Delivery of the private key to the subscriber	68
6.1.3.	Delivery of the public to the certificate issuer.....	69
6.1.4.	Subscriber Public Key Distribution	69

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


6.1.5.	ANDES SCD public key distribution to users	70
6.1.6.	Period of use of the private key	70
6.1.7.	Size of keys.....	70
6.1.8.	Public key generation and quality check parameters	71
6.2.	Private Key Protection Controls	71
6.2.1.	Private Key Protection Controls	71
6.2.2.	Control over the private key (Multi-person)	71
6.2.3.	Private Key Backup	71
6.2.4.	Private key storage.....	72
6.2.5.	Transfer of the private key from or to a cryptographic module	72
6.2.6.	Storage of the private key in a cryptographic module.....	73
6.2.7.	Method of activating the private key	73
6.2.8.	Private key disabling method.....	73
6.2.9.	Method of destruction of private key	74
6.2.10.	Classification of cryptographic modules.....	75
6.3.	Other aspects of key pair administration	75
6.3.1.	Public Key File	75
6.3.2.	Operational periods of the certificate and periods of use of the key pair.....	75
6.4.	Activation data.....	75
6.4.1.	Generation and Installation of Activation Data	75
6.4.2.	Activation Data Protection.....	76
6.5.	Informatic security controls.....	77
6.5.1.	Specific technical safety requirements.....	77
6.5.2.	Information security level.....	77
6.6.	Technical life cycle controls.....	77
6.6.1.	Controls in system development.....	77
6.6.2.	Safety Management Controls.....	78

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


6.6.3. Life Cycle Safety Controls.....	78
6.7. Network security controls.....	78
6.8. Time stamp.....	79
7. Certificate profiles, CRL y OCSP.....	79
7.1. Certificate profiles.....	79
7.1.1. Version number.....	79
7.1.2. Certificate Extensions.....	79
7.1.3. Identifiers object of the algorithm.....	80
7.1.4. Name Formats.....	80
7.1.5. Name Restrictions.....	80
7.1.6. Object identifier of the certification policy.....	80
7.1.7. Syntax and semantics of policy qualifiers.....	81
7.1.8. Profile of the CRL.....	81
7.1.8.1. Version number.....	81
7.1.8.2. CRL and extensions.....	81
7.2. Profile OCSP.....	84
7.2.1. Version number.....	84
7.2.2. Extensions OCSP.....	84
8. Audit and other valuations.....	85
8.1. Frequency or circumstances of assessment.....	85
8.2. Identity and Qualifications of the Advisor.....	85
8.3. Relationship between the assessor and the assessed entity.....	85
8.4. Topics covered in the valuation.....	85
8.5. Actions taken as a result of Non-Conformities.....	86
8.6. Communication of results.....	86
9. Business and legal matters.....	86
9.1. Rates.....	86

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.1.1.	Certificate issuance fees	86
9.1.2.	Certificate Access Fees.....	86
9.1.3.	Fees for information on the status of revoked certificate(s)	86
9.1.4.	Reimbursement policy	86
9.1.5.	Inappropriateness of the claim for reimbursement	87
9.2.	Financial responsibility	88
9.3.	Confidentiality of Business Information.....	89
9.3.1.	Scope of confidential information	89
9.3.2.	Information not considered confidential	89
9.3.3.	Responsibilities for protecting confidential information.....	90
9.4.	Confidentiality of personal information.....	90
9.4.1.	Privacy plan	90
9.4.2.	Information considered confidential.....	90
9.4.3.	Information not considered confidential	90
9.4.4.	Responsibility to protect information.....	91
9.4.5.	Notification and consent to use confidential information	91
9.4.6.	Access to information from judicial or administrative proceedings	91
9.5.	Intellectual property rights	91
9.6.	Rights and duties.....	91
9.6.1.	Rights and duties of ANDES SCD	91
9.6.2.	RA Rights and duties	93
9.6.3.	Applicant's rights and duties	94
9.6.4.	Subscriber Rights and Duties	94
9.6.5.	Rights and duties of the relying parties	99
9.7.	Limitations of liability	100
9.7.1.	Responsibility for the veracity of the Subscriber's information	100
9.7.2.	Responsibility for service availability	100

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.7.3. Responsibility for the functionality of the service in the Subscriber's infrastructure	100
9.7.4. Responsibility in cybercrimes.....	101
9.7.5 Warranty disclaimers.....	101
9.8. Protection of personal data	102
9.9. Indemnifications	102
9.10. Term and termination.....	103
9.10.1. Termination of provisions.....	103
9.10.2. Termination and survival effect.....	103
9.11. Individual Notification and Communication with Participants	103
9.12. CPS and CP change procedure.....	103
9.12.1. Change procedure.....	103
9.12.2. Notification mechanism and reporting period.....	104
9.12.3. Circumstances under which the OID must be changed.....	104
9.13. Dispute Prevention and Resolution	104
9.14. Applicable Law.....	104
9.15. Compliance with applicable law.....	105
10. Change Control.....	105

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Introduction

ANDES SCD is an Open Certification Entity accredited by the National Accreditation Organization of Colombia ONAC to provide its digital certification services in the Colombian territory and in accordance with the Colombian regulations in force. The accreditation certificate **16-ECD-004** granted to ANDES SCD is available in the final accreditation directory - Ent. Certificación digital: <https://onac.org.co/certificados/16-ECD-004.pdf>

1. Document presentation


This document compiles the certification practices statement (CPS) which defines the functioning and operation from the infrastructure of the public key PKI from Andes SCD, also explain the norms and practices from the Certification Authority (CA) to provide the service, also have the technical and legal rules to approve, issue, use and revoke certificates inside to the hierarchy of certification.

The certification practices are a mechanism to evaluate the trust grade that has been deposited in a digital certificate, which should be recognized and applied by the members from the certificated authority, the members from the register authority, subscribers, applicant and users that trust in the issued certificates by Andes SCD.

This CPS takes for granted the reader knows all the basic concepts about the system from the public key infrastructure, certificate and digital signature; otherwise Andes SCD recommends to the reader that is formed in the knowledge from these concepts before proceeding with the reading of this document.

1.1. Document Name and Identification

Document	CERTIFICATION PRACTICES STATEMENT
Description	This document presents the statements from the authority of certification ANDES SCD about the operation and procedures used as support to the certification service in compliance with the current legislation
OID Identifier	1.3.6.1.4.1.31304.1.1.1.8.0
Version	8.0
Date of issue	November 16th, 2023
Ubication	https://www.andesscd.com.co/docs/CPS_AndesSCD.pdf

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.2. Identification of the Digital Certificacton Entity

Name	Andes Servicio de Certificación Digital S.A.
Company's business name	Andes Servicio de Certificación Digital S.A.
TIN	900.210.800 – 1
Chamber of Commerce registration	01774848 February 15, 2008
Certificate of existence and legal representation	https://www.andesscd.com.co/docs/Certificado_de_existencia_y_representacion_legal.pdf
Office address and correspondence	Calle 26 #69c-03 Torre B oficina 701, Bogotá D.C.
Telephone	(601) 2415539
Email address	info@andesscd.com.co
Address for requests, queries and claims	Calle 26 #69c-03 Torre B oficina 701, Bogotá D.C.

The above information it's available in the web page from ANDES SCD section who we are.

1.3. Identification of Data Center Main

Name	Comunicación Celular S A Comcel S A
Company's business name	Comunicación Celular S A Comcel S A
TIN	800.153.993-7
Chamber of Commerce registration	00487585
Certificate of existence and legal	https://www.andesscd.com.co/docs/Certificado_de_existencia_y_representacion_legal_Comcel.pdf

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

representation	
Office address and correspondence	Carrera 68ª # 24B – 10
Telephone	601-7429797
FAX	601-7429797
Email address	notificacionesclaro@claro.com.co
Address for requests, queries and claims	Carrera 68ª # 24B – 10
Data center main address	Telmex Colombia S.A. (Claro) / Medellín Highway Km 7 Celta Trade Park via Bogotá, 32, Triara, Funza, Cundinamarca, Colombia

1.4. Identification of Data Center Alternate

Name	Cirion Technologies Colombia S.A.S
Company's business name	Cirion Technologies Colombia S.A.S
TIN	800.136.835-1
Chamber of Commerce registration	00464163
Certificate of existence and legal representation	https://www.andesscd.com.co/docs/Certificado_de_existencia_y_representacion_legal_Datacenteralternativo.pdf
Office address and correspondence	Carrera 185 No. 45 – 03 Centro Comercial Santafe Torre Empresarial P
Telephone	601 6119000
FAX	601 6119000
Email address	gustavo.torres@ciriontechnologies.com
Address for requests, queries and claims	Street 45 No. 185 – 03 Shopping Mall Santafe Torre Empresarial P
Data center alternate address	Street 16 A # 68 -27 Bogota D.C, Colombia

	<p align="center">CERTIFICATION PRACTICES STATEMENT</p>	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.5. Scope

This document states the norms and rules to follow for the certificate authority ANDES SCD in the providing of its certification services, stipulates certificate lifecycle procedures, and the legal regime applied to the members of the trust model.

There are additional documents supplementing this statement, called Certification Policies (CP) every Policies of Certification it's been for a type of certificate in particular and give all conditions, procedures and use for the type of certificate.

This document and the additional called Certificates Policies that with the RAC

1.6. Activities and services accreditates from ANDES SCD

For knowledge of the activities and services accredited by Andes SCD, reference is made to consumers and the general public that, on the Andes SCD website,

accredited activities and services are found, such as:


- ✓ Issuance of digital certificates for legal representation, company membership, public function, qualified professional, natural person, legal person, the academic community, and electronic invoicing.
- ✓ Chronological stamping.

1.7. References

This Statement of Certification Practices is issued taking into account the recommendations of the (Requestforcomments) **RFC 3647**: Internet X.509 Public Key Infraestructure: Certificate Policy and Certification Practices Framework.

The following standars have been taken into account:

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

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.8. Definitions

Word	Description
Audit	A procedure used to validate that controls are operational and fit for purpose. Includes logging and analysis of activities to detect intrusions or abuses in an information system. Defects found in an audit must be reported to the appropriate management staff to be addressed and fixed.
Public Key and Private Key	The public key is included in the digital certificate and the private key is used only by the certificate holder. Anything that is encrypted with one of the keys can only be decrypted with the other and vice versa.
Data Center	A data center is a building or portion of a building whose primary function is to house a computer room and its support areas. Computer centers are the brain of the information systems of companies, operating 7x24x365 with very high reliability requirements
IT Component	Any hardware or software device capable of using digital certificates, for your own use, for the purpose of identifying yourself or exchanging signed or encrypted data
HSM	Hardware Secure Module. Componente que ofrece una mayor seguridad para la generación y almacenamiento de Llaves Component that offers greater security for the generation and storage of Keys
Public Key Infrastructure (PKI)	. It is the set of people, policies, procedures and computer systems necessary to provide authentication, encryption, integrity services. and non-repudiation through cryptography of public and private keys and digital certificates.
Trusted Hierarchy	Set of Certificate Authorities that maintain relationships of trust by which a higher-level CA ensures the reliability of one or more lower-level CA. For Andes SCD In the case of ANDES SCD the hierarchy has 3 levels, the root CA at the top level guarantees the trust of your Class I, Class II, and Class III subordinate CA, And at the third level are the subordinate CA of the CA Class III conventions

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Word	Description
Certificate Revocation List	(CRL: CertificateRevocationList): Restricted access list containing only revoked certificates.
Online Certificate Status Protocol	OCSP (Online Certificate Status Protocol): Protocol that allows you to quickly and easily check the validity of an electronic certificate
PKCS10	Public key cryptography standard No. 10 that defines the structure for a certificate signing request.
Certificate Policies (CP)	Provisions for indicating the applicability of a certificate to a community, moreover indicate the suitability of a certificate to an application type with common security requirements
X.509	Standard developed by the ITU for Public Key Infrastructures and so-called "Attribute Certificates"

1.9. List of abbreviations and acronyms

Abbrev	Description
CA	Certification Authority
CRL	Certificate Revocation List
CPS	Certification Practices Statement
FIPS	Federal Information Processing Standard
RA	Registration Authority
OID	ObjectIdentifier Digital
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure

1.10. Participants of PKI or Trust Model

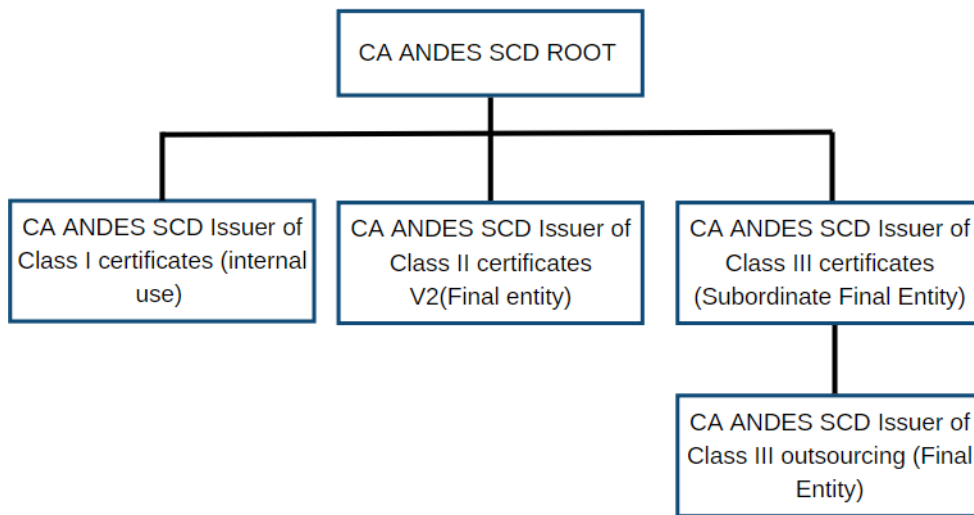
The entities and people that intervene in the trust model are:

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.10.1. Certification Authority (CA)

Andes SCD is a trusted entity that provides certification services, is empowered to issue, manage and revoke digital certificates, acting as a third party of trust between the subscriber and the user in online transactions.

The ANDES SCD certification hierarchy is composed of the following Certification Authorities:




	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

CA ANDES SCD Root: It is the first level Certificate Authority that issues certificates for itself and for its Subordinate Certificate Authorities (CAs: CA ANDES SCD Issuer of Class I certificates (internal use) : CA ANDES SCD Issuer of Class II certificates (Final entity) and CA ANDES SCD Issuer of Class III certificates (Subordinate Final entity)

Certificate Details of CA Root		
Distinctive Name	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Serial number	2c 31 02 20 35 d1 91 b2	
Distinctive Name of the issuer	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Period of validity	From Saturday, September 24, 2016 11:50:57 AM To Monday, July 09, 2035 11:36:59 AM	
Key Uses	Digital signature, Certificate signature, Signature CRL	
Digital footprint (SHA-1)	39 77 88 4d a7 b8 3a 00 6a ed 15 8d 50 6a ac 86 1b ca 1a 4f	

CA ANDES SCD Issuer of Class I certificates (internal use): It is the second level Subordinate Certificate Authority CA ANDES SCD Root that issues from an internal use for the employees and informatics components from the Certification Authority and Registration Authority


Certificate Details of CA class I		
Distinctive Name	CN	CA ANDES SCD S.A. Clase I
	O	ANDES SCD
	OU	Certification Division internal use
	C	CO

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

	L	Bogota D.C.
	E	info@andesscd.com.co
Serial number	75 4d 22 a1 3e f3 29 88	
Distinctive Name of the issuer	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogota D.C.
	E	info@andesscd.com.co
Period of validity	From Friday, July 03, 2020 11:03:12 AM. To Monday, July 01, 2030 11:03:12 AM	
Key Uses	Firma digital, Firma de certificados, Firma CRL	
Digital footprint (SHA-1)	b0 50 07 ac 9b 5a 13 f2 e3 da 72 67 38 47 01 d9 45 93 58 cc	

CA ANDES SCD Issuer of Class II certificates V2(Final entity): It is the second level Subordinate CA ANDES SCD Root, Certificate Authority his function is issues Final entity certificates.

Certificate Details of CA class II v2		
Distinctive Name	CN	CA ANDES SCD S.A. Clase II v2
	O	ANDES SCD.
	OU	Certification Division final entity
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Serial number	44 b6 b4 c3 3d e1 0b 68	
Distinctive Name of the issuer	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Period of validity	From Tuesday, August 06, 2019 11:14:53 a.m. Until Saturday, November 15, 2025 12:34:30 p.m	
Key Uses	Digital signature, Certificate signature, Signature CRL	

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Digital footprint (SHA-1)	47 e8 57 1a 58 09 7a 48 8d 9b 6d 04 73 d4 c1 5b c3 e3 8e 7e
---------------------------	---

CA ANDES SCD Issuer of Class III certificates: It is the second level Subordinate CA ANDES SCD Root, Certificate Authority his function is issues Final entity certificates outsourcing Subordinate.

Certificate Details of CA class III		
Distinctive Name	CN	CA ANDES SCD S.A. Clase III
	O	ANDES SCD.
	OU	Certification Division subordinate final entity
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Serial number	62 8f b0 4f f1 62 ff c2	
Distinctive Name of the issuer	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Period of validity	From Saturday, July 18, 2017 10:24:48 a.m. Until Saturday, November 15, 2025 12:34:30 M	
Key Uses	Digital signature, Certificate signature, Signature CRL	
Digital footprint (SHA-1)	46 00 c4 d8 3a 1d 97 55 b8 8a 91 5d ae 97 cc 40 83 28 b9 66	

CA ANDES SCD Issuer of Class III certificates outsourcing: It is the third level Subordinate CA ANDES SCD Root, Certificate Authority his function is issues Final entity certificates for people who interact with platforms of entities with outsourcing.

1.10.2. Registration Authority (RA)

The Registration Authority are entities of the trust model that represent the contact point between the user and the Certification Authority, have functions of Identity verification, approve or reject issuance requests.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

In the trust model of ANDES SCD to the registration Authority it's compose by:

- a) Management software RA provided by the CA where is it manages the procedures authorized to be.
- b) Authorized operator who uses the software of administration to the RA. the control access of the operator to the software of RA is done by certificates of digital signatures that's been issued and management by Andes SCD.

1.10.3. Subscriber

Is the holder of a digital certificate whose identity is linked to signature creation and signature verification. In the certification hierarchy of Andes SCD there are two types of subscribers for the issues certificate: Final Entity and Final Entity (Outsourcing)

Certification Environment	Subscribers
Issuer of Class II certificates (Final Entity)	Single Natural Person Juridical Person
Issuer of Class III certificates (Outsourcing Final Entity)	Single Natural Person Juridical Person

1.10.4. Applicant


Es la persona que ha solicitado la emisión de un certificado digital a ANDES SCD
Is a person who solicited give off from a digital certificate to Andes SCD.

1.10.5. Accepting user Input

Any user its trust in the certificates issued by the ANDES SCD Certification Authority.

1.10.5.1. Precautions to be observed by third parties

- Consult the regulations associated with digital certification services.
- Validate the origin of the certificate (Certification Chain)
- Validate the accreditation status of the ECD issuing the certificate in the site directory.
<https://onac.org.co/servicios/entidades-de-certificacion-digital/>
- Validate your conformity with the contents of the certificate.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Validate that the digital signature was generated correctly.
- Verify the integrity of a digitally signed document.
Validate the scope of the certificate in the associated certification policy (certificate policy in the certificate content).

1.11. Scope of application

ANDES SCD Certification Authority is structured to provide certification services to the public. and provide internal certification services for personnel and IT components of the Certification Authority and Registration Authorities.

This CPS applies to all certificates issued by the CA. The practices described in the CPS apply to the publication and use of certificates, revocation lists and OCSP publishers for users within the CA domain.

1.11.1. Certificate Uses

The certification policies (CP) corresponding to each type of certificate are those that determine the appropriate uses to be given to each certificate. It is not the purpose of this CPS for specify such uses.

1.11.2. Limits on the use of certificates

Certificates must be used in accordance with the purpose and functions defined in their respective certification policy (CP), and may not be used for other uses or purposes not contemplated therein.

The certification policies corresponding to each type of certificate determine the additional limitations and restrictions on the use of the certificates. It is not the purpose of this CPS to determine such limitations and restrictions.

1.11.2.1. Limits on the use of certificates in operating systems

For the use of certificates, consider the following forms of delivery:

- Virtual Token:

For the subscriber can use the virtual token it is essential to have the operating system Windows XP service pack 2 and onwards; for the MacOs operating system it is required to use the online signature service provided by Andes SCD through our website.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Physical Token :

For the subscriber can use the physical token, it is essential to have the Windows 7 service pack 2 operating system onwards; For the MacOs operating system, you must have the Monterrey version 12.0.1 and onwards, as well as an Intel processor, to guarantee its operation.

1.11.3. General Prohibitions

In addition to the prohibition against the use of the digital certificate, the subscriber will have the following prohibitions in the use of the certification service:

- Will not interfere with the ability of other subscribers to access or use the Service.;
- will not interfere with or disrupt the ANDES Digital Certification Service, its servers or networks connected to it, or disobey any requirements, procedures, policies or regulations of the networks connected to the Service.;
- Don't reproduce, duplicate, copy, use, distribute, sell, resell or otherwise exploit for any commercial purpose any portion of the Service;
- Will not copy, reproduce, publish, distribute, distribute, modify, create derivative works from, rent, sell, transfer, display, transmit, compile or compile into a database or commercially exploit any part of the Service, Content, in whole or in part.;
- will not "mirror" the Service provided by Andes SCD, or other proprietary content on any other server.

1.11.4. Prohibitions on the use of certificates

Prohibitions on the use of certificates shall be interpreted as all those that are not expressly defined in the certificate uses section of each Certificate Policy.

All applications that contravene the provisions, obligations and requirements of this Certification Practice Statement shall be considered as prohibited applications.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

The unauthorized operations by third parties or subscribers to the service will exempt the Andes SCD Certification Authority from any responsibility for this prohibited use.

- The use of the certificate to violate any normative or regulation is not allowed, as well as transgress the procedures regulated by the Certification Entity that grants the digital certificate..
- The use of the certificate in order to infringe any intellectual or property right of ANDES SCD or third parties, including, for example, software, code, copyrights, trademarks, service marks and patents is not allowed..
- Andes SCD will not be liable for the improper use of the certificate, caused by the subscriber's negligence in managing their private key, such as allowing third parties to manage it, or failing to comply with the duty of confidentiality necessary to safeguard the private key. unauthorized or fraudulent access.

The Certification Policies corresponding to each type of certificate determine the additional prohibitions of use..

1.11.5 Minutes and Contracts

In each certification policy (PC) the information regarding the minutes and service contracts is established.

1.12. Certification services catalog

1.12.1. Certificates for Final Entity

ANDES SCD issues 8 types of certificates to the final entities of the certification service, then reference is made to each type of certificate and the certification policy where you can obtain detailed information.

Single Natural Person Certificates: They are certificates issued to natural persons that accredit the identity of the holder in the signing of documents, guaranteeing the authenticity of the issuer of the communication, the non-repudiation of the origin and the integrity of the content. The holder of a personal certificate acts in his own name and interest.

Policy Name	OID
SINGLE NATURAL PERSON CERTIFICATES	1.3.6.1.4.1.31304.1.2.1.8.0

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Certified professional certificates:

The Certified Professional certificate accredits the identity of the subscriber and his professional title, and allows the subscriber to sign documents digitally in his own name and interest.

Policy Name	OID
CERTIFIED PROFESSIONAL CERTIFICATES	1.3.6.1.4.1.31304.1.2.3.8.0

Legal representative certificates: The legal representative certificate accredits the identity of the subscriber and his condition as legal representative of a legal entity or person. Allows the subscriber to digitally sign documents on behalf of the entity or legal person they represent.

Policy Name	OID
LEGAL REPRESENTATIVE CERTIFICATES	1.3.6.1.4.1.31304.1.2.4.8.0

Company membership certificates The company membership certificate certifies the identity of the subscriber and his condition of belonging, function or employment in an entity or legal person, and allows the subscriber to digitally sign documents in the quality that his certificate accredits.

Policy Name	OID
Company membership certificates	1.3.6.1.4.1.31304.1.2.5.8.0

Public Function Certificates

Public Function certificates are issued in the name of natural persons; certify the identity of the owner and his character as a public official or individual in the exercise of a public function, either by designation or as a result of signing a contract that enables him as such, in the signing of electronic documents guaranteeing the authenticity of the document. issuer of the communication, the non-repudiation of the origin and the integrity of the content.

Policy Name	OID
PUBLIC FUNCTION CERTIFICATE	1.3.6.1.4.1.31304.1.2.8.8.0

Juridical Person Certificates

The Juridical Person Certificates accredits the identity of the subscriber and his condition as a company or legal person, and allows the subscriber to digitally sign documents in the quality that his certificate accredits.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Policy Name	OID
JURIDICAL PERSON CERTIFICATES	1.3.6.1.4.1.31304.1.2.9.8.0

Academic Community Certificates: The Academic Community certificate accredits the identity of the subscriber and their quality as a teacher, student or member of an academic community, and allows the subscriber to digitally sign documents in their own name and interest.

Policy Name	OID
ACADEMIC COMMUNITY CERTIFICATES	1.3.6.1.4.1.31304.1.2.2.8.0

Electronic Billing Certificates

The electronic billing certificate certifies the identity of the subscriber and his condition as an electronic biller and allows the subscriber to digitally sign documents in the quality that his certificate accredits.

Policy Name	OID
ELECTRONIC BILLING CERTIFICATES	1.3.6.1.4.1.31304.1.2.6.6.0

1.12.2. E-Signature Electronic signature

Andes SCD have a service of electronic signature, this service have been indentified in the next way:


Policy Name	OID
ELECTRONIC SIGNATURE CERTIFICATES	1.3.6.1.4.1.31304.1.2.11.3.0

1.13. Policy Administration

The content of this Certification Practice Statement is managed by the Policies and Security committee in charge of preparing, registering, maintaining and updating the CPS, PCs for internal use and PCs for final entities. The details of the policy and security committee and a contact person available to answer questions regarding this document are detailed below.

1.13.1. Organization is administering this 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

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.13.2. Contact Person

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

Telephone : PBX 601 2415539

1.13.3. Policy approval procedures

The ANDES SCD Certification Practices Statement is managed by the Policy and Security Committee and is approved by the ANDES SCD General Management, following the documented information procedure.

1.13.4. Document publication

ANDES SCD immediately discloses on the website any modification in the CPS Certification Practice Statement and in the Certification Policies for end-entity certificates, maintaining a version history. The certification policies for certificates for internal use are not available on the website and are provided to the staff at the time they receive the certificate for internal use.


2. Publication and registration of certificates

2.1. Certificate Directory

The certificate directory is a WEB directory available for consultation 24 hours a day, 7 days a week, where all the final entity certificates issued by ANDES SCD that have not been revoked are found.

The ANDES SCD web page also contains the list of revoked certificates where the reason for revocation, the date and time from which the certificate is no longer valid is specified. Revoked certificates remain indefinitely in the CRL of the CA that issued them. See section Means of communication – Revocation lists (CRL)

A certificate query service remains available through the online protocol (OCSP) and is permanently accessible by anyone to query end-entity certificates. The directory of class I certificates and the CRLs of class I certificates are for internal use and can only be accessed from the internal network of ANDES SCD.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

To guarantee a continuous certificate and OCSP directory service, there is a backup server, in such a way that, in the event of failure or failure of the main server, the backup server will offer the availability of the service.

2.2. Publication media

Certificates of the CA Root and Subordinates

Certificate Type	publication medium
CA ANDES SCD Root:	http://certs.andesscd.com.co/Raiz.crt
CA ANDES SCD Class II – Final Entity	http://certs.andesscd.com.co/Clasell.crt
CA ANDES SCD Class II v2 – Final Entity	http://certs.andesscd.com.co/Clasellv2.crt
CA ANDES SCD Class III – Subordinate Final entity	http://certs.andesscd.com.co/Claselll.crt
CA ANDES SCD Class III FNA	http://certs.andesscd.com.co/ClaselllFNA.crt
CA ANDES SCD Class III SYC	http://certs.andesscd.com.co/ClaselllSYC.crt
CA ANDES SCD Class III SYC v2	https://certs.andesscd.com.co/CASyCv2.crt
CA ANDES SCD Class III ESP	http://certs.andesscd.com.co/ClaselllESP.crt
CA ANDES SCD Class III ESP v2	https://certs.andesscd.com.co/ESPv2.crt
CA ANDES SCD Class III FNA v2	http://certs.andesscd.com.co/FNAv2.crt

LDAP Certificate repositories

Certificate repositories	publication medium
Class I – Internal use	Internal access only


	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Class II – Final Entity Class III Outsourcing – Final Entity	LDAP access through certificate directory section.
---	--

Certificate Revocate List (CRL)

The revocation lists will be electronically signed by the CA of ANDES SCD that issues them.

CRL	publication medium
ROOT CA ANDES SCD S.A	http://crl.andesscd.com.co/Raiz.crl
CA ANDES SCD S.A. Class I	Solo acceso interno
CA ANDES SCD S.A. Class II	http://crl.andesscd.com.co/Clasell.crl
CA ANDES SCD S.A. Class IIv2	http://crl.andesscd.com.co/Clasellv2.crl
CA ANDES SCD S.A. Class II SIIF NACION	http://crl.andesscd.com.co/claseii_critical.crl
CA ANDES SCD S.A. Class III	http://crl.andesscd.com.co/Claselll.crl
CA ANDES SCD Class III FNA	http://crl.andesscd.com.co/ClaselllFNA.crl
CA ANDES SCD Class III SYC	http://crl.andesscd.com.co/ClaselllSYC.crl
CA ANDES SCD Class III SYC v2	https://crl.andesscd.com.co/CASYCv2.crl
CA ANDES SCD Class III ESP	http://crl.andesscd.com.co/ClaselllESP.crl
CA ANDES SCD Class III ESP v2	https://crl.andesscd.com.co/ESPv2.crl
CA ANDES SCD Class III FNA v2	http://crl.andesscd.com.co/FNAv2.crl

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Online Certificate Status Protocol (OCSP)

OCSP	publication medium
CERTIFICATE DE ROOT CA	http://ocsp.andesscd.com.co
CERTIFICATES Class I – Internal Use	
CERTIFICATES Class – Final Entity	
CERTIFICATES Class II v2 – Final Entity	
CERTIFICATES Class III – Subordinate Final Entity	
CERTIFICATES Class III Outsourcing – Final Entity	

CPS y PC Documentation

Available at the next link: <https://www.andesscd.com.co/> section "Documentación"

2.3. Frecuencia de publicación Publication frequency

The declaration of certification practices and the certification policies for the final entity are published on the ANDES SCD website each time there are changes in accordance with the procedure stipulated in this document in the section "Change procedure in the CPS and PC" The certificate directory is continually updated to reflect certificates that are not revoked.

ANDES SCD includes the revoked certificates to the CRL of the CA that issued the certificate within the period stipulated in the Publication of revoked certificates point.

2.4. Certificate directory access control

Access to consulting the certificate directory has no restrictions, however, to protect the integrity and authenticity of the published information, there are controls that prevent unauthorized persons from altering the directory information (by including, updating or deleting data).

The certificates and public keys of the ANDES SCD Certifying Authority are downloaded using the secure http protocol.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

3. Identification and authentication

The procedures and criteria applied by the Registration Authorities and the ANDES SCD Certifying Authority are described below at the time of authenticating the identity of the applicant and approving the issuance of a certificate.

3.1. Names

3.1.1. Name Types

All certificates have a section called Subject, the purpose of which is to allow the certificate subscriber to be identified. This section contains a DN or DistinguishedName characterized by a set of attributes that make up an unequivocal and unique name for each subscriber of the certificates issued by ANDES SCD

The certification policy (PC) of each type of certificate specifies the attributes that make up the DN or DistinguishedName.

3.1.2. Need for names to be meaningful

Every certificate issued by ANDES SCD has as its main characteristic the full identification of the subscriber and the assignment of a meaningful name to the certificate.

3.1.3. Anonyms and pseudonyms in names

Neither anonymous nor pseudonyms are allowed to identify the name of a natural or legal person.

In the case of an entity or legal person the name must be exactly the same as the corporate name, abbreviated names are not allowed.

In the case of a natural person, the name must consist of the first and last names as they appear in the recognized identification document.

3.1.4. Rules for interpreting name formats

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

3.1.5. Singularity of names

The distinguished names of the certificates issued by ANDES SCD will be unique for each subscriber, and the guarantee of uniqueness is established in each of the certification policies.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

3.1.6. Recognition, authentication and function of registered trademarks

ANDES SCD does not deliberately admit the use of a registered trademark name whose right of use is not owned by the subscriber. However, the Certification Authority is not obliged to search for evidence of trademark ownership prior to issuing certificates.


ANDES SCD does not assume commitments in the issuance of certificates regarding the use by subscribers of a trademark..

The following is a description of the procedure defined by ANDES SCD for the resolution of disputes over the use of names or use of trademarks

In the case of natural persons, the existence of homonymity is irrelevant, since the differentiating element is the identification document number.

In the case of legal entities it is not possible to register two users with the same name. In this sense, the first in time to complete the necessary information for the application of the certificate will have the right to the respective name. The following rules shall also apply:

- The expressions and abbreviations that identify the type of company (Ltda., S.A., S. en C., etc.) are not part of the name and, therefore, do not serve as a differentiator.
- Phonetic equality alone is not a sufficient criterion for considering two names to be identical.
- The addition of numbers is sufficient to consider that two names are not identical
- Two names composed of the same words, but in different order, are not identical..
- Diminutives are differentiators.
- In names consisting of words such as Banks, Corporations and Cooperatives, the relevant rules apply. (D. 1997/88 y L. 78/79). If there is any doubt, the Superintendency of Finance should be consulted regarding the names that may indicate intermediation, as indicated in the aforementioned decree.
- Any numeric, alphabetic or alphanumeric character is considered a differentiator for purposes of verifying homonymity, therefore, any company name that has a number, a letter, a dot, a hyphen, a space, an apostrophe, an apostrophe, an at symbol, makes a name or company name different from another name or company name.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

3.2. Identity Approval

3.2.1. Method for proving possession of the private key

ANDES SCD has 2 mechanisms for the issuance of End Entity certificates where the procedure for managing the private key varies.

1. **Mechanism 1**- The key pair generated by the subscriber himself.
When the subscriber generates his key pair, processes his request from the website, chooses the "PKCS10" certificate delivery method and associates the CSR containing the public key and implicitly signed by the associated private key.
2. **Mechanism 2** - Key pair generated by ANDES SCD
ANDES SCD reserves the right to generate the key pair when the subscriber so determines or depending on the certificate delivery format.

The method for demonstrating possession of the private key for each of the end-entity certificate issuance mechanisms is described below:

1. **Mechanism 1**- The key pair generated by the subscriber himself.

The future subscriber is the only person authorized to create his own key pair (private key and public key), the private key remains exclusively in the possession of the subscriber and is never known by ANDES SCD, while the public key is known to ANDES SCD because it must be contained in the certificate to be issued.


The method used by ANDES SCD to verify that the applicant possesses the private key corresponding to the public key for which the certificate is requested is verified as follows

When the form of certificate delivery is PKCS10

Activity		Details	Responsible
1	Generate key pair	Generate the key pair and obtain the CSR containing the public key and implicitly signed by the associated private key	Applicant
2	Process application from web site	Enter the Andes SCD web site option Request Certificate and do the following: 1. Select the type of certificate you wish to acquire	Applicant

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Activity		Details	Responsible
		<ol style="list-style-type: none"> 2. Attach the required documentation according to the PC applicable to the type of certificate 3. Fill in the application data 4. Select the effective date of the certificate and the period of validity 5. Select "PKCS10" as the certificate delivery method and report CSR containing the public key and implicitly signed by the associated private key. 6. Fill in the service payment and billing information. 7. Accept terms and conditions 8. Register the request and receive e-mail with instructions 	
3	Study application	<p>Verify the application information and determine whether it is approved or rejected.</p> <ul style="list-style-type: none"> • If the application is rejected, an e-mail is sent to the applicant indicating the reasons for the rejection of the application and the process is completed. • If the application is approved, proceed to the next step of this procedure. 	Andes SCD RA Supervisor
4	Issue the certificate	<p>Verify the approved certificate issuance request and give the order to generate the certificate.</p> <ul style="list-style-type: none"> • ANDES SCD verifies that the private key is in the subscriber's possession by verifying the SIGNATURE using the public key sent in the PKCS10 certificate request. • Generate the digital certificate 	Andes SCD Agent of Emission

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Activity		Details	Responsible
		<ul style="list-style-type: none"> Send email to the applicant to access the secure subscriber area 	
5	Download the certificate	Access the secure subscriber area and follow instructions to download the certificate.	Applicant (Now Subscriber)

Mechanism 2 - Key pair generated by ANDES SCD

ANDES SCD reserves the right to generate the key pair when the subscriber so determines or depending on the certificate delivery format.


The method used by ANDES SCD to verify that the applicant has the private key corresponding to the public key for which the certificate is requested may vary depending on the entity with which Andes SCD has a certificate issuance agreement.

3.2.2. Identity Authentication

Identity Authentication of Registration Authorities

The RA linked to the ANDES SCD trust model comply with the following protocol:

1. The Registration Authority has the technological infrastructure required to carry out the functions delegated by ANDES SCD
2. There is a contract in force between ANDES SCD and the Registration Authority where the aspects of the delegation and the responsibilities are specified.
3. The identity of the operators of the Registration Authority is verified and validated.
4. The operators of the Registration Authority have received the necessary information for the correct performance of their functions.
5. The registration authority authentication procedure has been validated by ANDES SCD.
6. The Registration Authority assumes all obligations and responsibilities relating to the performance of its functions.
7. The communication between the Registration Authority and ANDES SCD is carried out in a secure manner through the use of digital certificates.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- **Applicant's and Subscriber's Identity Authentication**

The identification of the applicant will be made by means of the personal information provided in the form together with the documentary supports required for the type of certificate desired, this information will be verified with external services developed for this purpose, additionally as part of the identification process of the applicant. Andes SCD may use biometric information or patrimonial data that will be matched to authenticate the identity, these methods are detailed in the certificate issuance procedure.

Certificate issuance request processed from web page

The applicant's information is provided from the WEB page along with the required supports for the type of certificate. The applicant must provide ANDES SCD with original, sufficient and appropriate information regarding the requirements of the applicable CP.

Request for issuance of certificate processed by outsourcings.

The identity authentication mechanism for applicants and subscribers may vary depending on the entity with which Andes SCD has a certificate issuance agreement.

- **Identity Authentication for Juridicals Persons**

Each certification policy (CP) establishes the information to be submitted by the applicant to prove the identity of a legal entity, if it is applicable for the type of certificate.

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. Criterion for interoperation

Interactivity between external Certification Authorities can be achieved by means of cross-certification

Before establishing interactivity relationships with external Certification Authorities, the ANDES SCD Policy Approval Committee must conduct a study

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

of the cross-certification model to be implemented and determine the minimum criteria that external CAs must meet in order to comply with certain technical and procedural requirements to interact with ANDES SCD.

1. The external CA must provide a level of security in the management of certificates throughout their lifecycle, at least equal to that of ANDES SCD.
2. The external CA must comply with the specific criteria for accreditation of digital certification entities established in the CEA document issued by ONAC.
3. It must provide an audit report from an external authority of recognized prestige regarding its operations as a means of verifying the existing level of security.
4. To establish a collaboration agreement establishing the commitments acquired in security matters for the certificates included in the interaction.

The ANDES SCD Policy and Security Committee reserves the right to accept the interactivity request even if the external CA meets the requirements.

3.2.5. Identification and authentication to request revocation

The identification and authentication process to request revocation is defined in the certification policy applicable to each type of certificate.

4. Certificate lifecycle and operating procedures

4.1. Request for certificates

4.1.1. Who can request the issuance of a certificate


The application for a digital certificate can be made by any person of legal age who is fully capable of assuming the obligations and responsibilities inherent to the possession and use of the certificate.

Each certification policy specifies who may apply for a certificate and the information that must be provided in the application.

4.1.2. Procedure for requesting the issuance of certificates

The request for certificate issuance is received by the registration authority through the application forms provided for this purpose.

The mechanisms exposed for the registration of the request are:

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1. Website:

- The user registers his request through the forms available on the following website <https://www.andesscd.com.co/solicitud-de-certificados/>
- Select the type of certificate and validity required..
- Provides the required information and documentation according to the type of certificate requested.
- Generates the payment according to the type of certificate and validity requested.
- Identity validation mechanism is carried out

2. External coordinator panel:


The external coordinator panel is a web platform provided to authorized officials of the entities with which ANDES SCD has signed an agreement for the issuance of certificates, the official of the agreement entity will be in charge of gathering the information and documentation required for the issuance of the certificates and registering such information through the web form.

- ### 3. Webservices:
- ANDES SCD presents a web service that allows the integration of the methods of requesting and delivering certificates, allowing the request for certificates to occur through the web platforms of the entities with which it has signed an agreement for the issuance of digital signature certificates..

The agreement entity will be responsible for building the web forms that allow the collection of information and documentation required according to the type of certificate requested.

4.1.3. Acceptance of the certificate

By accepting the terms and conditions, the applicant accepts the certificate and its contents once it has been issued. If the subscriber rejects the certificate or its

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

contents, the subscriber must inform the RA of this decision by sending an e-mail to supervisionra@andesscd.com.co within 3 business days from the date of issuance, including the reason for the rejection of the certificate and the incorrect or incomplete certificate fields.

4.1.4. Publication of the certificate by ANDES SCD

Once the certificate is 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 responsibilities and limitations of use of the key pair and certificate are specified in the corresponding certification policy.

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 are enabled for the following uses:

- Digital signature
- Non-repudiation
- Encryption of information

The subscriber can only use the certificate and the key pair after accepting the conditions of use established in the CPD and 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 key pair associated with Andes SCD's subordinate CA certificates has the following enabled uses:

- Digital signature

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Signature of certificates
- CRL signature

4.1.5.2. From users who trust

Users who trust the ANDES SCD certification service must verify the uses established in the 'Key usage' field of the certificate or in the corresponding PC to know the scope of application of the certificate.

Users who trust on ANDES SCD's certification service must take responsibility for verifying the status of the certificate before placing their trust in it.

4.2. Processing of certificate requests

Once the application is received, the Registration Authority must ensure and perform the inspection of the requests for issuance, maintaining the commitment to verify the quality and compliance with the Certification Policies and Practices, therefore each of the review steps are detailed in the RA supervisory user manual and in each PC in the section "procedure to request and issue certificate.

4.2.1. Response Times

The certification policies (CP) corresponding to each type of certificate establish the time limit for processing a request by the ANDES SCD RA and CA.


4.3 Issuance of certificates

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

4.3.1 Certificate Issuance Procedure

1. Agent of Emission Verify the certificate issuance request approved by the RA and give the order to generate the certificate.
2. Check certificate delivery format
3. Generate the digital certificate
4. Notifying the issuance of the certificate to the subscriber.

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

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.4. Certificate Renewal - Key Pair.

ANDES SCD does not contemplate the renewal process of certificates with the same public key of the subscriber, if the subscriber wishes to obtain a new certificate, he/she must request the issuance of the certificate when it has expired.

4.4.1. 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.

4.5. Modification of certificates

Digital certificates issued by ANDES SCD cannot be modified.

4.6. Suspension of certificates

Digital certificates issued by ANDES SCD cannot be suspended.

4.7. Declination of Application

Andes SCD reserves the right to decline a application or generate the revocation from a certificate issued, when we have knowlegde about the participation of the applicant and/or suscriber in ilegal activities. or similar related issues that may compromise the good name of the digital certification entity.

4.8. 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 has been revoked, the Certification Authority publishes the revocation list in order to notify third parties that a certificate has been revoked, at the time that verification of the certificate is requested.


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

4.8.1. Causes of revocation

A digital certificate issued by the ANDES SCD Certification Authority is revoked in the following events.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Causes	Circumstances
Key commitment	For compromise of safety for any reason, in any way, situation or circumstance
	When the subscriber reports that the certificate's private key has been compromised or has lost its Confidentiality.
	For any cause that reasonably leads to believe that the certification service has been compromised to the extent that the reliability of the service is in doubt
	When the subscriber, RA or ANDES SCD has breached an obligation, declaration or responsibility established in the terms and conditions of service or makes irregular use of the certificate.
Replaced	When there is a subsequent modification of the subscriber's background (e.g., the subscriber changes his/her name or the entity changes its corporate name)
Cessation of Operations	a) When the subscriber has passed away. b) When the subscriber has been abducted. c) Loss of your capacity or disablement of the subscriber
	When the liquidation of a juridical person that is linked in a certificate is presented.
	For loss, disablement of the digital certificate that has been reported to the CDE.
	For the termination of the subscription contract, in accordance with the causes established in the contract.
Cancellation of Privileges	When there is falsification of the subscriber's background (e.g., after the certificate is issued, it is discovered that false documents were presented).
	When revocation of the certificate is authorized by court or administrative order.
	For the improper handling by the subscriber of the digital certificate.
	for the default of the subscriber or of the juridical person to which he is bound through the digital certification contract
	When it is reported that the subscriber has fraudulently used his digital certificate.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

	When the certificate issued does not comply with the procedures required by the Certification Practice Statement (CPD) or when a requirement was not satisfied.
	When it is found that any of the certificate data is incorrect or that any requirement is not met.
	When a violation has been committed by the RA or ANDES SCD regarding the requirements and procedures established for certificate management.

4.8.2. Who can request the revocation of certificates

ANDES SCD or any of its component authorities may request the revocation of a certificate if it has knowledge or suspicion of the compromise of the subscriber's private key or any other determining fact that requires revocation of the certificate.


The subscriber may revoke the certificate directly online or may request its revocation in accordance with the conditions stipulated in the grounds for revocation section of this CPS.

Related third parties may also request the revocation of a certificate if there is evidence of any of the grounds for revocation, via email as indicated in the procedure to revoke certificates.

4.8.3. Means of revoking certificates

The Final Entity's digital certificates can be revoked through the following means:

1. **INTERNET:** The ANDES SCD website, presents in its main banner the services menu, the subscriber will find the Digital Signature submenu which in turn contains the option Revoke Certificate, in which you have the possibility to revoke your digital certificate based on your document type + identification number + certificate serial number + the revocation code provided at the time the certificate was delivered to you, additionally, the subscriber must choose the reason of revocation + a remark stating in detail the reason for the revocation of the certificate. Once you have

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

registered all the data, you will be able to revoke your certificate immediately.

This service is available 24 hours / 7 days a week.

2. **IN PERSON:** The subscriber may appear in person at Andes SCD's facilities during business hours, request the revocation service, inform their personal data and the reason for the revocation.

This service is available from Monday to Friday from 8:00 am to 5:00 pm continuous working day.

3. **EMAIL:** This form is used as a last resort when the subscriber does not have the revocation code or when a third party handles the request for revocation of a certificate of type Company Membership, Legal Representative or Public Function to notify that the subscriber is no longer linked to the entity as evidenced by the certificate.

4. **OUTSOURCING:** Entities with agreements can request the revocation of certificates processed under the agreement using web services provided by ANDES SCD.

The above mechanisms to manage revocation requests are immediate, except for the email method, which implies verification by the Supervisor within 24 hours after receipt of the request.

The means to revoke digital certificates for internal use are specified in the corresponding Certification Policy.

4.8.4. Procedure to revoke certificates

The following procedures to revoke a certificate apply only to Final Entity certificates.

Online Procedure

1. Go the Andes SCD website in the revoke certificate section <https://www.andesscd.com.co/revocar-certificado/>
2. S Select the type of document and enter the identification number, certificate serial in hexadecimal, and revocation code of the certificate you wish to revoke (These last two data are found in the certificate issuance

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

notification). Select the revocation circumstance and detail the reason for which the certificate will be revoked..

3. Click on the “Revoke certificate” button”.
4. The certificate will revoke immediately.
5. The system automatically sends an email to the subscriber confirming that the certificate has been revoked
6. The certificate is published in the next CRL of the CA that issued the certificate.

In person procedure

1. The subscriber must appear in person at Andes SCD's facilities during business hours (Monday through Friday from 8:00 am to 5:00 pm).
2. Request the revocation service, inform your personal data and the reason for revocation in writing.
3. The RA Supervisor performs the identity validation of the subscriber.
4. The RA Supervisor shall immediately manage the revocation of the certificate.
5. The system automatically sends an e-mail to the subscriber informing that the certificate has been revoked.
6. The certificate is published in the next CRL of the CA that issued the certificate.

E-mail Procedure

1. The subscriber have to do a letter of request for revocation which must contain the following information.
 - a. Date of request for revocation
 - b. Serial number of the certificate to be revoked
 - c. Type of certificate
 - d. Certificate holder (Full name and identification)
 - e. Reason for revocation
 - f. Full name, identification and contact telephone number (if the applicant is not the subscriber)
 - g. Signature of applicant

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

2. The applicant must send an e-mail to revocaciones@andesscd.com.co with the subject "Certificate Revocation Request" attaching a letter formally requesting the revocation of the certificate.
3. The Revocation requests received at revocaciones@andesscd.com.co are dealt with by the RA CA supervisor no later than the next business day following receipt of the request.
4. The RA Supervisor performs the corresponding verification of the data provided in the revocation request letter and executes the revocation process in case of conformity.
5. The system automatically sends an e-mail to the subscriber informing that the certificate has been revoked
6. The certificate is published in the next CRL of the CA that issued the certificate.

4.8.5. Time for processing revocation request

The revocation request submitted by the subscriber is executed immediately as long as it is made in person by the subscriber or via web or telephone by providing the revocation code.

The revocation management service is available via web 7 days a week and 24 hours a day. In the event of a system failure or any other factor beyond ANDES SCD's control, every effort will be made to ensure that the revocation service is not suspended for longer than the maximum 24-hour period

4.8.6. Requirements for verification of revocations from Users who trust in ANDES SCD

The verification of revocations is required for use by third parties, this verification is performed by direct CRL query of the CA that issued the certificate or by OCSP

It is mandatory for users to check the CRLs to see the status of the certificates they are going to trust. Users must download the latest CRL from the ANDES SCD website and check the validity of the CRL before each use.

4.8.7. Publication of revoked certificates

Information relating to the revocation of a certificate is disseminated through the periodic publication of the following revocation lists:

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

CRL	Periodicity of publication
CRL de CA ANDES SCD S.A. Clase II	24 hours
CRL de CA ANDES SCD S.A. Clase II v2	24 hours
CRL de CA ANDES SCD S.A. Clase III	30 days
CRL de CA ANDES SCD S.A. Clase III Convenios	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 one.

The CRL of CA ANDES SCD S.A. Class I is generated every 15 days and are not published because they are for internal use of ANDES SCD.

The CRL of CA ANDES SCD S.A. with 24-hour validity are published every 12 hours so that there is an overlap and contingency in case of failure or generation.

The CRL of CA ANDES SCD S.A. with 30-hour validity are published every 15 hours so that there is an overlap and contingency in case of failure or generation.

Note: The ROOT CA CRL is generated when needed by momentarily activating the Root CA (the Root CA remains offline).

4.9. Certificate status information services

4.9.1. Operational characteristics

There are 2 services that provide information on the status of issued certificates:

1. Publication of CRLs: CRLs are accessed via HTTP/HTTPS
2. OCSP online validation service: By using this RFC 2560, 5019 and 6960 compliant protocol, the current status of any certificate is determined without requiring CRLs.

4.9.2. Service availability

The on-line revocation checking service is available 24 hours a day, 7 days a week, 365 days a year with an availability of 99.8%. ANDES SCD makes every effort to ensure the availability of the service.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.9.3. End of subscription

Termination of subscription occurs when the certificate's validity period expires or the certificate is revoked for any of the reasons described in the Revocation Causes section.

4.10. Replenishment of certificates

The certification policies specify the process for the replacement of certificates.

4.11. Validity of certificates

Certification policies specify the period of validity of the respective certificate and additionally the period of validity of the key pair.

5. Security controls

The aspects related to technical and procedural measures that guarantee the security of ANDES SCD's services and information are specified in detail in the Information Security Policies (ISP)


These policies contemplate the responsibilities of the different areas of the trust model belonging to ANDES SCD, notifying each person of the procedures and controls that correspond to him/her within the organization

ANDES SCD's Security Policy Statement consists of the following sections or documents for internal use.

SECTION
Information security policy
Integrated management system manual
Information Security Incident Management Procedure
Technology asset inventory management procedure
Risk Management Methodology
Personal data protection procedures manual

5.1. Conditions required of critical suppliers

For Andes SCD, it is a duty to provide an excellent service, for this reason, suppliers must be the first line to support our commitment to service and its quality, so our suppliers are evaluated annually to validate compliance with the contractually defined service levels.

	<p align="center">CERTIFICATION PRACTICES STATEMENT</p>	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Suppliers linked to the provision of accredited services in Andes SCD and that have been defined as critical, must be aware of this Certification Practices Statement. They are also required to comply with specific accreditation criteria, both administrative and technical, which are directly related to the service they provide.

The main data center must comply with a site availability of 99.9% for the provision of digital certification services, and must also comply with the other administrative and technical requirements defined in the contract.

5.2. Physical security controls

5.2.1. Location and Environmental Safety

The systems and equipment used by ANDES SCD to offer the certification service are physically located in the Triara Data Center, a world-class data center located in the Sabana of Bogota in a strategic location of great business development.

The Triara Data Center is a site that has been designed according to TIA/EIA 942 - TierIV specifications and complies with strict construction standards and follows rigorous operating standards to ensure that the equipment and information housed therein have the highest level of security.

Its facilities are located in an area with zero seismic activity and are housed in a reinforced concrete and steel bunker. The buildings are resistant to floods, windstorms, electrical discharges and atmospheric precipitation and are equipped with an architectural subsystem, a telecommunications subsystem, an electrical subsystem, a mechanical subsystem and a physical security system articulated by risk management and security methodologies.

The security services offered by the Triara Data Center have been integrated to the security policies and procedures of ANDES SCD describing each of the controls implemented to avoid the risk, alteration, subtraction, damage or loss of the assets involved in the provision of the digital certification service

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

To guarantee the provision of critical services in case of an incident with its main Data Center, ANDES SCD has an alternate data center contracted by Cirion Technologies Colombia S.A.S. This data center is located at Cra 68 # 169 A-73, Bogotá. Cirion Technologies Colombia S.A.S. is qualified as TIERIII type and has optimal security mechanisms for the provision of services.

Physical security perimeter


The physical security perimeter of ANDES SCD comprises the area where the digital certificates are generated and where the set of servers required to provide the digital certification service is stored. This security perimeter is located in the Triara Data Center and is protected by the following mechanisms:

1. The facilities have 3 permanent security rings: Access to the business center, access to Triara facilities and access to the Data Center.
2. The data center has a single point of access protected by security staff 7x24x365.
3. Access systems through authorization in access lists and identity document verification.
4. Access to the building and secure areas for administration personnel through authentication devices including biometrics and proximity cards.
5. Visitor access by appointment and escort if going to secure areas.
6. Certified physical security systems with CCTV and security camera systems inside and outside the data center.
7. Camera monitoring from the control cabin
8. Loading and unloading areas isolated from the data center, where everything entering and leaving the facilities is controlled

Protection against external and environmental threats

The place where the servers and critical devices for the operation of ANDES SCD are located has physical protections in order to minimize the risk of theft, fire, flooding and environmental conditions that may affect the operation of the information processing facilities

1. Redundant air conditioning systems designed to allow the equipment to always obtain optimal environmental conditions in terms of temperature and humidity for its good performance.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

2. Inergen firefighting systems (clean agent according to Kiotol protocol), which consists of a gas extinguishing system that does not create mist when expelled so as not to diminish the visibility of emergency exits and not to leave residues that affect computer equipment..
3. Certified ventilation and cooling systems
4. Redundant 34.5 KV power supply from different substations and independent connections.
5. The infrastructure ensures the continuity of its operations in the event of supply failures, through the use of high-capacity uninterruptible power supply systems that provide energy to critical facilities.
6. Perimeter intrusion detection system that includes permanent monitoring of the perimeter.
7. Control of inputs and outputs of information, applications or equipment by keeping an inventory of existing material and the inputs and outputs that have been produced.

5.2.2. Access system management


The physical access control system is guaranteed by the security services provided by Data Center Triara through the mechanisms described in the previous section entitled "Physical security perimeter" and "Protection against external and environmental threats".

The logical access control system to ANDES SCD's critical applications is carried out by applying the following mechanisms:

1. Authentication to critical applications through Digital Certificates combined with username and password.
2. High-availability firewall-based controls
3. Updated list of users authorized to access the system specifying the level of access and privileges that each user has.
4. Monitoring to detect unauthorized access immediately.

5.2.3. Security of servers

Each ANDES SCD critical server has a backup server that is kept in sync with the main server and comes on line to replace the main server when it fails.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

The servers have a procedure for detecting and recording unauthorized access attempts so that the origin, date and time, the areas where access has been attempted and the manipulations carried out can be known.

Servers exposed to the Internet have an application-level firewall configured to protect the private network from intruders while allowing authorized access to and from the outside.

The CA server that performs the certificate management is not exposed to the Internet and has a firewall configured to reject all entries, the CA server periodically tracks the certificate requests found in the RA server, processes them and generates the respective digital certificates.

Monitoring of server operating systems, access control, certificate lifecycle and aspects that indicate unauthorized use of the system and that can minimize the risk of disruption to business processes.

5.3. Procedural controls

Procedural controls are responsible for ensuring a distribution of functions by controlling the different hierarchies of the trust model to limit internal fraud and prevent a single person from being in charge of the entire process from start to finish. The following aspects are defined for each area:

- Skills required
- Training and awareness
- Duties and responsibilities of the position o Function Manual
- Security measures to which it is subject
- Levels of access to information and systems
- Monitoring and auditing of the function

Procedural controls are considered confidential information of ANDES SCD and are described in detail in the function manuals and in the PSI Security Policy Statement.


Through internal audits carried out periodically it is ensured that all the management of procedures operational and management procedures are carried out safely.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.3.1. Roles of confidence


The trust model has a hierarchy that ensures segregation of duties, distributes control and avoids internal fraud, preventing a single person from controlling all certification functions from start to finish.

- a. Agent of Emission: Responsible for reviewing the certificate issuance requests approved by the RA Supervisor and making the decision on the certificate generation and revocation procedure.
- b. RA Supervisor: Responsible for procedural security, inspects requests for issuance and revocation of certificates and is responsible for verifying the quality and compliance with the Certification Policies and Practices
- c. Infrastructure Coordinator: He's responsible for managing the cryptographic device that creates and stores the private keys of the root CA and the subordinate CAs, is responsible for the operation of the PKI components, hardware and software. He is authorized to make changes to the system configuration and to supervise the correct operation of the certification service.
 - Recovery of HSM functionality in case of failure.
 - Recovery of keys in case of accidental deletion.
 - Expansion of the number of HSMs integrated into the infrastructure
 - Administration of HSM user accounts (Administrators or operators).
 - Ceremony for the generation of keys for the CAs
 - Activating CA private keys for use.
 - Manage user access controls to equipment, applications and components of ANDES SCD's technological infrastructure
 - Perform tasks related to CA administration, such as managing certificate lifecycle, creating new certificate profiles, and maintaining agreed security controls.
 - Install and configure operating systems and software products on ANDES SCD servers.
 - Perform maintenance to servers and systems and will be in charge of covering the security requirements established for the operation,


	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

administration and communication of ANDES SCD's systems and technological resources.

- Resolves issues related to security vulnerabilities
 - Monitor and verify the correct service of CRL, OCSP.
 - Establish and document processes for monitoring systems, applications and services
 - Oversee the implementation of data protection policies and backup systems.
 - Oversee that the directory of certificates is kept up to date.
 - Supervise the correct operation of the servers and components of the certification system.
 - Supervise the correct operation of the certification service and certificate lifecycle management.
- d. Infrastructure Administrator: Responsible for administering and configuring the RA.
- e. System Auditor: Es responsible for performing periodic audits on the systems and activities related to information technology, reporting on compliance with the specifications and security measures established in the PSI and by the standards, procedures and practices arising therefrom
- f. Policy and Security Committee: The Policy and Security Committee is in charge of the administration of the CPS, CP, ISP and Business Continuity Plan.
- Functions of the Policy and Security Committee:
- Review at least once a year the Information Security Policies (ISP) and if there are modifications propose them to the management for approval
 - Review at least once a year the Information Security Policies (ISP) and if there are modifications propose them to the management for approval.
 - Implement methodologies to communicate security risks and incidents presented in the different components of the trust model (ANDES SCD, RA, end entities, etc.)
 - Establish and support training plans to update employees on safety issues.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Ensure that exceptions to the security policy are authorized only by the General Management of ANDES SCD and that there is a record of the risks that are being consciously assumed and the period of validity of the exception.
 - Follow up on disciplinary and legal actions associated with investigated security breaches.
- g. Information Security Officer: Must ensure the design, implementation and compliance with security procedures and practices in the facilities and security procedures and practices to protect the information managed in ANDES SCD.
- Develop methods and techniques to effectively monitor information security systems and periodically report on their performance to senior management.
 - Track and document risks and incidents affecting resources and information and create specific controls.
 - Ensure that systems are properly documented.
 - Maintain updated Security Policies in accordance with current regulations.
 - Prepare and maintain the contingency and disaster recovery plan in case of emergency.
 - Lead periodic testing of the contingency and disaster recovery plan.
- h. Legal Area Advisor: The legal advisor is responsible for verifying compliance with the Security Policies (PSI) in the management of all contracts, agreements or other documentation of ANDES SCD with its employees and third parties. It also advises ANDES SCD on legal matters related to information security. Draft the confidentiality commitment with Employees, Registration Authorities and Subscribers and advises on sanctions applied for non-compliance with the Security Policy.
- i. Call Center Sales Advisor ANDES SCD: These are the persons in charge of attending to the concerns of users, applicants and subscribers
- Customer service via chat, email or telephone
 - Provide non-confidential information

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Performs incident logging and support management

5.3.2. Number of persons required by task

Andes SCD ensured that at least 2 persons are available to perform tasks requiring multi-person control, such as:

- CA key generation
- The recovery and backup of the CA private key
- Issuance of certificates by CAs
- Activation of the CA private key

5.3.3. Identification and authentication of each role

Access to resources is done depending on the asset by means of digital certificates and username and password.

Each person only controls the assets required for his role, thus ensuring that no person accesses unallocated resources.

The persons assigned to each role are identified by the internal auditor who verifies that each person performs the operations for which he/she is assigned.

5.3.4. Roles requiring separation of duties


The assignment of personnel ensures that the following conditions are met:

- An Infrastructure Coordinator cannot be an RA administrator.
- An RA supervisor cannot be a Agent of Emission.
- A security officer cannot be an RA administrator.
- An internal auditor cannot be an Infrastructure Coordinator.

5.3.5. Relationship between ANDES SCD and the Registration Authorities

The following aspects are taken into account in the relationship of the trust model:

- The contract stipulated between ANDES SCD and RA details the aspects of delegation and responsibilities of personnel and must be fully complied with by the parties.
- RA supervisors should be trained and evaluated periodically to ensure the proper performance of their duties.
- The RA assumes all obligations and responsibilities related to the performance of its duties

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


- The identity of the RA and the supervisors linked to the RA is verified and validated by authorized ANDES SCD personnel.
- The communication between ANDES SCD and RA is carried out in a secure way through the use of digital certificates, in this way each of the RA supervisors is issued a digital certificate for internal use that identifies him/her and that is essential for the performance of his/her activities, the use is personal and non-transferable, being the RA supervisor the only responsible for the consequences that may arise from the misuse, disclosure or loss of the same.
- The contract between ANDES SCD and the RA includes indemnity clauses in case of breach of its legal or contractual obligations.

5.3.6. Personal security controls

5.3.6.1. Qualifications, experience and requirements

All ANDES SCD personnel and each RA are trained to perform their assigned activities and are monitored and evaluated to determine whether they are qualified to perform their assigned functions. The training programs involve the following points:

1. PKI basics concepts
2. Job Responsibilities
3. Use and operation of the software and hardware used
4. Backup copies and security measures to be taken into account when the work equipment is momentarily abandoned.
5. ANDES SCD's security and operational policies and procedures
6. Preparation of reports to notify incidents or anomalies that may affect the security of data or access to computer platforms. Incidents are understood as the following circumstances
 - Unauthorized changes to information
 - Attempted access or access to confidential information by unauthorized individuals
 - Errors in the computer application
 - Any other type of problem that may affect the provision and quality of the service.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.3.7. Background check procedures

ANDES SCD performs the pertinent investigations before hiring any person, the personnel must have an authorization to perform RA activities. The Registration Authorities may establish criteria being responsible for the performance of the persons they authorize.

5.3.8. Training requirements

ANDES SCD personnel involved in the life cycle of certificates must be familiar with the Security Policy documentation and apply it in order to competently perform their duties.

Personnel should be trained in the following aspects:

- Certification Practices Statement.
- Certification Policies
- Information security awareness.
- Specific accreditation criteria issued by ONAC.

5.3.9. Training frequency and requirements

ANDES SCD personnel involved in the life cycle of certificates must be updated on procedures and the latest versions of the Certification Policies and Practices in order to ensure the correct performance of their functions.


5.3.10. Frequency of job rotation

Job rotation among ANDES SCD personnel is contemplated to guarantee the continuity of service provision in case of absence of any of the employees. Job rotation among the roles of trust is carried out only with qualified personnel to perform the functions of the position.

5.3.11. Penalties for unauthorized actions

If any member of the RA or ANDES SCD commits any infraction or criminal act that affects the trust model, a disciplinary process will be applied and, depending on the seriousness of the matter, he/she will be removed from his/her functions by ANDES SCD.

Disobedience of any of the following prohibitions generates a disciplinary process:

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- It is forbidden to share keys, passwords or data to access ANDES SCD systems and applications, even within the same organization. The user is solely responsible for what is done with his key, therefore he must protect it.
- Prohibition of any attack against security elements or systems (e.g. deletion of programs, files and vital information for ANDES SCD).
- Prohibition of the installation of software that does not have a license of use and uninstallation of software required to carry out its activities.
- Prohibition of the use of infrastructure assets for purposes not entrusted to it.
- Prohibition of illicit or illegal activities that violate the morals and rights of third parties
- Prohibition to dispose of sensitive or confidential information for uses outside its activity within the trust model (e.g. clandestinely extracting confidential information from ANDES SCD or RA facilities and disclosing it to third parties).
- Commitment to confidentiality regarding the information accessed in the performance of their duties, even after the termination of their relationship with ANDES SCD.

5.3.12. Recruitment requirements

At the time of hiring ANDES SCD personnel, the confidentiality clauses and operational requirements must be made known, and the RA must carry out the same procedure within the company with the operators.

5.3.13. Documentation provided to personnel


ANDES SCD makes available to all personnel the documentation detailing the functions entrusted, the Certification Policies and Practices, the Security Policies applicable to the role and user manuals of the digital certification system so that they can perform their functions competently.

5.4. Audit Controls

5.4.1. Types of audited events

The following events related to ANDES SCD's security system have been audited

1. Switching the servers on and off
2. Successful and unsuccessful attempts to change security settings of the server operating system.
3. Server log on and log off

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

4. Attempts of unauthorized accesses to the system through the network to the certification system
5. Registrations made from the Certification Authority's applications
6. Password change
7. Changes in the creation of certificate profiles
8. Successful and failed attempts generate, sign, issue or revoke certificates
9. Successful and failed attempts to generate, sign, or issue a CRL
10. Administration and life cycle of digital certificates
 - Update of subscriber related information
 - Certificate issuance request registration
 - Certificate Revocation
 - Certificate issuance request review result
 - Certificate generation
 - Certificate download

Syslog events detail the date and time, the severity of the event, the server where the event occurred, which application generated the event and a description of the event.

The severity of the event is classified into the following categories:

- Info : Informative message
- Debug : Low level debug message
- Notice : Unusual event message, but not an error condition
- Warning: A message indicating that an error may occur if an action is not taken.
- Error : Error condition message

The events audited by ANDES SCD applications detail the date and time, user responsible, type of event audited and description of the action performed.

5.4.2. Frequency of processing of audit records

Audit logs are reviewed once a week for suspicious activities

5.4.3. Period of storage of audit records

Backup copies of audit records shall be stored for at least 4 years.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.4.4. Protection of Audit Records

Logs are automatically stored containing follow-up information on events related to the service activities offered by ANDES SCD.

5.4.5. Procedures for backing up audit records

An audit log backup procedure is in place that consists of collecting in a centralized database the syslog audit logs obtained from each of the servers offering the certification service. The collection of audit logs is done in real time.

5.4.6. Audit information collection systems

The collection of ANDES SCD audit information is done through automatic processes executed from the PKI applications. The audit logs of the Certification Authority and Registration Authorities systems are stored in ANDES SCD's internal systems.

Auditing of sensitive events related to the certificate lifecycle is stored at the database level.

The data collection systems have the following characteristics:


1. They allow to verify the integrity of the database, i.e., they detect possible fraudulent manipulation of data.
2. Ensures the non-repudiation by the authors of the operations carried out on the data.
3. Stores audits, keeping a permanent history of the operations carried out..

5.4.7. Event review systems

Tools are available to consult audited events based on multiple search parameters that facilitate the detection of events by severity category.

5.4.8. Vulnerability analysis

ANDES SCD periodically performs a review of discrepancies in the information of audit records and suspicious activities, in accordance with the internal procedure established for this purpose in the security policies.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.5. Information storage and archiving controls

5.5.1. Type of information to be safeguarded

The events recorded during the life cycle of each digital certificate issued by ANDES SCD are retained.

- All syslog audit events
- All data related to issued certificates
- Requests for issuance and revocation of certificates.
- Documentation versions (Certification Practices and Policies, Security Policies, technical and operational manuals).

5.5.2. Information storage period

All system data related to the life cycle of 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.

Subscriber identification and authentication information is retained for at least 15 years.

5.5.3. Information protection

ANDES SCD ensures the correct protection of information by assigning qualified personnel for its treatment and high availability systems.


Technical and configuration documentation is available detailing all actions taken to ensure the protection of files.

5.5.4. Information backup procedure

The information and application software used by ANDES SCD on critical servers are synchronized by an automatic online mechanism to backup servers.

5.5.5. Internal and external storage systems

Electronically stored information is protected against unauthorized changes, deletion or alteration through the implementation of logical and physical access controls stipulated in ANDES SCD's Security Policy Statement.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.5.6. Procedure for obtaining and verifying archived information

ANDES SCD does not store on paper any type of document resulting from the provision of the certification service, all the necessary supports for the provision of the service are stored on electronic media that are protected by physical and logical access controls so that only authorized and trusted personnel can have Access

Digitally stored data are signed to ensure the integrity and authenticity of the information. The procedure for verifying the information in the file is confidential and is applied only by authorized personnel.

5.6. Key change

ANDES SCD CA key changes are made upon expiration of their validity period and following the CA key change protocol.

The old private key is only used for signing CRLs as long as there are active certificates issued by the old key.

When the period of validity of the CA keys expires, a new pair of keys will be created and a new certificate will be issued to support them.

The internal use document CA Private Key Management details the process of changing the root CA keys of the subordinate CAs.

The change of subscriber keys for internal and end-entity certificates varies according to the type of certificate and is defined in each Certification Policy (CP)

5.7. Engagement and disaster recovery

ANDES SCD has developed a contingency and business continuity plan established and tested to ensure the provision of services in accordance with applicable standards.

The technical mechanisms implemented by ANDES SCD to support recovery after incidents are detailed in the ANDES SCD Technological Infrastructure Document.

5.7.1.1. Incident management procedures


ANDES SCD has an information security incident management procedure for the treatment of incidents that may affect the confidentiality, integrity and availability of information and services.:

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

1. **Incident detection and reporting:** Awareness of the incident through monitoring systems, intrusion detection systems, system logs, notice by staff or by customers..
2. **Incident analysis and evaluation:** Once the incident is detect, the response procedure is determined and the responsible persons are contacted to evaluate and document the actions to be taken according to the seriousness of the incident. An investigation is carried out to determine the scope of the incident, i.e. to find out the extent of the attack and the maximum possible information about the incident.
3. **Incident damage control:** React quickly to contain the incident and prevent it from spreading by taking measures such as blocking access to the system.
4. **Investigation and evidence gathering:** Review audit records to follow up on what happened.
5. **Recovery and countermeasures:** Restore the system to its correct operation and document the procedure and ways to prevent the incident from recurring.
6. **Subsequent analysis of the incident to improve the procedure:** Perform an analysis of everything that happened, detect the cause of the incident, correct the cause for the future, analyze the response and correct errors in the response..

ANDES SCD has established a Contingency Plan that specifies the actions to be taken, components or resources to be used and how personnel should react in the event of an intentional or accidental event that renders resources and certification services useless or degrades them.

- a. When the security of the certification authority's private key has been compromised.
- b. When the certification authority's security system has been breached.
- c. When there are failures in the certification entity's system that compromise the provision of the service.
- d. When the encryption systems become invalid because they do not offer the security level contracted by the subscriber.
- e. When any other event or incident of information security occurs.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

5.7.2. Informatics resources, software and corrupted data

If any of the IT resources, software or information critical for the provision of the certification service should fail or be altered, the recovery procedure established in the Business Continuity Plan or incident management procedure, as the case may be, shall be followed.

At the same time, an audit is carried out to determine the origin of the problem and the pertinent measures are taken to prevent it from recurring.

5.7.3. Procedures in the event of private key compromise

If the private key of an ANDES SCD CA is compromised, the certificate is revoked, the revocation is published in the respective CRL and all affected trust model participants are notified. The revoked CA certificate will remain accessible in the ANDES SCD repository for the purpose of continuing to verify certificates issued during its period of operation.

Immediately the procedure to acquire a new certificate and key pair for the CA will be managed, keeping the same denomination. In case the compromised private key is that of the Root CA ANDES, a new certificate will be issued for the subordinate CAs signed by the new private key of the root CA. Subordinate CAs will not issue certificates until the new certificate is issued..


A new certificate will be issued to each of the subscribers whose certificate was revoked due to the compromise of the ANDES SCD private key. All procedures are documented in the business continuity plan:

- How to revoke the ANDES SCD private key
- How to generate a new key and distribute it to users
- How to revoke and forward subscribers' certificates

5.7.4. Business continuity capabilities in the event of disaster

To ensure business continuity in the event of a disaster, the following aspects are considered

- Redundancy of the most critical components
- Periodic checking of services
- In the event of an incident with its main Data Center, ANDES SCD has an alternate data center. This data center is located at Cra 68 #

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

169A-73, Bogotá. The alternate data center is qualified as type TIERIII and has optimal security mechanisms for the provision of services.


5.7.5. Measures to Correct Detected Vulnerabilities

ANDES SCD contemplates in the Business Continuity Plan document, the security procedures for the management of events that may affect the provision of the certification service.

5.8. Cessation of activities of the Certificate Digital Entity

In the event that ANDES SCD ceases its activities as a certification service provider, the following measures will be taken in order to cause the least possible damage to subscribers and users of the certification system and in compliance with the Andes SCD's plan for ceasing its activities:

- The ANDES SCD Certification Authority shall notify 30 days in advance to the Superintendence of Industry and Commerce and the National Accreditation Body the intention to cease its activities as a certification service provider.
- Once authorization has been received from the Superintendence of Industry and Commerce and the ONAC for the cessation of activities, it shall be done in the manner and following the schedule submitted by the ECD to the surveillance and control entity and approved by it, and shall use the media to notify the users of the certification system of the cessation of the activity as Certification Service Provider.
- The communication of the cessation of activities to the users of the certification service is done through 2 notices published in newspapers of wide national circulation, with an interval of 15 days, informing about the termination of activities, the precise date of the cessation, the legal consequences of the cessation with respect to the certificates issued, The possibility for a subscriber to obtain the reimbursement equivalent to the value of the remaining time of validity of the certificate and the authorization issued by the Superintendence of Industry and Commerce for the ECD to cease the service, and if it is the case, the CRLs will continue to be published until the last of the issued certificates expires.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Transfer all responsibilities, obligations and rights within the certification system to another Certification Authority that is willing to continue with the service. If no other Certification Authority is found that accepts the transfer of rights and obligations, all unexpired certificates are revoked at the time of the final termination of the Certification Authority..
- ANDES SCD will make an effort to ensure that the interruption of the certification service causes the least inconvenience to subscribers and persons who need to verify digital signatures.
- Revoke any authorization to subcontracted entities to act on behalf of ANDES SCD in the certificate issuance procedure.
- ANDES SCD must comply with the above plans, maintain documentation and annual test records at its head office and accessible to ONAC.
- Comply with the obligations imposed by Colombian law.

In the event that the Registration Authority ceases to perform its functions, all authorization to act as delegated Registration Authority of ANDES SCD Certification Service will be cancelled and the digital certificates for internal use issued to operators will be revoked.

6. Technical safety controls


6.1. Key generation and installation

6.1.1. Key Pair Generation

CA Keys

ANDES SCD has a 3-level trust hierarchy made up of the top-level CA or Root CA that guarantees the trustworthiness of its 3 second-level subordinate CAs that have been created for different purposes:

- CA Issuer of Class I certificates: Issues certificates for internal use for personnel and computer components that are essential for the internal and operational functioning of the Certification Authority and Registration Authorities..
- CA Issuer of Class II or final entity certificates: Issues certificates to persons who in their own name, representing an entity or accrediting a position has requested the issuance of a digital certificate to ANDES SCD.
- CA Issuer of Class III certificates or subordinate end entity certificates: Issues certificates to subordinate CAs of end entity agreements

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Class III Certificate Issuing CA Agreements: There are different third level CAs subordinate to the Class III CA. Each third level CA issues certificates to individuals to interact with the platform of the entity with an agreement that processed the request.

The key pair for each of the above CAs has been generated according to the Key Generation Ceremonies procedure, the key generation process was performed by authorized personnel according to the trust roles using a FIPS 140-2 level 3 certified Hardware Cryptographic Module (HSM) which uses the AIS 20 standard for random number generation.

Subscriber keys

1. **Mechanism 1** - The subscriber-generated key pair
Applies when the subscriber has chosen the PKCS10 certificate delivery method.
The key pair (public key and private key) is created by the subscriber himself, the private key remains exclusively in the subscriber's possession and is never known by Andes SCD, while the public key is sent by the subscriber to Andes SCD in the CSR for the issuance of the certificate.
2. **Mechanism 2** - Key pair generated by ANDES SCD
Applies when the certificate issuance request has been made through agreements or when the subscriber has delegated ANDES SCD to generate the key pair.

Mechanism 1 - The subscriber-generated key pair

The public and private keys of End Entity certificate holders are securely generated by the subscriber himself using TOKEN, HSM or by software.

The characteristics of the TOKEN used are described below.

The TOKEN is a cryptographic device of custody of the private key providing a level of security equal or superior to that established for signature data creation devices offering the following:

- Generates RSA key pairs of up to 2048 bits
- Algorithms for RSA, DES, 3DES, MD5 and SHA-256 generation implemented by hardware.
- Random number generator hardware
- Digital signature generator hardware

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Available space of 64 Kb
- CE and FCC certification
- FIPS 140-2 Level 3 certification.
- Full support for PKI applications
- CAPI and PKCS#11 interfaces support
- Support for multiple key storage
- Support for X.509 V3 standard certificate format

The cryptographic device has an activation key (PIN) to make use of the private keys, this activation key must be for the exclusive use of the subscriber to ensure that the signature creation data is protected against use by third parties.

Mechanism 2 - Key pair generated by ANDES SCD

The public and private keys of end entity certificate holders are generated by ANDES SCD as long as the request is for agreements or when the subscriber so determines.

For certificate issuance requests processed through agreements, the process may vary depending on the entity with which Andes SCD has a certificate issuance agreement.

Guarantee of the security offered by the keys

ANDES SCD uses the RSA algorithm to generate all public and private keys for its CAs and certification service subscribers.

The RSA algorithm bases the security of its keys on the computational difficulty involved in factoring very large prime numbers. For example, factoring a 232-digit prime number that is equivalent to a 768-bit key required about 670 2.2GHz Opteron processor machines working in parallel for 3 years.


ANDES SCD uses 2048-bit length keys for internal and end-entity certificates.

6.1.2. Delivery of the private key to the subscriber

According to the key generation mechanism, the delivery of the subscriber's private key varies:

Mechanism 1- The subscriber-generated key pair

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

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Mechanism 2 - Key pair generated by ANDES SCD

When the key pair is generated by ANDES SCD, the private key will be delivered directly to the subscriber. The private key is delivered through a cryptographic device that prevents its export, therefore there is no copy of it and the subscriber will be solely responsible for its use and custody.

When the certificate delivery format corresponds to a virtual token ANDES SCD will keep the subscriber's private key in secure cryptographic devices that comply with the FIPS 140 2 Level 3 standard, this key will remain encrypted and its access will only be possible through the credentials delivered directly to the certificate holder.

6.1.3. Delivery of the public to the certificate issuer

According to the key generation mechanism, the delivery of the subscriber's public key to ANDES SCD varies.

Mechanism 1- The subscriber-generated key pair

The delivery of the subscriber's public key to ANDES SCD is done securely in PKCS10 format, which is generated when registering from the web page the certificate issuance request with delivery form "PKCS10" and contains the public key generated by the subscriber himself.


Mechanism 2 - Key pair generated by ANDES SCD

The Public Key is embedded in your digital signature certificate.

6.1.4. Subscriber Public Key Distribution

The public key of any End Entity Certificate subscriber whose certificate was issued by ANDES SCD is permanently available for download in the certificate directory of the web page.

The public key of Class I Certificate subscribers (internal use) is permanently available for ANDES SCD internal use.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

6.1.5. ANDES SCD public key distribution to users

The ANDES Root CA public key and the Subordinate CAs are permanently available for download on the ANDES SCD Website.

6.1.6. Period of use of the private key

CA private key

The period of use of the private key of the Root ANDES CA is 25 years, the start and end date is explicit in the certificate and in the "Certification Authority (CA)" section of this document.

The period of use of the key of the CA issuing Class I Certificates and the CA issuing Class III Certificates is 10 years.

The period of use of the CA issuing Class II v2 Certificates is 2,293 days.

The start and end date of each of these certificates is explicit in the respective certificate and in the "Certification Authority (CA)" section of this document.

The period of use of the key of the third level CAs subordinate to the Class III CA is 5 years. The start and end date of each of these certificates is explicit in the respective certificate.

Subscriber private key


The period of use of the private key for internal use certificates and end-entity certificates is defined in the applicable Certification Policy. For some types of certificates the period of use of the private key is the same as the period of validity of the certificate.

6.1.7. Size of keys

The size of the certified keys of the Root CA and subordinate CAs is 4096 bits long based on the RSA algorithm.

The size of the certified keys for internal use is 2048 bits based on the RSA algorithm.

The size of the certified keys for end-entity is 2048 bits based on the RSA algorithm.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

6.1.8. Public key generation and quality check parameters

The public key of the Root CA and subordinate CAs are encrypted according to PKCS#1. The key generation algorithm is RSA.

The key generation parameters and the means of checking the quality of the key generation parameters for end-entity Certificates are defined in the applicable Certification Policy.

6.2. Private Key Protection Controls

6.2.1. Private Key Protection Controls

The cryptographic module used to generate and store ANDES CA private keys is an HSM module that complies with the NIST FIPS140-2 standard and meets security level 3.

6.2.2. Control over the private key (Multi-person)


Access to the private key used by the Root CA and Subordinate CAs is done through the cryptographic module (HSM) by involving 2 people out of a possible 4. This multi-person control ensures that no one has individual control of critical activities such as activating and using the private key of the Root and Subordinate CAs.

6.2.3. Private Key Backup

Periodically a test run is performed to ensure the correct operation of the HSM device containing the private keys of the root and subordinate CAs.

There is at least one backup copy of the CA private keys that makes possible their recovery in case of disaster, deterioration or loss, is stored and recovered only by authorized personnel according to trust roles, using at least a dual control in a secure physical medium.

Backup copies of the CAs' private key signatures are securely stored. This procedure is described in detail in the ANDES SCD Security Policies.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

In the case of subscriber private keys, no backup is performed because this key only remains in the custody of the subscriber and is never in the possession of ANDES SCD.

6.2.4. Private key storage

CA private key

When the CA's private keys are outside the HSM cryptographic module, they are kept encrypted and the key with which the encryption was performed is divided and safeguarded in 2 cryptographic devices stored in a safe protected by a key, this key is divided and assigned to the PKI Auditor and Infrastructure Coordinator, so for access to the HSM keys, both trust roles must be present.

Subscribers' private key

The private keys of the internal certificates used by the various components of the CA system to communicate with each other, sign and encrypt information are stored by ANDES SCD for a period of at least 10 years.

Mechanism 1- The subscriber-generated key pair

The private keys generated by the subscriber himself are NEVER stored by ANDES SCD, they must be stored by themselves, through the conservation of the signature creation device or other methods, because they may be necessary to decrypt the historical information encrypted with the public key, provided that the custody device allows the operation.

Mechanism 2 - Key pair generated by ANDES SCD

The storage of the subscriber's private key generated by ANDES SCD may vary according to the certificate issuance agreement or depending on the delivery format.

6.2.5. Transfer of the private key from or to a cryptographic module

CA private key

CA private keys are generated directly in the HSM cryptographic module following the documented procedure of the Key Generation Ceremony, the transfer of private keys from the cryptographic module is limited only to backups in accordance with the "Private Key Backup" section of this document.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Subscribers' private key

Mecanismo 1 - The subscriber-generated key pair

In the case of subscribers requesting PKCS10 certificate delivery, they must generate their own key pair and protect the use and custody of their private key.

Mechanism 2 - Key pair generated by ANDES SCD

The transfer of the subscriber's private key generated by ANDES SCD may vary according to the entity with which Andes SCD has a certificate issuance agreement or depending on the delivery format.

6.2.6. Storage of the private key in a cryptographic module

The private key of the Root CA and Subordinate CAs are created and stored in encrypted form in an HSM cryptographic module.

6.2.7. Method of activating the private key

Activating the private key consists of logging on to the device that stores it, allowing operations to be performed with the private key for an indefinite period of time until it is deactivated.

Activation of CA keys

The activation of ANDES SCD private keys is done automatically once the HSM is started.


Subscriber key activation

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. The protection of the activation data is the sole responsibility of the subscriber.

The activation of the subscriber's private key generated by ANDES SCD may vary according to the certificate issuance agreement..

6.2.8. Private key disabling method

Deactivating the private key consists of terminating the session on the device that stores it, preventing operations with the private key from being performed.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Any operation with the private key after deactivation requires activation of the device.

CA private key deactivation

The CA private key becomes inactive once the HSM is turned off.

Private key deactivation subscribers

The method to deactivate the subscriber's private key is to remove the TOKEN device from the computer, immediately any associated content is disabled including the private key.

The deactivation of the subscriber's private key generated by ANDES SCD may vary depending on the certificate issuance agreement.

6.2.9. Method of destruction of private key

CA private key destruction


The destruction of CA private keys is performed when their operational period or validity period is over, when the keys are compromised or when the Certification Authority is terminated.

The key destruction process is performed by authorized personnel using the functions provided by the HSM cryptographic module so that other private keys residing in the device are not affected.

The CA key destruction process is detailed in the internal document CA Key Destruction Procedure.

Destruction of subscribers' private keys

The destruction of the subscriber's private key can be performed by the subscriber himself using the functions provided by the TOKEN device, taking into account that, if he has more private keys inside the device, these are not affected.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

The destruction of the subscriber's private key generated by ANDES SCD may vary according to the certificate issuance agreement.

6.2.10. Classification of cryptographic modules

The cryptographic module used to generate the private keys of ANDES SCD CAs complies with the FIPS 140-2 level 3 standard.

6.3. Other aspects of key pair administration

6.3.1. Public Key File

ANDES SCD maintains archives of all certificates for a period of 15 years, each of these certificates including the corresponding public key. These files are protected by access controls to the other components of the infrastructure.

6.3.2. Operational periods of the certificate and periods of use of the key pair

The lifetime of the certificate 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 either of these events occurs, the certificate's validity is terminated and it can only be used for historical verification purposes.

The key pair is valid as long as there is a valid 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.

6.4. Activation data

Activation data are values required by cryptographic devices to allow access to the private keys they contain.

6.4.1. Generation and Installation of Activation Data

The generation and installation of the activation data consists of the creation of the data that allows authentication to the device containing the private key approving its use.

HSM device activation data

The Infrastructure Coordinator has an administration and options key that allows him to generate and manage the user accounts for the operators that

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

will activate the ANDES SCD private keys. Each of the HSM operators in turn has a key that they must keep under their responsibility so that no operator knows more than one key and ensures that no one has individual control of critical HSM activities such as activating and using the private key of the root and subordinate CAs.

TOKEN device activation data

The subscriber must generate the activation data of his TOKEN by changing the initial PIN that comes by default with the device using the software application provided by the TOKEN manufacturer. 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.

Activation data to access subscriber's private key generated by Andes SCD

The activation mechanism may vary according to the certificate issuance agreement.

6.4.2. Activation Data Protection

Protection of cryptographic device activation data prevents unauthorized use of the private key.

HSM activation data protection

HSM device activation data is classified as confidential information and each particular access key should be known only to the operator responsible for activating the device simultaneously with another operator. In no case should an operator know more than one Activation key.

HSM operators are responsible for safekeeping their password and must not disclose their status as HSM operators or other operators to any third party.

HSM operator passwords are changed periodically to reduce the possibility of compromise.

TOKEN activation data protection

The PIN or TOKEN activation data must be personalized by the subscriber.

The subscriber must change the PIN of his TOKEN if there is any suspicion that a third party knows this data. To change the PIN it is necessary to download the

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

software application offered by the TOKEN manufacturer and available on the ANDES SCD website.

The protection of the activation data is the sole responsibility of the subscriber.

Activation data protection for access to subscriber's private key generated by ANDES SCD

The protection mechanism may vary according to the certificate issuance agreement.

6.5. Informatic security controls

6.5.1. Specific technical safety requirements

Each CA server includes the following functionalities:

- Access control to CA services
- Privilege management to assign relevant tasks to each user.
- User identification and authentication for CA applications based on digital certificates.
- Auditing of security-related events.
- CA system and key recovery mechanisms. Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Information security level

- Operating system security configuration
- CA technical and configuration documentation
- Application security configuration
- Configuration of users and privileges
- High availability system maintenance and administration plan
- Contingency and disaster recovery plan

6.6. Technical life cycle controls

6.6.1. Controls in system development

ANDES SCD has designed a methodology to control changes in the versions of operating systems and applications that imply an improvement in their security functions or that eliminate any vulnerability discovered.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

6.6.2. Safety Management Controls

ANDES SCD conducts training and awareness-raising sessions for employees regarding the implementation of security policies, using descriptive documentation resulting from feedback and monitoring of security management.

According to the risk analysis ANDES SCD classifies assets according to their protection needs and performs capacity planning in such a way that it is possible to guarantee high availability and scalability of services.

6.6.3. Life Cycle Safety Controls

ANDES SCD covers the following security controls, specifying the treatment of each control in the Information Security Policies (ISP):

- Controls for CA key management indicating how the private keys of the root CA and subordinate CAs are generated, how they are stored and how they are protected.
- Controls for securely distributing the CA public key to subscribers and trusted third parties.
- Security controls on certificate issuance from the time the certificate issuance request is received until the certificate is delivered to the subscriber.
- Security controls for certificate revocation (fast and secure revocation mechanisms, controls to revoke certificates in person, on-line or by telephone, acknowledgement of receipt provided by the CA to indicate receipt of the revocation request, CRL update, sending an email informing the subscriber that his/her certificate was revoked)
- Certificate issuance security controls: (CA maintains controls to provide assurance that at the time of issuance the certificate is available to subscribers and relying parties, repository management by authorized personnel only, integrity of repository information)

6.7. Network security controls

Network access control is restricted to authorized personnel.

- Network components are located in secure facilities with permanent monitoring.
- ANDES SCD's internal network is protected by firewalls configured with access policies and alert systems to prevent unauthorized access.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- The communication of sensitive information between ANDES SCD and the Registration Authorities is done through SSL protocol that guarantees the confidentiality and integrity of the information exchanged.
- Firewalls and controls are implemented to protect the internal network from external access.
- There are procedures and provisions regarding the use of networks and network services.
- The technological infrastructure that supports the certification services that are continuously monitored through a NOC/SOC is located in the administrative office in the city of Bogotá, Av. Calle 26 NO 69C-03 Torre B Oficina 701.

6.8. Time stamp

The requirements, practices, uses and applications of time stamping can be found in the statement of practice for time stamping service.

7. Certificate profiles, CRL y OCSP

7.1. Certificate profiles

7.1.1. Version number

All certificates issued by ANDES SCD are compliant with the X.509 V3 standard and in accordance with RFC 5280 for certificate profiles and CRLs.

7.1.2. Certificate Extensions

The extensions used generically in the certificates are:

- BasicConstraints: Qualified as critical.
- KeyUsage: Qualified as critical.
- ExtendedKeyUsage: Qualified as critical
- CertificatePolicies: Qualified as non-critical.
- SubjectAlternativeName: Qualified as non-critical.
- CRLDistributionPoint: Qualified as non-critical.
- OCSPServiceLocator: Qualified as non-critical.
- UseCertificatePolicies: Qualified as non-critical.

Each Certification Policy establishes the variations in the set of extensions used by each type of certificate.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

7.1.3. Identifiers object of the algorithm

- 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

7.1.4. Name Formats

The digital certificates issued by ANDES SCD are restricted to 'Distinguishedname' (DN) X.500 which are unique and unambiguous, the certificates contain the DN of the issuer and subscriber of the certificate in the issuername and subjectname fields respectively. In each Certification Policy the DNs used for the subscriber are described.

7.1.5. Name Restrictions

The digital certificates issued by ANDES SCD have a DN in accordance with X.500 recommendations that are unique and unambiguous.

7.1.6. Object identifier of the certification policy

An OID or object identifier is a unique sequence of numbers assigned hierarchically by one of the existing registration agencies such as IANA, ANSI or BSI in order to enable the identification of objects on the network. Once an organization has acquired an OID it has the right to freely assign that branch of the hierarchy according to its interests.

ANDES SCD has been assigned OID 31304 since June 2008, registered with the international organization IANA (Internet AssignedNumbersauthority), under the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA RegisteredPrivate Enterprise). This can be found at: <http://www.iana.org/assignments/enterprise-numbers>.

In this way ANDES SCD hierarchically assigns an OID to each of its policies and CPS starting from the root: **1.3.6.1.4.1.31304**.

The OID assigned to this statement of certification practices (CPS) is **1.3.6.1.4.1.31304.1.1.1** additionally, a Y.Z format extension is added specifying the version. Then the OID **1.3.6.1.4.1.31304.1.1.1.Y.Z** is interpreted as the CPS publication Z of the Y version.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Each Certification Policy is assigned an OID within the private numbering range, all CPs start with the prefix **1.3.6.1.4.1.31304.1.2**

7.1.7. Syntax and semantics of policy qualifiers

The certificate extension concerning the qualifiers of the certification policy contains the following information:

- **PolicyIdentifier:** Contains the identifier of the PC that applies to the certificate type.
- **CPS:** Indicates the URL where the Certification Practices (CPS) are published to be consulted by users.
- **UserNotice:** The use of this certificate is subject to the Certificate Policies (CP) and Certification Practices (CPD) established by ANDES SCD, Accreditation Code: 16-ECD -004.

7.1.8. Profile of the CRL

7.1.8.1. Version number

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


7.1.8.2. CRL and extensions

The CRL revocation list is issued as stipulated in RFC 2459.

The following is the format of the CRL profile for each of the Class

CRL of ROOT CA ANDES SCD S.A

CRL profile by standard X.509V2 – CRL CA Root		
Name	Description	Value
Version	CRL version	V2
CRL number	Unique number of CRL	Identifier of CRL
Issuer	CN	ROOT CA ANDES SCD S.A.
	O	ANDES SCD
	OU	Certification Division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Signature Algorithm	Signature algorithm of the CRL	SHA256withRSA

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Effective date of issue	Validity period of the CRL	Date of issuance of the CRL in UTC time
Next update	Next issue date CRL	Next CRL issue date in UTC time
URL distribution	URL where the CRL is published	http://crl.andesscd.com.co/Raiz.crl
Certificates revoked	List of revoked certificates specifying serial number, date of revocation and reason for revocation.	

CRL of CA ANDES SCD S.A. Class I

CRL profile according to X.509V2 standard - CRL Class I		
Name	Description	Value
Version	CRL versión	V2
CRL Number	Unique number of the CRL	Identifier of CRL
Issuer	CN	CA ANDES SCD S.A. Class I
	O	ANDES SCD
	OU	Certification division for internal use
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Signature Algorithm	CRL Signature Algorithm	SHA256withRSA
Effective date of issue	Validity period of the CRL	Date of issuance of the CRL in UTC time
Next update	Next issue date CRL	Next CRL issue date in UTC time
URL distribution	URL where the CRL is published	INTERNAL USE
Certificates revoked	List of revoked certificates specifying serial number, date of revocation and reason for revocation.	

CRL of CA ANDES SCD S.A. Class II

CRL profile according to X.509V2 standard - CRL Class II		
Name	Description	Value
Version	CRL Version	V2
CRL number	CRL unique number	Identifier of CRL
Issuer	CN	CA ANDES SCD S.A. Class II
	O	ANDES SCD

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

	OU	Final entity certification division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Signature Algorithm	CRL Signature Algorithm	SHA256withRSA
Effective date of issue	Validity period of the CRL	Date of issuance of the CRL in UTC time
Next update	Next issue date CRL	Next CRL issue date in UTC time
URL distribution	URL where the CRL is published	http://crl.andesscd.com.co/Classell.crl
Certificates revoked	List of revoked certificates specifying serial number, date of revocation and reason for revocation.	

CRL of CA ANDES SCD S.A. Class II v2

CRL profile according to X.509V2 standard - CRL Class II v2		
Name	Description	Value
Version	Version of CRL	V2
CRL Number	Unique number of CRL	Identifier of CRL
Issuer	CN	CA ANDES SCD S.A. Class II v2
	O	ANDES SCD
	OU	Final entity certification division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Signature Algorithm	CRL Signature Algorithm	SHA256withRSA
Effective date of issue	Validity period of the CRL	Date of issuance of the CRL in UTC time
Next update	Next issue date CRL	Next CRL issue date in UTC time
URL distribution	URL where the CRL is published	http://crl.andesscd.com.co/Classellv2.crl
Certificates revoked	List of revoked certificates specifying serial number, date of revocation and reason for revocation.	

CRL of CA ANDES SCD S.A. Class III

CRL profile according to X.509V2 standard - CRL Class III

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Name	Description	Value
Version	Version of CRL	V2
CRL Number	Unique number of CRL	Identifier of CRL
Issuer	CN	CA ANDES SCD S.A. Class III
	O	ANDES SCD
	OU	Subordinate final entity certification division
	C	CO
	L	Bogotá D.C.
	E	info@andesscd.com.co
Signature Algorithm	CRL Signature Algorithm	SHA256withRSA
Effective date of issue	Validity period of the CRL	Date of issuance of the CRL in UTC time
Next update	Next issue date CRL	Next CRL issue date in UTC time
URL distribution	URL where the CRL is published	http://crl.andesscd.com.co/Cla selll.crl
Certificates revoked	List of revoked certificates specifying serial number, date of revocation and reason for revocation.	

7.2. Profile OCSP

ANDES SCD offers a free service of access to online validation of the status of certificates through the OCSP protocol, as specified in RFC 5019 and 6960.

7.2.1. Version number

The OCSP certificate is issued in accordance with the X509 V3 standard.

7.2.2. Extensions OCSP

OCSP extensions according to standard X.509V3	
Name	Value
Basic Constraints, critical	CA false
Key Usagecritical	Firma digital
Extended Key Usage	OCSPSigner
Subject Key Identifier	identificador de llave

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

8. Audit and other valuations

8.1. Frequency or circumstances of assessment

Internal audits will be conducted periodically to ensure the adequacy of the functioning and operation with respect to the stipulations included in this Certification Practices Statement, the Certificate Policies and the Information Security Policies

An external audit will be performed annually to verify compliance with the Web Trust principles for Certification Authorities.

8.2. Identity and Qualifications of the Advisor

External audits are carried out by companies of recognized prestige in the area of auditing.

8.3. Relationship between the assessor and the assessed entity

The internal auditor should have no functional relationship with the areas being audited.

Apart from the audit function, the external auditor and the audited party should not have any relationship that could lead to a conflict of interest.


8.4. Topics covered in the valuation

The audit determines the adequacy of ANDES SCD services with this CPS and the applicable CPs and verifies the following aspects:

Publication of information: Verifying that the Certification Practices Statement (CPS) and Certification Policies (CP) are made public and that it provides its services in accordance with these statements.

Service integrity: Verifies that the Certification Authority maintains effective controls to ensure that the subscriber's information is properly authenticated, the integrity of the keys and certificates managed and their protection throughout their life cycle.

Security controls: Verify that the Certification Authority uses effective controls to ensure the confidentiality of subscriber data, that administration and management is restricted to authorized personnel, that there are continuity plans

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

in the operations of the certification service and certificate life cycle, and that there are security policies to reduce vulnerabilities and risks that may arise.

8.5. Actions taken as a result of Non-Conformities

In the event that the auditor detects any nonconformity, all necessary corrective actions will be taken to resolve it in the shortest possible time.

8.6. Communication of results

The auditor communicates the results of the audit to the area where the nonconformity was detected.

9. Business and legal matters

9.1. Rates

9.1.1. Certificate issuance fees

The fee for the digital certificate issuance service is available on the PC of each of the services.

9.1.2. Certificate Access Fees

However, ANDES SCD reserves the right to impose a fee in cases of massive downloading of certificates or any other case in which it considers it must charge a fee

9.1.3. Fees for information on the status of revoked certificate(s)

Access to consult and download the revocation lists is a free service, however, ANDES SCD reserves the right to impose a fee for other means of checking the status of certificates or any other case in which a fee is considered necessary.

9.1.4. Reimbursement policy

The money received for certification services will be refundable only in the following cases:

1. When a payment is received for a higher value than the one defined for the service requested: The excess value over the rate of the service purchased will be refunded.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

2. Failure to provide services within the established time: This reason for reimbursement will apply in the following cases:

2.1. For the digital certificate service, if once the subscriber's identity verification process has been successfully completed, the corresponding digital certificate is not issued within the term established in the PC corresponding to the type of digital certificate to be issued.

2.2. For the time stamp service, if the respective time stamps are not supplied within the term established in the supply contract entered into between the parties or, failing that, within the time established in the terms and conditions of use of the time stamp service.


If any of these situations occurs, the amount paid for the requested service will be refunded; however, in order to be refunded, the client must make the corresponding request. If once the term established for the provision of the service has expired, ANDES issues the corresponding digital certificate or provides the respective time stamps, before receiving the request for reimbursement from the client, there will be no reimbursement, since the fee is caused by the mere fact of receiving the request and proving the identity of the applicant.

3. Non-compliance with the technical and/or legal requirements of the digital certification services: When any of ANDES' digital certification services present a duly demonstrated non-compliance with the technical and/or legal requirements established in the Law for digital certification entities, the applicant may request the refund of the amount paid for the services, notwithstanding the aforementioned refund will be proportional from the date on which ANDES' services ceased to comply with the technical and/or legal requirements established in the Law for digital certification entities.

9.1.5. Inappropriateness of the claim for reimbursement

The request for reimbursement will not be admissible and ANDES SCD will not refund the money to the subscribers in the following cases:

a) If, once the payment has been made, the customer does not comply with his duty to request the issuance of the corresponding digital certificate, for which he

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

has 3 months following the date of payment, once this period has elapsed, the request for reimbursement will not proceed.

b) 2.1. and 2.2. of the previous section, if once the term established for the provision of the service has expired, ANDES issues the corresponding digital certificate or provides the respective time stamps before receiving the request for reimbursement from the client, the request for reimbursement shall no longer be applicable nor shall there be any refund of the money, since the fee is caused by the mere fact of receiving the request and accrediting the identity of the applicant

c) For the case contemplated in numeral 3 of the previous paragraph, if the client does not make the reimbursement request within 3 months following the date on which a duly demonstrated breach of the technical and/or legal requirements established in the Law for digital certification entities has occurred, the reimbursement request shall not be admissible.

For the case contemplated in numeral 1, the reimbursement request shall apply at any time.

Requests for reimbursement must be submitted through the PQRSF form available on the ANDES SCD website or by e-mail. pqrs@andesscd.com.co.

9.2. Financial responsibility

In order to indemnify the damages that may be caused to the users of the digital certification service, a civil liability insurance is available to cover the contractual and extra-contractual damages of the subscribers and third parties in good faith exempt from fault, as long as the damages derive from errors, omissions or acts of bad faith on the part of ANDES SCD.

It is clarified that ANDES SCD will not assume any responsibility for the non-performance or delay in the provision of certification services, if this failure or delay is the result of acts of God, force majeure, exclusive fault of the victim, the act of a third party in general, of any circumstance beyond the control of ANDES SCD and in particular of the situations stated in the "Limitations of Liability" section of this CPS.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

ANDES SCD is not liable for any damages arising from:

1. Non-compliance or incorrect execution of the obligations in charge of the Applicant, subscriber and/or User.
2. Incorrect use of the digital certificates and private keys by the subscriber, or any indirect damage or harm that may result from the use of the digital certificates and private keys..

Liability policy information

Insurance company : SBS SEGUROS
 Taker : ANDES Servicio de Certificación Digital S.A SIGLA ANDES SCD S.A.
 Insured : ANDES SCD S.A.
 Beneficiary : Terceros afectados de buena fe.
 Value : \$ 8.700.000.000Pesos.

9.3. Confidentiality of Business Information

9.3.1. Scope of confidential information

All information that is not considered public by ANDES SCD is considered confidential.


Se cataloga como confidencial la siguiente información:

1. Private keys of the Root CA and Subordinate CA of ANDES SCD.
2. Personal information of subscribers that is not contained in the digital certificate.
3. Information of security parameters, control and audit procedure.
4. Technical infrastructure documentation, Security Policy Statement, Key Generation Ceremony Guidance Document and Contingency Plan.

9.3.2. Information not considered confidential

The following information is classified as public

- 1- Certification Practice Statement (CPD) and Certification Policies for End Entity certificates.
2. Certificates issued by ANDES SCD
3. Lists of Revoked Certificates (CRL)

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.3.3. Responsibilities for protecting confidential information

ANDES SCD personnel participating in any activity or operation of the Certification Service are subject to the duty of secrecy within the framework of the contractual obligations contracted with ANDES SCD.

9.4. Confidentiality of personal information

All subscriber information that is not included in the certificate is considered confidential.

9.4.1. Privacy plan

The privacy plan to protect information classified as confidential is defined in the Personal Data Protection Policy and the Information Security policies include controls to protect and assign each type of information a degree of criticality.


9.4.2. Information considered confidential

ANDES SCD considers confidential all information that is not expressly classified as public and that does not have the disclosure approval of the owner of the information.

9.4.3. Information not considered confidential

The information considered non-confidential is as follows

- Issued certificates
- Binding of the subscriber to a certificate issued by ANDES SCD
 - The serial number of the certificate
- The name and surname of the certificate subscriber, in the case of individual certificates, as well as any other circumstance or personal data of the holder as long as it is significant for the purpose of the certificate.
- The e-mail address of the certificate subscriber.
- The validity period of the certificate, specifying the date of issue and expiration date.
- The statuses or situations that affect the certificate and the start date of each one, i.e. from which date it is revoked.
- The revocation lists of the Root CA and Subordinate CAs.
- Certification policies and practices

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Any information whose publication is required by law.

9.4.4. Responsibility to protect information

Subscriber and user information is restricted to authorized personnel and protected from uses not specified in business practices.

9.4.5. Notification and consent to use confidential information

No dissemination of information declared as confidential without the express written approval or consent of the entity or organization that owns the information, unless legally compelled.

9.4.6. Access to information from judicial or administrative proceedings

ANDES SCD will not deliver information about its subscribers to third parties without prior, express and informed written authorization in writing from the subscriber, except in cases where such information is requested by a judicial authority in the exercise of its legal and constitutional functions, in which case ANDES SCD will proceed to deliver the information and inform the subscriber of the request made by the authority, so that it can take appropriate actions to protect the confidentiality of their personal data.

9.5. Intellectual property rights

The intellectual property rights of this Certification Practices Statement belong to ANDES SCD.

ANDES SCD is the only entity that holds the intellectual property rights over the digital certificates issued by ANDES SCD.

The Subscriber acknowledges that, in the use of the assigned digital signature certificate, any underlying technology used and all content available on the Service is the property of ANDES and its suppliers, is protected by national laws and international treaties covering intellectual property rights, including moral rights and economic rights of authorship.

9.6. Rights and duties.

9.6.1. Rights and duties of ANDES SCD

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Infrastructure:


- a) To have the technological, economic and human elements and facilities required to offer certification services, as well as the physical security controls, procedures and strategies necessary to guarantee the trust and operation of the services.
- b) Guarantee compliance with the requirements imposed by current legislation.

Technical

- c) Protect the private keys of the ANDES SCD Certification Authority.
- d) Not to copy or store the private keys corresponding to the certificates issued to the Final Entity or certificates for internal use issued for the purpose of being used for electronic signature, when these are generated on the cryptographic devices of the Final Entity. In the case of agreements, the provisions established with the entity with which Andes SCD has an agreement shall be followed.
- e) Issue Certificates in compliance with the X.509 V3 standard and in accordance with the subscriber's request.
- f) Guarantee that the date and time when a certificate was issued or revoked can be determined.
- g) Use reliable systems to store the certificates and prevent unauthorized persons from modifying the data and detect any evidence that affects security.
- h) Maintain the certificate directory up to date, indicating which certificates have been issued and whether they are valid or revoked.
- i) Store in the PKI infrastructure indefinitely the CRLs and the current, expired and revoked digital certificates.
- j) Publish in a timely manner on the WEB page the certificates that are in force and the CRLs of the Root CA and the Subordinate CAs.
- k) Inform subscribers of the approaching expiration of their certificate by sending an email 30, 15, 7 and 1 days prior to expiration.

Organizational


- l) Comply with the provisions of the Certification Policies and Practices.
- m) To have qualified personnel with the necessary knowledge and experience to provide the certification service offered by ANDES SCD.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- n) Approve or deny requests for the issuance of certificates sent by the Registration Authority.
- o) Provide the applicant with the following information free of charge on the ANDES SCD website: Statement of certification practices and certification policies.
- p) Inform subscribers of the revocation of their certificates immediately upon the occurrence of such event.
- q) Inform the Colombian National Accreditation Organism ONAC about events that may compromise the service rendered by ANDES SCD.
- r) Guarantee the protection, confidentiality and proper use of the information provided by the subscriber.
- s) Take measures against forgery of certificates and guarantee their confidentiality during the generation process and their delivery to the subscriber by means of a secure procedure.
- t) Inform suppliers that it extends compliance with the requirements of this document to them, when applicable.
- u) Make available on the Andes SCD website the services that are accredited.

9.6.2. RA Rights and duties

- a) Respect and comply with the provisions stipulated in the Certification Policies and Practices and in the terms and conditions of the service.
- b) Require the applicant to provide all the documents required for the type of certificate to be obtained.
- c) Verify the identity of certificate applicants by verifying the accuracy, sufficiency and authenticity of the information provided by the applicant.
- d) Before starting the certificate issuance process, verify that the applicant has paid for the digital certificate he/she wishes to acquire.
- e) Communicate to ANDES SCD with due promptness the requests received for issuance and revocation of the certificate.
- f) Protect the personal data provided by the applicant in accordance with the policy for the handling of confidential information.
- g) To deliver the certificate to the subscriber.
- h) All procedures carried out must be electronically signed by the RA operators who carry them out, thus assuming full responsibility for the process.

	<p align="center">CERTIFICATION PRACTICES STATEMENT</p>	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- i) Formalize the use of the service with the subscriber under the terms and conditions established by the ANDES SCD Certifying Authority

9.6.3. Applicant's rights and duties

Rights:


- ✓ Receive the necessary instructions from ANDES SCD to use the digital certification services.
- ✓ Submit complaints, petitions, claims, suggestions, requests and congratulations in a respectful manner, regarding the digital certification service, using the processes that ANDES SCD has available for this purpose.
- ✓ That their personal information is guarded and stored under appropriate conditions of confidentiality, security, access and restricted circulation, in order to prevent its leakage, unauthorized or fraudulent use by third parties, as well as any other conduct that violates the privacy of the Applicant.
- ✓ To be attended by qualified personnel, with the necessary knowledge and experience to provide the certification service offered by ANDES SCD.
- ✓ Have access to the CPS and the certification policy that applies according to the type of certificate, which are available on the ANDES SCD website free of charge.

Duties:

- ✓ Provide truthful and updated information in accordance with the requirements stipulated in the Certificate Policy that applies to the type of certificate you wish to obtain.
- ✓ Notify during the period of validity of the certificate any change in your background contained in the certificate. For example, change of name, email, etc.

9.6.4. Subscriber Rights and Duties

Rights:

	<p style="text-align: center;">CERTIFICATION PRACTICES STATEMENT</p>	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- ✓ Use the digital certificate for the uses and in accordance with the conditions specified in the digital certificate, in the Certification Practices Statement and the applicable Certification Policy.
- ✓ Request the revocation of the digital certificate when there is a subsequent modification of the subscriber's background, when there is a liquidation of a legal entity that is linked in a certificate, when there is a falsification of the subscriber's background or when it is proven that any of the certificate data is incorrect or that any requirement is not met. Inform and receive attention from ANDES SCD and the corresponding management, when there are changes or alterations in the information that has been incorporated in the digital certificate, or any alteration that may affect the provision of the ANDES SCD service.
- ✓ Receive the necessary instructions from ANDES SCD to make proper use of the digital certification services.
- ✓ Submit complaints, requests, claims, suggestions, SOLICITUDES and congratulations in a respectful manner, about the digital certification service, using the processes that ANDES SCD has available for this purpose.
- ✓ That your personal information is guarded and stored under appropriate conditions of confidentiality, security, access and restricted circulation, in order to prevent its leakage, unauthorized or fraudulent use by third parties, as well as any other conduct that violates the subscriber's privacy.
- ✓ Make requests to know, update, rectify, delete, hide or include personal data in accordance with the provisions of Law 1581 of 2012 on personal data protection and in accordance with the ANDES personal data protection policy, which is available on its website www.andesscd.com.co.
- ✓ Receive a quality certification service that complies with the technical requirements established in the Law, as well as with the legal effects contemplated therein, for the purposes of signing contracts in electronic media, establishing time stamps, making electronic notifications and the other purposes contemplated in the services provided by ANDES SCD.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


- ✓ To know, if required, the date and time of issuance or revocation of a digital certificate.
- ✓ To be informed about the approaching expiration of the services subject to digital certification of which he/she is a user, by e-mail 30, 15, 7 and 1 day before the expiration date.
- ✓ To be attended by qualified personnel, with the knowledge and experience necessary to provide the certification service offered by ANDES SCD.
- ✓ To have access to the CPS and the certification policy applied on the ANDES SCD website free of charge.
- ✓ Have its digital certificate revoked in the event that an inconsistency caused by an error not attributable to the subscriber is found in the certificate and a new certificate is issued immediately.
- ✓ Other rights recognized by the constitution and the law.

Duties:


- ✓ The private key is personal and non-transferable; therefore, it must be carefully guarded to prevent others from impersonating you and signing documents in your name or accessing confidential messages. The use of the private key by others is the responsibility and risk of the holder. The use of the private key by others is the responsibility and risk of the holder, because if the necessary measures are not taken, the security system that is intended to be put in place will be meaningless.
- ✓ Keep the revocation code provided at the time of delivery of the certificate confidential, it is recommended to keep it in a different place than the certificate.
- ✓ Use the certificate according to the Certification Policies and Practices applicable to the type of certificate.
- ✓ Respect the provisions of the terms and conditions.
- ✓ Respect the limitations of use of the certificate.
- ✓ Respect the provisions and limitations of use of the certificate.
- ✓ Use the private key only with cryptographic devices according to the security levels required by ANDES SCD.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- ✓ Inform as soon as possible the existence of any cause for revocation.
- ✓ Report any change in the data provided for the creation of the certificate during its period of validity.
- ✓ Do not use the private key and certificate from the moment revocation is requested and also when the certificate supporting the key pair is not valid.
- ✓ Verify that the information contained in the certificate is true and exact. If there is any incomplete or incorrect information, notify ANDES SCD immediately.
- ✓ Respect the rights of third parties and be responsible before them for the damages that the misuse of the assigned digital signature certificate may cause, as well as to defend ANDES, if it is sued for any circumstance related to the misuse of the same.
- ✓ To make and keep by its own means the backup files or backup copies of the information related to the invoices digitally signed with the assigned certificate.
- ✓ Verify that the certification statements are consistent with the scope of the digital certification service.
- ✓ Abstain from:
 - Use the digital certification service in a manner that contravenes the law or causes ANDES SCD to be disreputable.
 - Make any statement related to its digital certification that ANDES SCD may consider misleading or unauthorized "
- ✓ Inform persons relying on the digital certificate of the measures and precautions to be taken to trust an ANDES SCD digital certificate.
- ✓ Use the digital certificate only for the uses and in accordance with the conditions specified in the digital certificate, in the Certification Practices Statement and the applicable Certification Policy.
- ✓ Request the revocation of the digital certificate when any of the causes contemplated in the Certification Practices Statement occurs.
- ✓ Respect the rights of third parties and be responsible to them for the damages that the use of the digital certificate may cause, as well as to defend ANDES SCD if it is sued for any circumstance related to the use of the digital certificate:
 - a) To guarantee the veracity of the declarations made at the time of requesting the digital certificate and the information contained in the certificate.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- b) The private key is personal and non-transferable for this reason it must be guarded diligently to avoid that other people can impersonate your identity and sign documents in your name or access confidential messages. The use of the private key by other persons is the responsibility and risk of the holder, because if the necessary measures are not taken, the security system that is intended to be established would be meaningless.
- c) Keep the revocation code provided at the time of delivery of the certificate confidential, it is recommended to keep it in a different place from the certificate.
- d) Use the certificate in accordance with the provisions of the applicable Certification Policies and Practices for the type of certificate.
- e) Respect the provisions of the terms and conditions and limitations of use of the certificate.
- f) Use the private key only with cryptographic devices according to the security levels required by ANDES SCD.
- g) Inform as soon as possible the existence of any cause for revocation.
- h) Report any change in the data provided for the creation of the certificate during its validity period.
- i) Not to use the private key and the certificate from the moment revocation is requested and also when the certificate that endorses the pair of keys is not valid.
- j) Verify that the information contained in the certificate is true and accurate; if there is any incomplete or incorrect information, notify ANDES SCD immediately.
- k) Respect the rights of third parties and be responsible before them for the damages that the misuse of the assigned digital signature certificate may cause, as well as to defend ANDES, if it is sued for any circumstance related to the misuse of this certificate.
- l) Make and keep by its own means the backup files or backup copies of the information related to the invoices digitally signed with the assigned certificate.
- m) Refrain from:
 - 1). Use the digital certification service in a manner that contravenes the law or cause bad reputation for ANDES SCD.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- 2). Make any kind of statement related to its digital certification that ANDES SCD may consider misleading or unauthorized.
- n) Verify that the statements about the certification are consistent with the scope of the digital certification service.
 - o) Stop using the digital certification in all advertising material containing any reference to it, once the digital certification service with ANDES SCD is cancelled or terminated, and take the actions required by the digital certification service and any other action required. In compliance with the Logo and Trademark Use Policy.
 - p) Report that it complies with the requirements specified in the ANDES SCD Digital Certification Policies when making reference to the digital certification service in media, such as documents, brochures or advertising.
- ✓ For certificates: Legal Entity and Electronic Invoicing, in the event that the subscriber generates his own pair of keys, he must:
- a) Use the RSA2048 algorithm or the one that updates or replaces it.
 - b) Attach in the request for issuance of digital certificate the Request that proves the possession of the private key.
 - c) Not to share the password of its private key.
 - d) Generate the private key in an equipment for personal use.
 - e) To carry out the safe custody of its private key.

The subscriber declares that he/she is aware of and accepts the risks associated with the application for software certificates, and agrees to establish adequate security mechanisms to safeguard confidentiality and prevent access by unauthorized third parties.

9.6.5. Rights and duties of the relying parties

- a) Verify before placing their trust in a certificate its validity at the time of any action based on the same and ensure that the certificate is appropriate for the intended use.
- b) Accept that messages or documents signed with the subscriber's private key have the same effect and legal validity as if the autographic signature had been made.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- c) To know and to be subject to the guarantees, limits and responsibilities applicable in the acceptance and use of the digital certificates in which it trusts.
- d) To notify any anomalous fact or situation related to the certificate that may be considered as a cause for revocation.

9.7. Limitations of liability

9.7.1. Responsibility for the veracity of the Subscriber's information

The Subscriber assumes all risks for damages that may arise from conduct such as providing false information, impersonating third parties, validating documents or incomplete or outdated information.

9.7.2. Responsibility for service availability

The Subscriber acknowledges and accepts that neither ANDES nor any of its representatives, employees or partners shall be liable for the unavailability of the service at any time due to force majeure, acts of God or acts of a third party; however, the Subscriber agrees to act diligently to minimize the possibility of failures or interruptions in the service.

Failures caused by the inability or inadequacy of the Subscriber's equipment, or by his lack of knowledge regarding the use of the service, shall in no case be attributable to ANDES and no compensation for any damage may be demanded from him.

9.7.3. Responsibility for the functionality of the service in the Subscriber's infrastructure

The Subscriber shall be solely responsible for the provision and payment of the costs necessary to ensure the compatibility of the service (digital signature certificate) with its equipment, including all hardware, software, electrical components and other physical or logical components required to access and use the same, including but not limited to telecommunications services, access and connection to the Internet, links, browsers, or other programs, equipment and services required to access and use the service.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.7.4. Responsibility in cybercrimes


In the event that the Subscriber is the victim of any of the behaviors typified as a crime by Law 1273 of 2009 (Computer Crimes Law), in its information systems, in its applications and technological infrastructure, in the execution of electronic transactions, or in the access and use of the service, phishing attacks, identity theft, due to negligence in the handling and confidentiality of the digital certificate, the Subscriber shall be solely responsible and shall be liable for the damages that may arise, since it is your obligation to adopt security measures, policies, cultural campaigns, legal instruments and other mechanisms to safeguard the confidentiality and proper use of your digital certificate.

9.7.5 Warranty disclaimers

In addition to the situations listed above, ANDES SCD shall not be liable for the following circumstances:

- a) Use of the certificates as long as it exceeds the provisions of the current regulations and this CPS, use of a revoked certificate or for placing trust in it without first verifying its status.
- b) For fraudulent use of certificates or CRL (List of revoked certificates).
- c) For damages and/or losses resulting from the misinterpretation of the Certification Practices by users and subscribers in the use of the services.
- d) Failure to comply with the obligations established for the subscriber or users in the current regulations.
- e) For the content of signed messages or documents or for the content of web pages that have a certificate.
- f) For practices not notified to ANDES SCD that affect the subscriber's private key allowing its use by third parties (e.g. theft, loss or compromise).
- g) Failure to recover documents encrypted with the subscriber's public key.
- h) Fraud in the documentation presented by the applicant or data entered incorrectly in the application.
- i) Use of the certificate by the subscriber outside its period of validity or when ANDES SCD has informed of the revocation of the certificate.

By accepting the terms and conditions of use of the digital signature certificate provided by ANDES SERVICIOS DE CERTIFICACIÓN DIGITAL S.A., the subscriber agrees to indemnify ANDES SCD as certification authority for any act or omission that causes damages, losses, debts and procedural expenses that ANDES SCD

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

may incur, which are caused by the use and publication of the certificates and that arise from:

- a) Failure to comply with the terms and obligations established in the Certification Practices Statement.
- b) False information provided by subscribers.
- c) Omission of fundamental facts that affect the nature of the certificate.
- d) Non-compliance in the safekeeping of private keys

9.8. Protection of personal data


ANDES, will treat the personal information of its subscribers, according to legal parameters, and with due diligence, to ensure its confidentiality, security and restricted circulation, for this it has policies for the protection of personal data, which are published on its website, at the link https://andesscd.com.co/docs/SGI/Políticas_Tratamiento_Datos_Personales.pdf these policies may be consulted by subscribers, in order to know their rights derived from Habeas Data, such as to know, update, rectify and delete personal data held by Andes SCD, as long as there is no legal or contractual duty of permanence of this data in our database.

9.9. Indemnifications

ANDES SCD includes in the legal instruments binding it to the subscriber indemnity clauses in case of breach of its legal or contractual obligations.

The subscriber must indemnify ANDES SCD as certification authority for any act or omission causing damages, losses, debts and legal expenses ANDES SCD may incur, which are caused by the use and publication of the certificates and which arise from:

- a) Failure to comply with the terms and obligations established in the certification practices statement.
- b) False information provided by the subscribers.
- c) Omission of fundamental facts that affect the nature of the certificate.
- d) Non-compliance in the custody of private keys

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.10. Term and termination

9.10.1. Termination of provisions

The Certification Practices Statement and each of the Certification Policies come into force from the moment they are published on the ANDES SCD website, from that moment the previous version of the document is repealed and the new version replaces the previous version in its entirety. ANDES SCD keeps in the repository the previous versions of the CPS and of each CP.

9.10.2. Termination and survival effect

For digital certificates that have been issued under an old version of the CPD or CP, the new version of the CPD or CP applies in everything that does not oppose the statements of the previous version.

9.11. Individual Notification and Communication with Participants

ANDES SCD notifies the changes in the present certification policy as long as these changes are relevant and affect the declarations and procedures of the digital certification service, in each notification the text of the sections that suffered changes will be specified. No notification is made when the changes are not relevant such as typographical errors, URL, contact information and updated references.

9.12. CPS and CP change procedure

9.12.1. Change procedure

The procedure for changing the Certification Practices Statement and the Certification Policies is as follows:

- The Policy and Security Committee makes changes to the CPD and CP as it deems appropriate.
- The updated CPD and CP is published on the ANDES SCD website once the changes are approved by the committee

Note: ANDES SCD's web page maintains a history of versions of the CPD and final entity CP from the version in force on March 23, 2011, date on which the Superintendence of Industry and Commerce authorized ANDES SCD to operate as a Certification Entity through resolution 14349.

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Users of the certificates are informed of the corresponding changes to the CPD or CP if the changes could affect the acceptability of the certificates.

9.12.2. Notification mechanism and reporting period

In the event that the ANDES SCD Policy and Security Committee considers that changes to the CPD or CP may affect the acceptability of certificates for specific purposes, users of certificates corresponding to the modified CP or CPD are informed that a change has been made and that they should consult the new CPD available on the web page.

9.12.3. Circumstances under which the OID must be changed

In the event that changes to the CPD and CP may affect the acceptability of the certificates for specific purposes, the document version will be upgraded. This type of modifications will be communicated to the users of the certificates corresponding to the CP or CPD and will be published on the Andes SCD web page.

9.13. Dispute Prevention and Resolution

ANDES SCD has a procedure for the treatment of any request, complaint, claim, and suggestion in relation to the provision of digital certification service or in matters of personal data protection and fairness. This procedure applies to all processes responsible for the provision of services Andes SCD S.A., know our PQRS procedure on our website <https://www.andesscd.com.co/>.

9.14. Applicable Law

The operation and operations performed by the ANDES SCD Certification Authority, as well as this Certification Practices Statement and the Certification Policies applicable to each type of certificate are subject to the applicable regulations and in particular to:

- a) Law 527 of 1999, which defines and regulates the access and use of data messages, electronic commerce and digital signatures, and establishes the certification entities and other provisions.
- b) Decree 333 of 2014, which regulates Article 160 of Decree-Law 19 of 2012 with respect to the characteristics and requirements of certification entities, and the related with digital certificates.


	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.15. Compliance with applicable law


ANDES SCD declares compliance with Law 527 of 1999 and that the Certification Practices Statement is satisfactory in accordance with the requirements established by the National Accreditation Agency Colombia

10. Change Control

Version	Date	Detail	Responsible
1.3	24/02/2011	Initial version authorized by the SIC according to resolution 14349 of March 2011.	Policy and Security Committee
1.4	02/11/2011	<p>Introduction: Introduction is modified to include SIC- Authorization Resolution.</p> <p>1.1 - Updated OID, CPD version, issue date and publication address of CPD V 1.4.</p> <p>1.4 - Definition of PKCS#12 is included.</p> <p>1.6.1 - CA Class II certificate data is updated.</p> <p>1.8.2 - Incorporation of the certificate type Public Function and Legal Entity in the Andes SCD service catalog.</p> <p>1.9 - Andes SCD's physical address and telephone number are updated.</p> <p>2.1.2 - The CRLs that are published in the CRL history are indicated and the time of publication is determined.</p> <p>3.2 - The method to prove the possession of the private key when the certificate is delivered in PKCS12 file is included and the way to authenticate the identity of Applicants and Subscribers of certificates in PKCS12 file is indicated.</p> <p>4.4.7 - Issuance period of Class I and Class II CRLs is updated</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
2.0	09/10/2014	<p>1.6.2 - Updated the registration authority section regarding communication with Andes SCD.</p> <p>1.6.3 - Class I certificate subscribers table is updated.</p> <p>1.8.2 - Updated OID of current certificate policies</p> <p>1.9 - Updated contact information and organization that administers the document.</p> <p>3.2 - Identity Approval section updated</p> <p>4.4.1 - Updated revocation grounds sections</p> <p>4.4.2 - Reference is made to an additional document describing the procedure for requesting the issuance of a certificate.</p> <p>5 - The term Telmex is changed to Triara.</p> <p>5.2.1 - The RA representative and RA administrator trust role is eliminated.</p> <p>5.5.4 - Information backup procedure is modified.</p> <p>6.1.7 - The size of class I certificate keys - Internal use is 2048 bits.</p> <p>9.2 - Liability policy information is updated</p> <p>All the document - The term private key and public key is changed to private key and public key.</p>	Policy and Security Committee
2.1	24/11/2015	<p>1.1 - Updated CPD document version and issue date</p> <p>1.4 - Reference to Class III CA in the definition of trust hierarchy</p> <p>1.6 - Class III CA information is included.</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
		1.8 - Updated the OID of current certificate policies 1.9 - Updated contact information and organization managing the document. 2.0 - Included information on means of publishing certificates and CRLs for Class III hierarchy. 3.2.1, 3.2.2, 6.1.2, 6.1.3 and 9.6.1d - Referenced OID document describing procedures in conventions. 4.4.6 , 9.4.3 and 9.6 j - Reference to CRL for Class III hierarchy. 4.4.7 - Include periodicity of publication of CRLs for Class III hierarchy. 6.1.1 - CA Class III hierarchy information and CA Class III key generation OIDs are included. 6.1.5 - Reference to public key for Class III CA hierarchy 6.1.6 - CA private key usage period is included.	
2.2	26/09/2016	1.1 - DPC document version and date of issuance are updated. 1.2 - Digital Certification Entity Identification is added. 1.10.2 - Updated contact person's email address 1.7.1 - Root CA and Sub CA data updated due to change of signature algorithm from sha1 to sha256 .1 and 2.3 - It is specified that certificates that have not been revoked are published in the certificates directory.2.2 and 4.4.7 -	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>Reference to CRL history is eliminated.</p> <p>3.2.1, 6.1.1, 6.1.2 and 6.1.3 - Change in the procedure to manage keys according to the certificate delivery method chosen by the client. New PKCS10 Token procedure is described.</p> <p>4.4.4 - The procedure for face-to-face revocation is updated.</p> <p>4.4.7 - A note is included indicating that the ROOT CA CRL will not be published periodically because the CA remains Offline.</p> <p>4.6 - Certificate replacement is included.</p> <p>5.2.1 - Trusted Roles Update</p> <p>5.4.1 - Updated the severity types of the syslog audited events.</p> <p>5.8 - CA or RA termination section is supplemented.</p> <p>7.1.1 - RFC 3280 updated to 5280</p> <p>7.1.3 - Updated reference to the sha1 signature algorithm OID to sha256 signature algorithm OID.</p> <p>Introduction: Reference to the Colombian territory is made.</p>	
2.3	06/01/2017	<p>The introduction of the document is updated to include a reference to the ONAC accreditation certificate.</p> <p>1.5 Reference to the term PKCS12 is eliminated.</p> <p>1.7. Reference is made to document agreements for CAs with third level hierarchy.</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>2.2 Updated URL for publication of CA and CRL certificates.</p> <p>3.2.1 Include procedure for certificates with PKCS10 delivery form and remove PKCS12 delivery form.</p> <p>3.2.4 Reference is made to compliance with CEA-4 1-10 as an interoperability requirement.</p> <p>4.4.3 revocation telephone and face-to-face service hours.</p> <p>4.4.4 Reference is made to the procedure for revocation of agreement certificates.</p> <p>4.4.6, 4.4.7, 6.1.1, 6.1.2 and 6.1.3 Reference to PKCS10 delivery method is included and PKCS12 delivery method is eliminated.</p> <p>6.1.5, 6.1.6 Generalized CA subordinate covenants</p> <p>6.2.7, 6.2.8 and 6.2.9, 6.4.2, 9.6.1 d) reference to PKCS12 is eliminated.</p> <p>7.1.8 Reference is made to document conventions for CRL CA profile with third level hierarchy.</p>	
2.4	14/02/2017	1.9.1 The OID of the Company and Natural Person Certificate Policy has been updated.	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>4.4.3. Included means for requesting certificate revocation: E-mail.</p> <p>4.4.4 Describes the procedure for requesting certificate revocation by e-mail and details the other revocation procedures.</p> <p>5 updated reference to the documents that make up the Security Policy</p>	
2.5	01/07/2017	<p>1.9.1 Certificate type Academic community removed Replaced "subscription contract" with "terms and conditions of service" throughout the document.</p> <p>9.5 Updated Intellectual Property Rights section.</p>	Policy and Security Committee
2.6	26/10/2017	<p>1.7.1 CA Class III certificate data updated</p> <p>1.8.3 General prohibitions section added.</p> <p>1.8.4 Included prohibitions of use that apply to all certificates issued by Andes SCD.</p> <p>1.9 PC legal person and company membership version is increased. 3.2.1, 6.1.1, 6.1.2, 6.2.4 and 6.2.5. mechanism 2 includes the Token delivery format.</p> <p>4.5.1 and 7.2 reference to RFC OCSP is made.</p> <p>9.6.4 Section K and I in subscriber obligations and warranties are included.</p> <p>9.7 Updated limitation of liability section.</p> <p>9.8 Personal data protection section was added..</p>	Policy and Security Committee
2.7	20/03/2018	<p>1.7.3 Legal entity certificates are referenced within the Class III agreements.</p> <p>1.9.1 The OID of the policies of each of the certificates is updated.</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
		<p>3.2.1 The two mechanisms for issuing certificates (when the private key is generated by the subscriber and when the private key is generated by ANDES SCD) are defined.</p> <p>3.2.3 Reference is made to the registration authority as responsible for verifying the applicant's information.</p> <p>5. Information Asset Management Methodology is replaced by Technological Asset Inventory Management Procedure and its OID is updated.</p> <p>5.1 Reference to the conditions required of critical suppliers is included.</p> <p>5.3.1 HSM Administrator profile is modified, describing his/her functions.</p> <p>5.3.4 The section on segregation of duties is updated.</p> <p>5.4.3 Reference is made to the training of the people involved in the certificate life cycle.</p> <p>5.4.4 Training frequency is adjusted to refer to personnel involved in the certificate lifecycle.</p> <p>5.6.2 Reference is made to RFC 4523 related to LDAP.</p> <p>7.1.8.2 Updated signature algorithm in the Root and Class II CRL.</p> <p>9.1.1 PC service rates are referenced.</p> <p>9.2.2 Liability Policy value updated</p> <p>9.4.6 Reference is made to access to information from judicial or</p>	

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
		administrative process.	
2.8	22/06/2018	1.9.1 The type of certificate for the academic community and electronic invoice issuer is included in the certification services catalog. 1.9.1 Increased version of PC Legal person	Policy and Security Committee
2.9	16/07/2018	1.7.1 Updated renewed certificate data for Class II CA. 1.9.1 Updated version of all PCs.	Policy and Security Committee
3.0	14/09/2018	1.1 Date of issue and DPC download url are updated. 1.10.2 Name and email of general manager updated. 1.9.1 Updated version of all PCs.	Policy and Security Committee
3.1	15/08/2019	1.1 1.1 Issuance date and DPC download url have been updated: 1.2 Updated phone and deleted fax line. 1.7.1 Updated Andes SCD Class II V2 CA data. 1.10.1 Upgraded the phone 1.10.2 Updated the telephone 2.2 Included URL for downloading CA ANDES SCD Class II V2 certificate, URL for downloading CA ANDES SCD Class II V2 CRL and in OCSP table included CERTIFICATES Class II v2 - Final Entity. 4.1.2 OID number of the procedure to request certificate issuance was corrected. 4.4.7 The CRL of CA ANDES SCD S.A. Class II and the CRL of CA ANDES SCD S.A. Class III agreements were updated to 24 hours, and the	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>CRL of CA ANDES SCD S.A. Class II v2 was included with a 24-hour publication periodicity.</p> <p>5.7 The Change of password section was updated.</p> <p>5.8.4 Mention was made of the Alternate Datacenter.</p> <p>6.1.6 The period of use of the CA Class II V2 private key was included.</p> <p>6.2.4 Updated the Private Key Storage procedure.</p> <p>7.1.8.2 Included CA Class II v2 CRL data.</p>	
3.2	25/11/2019	<p>.2, 1.10.1, 1.10.2, ECD address updated</p> <p>1.9.1 OID codes for the respective PC's are updated.</p> <p>2.2 Added URLs for downloading class III certificate and class III CRL.</p> <p>4.4.4 Deletion of reference to the agreement procedure</p> <p>6.7 Added sites covered in the scope of accreditation (NOC/SOC) Deletion of document referenced to certificate issuance procedure.</p> <p>9.1.4 Reimbursement policy is updated</p> <p>9.13 Modified procedure for Dispute Prevention and Resolution</p>	Policy and Security Committee
3.3.	07/05/2020	<p>Update of numeral 9.1.4 Reimbursement Policy and inclusion of numeral 9.1.5 of reimbursement request inappropriateness.</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
3.4.	04/11/2020	<p>Update of the following items:</p> <p>Procedure for requesting certificate issuance (4.1.2): Specification of the procedure.</p> <p>Trust roles (5.3.1): Updating of positions</p> <p>Procedures to manage incidents (5.8.1): Procedure detail.</p> <p>Business continuity capabilities in the event of a disaster (5.8.4): Update of alternate data center address and SOC and NOC infrastructure.</p> <p>Mechanism 2 - The key pair is generated by Andes SCD (6.1.2, 6.1.3).</p> <p>Network Security Controls (6.7)</p>	Policy and Security Committee
3.5	01/02/2021	<p>Update of ETSI TS 101 456 and ETSI TS 102 042 by ETSI EN 319 411-2 and ETSI EN 319 411-1, respectively.</p> <p>Updated RFC 2459 to RFC 5280.</p> <p>Change of private key storage assignment from "Operations Manager" to "PKI Auditor".</p> <p>Update of the value of the liability policy.</p> <p>Updated the OID of the current certificate policies.</p>	Policy and Security Committee
3.6	28/04/2021	<p>-The information of Data Center Triara and Century Link is included in sections 1.3 and 1.4, respectively.</p> <p>- Section 1.6 is added. Provisions for activities and services accredited by Andes SCD.</p> <p>- The name of the alternate Lumen Datacenter is updated to Centurylink in section 5.8.4.</p>	Policy and Security Committee / Analyst Senior SGI

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager


Version	Date	Detail	Responsible
		<p>-Paragraph two is added to the conditions required of critical suppliers in section 5.1.</p> <p>- The organizational obligations t and u of Andes SCD are added in section 9.6.1</p>	
4.0	15/06/2022	<p>In section 1.1 the data is updated with the new version of the document.</p> <p>Section 1.5 clarifies that the CPD and CP are aligned with the provisions of RAC-3.0-01 and RAC-3.0-03.</p> <p>Section 1.10.5.1. Precautions to be observed by third parties is included.</p> <p>Section 1.11.5 Minutes and Contracts is included.</p> <p>Section 2.2 includes the publication media CA ANDES SCD Class III SYC v2 & CA ANDES SCD Class III ESP v2.</p> <p>In numeral 4.1 the definition "issuance" is updated to "request".</p> <p>Include in numeral 4.2 "Processing of certificate requests".</p> <p>Section 4.3 "Issuance of Certificates" is included.</p> <p>Inclusion of section 4.6 "Suspension of the Certificate".</p> <p>Updated in numeral 4.5.2 the availability of the service in accordance with the new CEA.</p> <p>The following functions are included in numeral 5.3.1. Prepare and maintain the contingency</p>	Policy and Security Committee / Analist Senior SGI

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>and disaster recovery plan in case of an emergency.</p> <ul style="list-style-type: none"> - Lead the periodic tests on the contingency and disaster recovery plan to the Information Security Officer. <p>The authorization for personnel performing AR activities is added to section 5.4.2.</p> <p>The period for the safekeeping of records is updated to 4 years in section 5.5.3.</p> <p>Section 6.8 Time Stamps is included.</p> <p>In numeral 9.14, Decree 1747 of 2000 is updated by Decree 333 of 2014.</p>	
5.0	12/10/2022	<ul style="list-style-type: none"> - The certificate data of the CA CLASS I validity period is updated. - In the section certificates for final entity, the OID identifier is updated for all types of certificates. - ANDES SCD legal representative data is updated. - The uses of the key pair are included in numeral 4.1.5.1. - In numeral 4.7, the definition of circumstances for grounds for revocation is updated, a table is included describing the circumstances required by CEA associated to the grounds defined in the web page, the events are eliminated. 	Policy and Security Committee / Operational Director / Analyst Senior SGI

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<ul style="list-style-type: none"> - The description of numeral 4.7.2 is updated detailing the process for certificate revocation. - The telephone is eliminated as a means of revocation. - The RFC technical standard required for the OCSP Profile in numeral 7.2 is updated. The definition of section 9.6 Duties and Responsibilities is updated to DUTES AND RIGHTS, and the duties of Andes SCD, rights of Andes SCD, duties of the applicant, rights of the applicants, duties of the subscribers, rights of the subscribers are delimited separately. 	
6.0	05/12/2022	<ul style="list-style-type: none"> - DPC OIDs are updated - Section 1.12.1 OID of each certificate is updated. - Section 9.6.4 includes subscriber's duties for legal entity and electronic invoicing certificates. - Limit of use of certificates in operating systems is included. - The link to the personal data treatment policy has been updated. 	Policy and Security Committee / Analyst Senior SGI
7	14/04/2023	<ul style="list-style-type: none"> - OID and CPD version updated - Updated the position of "Operations Manager" to "Director of Operations" - In numeral 1.3, the address of the main data center is included - address of the main data ce 	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<ul style="list-style-type: none"> - - In numeral 1.4, the address of the alternate data center is included. - of the alternate data center. - - In the limit of use of certificates in operating systems for virtual token specifications are included for the - Windows operating system - - In the end-entity certificates section, the OID for all - the OID is updated for all certificate types. - certificate types. 	
8.0	16/11/2023	<ul style="list-style-type: none"> - DPC OID and version updated - Updated phone number of - ANDES SCD PHONE NUMBER IS UPDATED. - Position name updated from - "CA Operator" to "Issuing Agent". - Revocation grounds are updated according to what is indicated in the CEA <p>Section 10.11.5.1</p> <p>The term "declination of the application" is included request</p> <ul style="list-style-type: none"> - The title of numeral 5.8 has been modified to Cessation of activities of the ECD, it is included information in accordance with section 10.7.4. 10.7.4. of the CEA. - In the rights and duties of ANDES, the Superintendence of Industry and <p>The Superintendence of Industry and Commerce is eliminated from the rights and</p>	Policy and Security Committee

	CERTIFICATION PRACTICES STATEMENT	OID:	1.3.6.1.4.1.31304.1.1.1.8.0
		effective date:	16/11/2023
		Version:	8.0
		Classify of the	Public
		Elaborated:	Director of Operations
		Revised:	Policy and Security Committee
		Approved:	General Manager

Version	Date	Detail	Responsible
		<p>commerce is eliminated from the rights and duties of ANDES.</p> <ul style="list-style-type: none"> - In item 9.4.6 Access to information based on judicial or administrative from a judicial or administrative process the following means of notification is included "electronic mail" is included. - The following items have been updated: PKI participants, means of publication PKI participants, publication means, revocation lists revocation lists, publication of revoked certificates revoked certificates, CRLs and extensions with the new new SubCA. 	

SANDRA CECILIA RESTREPO MARTINEZ
General Manager