CERTIFICATION POLICY ELECTRONIC BILLING

Andes SCD S.A.

2022

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Table of contents

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Introduction

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

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

1. Presentation of the document
1.1. Name and identification of the document

Documento	CERTIFICATION POLICY ELECTRONIC BILLING
Descripción	The company membership certificate certifies the identity of the subscriber and his or her membership, function or employment status in a legal entity or person, and allows the subscriber to sign documents digitally in the capacity that his or her certificate certifies.
Identificador OID	1.3.6.1.4.1.31304.1.2.5.4.0
Versión	V 4.0
Fecha de emisión	December 5, 2022
Ubicación	https://www.andesscd.com.co/docs/cp_electronicbilling.pdf

1.2. References

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

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

1.3. Policy administration

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

1.3.1. Organization that manages the document

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

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Telephone   : PBX 601 745 6884

1.3.2. Contact Person

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

1.3.3. Policy Approval Procedures

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

1.3.4. Publication of the document

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

1.4. User Community and Applicability

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

Certification Autority (CA)

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

Registration authority (RA)

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

Subscribers

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

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

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

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

1.5. Scope of application
1.5.1. Uses of the certificate
The Electronic Billing issued under this policy may be used for the following purposes:

Identity authentication
The certificate can be used to identify a natural person as a member of an entity or legal person in the scope of its activity..

Digital signature
The digital signatures made with Electronic billing Certificates offer the means of support by guaranteeing the authenticity of the origin, the integrity of the signed data and the non-repudiation

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

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

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.5.2. Limits on the use of certificates

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

1.5.2.1. Limits on the use of certificates in operating systems

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

- Virtual Token:

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

- Physical Token:

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

1.5.3. Prohibitions on the use of certificates

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

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.5.4. Minutes and contracts

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

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

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

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

2. Publication and registration of certificates

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

3. Identificación y autenticación

The following describes the procedures and criteria applied to verify the identity of the applicant and approve the issuance of a certificate of membership in a company..

3.1. Names

3.1.1. Types of names

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

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Abrev	Name	Description
CN	Name	Subscriber's full names and surnames
S	Serial	Subscriber identification number
E	Email	Subscriber's position email address
C	Country	Abbreviation for the country where the entity is located
ST	Department	Name of the department where the entity is located
L	City	Name of the municipality where the entity is located
STREET	Address	Address where the entity is located
T	Title	Subscriber's position in the entity
1.3.6.1.4.1.4710.1.3.2		Document number + entity dv
O	Organization	Corporate name of the entity or legal person
OU	Organizational Unit	Organizational unit of the entity to which the subscriber belongs. E.g. Operational, Financial, Administrative, etc.
OU	Organizational Unit	Andes SCD Issued by Andes SCD Calle 26 #69c-03 Torre B office 701.

3.1.2. The need for names to be meaningful

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

3.1.3. Anonyms and pseudonyms in names

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

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

3.1.4. Rules for interpreting name formats

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

3.1.5. Singularity of names

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

3.2. Identity Approval

3.2.1. Method for proving possession of the private key

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

3.2.2. Authentication of the applicant's identity

The applicant can process his request for the issuance of a company membership certificate in one of the following ways:

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

Requirement	In-person application	Remote request or agreement
Citizenship card or document that proves the identity (Enlarged to 150% and legible)	Present original and photocopy of document	Scanned document required
RUT or equivalent document proving identification of the entity (Complete and legible document, it is optional if you present a chamber of commerce - Date of issue less than 90 days)	Present original and photocopy of document	Digital PDF document required
Documents proving the person's affiliation with the entity (legible document with the requirements of the following table).	Submit Photocopy Document	Digital PDF document required
Identity Validation (successfully complete the enrollment and authentication process) or **Notarized request for signature certificate Digital (**Authenticated document (personal presentation before a notary) requesting the issuance of the certificate of belonging to the company and	Identity validation result greater than 70% is required, or digital document in PDF	Identity validation result greater than 70% is required, or digital document in PDF

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
andes Servicio de Certificación Digital	**CERTIFICATION POLICY ELECTRONIC BILLING**	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

informing: full name, address - city of residence, telephone and personal e-mail - date of issue less than 90 days)		

3.2.2.1. Information required in the document proving the applicant's relationship with an entity.

Requirement	Observation
Documento con membrete	Header and/or footer with name of entity, corporate image, address, contact telephone number
Date not exceeding 90 days	The date of issuance of the document must not exceed 90 calendar days
Proof of identity of the person belonging to the entity	Must include full name, type and number of identification and explicitly state the position held by the person in the entity..
Full name, area and signature of the person issuing the document	It must include the full name, area to which it belongs and digital or handwritten signature of the person authorizing the issuance of the certificate by the company.
E-mail address	You must include the email address of the person issuing the certification in order to confirm the certification.

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

In the case of applications processed by agreement, other documents or digital evidence may be accepted to verify the identity of the persons and their relationship with the entity or company..

In the case of persons linked to companies by service contracts or through temporary intermediary companies, the following rules apply for the document evidencing the position:
   a. Those who are linked to a company as contractors under a contract for the provision of professional services must provide a certificate to that effect issued by the organization to which they belong, indicating the position and its main function, requesting the issuance of the respective certificate for the contractor concerned.
   b. On the other hand, for those who are linked to the organization through a temporary company, they must provide a letter prepared and signed by the Temporary Services Company, indicating that the worker has been assigned, on assignment or as a temporary worker, to the company listed in the certificate to be issued, as well as the position he/she occupies..

It will be the responsibility of the organizations related to the issued certificate of belonging to a company, to sensitize contractors and workers on mission, on the use of the digital certificate, indicating the existing limits in the use of the same, and the consequences at legal and administrative level of stamping the digital

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

signature on documents that have no relation to the organization or the exercise of the functions assigned to their position..

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

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

The information provided in the request for the issuance of a company membership certificate is studied by the supervisor who is in charge of verifying that the information is original, sufficient and adequate in accordance with the internal procedures defined by Andes SCD..

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

3.2.3. Unverified Applicant Information

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

3.2.4. Response Times

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

When the delivery format is a physical token, the delivery time of the digital certificate after issuance depends on the destination, for major cities the delivery time will be 1 to 2 business days, for other national destinations

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
andes Servicio de Certificación Digital	**CERTIFICATION POLICY** **ELECTRONIC BILLING**	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

the delivery time will be 2 to 3 business days, for special destinations or if it is impossible to contact the subscriber the delivery time may take up to 5 business days

3.2.5.Identification and authentication for revocation requests

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

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

- To the authorized representative of the entity to which the subscriber is linked, in which case the subscriber must formally notify Andes SCD in writing the reason for requesting the revocation of the Certificate of Company Membership issued to the subscriber.

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

4. Certificate life cycle and operating procedures

Electronic Billing certificates issued by Andes SCD have an explicit validity period in the "valid from" and "valid until" attributes of the certificate itself. The period of validity of the certificate may not exceed 730 calendar days. At the end of the validity period, the certificate becomes invalid and permanently ceases to operate and the certification service between Andes SCD and the subscriber is terminated..

4.1. Request for certificates

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

4.1.1.Who can apply for the issuance of a certificate

The application for a digital certificate can be made by any person of legal age who can prove to be linked to an entity or legal person, who is authorized to act on behalf of the company according to the position he/she represents and who is in full capacity to assume the obligations and responsibilities inherent to the possession and use of the certificate.

4.1.2. Procedure for requesting a certificate

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

4.1.3 Acceptance of the certificate.

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

4.1.4. Publication of the certificate by Andes SCD

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.1.5. Key pair and use of the certificate

4.1.5.1. On the part of the subscriber

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

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

Once the certificate has expired or is revoked, the subscriber is obliged not to use the private key again
The subscriber can only use the private key and the certificate for the authorized uses on the PC and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate.

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

- Digital signature
- Certificate signature
- CRL signatura

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

- Digital signature
- Certificate signature
- CRL signatura

4.1.5.2. By relying users

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

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

4.2. Renewal of Certificates - Key Pair

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

4.2.1 Renewal of certificate keys

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

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

4.3. Modification of certificates

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

4.4 Suspension of Certificates

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

4.5 Revocation of certificates

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

ANDES SCD, publishes the CRL every 24 hours, the last CRL issued for each CA contains all the certificates issued by the respective CA that are revoked as of the CRL generation date. The user is recommended to check the date of the CRL to verify that it is the most recently issued CRL.
Certificates that are revoked will not be able to return to active status under any circumstances, as this is a definitive action.

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

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

4.6. Replacement of certificates

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

- Loss of Token device
- Loss or exposure of certificate PIN
- Change of certificate holder's information, except for the identification number

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

The procedure to request the replacement of a certificate consists of the following procedures.
- Certificate revocation.
- Certificate issuance request.

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

4.7. Certificate status services

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

4.8. Validity of certificates

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

5. Security controls

The systems and equipment used by ANDES SCD to offer the certification service are physically located in a Data Center designed with specifications with the strictest construction standards and following rigorous operating standards to ensure that the equipment and information housed therein have the highest level of security and availability. In the event of an incident with its main Data Center, ANDES SCD has an alternate data center with optimal security mechanisms to ensure continuity in the provision of services.

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
andes Servicio de Certificación Digital	**CERTIFICATION POLICY ELECTRONIC BILLING**	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

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

6. Technical safety controls
6.1. Key generation and installation
6.1.1. Key Pair Generation

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

6.1.2. Delivery of the private key to the subscriber

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

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

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

6.1.3. Delivery of the public key to the certificate issuer

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

6.1.4. Subscriber Public Key Distribution

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

6.1.5. Distribution of the Andes SCD Public Key to Users

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

6.1.6. Period of use of the private key

The period of use of the private key is the same as the period of validity of the Electronic Billing certificate or less if the certificate is revoked before expiration.

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
andes Servicio de Certificación Digital	CERTIFICATION POLICY ELECTRONIC BILLING	Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

The Andes SCD CPS details the period of use of the private key of the root CA and the subordinate CAs issuing end-entity certificates

6.1.7. Size of keys

The minimum size of keys for Enterprise Membership certificates is 2048 bits based on the RSA algorithm. The size of the certified keys of the issuing CA of the Enterprise Membership certificates is 4096 bits long based on the RSA algorithm.

6.2. Private Key Protection Controls

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

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

Protection control	Private key generated by subscriber from TOKEN and CSR device
Private key backup	Andes SCD does not back up subscribers' private keys generated from TOKEN device or when the certificate is generated from CSR. Andes SCD is never in possession of these keys and they only remain under the subscriber's custody.
Private key storage	Subscribers' private keys generated from TOKEN device are NEVER stored by Andes SCD. The same happens when the certificate is generated from CSR delivered by the subscriber. The private key must be stored by the subscriber himself by keeping the TOKEN device or other methods, because they may be necessary to decrypt the historical information encrypted with the public key.
Private key transfer	The subscriber's private key generated from the TOKEN never leaves the device. The TOKEN device generates the key pair and protects its use through a PIN that only the subscriber knows. The private key generated by the user who delivers the CSR for certificate generation is kept by the subscriber and is never sent to Andes SCD..
Private 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 at the time of generating the key pair. The protection of the activation data is the responsibility of the subscriber
Deactivation of the private key	The method to disable the subscriber's private key is to remove the TOKEN device from the computer, immediately any associated content is disabled including the private key.
Private key destruction	The destruction of the private key can be performed by the subscriber using the functions provided by the TOKEN device, taking care not to affect other private keys stored in the device. Destruction of the subscriber's private key can be performed by the subscriber himself by deleting the private key corresponding to the CSR sent to Andes SCD..

6.3. Supported Cryptographic Devices

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
andes Servicio de Certificación Digital	**CERTIFICATION POLICY ELECTRONIC BILLING**	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

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

6.3.1. Associated risks

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

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

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

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

6.4. Other key pair management issues
6.4.1. Public Key File

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

6.4.2. Certificate operational periods and key pair usage periods

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

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

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

6.5. Activation data

6.5.1. Generation of Activation and Installation Data

The subscriber must generate the activation data for his TOKEN by changing the initial PIN that comes with the device by default.

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

6.5.2. Protection of activation data

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

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

6.6. Informatic security controls

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

6.7 CA and RA Termination

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

7. Certificate, CRL and OCSP Profiles

7.1. Contents of the certificate

Eletronic Billing Certificate Form		
Field	**Description**	**Value**
Version	Certificate version	V3
Serial number	Number identifying the certificate	Subscriber's certificate serial number
Signature algorithm	Algorithm used by Andes SCD to sign the certificate	SHA256WithRSA
Signature hash algorithm	Algorithm used to obtain the data summary	Sha256
(issuer)	Data of the end-entity subordinate CA that issued the certificate.	See in the certificate the data of the Class II CA or the Subordinate CA of the Class III CA.
Valid from	Date and time UTC start validity	Start date of validity of the certificate
Valid until	Date and time UTC end of validity	End date of certificate validity
Subject	CN	Subscriber's full name
	Serial Number	Subscriber identification document

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

	E	Subscriber's email address
	C	Abbreviation country where the entity is located
	ST	Name of the department where the entity is located
	L	Name of the municipality where the entity is located
	STREET	Address of the entity
	T	Subscriber's position in the entity
	1.3.6.1.4.1.4710.1.3.2	Identification document + DV of the entity.
	O	Company name of the entity
	OU	Organizational unit of the position in the entity
	OU	Andes SCD Issued by Andes SCD Calle 26 #69c-03 Torre B office 701.
Public key	Certificate holder's public key	RSA (2048 Bits)
Extensions	Extensions used in certificates	See "Certificate Extensions" section of this document for more details.
Identification algorithm	Algorithm used to obtain the fingerprint of the certificate	Sha1
Digital fingerprint	The synthesis or fingerprinting of the certificate data	Digital fingerprint
Use of the key	Purposes for which the certificate is to be used.	Digital Signature Non-repudiation Encryption of information

7.2. Certificate profiles

7.2.1. Version number

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

7.2.2. Certificate Extensions

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

Extensions Certificates Eletronic Billing according to standard X.509V3	
Name	Value
Access to the issuing entity's information	Access method = Online certificate status protocol URL address =http://ocsp.andesscd.com.co
Holder's key identifier	Holder's key identifier

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Issuing entity key identifier	Andes SCD CA key identifier that issued the certificate
CRL distribution points	CRL publishing URL of the CA that issued the certificate.
Use of the key	Digital Signature Non-repudiation Encryption of information
Improved use of the key	Customer authentication Secure Mail
Alternate Name of Holder	Subscriber's emai RFC 822 Name (e-mail address)
Basic Restrictions	Type of case = Final entity Route length restriction = None

Certificate Directive	[1] Certificate Directive:
	    Policy Identifier =1.3.6.1.4.1.31304.1.2.5.6.0
	    [1,1] Policy certifier information:
	        Id. of directive certifier =User notice
	        Certifier:
	          Warning text = The use of this certificate is subject to the Certificate of Membership Policies (PC) and Certification Practices (CPS) established by Andes SCD. [1,2] Policy certifier information:
	        Id. of directive certifier =CPS
	            Certifier:
	              Current CPS URL

7.2.3. Algorithm Object Identifiers

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

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

7.2.4. Name formats

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

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

7.2.5. Name restrictions

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

7.2.6. Identifying object of the certification policy

Certification policies and practices are identified by a unique number called an OID, the OID assigned to this policy is 1.3.6.1.4.1.31304.1.2.5.4.0.

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

7.2.7. Syntax and semantics of policy qualifiers

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

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

7.3. Profile CRL

7.3.1. Version number

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

7.3.2. CRLs and extensions

The CRL revocation list is issued according to RFC 2459

CRL profile according to standard X.509V2 – CRL Class II		
Name	**Description**	**Value**
Version	CRL version	V2
CRL Number	Unique nummber of CRL	Identified CRL
Issuer	Data of the end-entity subordinate CA that issued the CRL	View in the CRL the data of the CA that issued the CRL
Signature algorithm	Algorithm used for CRL signature	SHA256withRSA
Effective date of issue	Validity period after issuance of the CRL	Date of issuance of the CRL in CUT time

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

Next update	Date on which the next CRL will be issued	Date of issue of the next CRL in UTC time
Issue distribution points	URL where CRLs issued by Andes SCD are published.	View the publication URL in the CRL
Revoked certificates	List of revoked certificates specifying the serial number, date of revocation and reason for revocation	

7.4. Profile OCSP

7.4.1. Version Number

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

7.4.2. Extensiones OCSP

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

8. Audit and other valuations

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

9. Business and legal matters

9.1. Rates

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

One Year	Two Years
$ 250.000	$ 450.000

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

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
	CERTIFICATION POLICY ELECTRONIC BILLING	Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.2. Financial responsibility

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

9.3. Confidencialidad de la información

As stipulated in the Andes SCD Certification Practices Statement

9.4. Derechos de propiedad intelectual

As stipulated in the Andes SCD Certification Practices Statement

9.5. Rights and duties

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

9.5.1. Rights and duties of ANDES SCD.

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

9.5.2. Applicant's Rights and Duties

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

9.5.3. Subscriber Rights and Duties.

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

9.5.4. Subscriber Prohibitions:

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

1. Alter or modify, in whole or in part, the digital certificate or software delivered by ANDES SCD, or allow third parties do
2. Copy or reproduce in any form the digital certificate, or allow its copying or reproduction.
3. Reverse engineer, decode, disassemble or perform any action aimed at knowing or deciphering the source code, object code or other relevant information regarding the digital certificate or software related to the provision of the ANDES SCD service.
4. Transfer, assign or negotiate the rights granted by virtue of ANDES services.
5. Allow third parties to benefit from or use, directly or indirectly, the rights derived from the provision of digital certification services, under the conditions of this document.
6. Give the digital certificate a use other than that which is derived from the Declaration of Certification Practices.

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
	CERTIFICATION POLICY ELECTRONIC BILLING	Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

9.6. Principle of Impartiality

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

9.7. Limitations of liability

As stipulated in the Andes SCD Certification Practices Statement

9.8. Indemnifications

As stipulated in the Andes SCD Certification Practices Statement

9.9. Term and termination

As stipulated in the Andes SCD Certification Practices Statement

9.10. Specification change procedure

As stipulated in the Andes SCD Certification Practices Statement

9.11. Dispute prevention

As stipulated in the Andes SCD Certification Practices Statement

9.12. Applicable Law and Compliance with Applicable Law

As stipulated in the Andes SCD Certification Practices Statement

10. Change control

Version	Date	Detail	Reponsible
1.0	26/06/2018	Initial version of the Electronic Invoice Issuer Policy	Policy and Security Committee
1.1	16/07/2018	- 7.2.2 reference is made to current CPD URLs	Policy and Security Committee
1.2	14/09/2018	- - 1.3.1 Date of issue and PC download url are updated. - - 1.3.2 Name and email of the general manager are updated. - - 7.2.2 PC OID identifier is updated. - - 7.2.6 OID identifier is updated.	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

1.3	25/11/2019	- - 1.3.1, 1.3.2, 3.1.1 Updated ECD address and telephone number. - - 3.2.4 Response times are added. - - 4.4 Updated publication periods of the CRL - - 5. Added sites covered in the scope of accreditation (Noc, Triara, IFX) - - 9.1 Updated 2019 Fees - - References to agreement procedures in section 6 are eliminated.	Policy and Security Committee
1.4	27/07/2020	- - Adjustment in the documents requested to natural persons.	Policy and Security Committee
1.5	04/11/2020	- - Document Name and Identification (1.1): Update location and version - - Policy Approval Procedures (1.3.3): Update of reviewers and approvers (1.3.4): Update of policy approval procedures (1.3.4) - - Security Controls (5): Update of datacenter address and location of SOC and NOC monitoring infrastructure	Policy and Security Committee
1.6	01/02/2021	- - Update of ETSI TS 101 456 and ETSI TS 102 042 by ETSI EN 319 411-2 and ETSI EN 319 411-1, respectively. - - Update RFC 2459 to RFC 5280. - - Update of the tariffs. - - Update of the scope of the certificate in accordance with the DIAN resolution, specifically in section 1.5.2. - - Update of the OID of the PC.	Policy and Security Committee
1.7	28/04/2021	- - The column "Conventions request" is added to the table in section 3.2.2. Authentication of the applicant's identity, the date of issuance and the registration of face-to-face requests are added. - - The response times in section 3.2.4 are updated. - - The OID of the PC is updated. - - The name of the position of the Director of Projects and Operations is updated.	Policy and Security Committee

	CERTIFICATION POLICY ELECTRONIC BILLING	OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
		Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

2.0	15/06/2022	- - Item 1.1 Document name and identification is modified, OID Identifier, Version, Date of Issue and Location are updated. - - In item 3,2,5 "- To the authorized representative of the entity to which the subscriber is linked, in which case he/she must formally notify Andes SCD in writing the reason for requesting the revocation of the Legal Representative certificate issued to the subscriber" is added. - - Item 4.1.3, Acceptance of the certificate is included. - - Item 4.2.1. Certificate key renewal is included. - - Item 4.4. Suspension of certificates is included. - - Modify item 4.6. Replacement of certificates - - Item 6.7 Termination of CA and RA is included. - - Item 7.2.6. User Notice is modified.	Policy and Security Committee
3.0	12/10/2022	- - The IOD identifier, date of issue, version and date of the document are updated. - - The name of the legal representative and the contact email address have been updated in numeral 1.3.2. - - In numeral 4.1.3 the certificate acceptance section is included. - - In numeral 4.1.5 the use of certificates is included. - - Section 4.3 modification of certificates in accordance with the requirements of the CEA is amended. - - Section 4.4 certificate suspension as required by the CEA is modified. - - Section 5 security controls is updated. - - The title of item 9.5 is updated to rights and duties. - - The content of numeral 9.5 Rights and duties of Andes SCD is modified. - - The title and content of item 9.5.1 Rights and duties of Andes SCD is modified.	Policy and Security Committee

		OID:	1.3.6.1.4.1.31304.1.2.5.6.0
		Effective date:	05/12/2022
	CERTIFICATION POLICY ELECTRONIC BILLING	Version:	4.0
		Classify of the information:	Public
		Elaborated:	Operations Manager
		Revised:	Policy and Security Committee
		Approved:	General Manager

4.0	05/12/2022	- - The OID, Version and date of issue of the document are updated. - - Section 3.2.2.2. includes the types of mechanism with the description of validation of the applicant's identity (onboarding or notarized letter). - - RUT validity is modified to 90 days. - - Risks associated to certificates issued in software (PKSC10) are included.	Policy and Security Committee

SANDRA CECILIA RESTREPO MARTINEZ

General Manager