POLITICA DE CERTIFICACION

CERTIFICADO DIGITAL DE COMUNIDAD ACADEMICA



AUTORIDAD CERTIFICADORA ANDES SCD

Versión 1.1 **FEBRERO 2011**

Índice de contenido

Introducción 5
1. Presentación del documento 5
1.1. Nombre del documento e Identificación 5
1.2. Referencias 5
1.3. Administración de la política 5
1.3.1. Organización que administra el documento 5
1.3.2. Persona de contacto 6
1.3.3. Procedimientos de aprobación de la política 6
1.3.4. Publicación del documento 6
1.4. Comunidad de usuarios y aplicabilidad 6
1.5. Ámbito de aplicación 7
1.5.1. Usos del certificado 7
1.5.2. Límites de uso de los certificados 7
1.5.3. Prohibiciones de uso de los certificados 8
2. Publicación y registro de certificados 8
3. Identificación y autenticación 8
3.1. Nombres 8
3.1.1. Tipos de nombres 8
3.1.2. Necesidad para los nombres de ser significativos 9
3.1.3. Anónimos y pseudónimos en los nombres 9
3.1.4. Reglas para interpretar los formatos de nombre 9
3.1.5. Singularidad de los nombres 9
3.2. Aprobación de la identidad 9
3.2.1. Método para demostrar la posesión de la clave privada 9
3.2.2. Autenticación de la identidad del solicitante 9
3.2.3. Información no verificada sobre el solicitante 10
3.2.4. Identificación y autenticación para solicitar revocación 10
4. Ciclo de vida del certificado y procedimientos de operación 10
4.1. Emisión de certificados 10
4.1.1. Quien pueden solicitar la emisión de un certificado 10
4.1.2. Procedimiento para solicitar certificado 10
4.1.3. Publicación del certificado por Andes SCD 10

4.1.4. Par de claves y uso del certificado 11
4.1.4.1. Por parte del suscriptor 11
4.1.4.2. Por parte de usuarios que confían 11
4.2. Renovación de certificados 11
4.3. Modificación de certificados 11
4.4. Revocación de certificados 11
4.5. Servicios de estado de certificado 12
4.6. Vigencia de los certificados 12
5. Controles de seguridad 12
6. Controles de seguridad técnica 12
6.1. Generación de claves e instalación 12
6.1.1. Generación del par de claves 12
6.1.2. Entrega de la clave privada al suscriptor 13
6.1.3. Entrega de la clave pública al emisor del certificado 13
6.1.4. Distribución de la clave pública del suscriptor 13
6.1.5. Distribución de la clave pública de Andes SCD a los usuarios 13
6.1.6. Periodo de utilización de la clave privada 13
6.1.7. Tamaño de las claves 13
6.1.8. Generación de los parámetros de clave pública y comprobación de calidad 14
6.2. Controles de protección de la clave privada 14
6.3. Otros aspectos de administración del par de claves 14
6.3.1. Archivo de la clave pública 14
6.3.2. Periodos operacionales del certificado y periodos de uso del par de claves 15
6.4. Datos de activación 15
6.4.1. Generación de datos de activación e instalación 15
6.4.2. Protección de datos de activación 15
6.5. Controles de seguridad informática 15
7. Perfiles de certificado, CRL y OCSP 16
7.1.1. Contenido *del certificado* 16
7.2. Perfiles de certificado 17
7.2.1. Número de versión 17
7.2.2. Extensiones del certificado 17
7.2.3. Identificadores de objeto de los algoritmos 17
7.2.4. Formatos de nombres 17
7.2.5. Restricciones de nombre 17

7.2.6. Objeto identificador de la política de certificación 18
7.2.7. Sintaxis y semántica de los calificadores de la política 18
7.3. Perfil de la CRL 18
7.3.1. Numero de versión 18
7.3.2. CRL y extensiones 18
7.4. Perfil OCSP 18
7.4.1. Numero de versión 18
7.4.2. Extensiones OCSP 19
8. Auditoria y otras valoraciones 19
9. Negocio y materias legales 19
9.1. Tarifas 19
9.2. Responsabilidad financiera 19
9.3. Confidencialidad de la información 19
9.4. Derechos de propiedad intelectual 19
9.5. Obligaciones y garantías 19
9.6. Limitaciones de responsabilidad 19
9.7. Indemnizaciones 19
9.8. Término y terminación 19
9.9. Procedimiento de cambio en las especificaciones 19
9.10. Prevención de disputas 19
9.11. Ley aplicable y cumplimiento con la ley aplicable 19

Introducción

La presente Política de Certificación para Certificados de Comunidad Académica complementa las disposiciones establecidas en la Declaración de Prácticas de Certificación y concretamente declara el conjunto de reglas definidas por la Autoridad de Certificación Andes SCD para la aplicación de los certificados de Comunidad Académica, los usos que se le pueden dar a este tipo de certificado y los requerimientos técnicos, legales y de seguridad exigidos para la emisión y revocación de Certificados de Comunidad Académica.

Se recomienda leer este documento antes de solicitar un certificado de Comunidad Académica o hacer uso del mismo para comprobación de firmas electrónicas con el fin de conocer el ámbito de aplicación y los efectos legales asociados al uso de este tipo de certificado

1. Presentación del documento

1.1. Nombre del documento e Identificación

Nombre del documento	POLITICA DE CERTIFICACION COMUNIDAD ACADEMICA
Descripción	El certificado de Comunidad Académica acredita la identidad del suscriptor y su calidad como docente o estudiante miembro de una comunidad académica, y le permite al suscriptor firmar documentos digitalmente en su propio nombre e interés.
Identificador OID	1.3.6.1.4.1.31304.1.2.2.1.1
Versión	V 1.1
Fecha de emisión	Febrero 24 de 2011
Ubicación documento	http://www.andesscd.com.co/docs/PC1.1/pc_comunidadacademica_v1.1.pdf

1.2. Referencias

El desarrollo del contenido de las políticas de certificación y la declaración de prácticas de certificación se emite teniendo en cuenta las recomendaciones de la (Request for comments) **RFC 3647**: Internet X.509 Public Key Infraestructure: Certificate Policy and Certification Practices Framework y de los siguientes estándares europeos:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

1.3. Administración de la política

El contenido de esta Política de Certificación es administrado por el comité de Políticas y Seguridad encargado de su elaboración, registro, mantenimiento y actualización. A continuación se detallan los datos del comité de políticas y seguridad y de una persona de contacto disponibles para responder preguntas respecto a este documento.

1.3.1. Organización que administra el documento

Nombre : Comité de Políticas y Seguridad
Dirección : Calle 26A No 13-97 Oficina 703
Email : comite.politicas.seguridad@andesscd.com.co
Teléfono : PBX 571 4775701

1.3.2. Persona de contacto

Razón social : Andes Servicio de Certificación Digital S.A SIGLA ANDES SCD SA.
Nombre : Juan David Castillo García –Gerente General
Dirección : Calle 26A No 13-97 Oficina 703
Email : juandavid.castillo@andesscd.com.co
Teléfono : PBX 571 4775701

1.3.3. Procedimientos de aprobación de la política

La Política de Certificación de Comunidad Académica es administrada por el Comité de Políticas y Seguridad y es aprobada por la Dirección de Andes SCD, siguiendo el protocolo de Análisis y Aprobación de la Política identificado con el OID 1.3.6.1.4.1.31304.100.2.1.1.0.

1.3.4. Publicación del documento

Las Políticas de Certificación de Comunidad Académica y la Declaración de Prácticas de Certificación son documentos de uso público que se encuentran disponibles en la página web de Andes SCD. Cualquier modificación en estos documentos se publica de forma inmediata manteniendo un histórico de versiones.

1.4. Comunidad de usuarios y aplicabilidad

Los certificados de Comunidad Académica son emitidos a personas Físicas, acreditan la identidad del titular y su calidad como docente o estudiante miembro de una comunidad académica en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado de Comunidad Académica actúa en su propio nombre e interés.

Autoridad de certificación (CA)

La Autoridad de Certificación Andes SCD es la entidad que actúa como tercera parte de confianza entre el suscriptor y los usuarios en el medio electrónico y es responsable de emitir y gestionar los certificados digitales para Comunidad Académica conforme a la presente Política de Certificación. En la Declaración de Prácticas de Certificación se detalla la jerarquía de las Autoridades Certificadoras que conforman Andes SCD

Autoridad de registro (RA)

Las Autoridades de Registro son las entidades delegadas por la Autoridad de Certificación Andes SCD para gestionar las solicitudes, corroborar presencialmente la identidad de los solicitantes y realizar un registro completo de los solicitantes que deseen adquirir un certificado digital de Comunidad Académica conforme a la presente Política de Certificación.

Suscriptores

El suscriptor es aquella persona física que ha adquirido un certificado de Comunidad Académica emitido por la Autoridad de Certificación Andes SCD para obrar en el entorno electrónico en su propio nombre y se considera suscriptor mientras dicho certificado se encuentre vigente.

Solicitantes

El solicitante es aquella persona física que desea acceder a los servicios de certificación digital al adquirir un certificado de Comunidad Académica emitido por Andes SCD. Bajo

ninguna circunstancia se aceptan solicitudes de este tipo de certificados a nombre de personas que no demuestren estar vinculadas como estudiantes o docentes a una universidad.

Usuarios

El usuario es cualquier persona que voluntariamente deposita su confianza en los certificados de Comunidad Académica emitidos por la Autoridad Certificación Andes SCD y que utiliza el servicio de certificación como medio para acreditar la autenticidad e integridad de un documento firmado por un tercero.

1.5. Ámbito de aplicación

1.5.1. Usos del certificado

El certificado de Comunidad Académica emitido bajo esta política puede ser utilizado para los siguientes propósitos:

Autenticación de identidad

El certificado puede utilizarse para identificar a una persona física como estudiante o docente miembro de una Comunidad Académica en el ámbito de su actividad.

Firma digital

Las firmas digitales realizadas con certificados de Comunidad Académica ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

- Autenticidad del origen: En una comunicación electrónica el suscriptor puede acreditar válidamente su identidad y su condición como miembro de Comunidad Académica ante otra persona demostrando la posesión de la clave privada asociada con la respectiva clave pública contenida en el certificado

- Integridad del documento: La utilización del certificado garantiza que el documento es integro, es decir, existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor. Además certifica que el mensaje recibido por el usuario es el mismo emitido por el suscriptor.

- No repudio: Evita que el emisor del documento firmado pueda negar en un determinado momento la autoría o la integridad del documento, puesto que la firma a través del certificado digital puede demostrar la identidad del emisor sin que este pueda repudiarlo.

Cifrado de información

Es el proceso de transformar la información para hacerla incomprensible para todos excepto para el receptor a quien va dirigida

1.5.2. Límites de uso de los certificados

Los certificados de Comunidad Académica no pueden ser usados para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando otros certificados de clave pública de ningún tipo ni listas de certificados revocados (CRL). Tampoco pueden ser usados para fines contrarios a la legislación vigente.

1.5.3. Prohibiciones de uso de los certificados

La realización de operaciones no autorizadas según esta política de certificación, por parte de terceros o suscriptores del servicio eximirá a la Autoridad de Certificación Andes SCD de cualquier responsabilidad por este uso prohibido.

- No se permite el uso del certificado de Comunidad Académica para firmar otros certificados o listas de revocación (CRL)
- Está prohibido utilizar el certificado para usos distintos a los estipulados en el apartado "Usos permitidos del certificado" y "Limites de uso de los certificados" de la presente Política de Certificación.
- Las alteraciones sobre certificados no están permitidas y el certificado debe usarse tal y como fue suministrado por la Autoridad Certificadora Andes SCD.
- Se prohíbe el uso de certificados en sistemas de control o sistemas intolerantes a fallos que puedan ocasionar daños personales o medioambientales.
- Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificación.
- No es posible por parte de Andes SCD emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, por lo tanto la responsabilidad del contenido del mensaje es responsabilidad única del signatario.
- No es posible por parte de Andes SCD recuperar los datos cifrados en caso de pérdida de la clave privada del suscriptor porque la CA por seguridad nunca guarda copia de la clave privada de los suscriptores, por lo tanto es responsabilidad del suscriptor la utilización de cifrado de datos.

2. Publicación y registro de certificados

En la Declaración de Prácticas de Certificación (DPC) de Andes SCD se detalla información del directorio de certificados, los medios de publicación, la frecuencia de publicación y el control de acceso al directorio de certificados.

3. Identificación y autenticación

A continuación se describen los procedimientos y criterios aplicados por las Autoridades de Registro y Autoridad Certificadora Andes SCD en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado de Comunidad Académica.

3.1. Nombres

3.1.1. Tipos de nombres

Los certificados de Comunidad Académica tienen una sección denominada Asunto cuyo objetivo es permitir identificar al titular ó suscriptor del certificado, esta sección contiene un DN o distinguished name caracterizado por un conjunto de atributos que conforman un nombre inequívoco y único para cada suscriptor de los certificados emitidos por Andes SCD.

- **(CN)** - Nombre : Nombres y apellidos completos del suscriptor
- **(T) –** Title: "Miembro de Comunidad Académica" + Docente ó Estudiante
- **(S)** - Serial: Abreviatura país + tipo documento + numero documento de identificación.
- **(E)** - Email : Correo electrónico del suscriptor
- **(C)** - País: Abreviatura del país donde reside el suscriptor
- **(ST) -** Departamento: Nombre completo del departamento donde reside suscriptor

- **(L) -** Ciudad: Nombre completo del municipio donde reside el suscriptor
- **(STREET)** - Dirección: Dirección donde reside el suscriptor
- **(O) -** Organización: Universidad a la cual pertenece como docente o estudiante
- **(OU) -** Unidad Organizacional: Nombre de facultad y carrera a la que se encuentra vinculado
- **(OU)** – Unidad Organizacional: Emitido por Andes SCD Calle 26A No 13-97 Of 703

3.1.2. Necesidad para los nombres de ser significativos

Todo certificado de Comunidad Académica emitido por Andes SCD tiene como característica principal la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado.

3.1.3. Anónimos y pseudónimos en los nombres

En esta Política de Certificado no se admiten anónimos ni seudónimos para identificar el nombre de una Persona Natural.

En el caso de una persona natural con nacionalidad Colombiana el nombre debe estar conformado por nombres y apellidos tal como figura en la cedula de ciudadanía. Si la persona natural es un extranjero el nombre debe estar conformado por nombres y apellidos tal como figura en el pasaporte o documento equivalente.

3.1.4. Reglas para interpretar los formatos de nombre

Las reglas para interpretar los formatos de nombre siguen lo señalado por el estándar X.500 de referencia en ISO/IEC 9594.

3.1.5. Singularidad de los nombres

Se garantiza que los nombres distinguidos de los certificados de Comunidad Académica son únicos para cada suscriptor porque contienen atributos serial y email que permiten distinguir entre 2 identidades cuando existan problemas de duplicidad de nombres.

3.2. Aprobación de la identidad

3.2.1. Método para demostrar la posesión de la clave privada

En la Declaración de Prácticas de Certificación de Andes SCD se detalla el procedimiento que utiliza la Autoridad Certificadora para demostrar que el solicitante posee la clave privada correspondiente a la clave pública que se pretende vincular al certificado de Comunidad Académica.

3.2.2. Autenticación de la identidad del solicitante

Para emitir un certificado se exige la presentación personal del Miembro de la comunidad académica ante una Autoridad de Registro (RA), el solicitante debe aportar los siguientes documentos

- ✓ Original y copia de la cedula de ciudadanía o documento equivalente que acredite la identidad del solicitante.
- ✓ Certificado emitido por la universidad donde haga constar la calidad del solicitante como docente o estudiante durante el semestre en curso.

La Autoridad de Registro verifica si la información es original, suficiente y adecuada y procede a diligenciar el formulario de solicitud y a tomar la fotografía y huella dactilar del solicitante.

En caso de que el suscriptor reclame la modificación de los datos personales respecto a los contenidos en el documento de identificación presentado, deberá enseñar el correspondiente certificado de registro civil donde figura la variación.

3.2.3. Información no verificada sobre el solicitante

En el proceso de solicitud del certificado el solicitante debe suministrar diversos datos que lo identifican plenamente, toda la información solicitada es verificada por la Autoridad de Registro aún si no hace parte de la información incluida en el certificado digital.

3.2.4. Identificación y autenticación para solicitar revocación

Se permite solicitar la revocación de un certificado a las siguientes personas:

- Al propio suscriptor, en cuyo caso debe facilitar la clave de revocación que se le entrego en el momento de adquirir el certificado ó debe presentarse personalmente ante una Autoridad de Registro donde será identificado a partir de su huella dactilar.
- Los operadores autorizados de Andes SCD o de la jerarquía de certificación pueden revocar cualquier certificado en aquellos casos en que se incurra a las circunstancias establecidas en apartado 4.4.1 de la Declaración de Prácticas de Certificación.

4. Ciclo de vida del certificado y procedimientos de operación

Los certificados de Comunidad Académica emitidos por Andes SCD tienen un periodo de vigencia de 1 año, la fecha inicial y final de este periodo está indicada en el contrato y esta especificada en el propio certificado. Al finalizar el periodo de vigencia del certificado se produce la invalidez del certificado cesando permanentemente su operatividad y se da por terminada la prestación del servicio de certificación entre Andes SCD y el suscriptor.

4.1. Emisión de certificados

La Autoridad de Certificación Andes SCD se asegura de que los suscriptores han sido plenamente identificados y que la petición de certificado es completa.

4.1.1. Quien pueden solicitar la emisión de un certificado

La solicitud de un certificado digital puede realizarla cualquier persona que demuestre ser docente o estudiante de Universidad y que este en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado.

La solicitud del certificado debe hacerla personalmente ante una Autoridad de Registro el individuo que figurará como suscriptor ó titular en el certificado.

4.1.2. Procedimiento para solicitar certificado

El procedimiento que debe realizar el solicitante para adquirir un certificado digital se encuentra descrito en la Declaración de Prácticas de Certificación DPC. Ver sección 4.1.2 “Procedimiento para solicitar la emisión de certificado” en la DPC.

4.1.3. Publicación del certificado por Andes SCD

Una vez emitido el certificado por Andes SCD se procede a la publicación en el directorio de certificados.

4.1.4. Par de claves y uso del certificado

4.1.4.1. Por parte del suscriptor

El suscriptor posee una clave pública y una clave privada legalmente validas durante el periodo de vigencia del certificado digital de Comunidad Académica que las legitima. La clave privada es de uso exclusivo del suscriptor para los fines estipulados en esta Política de Certificación y debe ser protegida para impedir el uso no autorizado por parte de terceros.

El suscriptor solo puede usar el certificado y el par de claves tras aceptar las condiciones de uso establecidas en la DPC y en la presente PC y solo para lo que estas establezcan.

Una vez el certificado haya expirado o este revocado el suscriptor está en la obligación de no volver a usar la clave privada.

4.1.4.2. Por parte de usuarios que confían

Los usuarios que confían en el servicio de certificación de Andes SCD deben verificar los usos establecidos en el campo 'Key usage' del certificado ó en la presente Política de Certificación para conocer el ámbito de aplicación del certificado de Comunidad Académica.

Los usuarios que confían en el servicio de certificación de Andes SCD deben asumir la responsabilidad de verificar el estado del certificado antes de depositar su confianza.

4.2. Renovación de certificados

Andes SCD no tiene contemplado el proceso de renovación de certificados, si el suscriptor desea obtener un nuevo certificado debe solicitar la emisión de certificado cuando su certificado original haya caducado

4.3. Modificación de certificados

Los certificados digitales emitidos por Andes SCD no pueden ser modificados.

4.4. Revocación de certificados

La revocación consiste en la pérdida de fiabilidad del certificado y el cese permanente de su operatividad impidiendo el uso por parte del suscriptor; una vez revocado el certificado la Autoridad Certificadora lo incluye en la lista de revocación con el fin de notificar a terceros que un certificado ha sido revocado, en el momento en que se solicite la verificación del mismo.

Los certificados que sean revocados no podrán por ninguna circunstancia volver al estado activo, siendo esta una acción definitiva.

Puede solicitar la revocación de un certificado de Comunidad Académica el propio suscriptor titular del certificado a partir de los medios de revocación que ofrece Andes SCD en la sección 4.4.3 de la DPC y siguiendo el procedimiento de revocación especificado en la sección 4.4.4 de la DPC. Adicionalmente, Andes SCD o cualquiera de las autoridades que la componen puede solicitar la revocación de un certificado de Comunidad Académica si se tuviera

conocimiento o sospecha del compromiso de la clave privada del suscriptor o cualquier otro hecho determinante que requiera proceder a revocar el certificado

En la Declaración de Prácticas de Certificación de Andes SCD se detallan las circunstancias por las cuales se recurre a la revocación de un certificado digital, los medios disponibles para efectuar la revocación, el procedimiento para revocar un certificado, el tiempo que tarda Andes SCD en procesar la solicitud de revocación y en publicar los certificados revocados en la CRL.

4.5. Servicios de estado de certificado

En la Declaración de Prácticas de Certificación de Andes SCD se proporciona información sobre los medios para publicar el estado de los certificados emitidos, la disponibilidad del servicio y el fin de suscripción al servicio de certificación.

4.6. Vigencia de los certificados

Los certificados digitales de Comunidad Académica tienen un periodo de vigencia de 1 año.
El par de claves tiene un periodo de vigencia de 1 año.

5. Controles de seguridad

Los controles procedimentales, de seguridad física, de seguridad personal y de auditoría definidos para trabajar bajo un ambiente seguro y las capacidades de recuperación ante desastres establecidos para garantizar la operación de los servicios de certificación se encuentran especificados en la Declaración de Prácticas de Certificación de Andes SCD.

6. Controles de seguridad técnica

6.1. Generación de claves e instalación

6.1.1. Generación del par de claves

Las claves pública y privada de titulares de certificados de Comunidad Académica son generadas por el propio suscriptor de forma segura utilizando un dispositivo criptográfico TOKEN. Estos dispositivos criptográficos de custodia de la clave privada aportan un nivel de seguridad igual o superior a lo establecido para los dispositivos de creación de datos de firma. Las características de los TOKENS utilizados son las siguientes:

- Genera pares de claves RSA hasta de 2048 bits
- Algoritmos para la generación RSA, DES, 3DES, MD5 y SHA-1 implementados por hardware.
- Hardware generador de números aleatorios
- Hardware generador de firma digital
- Espacio disponible de 64 Kb
- Certificación CE y FCC
- Soporte completo para aplicaciones PKI
- Compatible con interfaces CAPI y PKCS#11
- Soporte para el almacenamiento de múltiples claves
- Soporte para X.509 V3 formato estándar de certificado
- Soporte para Microsoft® Windows®98(Second Edition), Windows®Me, Windows®2000, Windows®XP, Windows®2003, Windows®Vista, Linux MAC OS X.

El dispositivo criptográfico posee una clave de activación (PIN) para hacer uso de las claves privadas, esta clave de activación debe ser de uso exclusivo del suscriptor para

garantizar que los datos de creación de firma están protegidos contra la utilización de terceros.

6.1.2. Entrega de la clave privada al suscriptor

No procede para certificados de Comunidad Académica porque la clave privada en ningún momento es conocida por Andes SCD. Para este tipo de certificados la clave privada es generada por el propio solicitante usando un dispositivo TOKEN que almacena la clave privada y protege su uso mediante un PIN.

6.1.3. Entrega de la clave pública al emisor del certificado

En los certificados de Comunidad Académica, el par de claves es generado por el futuro suscriptor por lo tanto el suscriptor siempre está en posesión de su propia clave pública.

La entrega de la clave pública del suscriptor a Andes SCD se realiza en el momento de presentar la solicitud de certificado ante la Autoridad de Registro, allí el solicitante suministra los datos indispensables para generar el certificado, entre ellos su clave pública; esta información es procesada por la Autoridad de Registro y transmitida de forma segura a Andes SCD en el formato PKCS#10.

6.1.4. Distribución de la clave pública del suscriptor

La clave pública de cualquier suscriptor de Certificados de Comunidad Académica cuyo certificado fue emitido por Andes SCD está permanentemente disponible para descarga en el directorio de certificados de Andes SCD.

6.1.5. Distribución de la clave pública de Andes SCD a los usuarios

La clave pública de la CA Andes raíz y de la CA emisora de certificados Clase II ó de entidad final está permanentemente disponible para descarga en la página WEB de Andes SCD.

6.1.6. Periodo de utilización de la clave privada

El periodo de utilización de la clave privada es el mismo que el de la vigencia del certificado de Comunidad Académica.

El periodo de uso de la clave privada de entidades finales que estén acreditadas por un certificado digital de Comunidad Académica tiene periodo de vigencia de 1 año ó menos si el certificado es revocado antes de caducar.

En la Declaración de Practicas de Certificación de Andes SCD se detalla el periodo de utilización de la clave privada de la CA raíz y de la CA emisora de certificados de Clase II ó de Entidad Final.

6.1.7. Tamaño de las claves

El tamaño mínimo de las claves de certificados de Comunidad Académica es de 1024 bits basadas en el algoritmo RSA.
El tamaño de las claves certificadas de la CA Clase II emisora de los certificados de Comunidad Académica tiene una longitud de 4096 bits basadas en el algoritmo RSA.

6.1.8. Generación de los parámetros de clave pública y comprobación de calidad

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento ETSI SR 002 176 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”.

- Signature suite entry index: 001
- Signature algorithm: rsa
- Signature algorithm parameters: MinModLen=1020
- Key generation algorithm: rsagen1
- Padding method: emsa-pkcs1-v1_5
- Criptographic hash function: sha1
- Valid until (signing): 31.12.2005

6.2. Controles de protección de la clave privada

En la Declaración de Prácticas de Certificación de Andes SCD se especifican los controles y estándares de los módulos criptográficos, el control, backup, almacenamiento, activación, desactivación y destrucción de las claves privadas de la Autoridad de Certificación.

A continuación se especifican los controles de protección de la clave privada del suscriptor

- **Backup de la clave privada**: Andes SCD no realiza ningún tipo de backup sobre las claves privadas de los suscriptores porque nunca está en posesión de dichas claves y solo permanecen bajo custodia del propio suscriptor.
- **Almacenamiento de la clave privada**: Las claves privadas de los suscriptores NUNCA son almacenadas por Andes SCD, deben ser almacenadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación.
- **Transferencia de la clave privada**: La clave privada de los suscriptores nunca sale del TOKEN, este dispositivo se encarga de generar el par de claves y proteger su uso a través de un PIN que solo conoce el suscriptor.
- **Activación de la clave privada**: La activación del dispositivo TOKEN que contiene la clave privada del suscriptor se realiza a través de un PIN que debe ser personalizado por el propio suscriptor en el momento de generar el par de claves. La protección de los datos de activación es responsabilidad exclusiva del suscriptor.
- **Desactivación de la clave privada**: El método para desactivar la clave privada del suscriptor es retirar el dispositivo TOKEN del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.
- **Destrucción de clave privada:** La destrucción de la clave privada del suscriptor puede realizarla el propio suscriptor utilizando las funciones que provee el dispositivo TOKEN, teniendo en cuenta que si tiene más claves privadas dentro del dispositivo, estas no se vean afectadas.

6.3. Otros aspectos de administración del par de claves

6.3.1. Archivo de la clave pública

Andes SCD mantiene archivados todos los certificados digitales de Comunidad Académica, los cuales incluyen la clave pública durante el periodo estipulado en el apartado 6.3.1 de la DPC.

6.3.2. Periodos operacionales del certificado y periodos de uso del par de claves

El tiempo de vida del certificado de Comunidad Académica está regido por la validez del mismo o mientras no se manifieste de forma explícita su revocación en una CRL o en el sistemas de verificación en línea. Si alguno de estos eventos sucede se da por terminada la validez del certificado y este solo podrá usarse para fines de comprobación histórica.

El par de claves tiene vigencia mientras exista un certificado de Comunidad Académica válido que las sustente. Una vez el certificado deje de ser válido las claves pierden toda validez legal y su uso se limita a fines exclusivamente personales

6.4. Datos de activación

6.4.1. Generación de datos de activación e instalación

El suscriptor debe generar los datos de activación de su TOKEN cambiando el PIN inicial que trae por defecto el dispositivo, esto debe realizarlo por primera vez en la Autoridad de Registro usando el aplicativo software que suministra el fabricante del TOKEN. El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del TOKEN.

6.4.2. Protección de datos de activación

El PIN ó dato de activación del TOKEN debe ser personalizado por el solicitante antes de generar su par de claves.

El suscriptor debe proceder a cambiar el PIN de su TOKEN si existe la sospecha de que un tercero conoce este dato. Para cambiar el PIN es necesario descargar el aplicativo software que ofrece el fabricante del TOKEN y que se encuentra disponible en la página web de Andes SCD.

La protección de los datos de activación es responsabilidad exclusiva del suscriptor

6.5. Controles de seguridad informática

En la Declaración de Prácticas de Certificación se describen los controles de Andes SCD para lograr un adecuado resguardo de los recursos informáticos.

7. Perfiles de certificado, CRL y OCSP

7.1.1. Contenido *del certificado*

El contenido de los certificados de Comunidad Académica es el siguiente

Formato de certificados de Comunidad Académica		
Campo	**Descripción**	**Valor**
Versión	Versión del certificado	V3
Serial number	Número que identifica unívocamente al certificado dentro de los emitidos por Andes SCD	Número de serie del certificado del suscriptor
Algoritmo de firma	Algoritmo usado por Andes SCD para firmar el certificado	SHA1WithRSA
Emisor (issuer)	CN	CA ANDES SCD S.A. Clase II
	O	Andes SCD
	OU	Division de certificación entidad final
	C	CO
	L	Bogota, D.C.
	E	info@andesscd.com.co
Valido desde	Fecha y hora UTC desde que es válido el certificado	Fecha de inicio de la validez del certificado del suscriptor
Válido hasta	Fecha y hora UTC hasta la cual es válido el certificado	Fecha final de la validez del certificado del suscriptor
Asunto	CN	Nombre completo del suscriptor
	T	Miembro de comunidad Académica + Estudiante o Docente
	Serial Number	Abreviatura del país + tipo de documento+ número de documento del suscriptor
	E	Correo electrónico del suscriptor
	C	Abreviatura del país donde reside el suscriptor
	ST	Nombre completo del departamento donde reside el suscriptor
	L	Nombre completo del municipio donde reside el suscriptor
	STREET	Dirección donde reside el suscriptor
	O	Universidad a la cual pertenece el docente o estudiante
	OU	Nombre de facultad y carrera a la que se encuentra vinculado
	OU	Emitido por Andes SCD Calle 26A No 13-97 Of 703
Clave pública	Clave pública del titular del certificado	RSA (1024 Bits)
Extensiones	Extensiones utilizadas en los certificados de Comunidad académica.	Ver apartado 7.2.2 de este documento para más detalles.
Algoritmo de identificación	Algoritmo hash que genera una síntesis de datos ó huella digital para las firmas digitales	Sha1
Huella digital	La síntesis o huella digital de los datos del certificado	fingerprint
Uso de la clave	Propósitos para los cuales se debe utilizar el certificado.	Digital Signature Non-repudiation Key encipherment

7.2. Perfiles de certificado

7.2.1. Número de versión

Todos los certificados de Comunidad Académica emitidos por Andes SCD bajo esta política están de conformidad con el estándar X.509 V3 y de conformidad con el RFC 3280 para perfiles de certificados y CRL's.

7.2.2. Extensiones del certificado

Los certificados de Comunidad Académica emitidos por Andes SCD utilizan una serie de extensiones que pretenden establecer los usos del certificado, hacer referencia a las Políticas de Certificación aplicables y restricciones adicionales. A continuación se detallan las extensiones incluidas en los certificados digitales de Comunidad Académica.

Extensiones certificados Comunidad Académica según estándar X.509V3		
Nombre	**Descripción**	**Valor**
Basic Contraints, critical	Permite identificar entre un certificado de Autoridad certificadora y uno de suscriptor final	CA false
Key Usage, critical	Las claves y el certificado deben ser usados solo para los propósitos definidos en esta extensión.	Digital Signature Non-repudiation Key encipherment
Extended Key Usage	Esta extensión define unos usos adicionales del certificado. El certificado debe ser usado solo para los propósitos definidos en esta extensión	Client Authenticacion Email Protection
Subject Key Identifier	Identificador único de la clave pública de Andes SCD	identificador de clave
Authority Key Identifier	Medio para identificar la clave pública de Andes SCD. El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier.	a8 4b b4 f4 0b a7 b6 5b d4 a0 28 85 10 9d 04 13 33 c4 a7 f7
Subject Alternative Name	Permite definir términos que identifican al titular del certificado	Email del suscriptor RFC 822 Name (e-mail address)
CRL Distribution Points	Especifica la ubicación de la CRL para consultar los certificados revocados	http://www.andesscd.com.co/includes/getCert.php?crl=1
OCSP Service Locator	Ubicación del servicio de consulta OCSP	http://www.andesscd.com.co:8080/ejbca/publicweb/status/ocsp
Use Certificate Policies	Indica el identificador de las políticas de certificación aplicables	1.3.6.1.4.1.31304.1.2.2.1.1

7.2.3. Identificadores de objeto de los algoritmos

Los certificados digitales de Comunidad Académica emitidos bajo esta política utilizan los siguientes algoritmos y sus correspondientes identificadores (OIDs)

OID del algoritmo de firma SHA1withRSAEncryption 1.2.840.113549.1.1.5

OID del algoritmo de la clave pública RSAEncryption 1.2.840.113549.1.1.1

7.2.4. Formatos de nombres

Los certificados digitales de Comunidad Académica emitidos por Andes SCD están restringidos a 'Distinguished names' (DN) X.500 que son únicos y no ambiguos, los certificados contienen el DN del emisor y del suscriptor del certificado en los campos issuer name y subject name respectivamente.

7.2.5. Restricciones de nombre

Los certificados digitales emitidos bajo esta política cuentan con DN conforme a las recomendaciones X.500 que son únicos y no ambiguos.

7.2.6. Objeto identificador de la política de certificación

Las políticas y prácticas de certificación son identificadas mediante un número único denominado OID, el OID asignado a la presente política es 1.3.6.1.4.1.31304.1.2.2.1.1.

En la Declaración de Prácticas de Certificación en el apartado 7.1.6 encuentra más información respecto a este tema.

7.2.7. Sintaxis y semántica de los calificadores de la política

La extensión de los certificados referente a los calificadores de la Política de Certificación contiene la siguiente información:

Policy indentifier: Contiene el identificador de la Política de Certificado de Comunidad Académica

CPS: Indica la URL donde esta publicada la Declaración de la Practicas de Certificación (DPC) para ser consultadas por los usuarios

User Notice: contiene el texto "La utilización de este certificado está sujeta a las Políticas de Certificado de Comunidad Académica (PC) y Declaración de Prácticas de Certificación (DPC) establecidas por Andes SCD".

7.3. Perfil de la CRL

7.3.1. Numero de versión

Las CRL emitidas por Andes SCD corresponden con el estándar X.509 versión 2

7.3.2. CRL y extensiones

Se emite la lista de revocación CRL según lo estipulado en la RFC 2459

Perfil de CRL según estándar X.509V2 – CRL Clase II		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Numero de CRL	Número único de la CRL	Identificado de la CRL
Emisor	CN	CA ANDES SCD S.A. Clase II
	O	Andes SCD
	OU	Division de certificación entidad final
	C	CO
	L	Bogota, D.C.
	E	info@andesscd.com.co
Algoritmo de firma	Algoritmo usado para la firma de la CRL	SHA1withRSA
Fecha efectiva de emisión	Periodo de validez después de emitida la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha en que se emitirá la siguiente CRL	Fecha de emisión de la próxima CRL en tiempo UTC
URL distribución	URL donde se publican las CRL emitidas por Andes SCD	http://www.andesscd.com.co/includes/getCert.php?crl=1
Certificados revocados	Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación	

7.4. Perfil OCSP

7.4.1. Numero de versión

El certificado OCSP se emite de acuerdo al estándar X,509 V3

7.4.2. Extensiones OCSP

Extensiones OCSP según estándar X.509V3		
Nombre	**Descripción**	**Valor**
Basic Contraints, critical		CA false
Key Usage critical		Firma digital
Extended Key Usage		OCSPSigner
Subject Key Identifier		identificador de clave

8. Auditoria y otras valoraciones

La información sobre la auditoria y otras valoraciones se encuentra especificada en la Declaración de Prácticas de Certificación de Andes SCD.

9. Negocio y materias legales

9.1. Tarifas

En la Declaración de Prácticas de Certificación se define donde se encuentra el marco tarifario por los servicios de certificación ofrecidos por la Autoridad Certificadora Andes SCD.

9.2. Responsabilidad financiera

En la Declaración de Prácticas de Certificación de Andes SCD se especifica el valor de la cobertura para indemnizar los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por Andes SCD.

9.3. Confidencialidad de la información

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.4. Derechos de propiedad intelectual

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.5. Obligaciones y garantías

En la Declaración de Prácticas de Certificación se listan las obligaciones y garantías por parte de la Autoridad de Certificación Andes SCD, las Autoridades de Registro, los solicitantes, suscriptores y usuarios del servicio de certificación

9.6. Limitaciones de responsabilidad

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.7. Indemnizaciones

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.8. Término y terminación

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.9. Procedimiento de cambio en las especificaciones

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.10. Prevención de disputas

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD

9.11. Ley aplicable y cumplimiento con la ley aplicable

Según lo estipulado en la Declaración de Prácticas de Certificación de Andes SCD