Agencia de Tecnología y Certificación Electrónica

Política de Certificación de Certificados Cualificados de sede electrónica administrativa en dispositivo seguro

Fecha: 12/02/2025	**Versión:** 6.0.3
Estado: APROBADO	**Nº de páginas:** 49
OID: 1.3.6.1.4.1.8149.3.14.6.0	**Clasificación: PÚBLICO**
Archivo: ACCV-CP-14V6.0.3-ES-2025.doc	
Preparado por: Agencia de Tecnología y Certificación Electrónica - ACCV	

Este documento es propiedad de la Agencia de Tecnología y Certificación Electrónica – ACCV.
Licenciado bajo Creative Commons Attribuion-NoDerivatives 4.0 (CC BY-ND 4.0)

Versión	Autor	Gecha	Observaciones
4.0.1	ACCV	27/06/2018	Sin cambios
4.0.2	ACCV	16/07/2019	CAB/Forum modificación
4.0.3	ACCV	16/07/2019	Extensión OCSP
4.0.4	ACCV	16/01/2020	RFC3647 cumplimiento
4.0.5	ACCV	09/03/2020	RFC3647 cumplimiento
4.0.6	ACCV	01/09/2020	Validez Certificado
4.0.7	ACCV	20/03/2021	Cambio Sede y Policy Notice
4.0.8	ACCV	20/06/2021	Cambia la emisión de certificados wildcard
5.0.1	ACCV	20/03/2022	Se eliminan los OU del perfil y se cambia el OID QNCP-w
5.0.2	ACCV	16/03/2023	Revisión y corrección
5.0.3	ACCV	10/09/2023	Adaptación a los requisitos 2.0 del CAB/Forum
5.0.4	ACCV	02/04/2024	Revisión
6.0.1	ACCV	10/06/2024	Nueva jerarquía y revisión
6.0.2	ACCV	13/01/2025	Corrección y eliminación de las referencias del mecanismo de validación 3.2.2.4.2
6.0.3	ACCV	12/02/2025	Nueva jerarquía y revisión

Tabla de Contenido

1. INTRODUCCIÓN....9

1.1. PRESENTACIÓN....9
1.2. IDENTIFICACIÓN....9
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN....10
1.3.1. Autoridades de Certificación....10
1.3.2. Autoridades de Registro....10
1.3.3. Suscriptores....10
1.3.4. Partes confiantes....10
1.3.5. Otros participantes....10
1.4. USO DE LOS CERTIFICADOS....10
1.4.1. Usos Permitidos....10
1.4.2. Usos prohibidos....10
1.5. POLÍTICA DE ADMINISTRACIÓN DE LA ACCV....11
1.5.1. Especificación de la Organización Administradora....11
1.5.2. Persona de Contacto....11
1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas....11
1.5.4. Procedimiento de aprobación de la CPS....11
1.6. DEFINICIONES Y ACRÓNIMOS....11

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS....12

2.1. REPOSITORIO DE CERTIFICADOS....12
2.2. PUBLICACIÓN....12
2.3. FRECUENCIA DE ACTUALIZACIONES....12
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS....12

3. IDENTIFICACIÓN Y AUTENTICACIÓN....13

3.1. REGISTRO DE NOMBRES....13
3.1.1. Tipos de nombres....13
3.1.2. Significado de los nombres....13
3.1.3. Interpretación de formatos de nombres....13
3.1.4. Unicidad de los nombres....13
3.1.5. Resolución de conflictos relativos a nombres....13
3.1.6. Reconocimiento, autenticación y función de las marcas registradas....13
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD....13
3.2.1. Métodos de prueba de posesión de la clave privada....13
3.2.2. Autenticación de la identidad de una organización....13
3.2.3. Autenticación de la identidad de un individuo....15
3.2.4. Información no verificada de los suscriptores....16
3.2.5. Validación de la representación....16
3.2.6. Criterios para la interoperación....16
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DEL PAR DE CLAVES....16
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias....16
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida....16
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DEL PAR DE CLAVES....16

4. EL CICLO DE VIDA DE LOS CERTIFICADOS....18

4.1. SOLICITUD DE CERTIFICADOS....18
4.1.1. Quien puede enviar una solicitud de certificado....18
4.1.2. Procedimiento de registro y responsabilidades....18
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS....18
4.2.1. Realización de las funciones de identificación y autenticación....18
4.2.2. Aprobación o rechazo de la solicitud de certificado....19
4.2.3. Plazo para resolver la solicitud....19
4.3. EMISIÓN DE CERTIFICADOS....19

4.3.1. Acciones de la CA durante el proceso de emisión 19
4.3.2. Notificación de la emisión al suscriptor 20
4.4. ACEPTACIÓN DE CERTIFICADOS 20
4.4.1. Conducta que constituye aceptación del certificado 20
4.4.2. Publicación del certificado por la CA 20
4.4.3. Notificación de la emisión a terceros 20
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO 20
4.5.1. Uso del certificado y la clave privada del suscriptor 20
4.5.2. Uso de la clave pública y del certificado por la parte que confía 20
4.6. RENOVACIÓN DE CERTIFICADOS 20
4.6.1. Circunstancia para la renovación del certificado 20
4.6.2. Quién puede solicitar renovación 21
4.6.3. Procesamiento de solicitudes de renovación de certificados 21
4.6.4. Notificación de nueva emisión de certificado al suscriptor 21
4.6.5. Conducta que constituye la aceptación de un certificado de renovación 21
4.6.6. Publicación del certificado de renovación por la CA 21
4.6.7. Notificación de emisión de certificado por la CA a otras entidades 21
4.7. RENOVACIÓN DE CLAVES 21
4.7.1. Circunstancia para la renovación de claves (re-key) certificado 21
4.7.2. Quién puede solicitar la certificación de una nueva clave pública 21
4.7.3. Procesamiento de solicitudes de cambio de claves del certificado 21
4.7.4. Notificación de nueva emisión de certificado al suscriptor 21
4.7.5. Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed) 21
4.7.6. Publicación del certificado con renovación de claves (re-keyed) por la CA 21
4.7.7. Notificación de emisión de certificado por la CA a otras entidades 21
4.8. MODIFICACIÓN DE CERTIFICADOS 22
4.8.1. Circunstancia para la modificación del certificado 22
4.8.2. Quién puede solicitar la modificación del certificado 22
4.8.3. Procesamiento de solicitudes de modificación de certificados 22
4.8.4. Notificación de nueva emisión de certificado al suscriptor 22
4.8.5. Conducta que constituye la aceptación de un certificado modificado 22
4.8.6. Publicación del certificado modificado por la CA 22
4.8.7. Notificación de emisión de certificado por la CA a otras entidades 22
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 22
4.9.1. Circunstancias para la revocación 22
4.9.2. Entidad que puede solicitar la revocación 22
4.9.3. Procedimiento de solicitud de revocación 22
4.9.3.1. Telemático 22
4.9.4. Periodo de gracia de la solicitud de revocación 22
4.9.5. Tiempo dentro del cual CA debe procesar la solicitud de revocación 23
4.9.6. Requisitos de comprobación de CRLs 23
4.9.7. Frecuencia de emisión de CRLs 23
4.9.8. Máxima latencia de CRL 23
4.9.9. Disponibilidad de comprobación on-line de la revocación 23
4.9.10. Requisitos de la comprobación on-line de la revocación 23
4.9.11. Otras formas de divulgación de información de revocación disponibles 23
4.9.12. Requisitos especiales de revocación por compromiso de las claves 23
4.9.13. Circunstancias para la suspensión 23
4.9.14. Entidad que puede solicitar la suspensión 23
4.9.15. Procedimiento para la solicitud de suspensión 23
4.9.16. Límites del período de suspensión 23
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS 23
4.10.1. Características operacionales 23
4.10.2. Disponibilidad del servicio 23
4.10.3. Características opcionales 24
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN 24
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES 24
4.12.1. Política y prácticas clave de custodia y recuperación 24
4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión 24

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....25
5.1. CONTROLES DE SEGURIDAD FÍSICA.....25
5.1.1. Ubicación y construcción.....25
5.1.2. Acceso físico.....25
5.1.3. Alimentación eléctrica y aire acondicionado.....25
5.1.4. Exposición al agua.....25
5.1.5. Protección y prevención de incendios.....25
5.1.6. Sistema de almacenamiento.....25
5.1.7. Eliminación de residuos.....25
5.1.8. Backup remoto.....25
5.2. CONTROLES DE PROCEDIMIENTOS.....25
5.2.1. Papeles de confianza.....25
5.2.2. Número de personas requeridas por tarea.....25
5.2.3. Identificación y autenticación para cada papel.....25
5.2.4. Roles que requieren separación de tareas.....26
5.3. CONTROLES DE SEGURIDAD DE PERSONAL.....26
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación.....26
5.3.2. Procedimientos de comprobación de antecedentes.....26
5.3.3. Requerimientos de formación.....26
5.3.4. Requerimientos y frecuencia de actualización de la formación.....26
5.3.5. Frecuencia y secuencia de rotación de tareas.....26
5.3.6. Sanciones por acciones no autorizadas.....26
5.3.7. Requerimientos de contratación de personal.....26
5.3.8. Documentación proporcionada al personal.....26
5.3.9. Controles periódicos de cumplimiento.....26
5.3.10. Finalización de los contratos.....26
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....26
5.4.1. Tipos de eventos registrados.....26
5.4.2. Frecuencia de procesado de logs.....26
5.4.3. Periodo de retención para los logs de auditoría.....27
5.4.4. Protección de los logs de auditoría.....27
5.4.5. Procedimientos de backup de los logs de auditoría.....27
5.4.6. Sistema de recogida de información de auditoría (interno vs externo).....27
5.4.7. Notificación al sujeto causa del evento.....27
5.4.8. Análisis de vulnerabilidades.....27
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS.....27
5.5.1. Tipo de informaciones y eventos registrados.....27
5.5.2. Periodo de retención para el archivo.....27
5.5.3. Protección del archivo.....27
5.5.4. Procedimientos de backup del archivo.....27
5.5.5. Requerimientos para el sellado de tiempo de los registros.....27
5.5.6. Sistema de recogida de información de auditoría (interno vs externo).....27
5.5.7. Procedimientos para obtener y verificar información archivada.....27
5.6. CAMBIO DE CLAVE.....28
5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....28
5.7.1. Alteración de los recursos hardware, software y/o datos.....28
5.7.2. La clave pública de una entidad se revoca.....28
5.7.3. La clave de una entidad se compromete.....28
5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre.....28
5.8. CESE DE UNA CA.....28

6. CONTROLES DE SEGURIDAD TÉCNICA.....29
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....29
6.1.1. Generación del par de claves.....29
6.1.2. Entrega de la clave privada a la entidad.....29
6.1.3. Entrega de la clave pública al emisor del certificado.....29
6.1.4. Entrega de la clave pública de la CA a los usuarios.....29
6.1.5. Tamaño de las claves.....29
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad.....29

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509v3) *30*
6.1.8. Hardware/software de generación de claves *30*
6.2. PROTECCIÓN DE LA CLAVE PRIVADA 30
6.2.1. Estándares para los módulos criptográficos *30*
6.2.2. Control multipersona de la clave privada *30*
6.2.3. Custodia de la clave privada *30*
6.2.4. Copia de seguridad de la clave privada *31*
6.2.5. Archivo de la clave privada *31*
6.2.6. Introducción de la clave privada en el módulo criptográfico *31*
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico *31*
6.2.8. Método de activación de la clave privada *31*
6.2.9. Método de desactivación de la clave privada *31*
6.2.10. Método de destrucción de la clave privada *31*
6.2.11. Clasificación de los módulos criptográficos *31*
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 31
6.3.1. Archivo de la clave pública *31*
6.3.2. Periodo de uso para las claves públicas y privadas *31*
6.4. DATOS DE ACTIVACIÓN 32
6.4.1. Generación y activación de los datos de activación *32*
6.4.2. Protección de los datos de activación *32*
6.4.3. Otros aspectos de los datos de activación *32*
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA 32
6.5.1. Requerimientos técnicos de seguridad informática específicos *32*
6.5.2. Valoración de la seguridad informática *32*
6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 32
6.6.1. Controles de desarrollo del sistema *32*
6.6.2. Controles de gestión de la seguridad *32*
6.6.3. Evaluación de la seguridad del ciclo de vida *32*
6.7. CONTROLES DE SEGURIDAD DE LA RED 32
6.8. TIMESTAMPING 32

7. PERFILES DE CERTIFICADOS Y CRL Y OCSP 33

7.1. PERFIL DE CERTIFICADO 33
7.1.1. Número de versión *33*
7.1.2. Extensiones del certificado *33*
7.1.3. Identificadores de objeto (OID) de los algoritmos *35*
7.1.4. Formatos de nombres *35*
7.1.5. Restricciones de los nombres *36*
7.1.6. Identificador de objeto (OID) de la Política de Certificación *36*
7.1.7. Uso de la extensión "Policy Constraints" *37*
7.1.8. Sintaxis y semántica de los cualificadores de política *37*
7.1.9. Tratamiento semántico para la extensión "Certificate Policy" *37*
7.1.10. Lista de Signed Certificate Timestamp (SCT) *37*
7.2. PERFIL DE CRL 37
7.2.1. Número de versión *37*
7.2.2. CRL y extensiones *37*
7.3. PERFIL DE OCSP 38
7.3.1. Número de versión *38*
7.3.2. Extensiones *38*

8. AUDITORÍA DE CONFORMIDAD 39

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD 39
8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR 39
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA 39
8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD 39
8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA 39
8.6. COMUNICACIÓN DE RESULTADOS 39
8.7. AUTO AUDITORIAS 39

9. REQUISITOS COMERCIALES Y LEGALES 40

9.1. TARIFAS....40
9.1.1. Tarifas de emisión de certificado o renovación....40
9.1.2. Tarifas de acceso a los certificados....40
9.1.3. Tarifas de acceso a la información de estado o revocación....40
9.1.4. Tarifas de otros servicios como información de políticas....40
9.1.5. Política de reintegros....40
9.2. CAPACIDAD FINANCIERA....40
9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACCV....40
9.2.2. Relaciones fiduciarias....40
9.2.3. Procesos administrativos....40
9.3. POLÍTICA DE CONFIDENCIALIDAD....40
9.3.1. Información confidencial....40
9.3.2. Información no confidencial....40
9.3.3. Divulgación de información de revocación /suspensión de certificados....41
9.4. PROTECCIÓN DE DATOS PERSONALES....41
9.4.1. Plan de Protección de Datos Personales....41
9.4.2. Información considerada privada....41
9.4.3. Información no considerada privada....41
9.4.4. Responsabilidades....41
9.4.5. Prestación del consentimiento en el uso de los datos personales....41
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales....41
9.4.7. Otros supuestos de divulgación de la información....41
9.5. DERECHOS DE PROPIEDAD INTELECTUAL....41
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL....41
9.6.1. Obligaciones de la Entidad de Certificación....41
9.6.2. Obligaciones de la Autoridad de Registro....41
9.6.3. Obligaciones de los suscriptores....41
9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV....42
9.6.5. Obligaciones del repositorio....42
9.7. RENUNCIAS DE GARANTÍAS....42
9.8. LIMITACIONES DE RESPONSABILIDAD....42
9.8.1. Garantías y limitaciones de garantías....42
9.8.2. Deslinde de responsabilidades....42
9.8.3. Limitaciones de pérdidas....42
9.9. INDEMNIZACIONES....42
9.10. PLAZO Y FINALIZACIÓN....42
9.10.1. Plazo....42
9.10.2. Finalización....42
9.10.3. Supervivencia....42
9.11. NOTIFICACIONES....42
9.12. MODIFICACIONES....43
9.12.1. Procedimientos de especificación de cambios....43
9.12.2. Procedimientos de publicación y notificación....43
9.12.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación....43
9.13. RESOLUCIÓN DE CONFLICTOS....43
9.13.1. Resolución extrajudicial de conflictos....43
9.13.2. Jurisdicción competente....43
9.14. LEGISLACIÓN APLICABLE....43
9.15. CONFORMIDAD CON LA LEY APLICABLE....43
9.16. CLÁUSULAS DIVERSAS....43
9.16.1. Acuerdo completo....43
9.16.2. Asignación....43
9.16.3. Separabilidad....43
9.16.4. Cumplimiento (honorarios de abogados y exención de derechos)....43
9.16.5. Fuerza mayor....44
9.17. OTRAS CUESTIONES....44
10. ANEXO I....45

1. INTRODUCCIÓN

1.1. Presentación

El presente documento es la Política de Certificación asociada a los certificados cualificados de sede electrónica administrativa en dispositivo seguro, que contiene las reglas a las que se sujeta la gestión y el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Agencia de Tecnología y Certificación Electrónica y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la Agencia de Tecnología y Certificación Electrónica.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados cualificados de sede electrónica en dispositivo criptográfico –HSM–.

La presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* propuesto por *Network Working Group* para este tipo de documentos, al igual que la Declaración de Prácticas de Certificación, para facilitar la lectura o comparación con documentos homólogos.

Esta Política de Certificación asume que el lector conoce los conceptos básicos de Infraestructura de Clave Pública, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

En el ámbito del proyecto Certificate Transparency, los precertificados se publicarán en el servicio CT Log de los proveedores de servidores de registro cualificados para cumplir con los requisitos del proyecto.

1.2. Identificación

Nombre de la política	Política de Certificación de Certificados Cualificados de sede electrónica administrativa en dispositivo seguro
Identificador del certificado	`Certificado cualificado de sede electrónica administrativa expedido por la ACCV (Pol. Ademuz, s/n. Burjassot, CP 46100, ESPAÑA. CIF A40573396)`
Versión de la política	6.0.3
Estado de la política	APROBADO
Referencia de la política / OID (Object Identifier)	1.3.6.1.4.1.8149.3.14.6.0
Fecha de emisión	12/02/2025
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACCV. Versión 4.0. OID: 1.3.6.1.4.1.8149.2.4.0 Disponible en `http://www.accv.es/pdf-politicas`
Localización	Esta Política de Certificación se puede encontrar en: http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN

1.3. Comunidad de usuarios y ámbito de aplicación

1.3.1. Autoridades de Certificación

Las Autoridades de Certificación que pueden emitir certificados acordes con esta política son:

- ACCVCA-120 perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de entidad final para los suscriptores de ACCV. El certificado de ACCVCA-120 es válido desde el día 27 de enero de 2015 hasta el 1 de enero de 2027.

- ACCV RSA1 TLS perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de autenticación de sitios web para los suscriptores de ACCV. El certificado de ACCV RSA1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

- ACCV ECC1 TLS perteneciente a la Agencia de Tecnología y Certificación Electrónica, cuya función es la emisión de certificados de autenticación de sitios web para los suscriptores de ACCV. El certificado de ACCV ECC1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

1.3.2. Autoridades de Registro

La Autoridad de Registro que gestiona este tipo de certificados es la Agencia de Tecnología y Certificación Electrónica.

1.3.3. Suscriptores

El grupo de usuarios que pueden solicitar certificados definidos por esta política está limitado exclusivamente al compuesto por el conjunto Jefes de Área o puestos organizativos equivalentes en cualquier tipo de Administración Pública (europea, estatal, autonómica y local), siendo éstos los responsables últimos de su uso dentro de los distintos proyectos o sistemas de información.

El soporte de claves y certificados es dispositivo seguro criptográfico -HSM- que se encuentre homologado por el Ministerio con las competencias correspondientes como dispositivo seguro, siguiendo las recomendaciones establecidas a nivel Europeo.

Se limita el derecho de solicitud de certificados definido en la presente Política de Certificación a personas físicas. No se aceptarán solicitudes de certificación realizadas por personas jurídicas, entidades u organizaciones.

1.3.4. Partes confiantes

Se limita el derecho a confiar en los certificados emitidos conforme a la presente política a:

a) Los usuarios de clientes de aplicaciones en el ámbito de la verificación de la identidad de la sede electrónica a la que se conectan y del cifrado del canal de los datos transmitidos entre ellos.

b) Las aplicaciones y servicios con capacidades de soporte SSL y/o TLS, en el ámbito de verificación de la identidad de las sedes electrónica a las que se conectan, y del cifrado del canal de los datos transmitidos entre ellos.

1.3.5. Otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.4. Uso de los certificados

1.4.1. Usos Permitidos

Los certificados emitidos por Agencia de Tecnología y Certificación Electrónica bajo esta Política de Certificación, pueden utilizarse para dotar a las sedes electrónicas de capacidades SSL/TLS.

Asimismo, pueden utilizarse como mecanismo de identificación de estas sedes de forma inequívoca ante servicios y aplicaciones informáticas.

1.4.2. Usos prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

1.5. Política de Administración de la ACCV

1.5.1. Especificación de la Organización Administradora

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.2. Persona de Contacto

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV

1.5.4. Procedimiento de aprobación de la CPS

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

1.6. Definiciones y Acrónimos

HSM: Hardware Security Module

SSL: Secure Sockets Layer

TLS: Transport Security Layer

2. Publicación de información y repositorio de certificados

2.1. Repositorio de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.2. Publicación

Ademas de lo especificado en la Declaración de Prácticas de Certificación (CPS), ACCV mantiene sitios web de test que permiten a los integradores y desarrolladores de aplicaciones probar sus desarrollos con certificados de usuario de la presente política.

- ACCVCA-120

VALID

https://activo.accv.es/test/hola.html

REVOKED

https://revocado.accv.es:442/test/hola.html

EXPIRED

https://caducado.accv.es:444/test/hola.html

- ACCV RSA1 TLS

VALID

https://activonjrsa.accv.es/test/hola.html

REVOKED

https://revocadonjrsa.accv.es:442/test/hola.html

EXPIRED

https://caducadonjrsa.accv.es:444/test/hola.html

- ACCV ECC1 TLS

VALID

https://activonjecc.accv.es/test/hola.html

REVOKED

https://revocadonjecc.accv.es:442/test/hola.html

EXPIRED

https://caducadonjecc.accv.es:444/test/hola.html

La Agencia de Tecnología y Certificación Electrónica (ACCV) se ajusta a la versión actual del documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", publicada en https://www.cabforum.org/. En el caso de cualquier incompatibilidad entre esta Política de Certificación y los requisitos del CAB Forum, dichos requisitos prevalecerán sobre el presente documento.

Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. **Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales (dependiendo del tipo de incumplimiento) y no es posible aplazamiento de ningún tipo.**

Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

2.3. Frecuencia de actualizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

2.4. Controles de acceso al repositorio de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3. Identificación y Autenticación

3.1. Registro de nombres

3.1.1. Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.2. Significado de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.3. Interpretación de formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.4. Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.5. Resolución de conflictos relativos a nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de posesión de la clave privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2.2. Autenticación de la identidad de una organización.

El derecho de solicitud de certificados definido en la presente Política de Certificación se encuentra limitado a personas físicas. No se aceptarán solicitudes de certificación realizadas en nombre de personas jurídicas, entidades u organizaciones.

La autentificación de la identidad del solicitante se realiza mediante el uso de su certificado personal cualificado, firmando con el la solicitud del certificado de sede electrónica al identificarse en la aplicación que para esta función pone a disposición de los usuarios la ACCV (NPSC https://npsc.accv.es:8450/npsc)

El solicitante debe presentar la documentación necesaria que determine

Los datos relativos a la entidad como la inclusión en el registro mercantil correspondiente, domicilio, localidad, estado o provincia, país, códigos de funcionamiento, etc.

Las capacidades de representación necesarias de la entidad propietaria del referido dominio.

La posesión del dominio

Esta presentación se realizará de forma digital utilizando las fuentes y aplicaciones que ACCV pone a disposición de los usuarios para ello.

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Agencias de Protección de Datos

https://sedeagpd.gob.es/sede-electronica-web/

Registros de Administraciones Públicas

https://face.gob.es/es/directorio/administraciones

https://sede.administracion.gob.es/

Registros mercantiles

https://sede.registradores.org/site/

Oficinas de Patentes y Marcas

https://www.oepm.es/en/index.html

Servicios de Verificación y Consulta de Identidad

https://administracionelectronica.gob.es/ctt/SVD

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

Verificación de dominio

ACCV verificará que el dominio de los certificados y sus direcciones asociadas pertenecen a los datos del solicitante utilizando para ello la información disponible de los registros personales y de dominios, exigiendo al solicitante las explicaciones o documentos adicionales que pudiera considerar necesarios e incluyendo en el proceso mecanismos de comprobación técnicamente fiables y aprobados por la industria.

ACCV conserva la información de comprobación dominio con fines de auditoría pero no la reutiliza, verificando el dominio para cada solicitud de forma independiente. ACCV no emitirá certificados para direcciones IP o nombres de dominio privados. En el caso de los gTLD, sólo se emitirán certificados con nombres de gTLD aprobados, y sólo se emitirán a los suscriptores que tengan el control del gTLD, tal y como aparece en ICANN/IANA.

En concreto:

- Comprobación de que el solicitante, cuya identidad ha sido verificada sin lugar a dudas, es uno de los propietarios del dominio. Para esta comprobación, la ACCV debe utilizar uno o varios de los siguientes métodos:
  - Contactar por correo, enviando un número aleatorio único en el correo a una o más direcciones creadas usando 'admin', 'administrator', 'webmaster', 'hostmaster', o 'postmaster' como parte local, seguido del signo de arroba ("@"), seguido de un nombre de dominio a autorizar, incluyendo un valor aleatorio en el correo electrónico, y recibiendo una respuesta de confirmación utilizando el mismo valor aleatorio del correo inicial. ACCV debe esperar la respuesta un tiempo no superior a 30 días y debe confirmar que la respuesta incluye el mismo número aleatorio.
    - (CAB/Forum BR 3.2.2.4.4 Correo electrónico construido al contacto del dominio)
  - Confirmar la presencia de un valor aleatorio incluido en el contenido de un archivo bajo el directorio "/.well-known/pki-validation" en el nombre de dominio a autorizar. Esta URL debe ser accesible por la CA a través de HTTP/HTTPS sobre un Puerto Autorizado. Una vez comunicado el valor al solicitante, sólo será válido durante 30 días. En la URL no aparece en ningún caso el contenido del fichero y solo se considera como valor correcto de respuesta HTTP 200 (no se permiten re direcciones).Para realizar la verificación del

valor aleatorio en la conexión HTTP/HTTPS se utilizaran múltiples perspectivas de red (al menos tres).

- (CAB/Forum BR 3.2.2.4.18 Cambio acordado en el sitio web v2)

- Confirmación del control del solicitante sobre un FQDN mediante la validación del control del dominio del FQDN utilizando el método ACME HTTP Challenge definido en la sección 8.3 de la RFC 8555.

  ACCV DEBE recibir una respuesta HTTP satisfactoria de la solicitud (lo que significa que se debe recibir un código de estado HTTP 2xx).

  El token (tal y como se define en RFC 8555, Sección 8.3) una vez comunicado el valor al solicitante, sólo será válido durante 30 días. En la URL no aparece en ningún caso el contenido del fichero y solo se considera como valor correcto de respuesta HTTP 200 (no se permiten re direcciones). Para realizar la verificación del valor aleatorio en la conexión HTTP/HTTPS se utilizaran múltiples perspectivas de red (al menos tres).

  - (CAB/Forum BR 3.2.2.4.19 Cambio acordado en el sitio web - ACME)

- Confirmar la presencia de un valor aleatorio en un registro DNS CNAME, TXT o CAA para 1) un Nombre de Dominio de Autorización; o 2) un Nombre de Dominio de Autorización que tenga como prefijo una etiqueta que comience con un carácter de subrayado. Una vez comunicado el valor al solicitante, sólo será válido durante 30 días. Para realizar la verificación se utilizaran múltiples perspectivas de red (al menos tres).

  - (CAB/Forum BR 3.2.2.4.7 Cambio de DNS)

ACCV comprobará la existencia de registros CAA justo antes de emitir el certificado, actuando como se define en el rfc 6844 y en los documentos del CAB/Forum si el registro está presente. Para realizar la verificación del registro CAA se utilizaran múltiples perspectivas de red (al menos tres). El identificador asociado a ACCV como registros CAA *issue* e *issuewild* es "accv.es".

Se realizarán pruebas de conexión con el dominio dado y pruebas de respuesta de DNS mediante protocolo seguro (por ejemplo, HTTPS).

La emisión de certificados comodín (*) no está permitida bajo esta política, a partir del 20/06/2021.

Ante cualquier irregularidad el solicitante del certificado será notificado por la ACCV y se suspenderá su emisión hasta su corrección. Si dicha corrección no se produce en un mes, la solicitud será denegada.

3.2.3. Autenticación de la identidad de un individuo.

La autentificación de la identidad del solicitante de un certificado se realizará mediante el uso de su certificado cualificado personal admitido para la firma de la solicitud del certificado cualificado de sede electrónica.

El solicitante deberá presentar además la documentación necesaria que determine la capacidad de representar a la entidad propietaria del dominio al que hace referencia y la posesión del dominio mismo. Esta presentación se realizará de manera telemática utilizando los medios y aplicaciones que a tal efecto la ACCV ponga a disposición de los usuarios (3.2.2.).

ACCV comprobará los datos suministrados (incluyendo el país del solicitante) utilizando para ello la información disponible en:

Agencias de Protección de Datos

https://sedeagpd.gob.es/sede-electronica-web/

Registros de Administraciones Públicas

https://face.gob.es/es/directorio/administraciones

https://sede.administracion.gob.es/

Registros mercantiles

https://sede.registradores.org/site/

Oficinas de Patentes y Marcas

https://www.oepm.es/en/index.html

Servicios de Verificación y Consulta de Identidad

https://administracionelectronica.gob.es/ctt/SVD

reclamando al solicitante las subsanaciones o documentos adicionales que pudiera considerar necesarios.

Todos los organismos y registros utilizados son oficiales y de alta fiabilidad, proporcionando pruebas rastreables de todas las búsquedas.

La ACCV conserva esta información a efectos de auditoría, permitiendo su reutilización durante un periodo no superior a 13 meses desde su última comprobación.

3.2.4. Información no verificada de los suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2.5. Validación de la representación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.2.6. Criterios para la interoperación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

3.3. Identificación y autenticación de las solicitudes de renovación del par de claves.

3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial (descrita en el punto 3.2.3 *Autenticación de la identidad de un individuo*, de esta Política de Certificación). ACCV puede reutilizar la información almacenada en comprobaciones previas si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio que no se reutiliza. Existe, por tanto, un mecanismo para la renovación:

- Formularios web firmados en el Área de Gestión de Certificados No Personales, disponible en https://npsc.accv.es:8450/npsc.

3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial, pudiendo reutilizar la información en posesión de la ACCV si no han pasado mas de 13 meses desde la ultima verificación de los datos, exceptuando la información de comprobación de dominio que no se reutiliza.

ACCV, por cuestiones técnicas y detallando todos los pasos, puede emplear algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

3.4. Identificación y autenticación de las solicitudes de revocación del par de claves

La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Telemática. Mediante la firma electrónica de la solicitud de revocación (ubicada en el Área de Gestión de Certificados No Personales https://npsc.accv.es:8450/npsc) por parte del solicitante del certificado o del responsable del mismo en la fecha de la solicitud de revocación.

ACCV o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada asociada al certificado de sede electrónica, o cualquier otro hecho que recomendará emprender dicha acción.

4. El ciclo de vida de los certificados.

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.1. Solicitud de certificados

4.1.1. Quien puede enviar una solicitud de certificado

Los suscriptores enumerados en el punto 1.3.3 pueden presentar una solicitud de certificado.

La solicitud de este tipo de certificados es responsabilidad de la Administración Pública o entidades de carácter público. Una solicitud de certificado puede ser realizada por el suscriptor del certificado o por un representante autorizado de dicho suscriptor.

4.1.2. Procedimiento de registro y responsabilidades

El proceso comienza por acceder al Área de gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc. Si se solicita por primera vez el certificado de sede asociado a una Administración Publica el usuario debe adjuntar el documento que lo acredita como capacitado para efectuar esa solicitud (documento de toma de posesión en el puesto o diario oficial donde se recoge el nombramiento correspondiente), en formato pdf firmado electrónicamente. Si el acceso se ha efectuado con certificado de Empleado Público o de Representante se utilizaran los datos de Organización, Unidad Organizativa y Cargo de dicho certificado.

ACCV comprobará los datos de la solicitud y acreditará al solicitante para la solicitud de certificados de sede electrónica, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional, exceptuando la información de comprobación de dominio que no se reutiliza. En el caso de identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

Ademas de comprobar las credenciales asociados a la entidad, ACCV comprobará en los registros autorizados la posesión del dominio o dominios que aparecen en la solicitud de certificado, de forma que no exista duda de dicha posesión. ACCV dejará constancia de estas búsquedas y comprobaciones de forma que puedan reproducirse en todos los pasos. Para esta comprobación ACCV utilizara los correos y teléfonos suministrados en el proceso de alta, siendo necesaria una vinculación directa entre estos datos y los dominios incluidos en la solicitud.

El usuario deberá marcar la opción HSM o dispositivo seguro en la solicitud de certificado.

4.2. Tramitación de la solicitud de certificados.

4.2.1. Realización de las funciones de identificación y autenticación

La autenticación de la identidad del solicitante se hará mediante la identificación con la Autoridad de Registro correspondiente (en este caso NPSC), utilizando los mecanismos descritos en la sección 3.2.3 *Autenticación de la identidad de un individuo*. Una vez identificado se procederá a proporcionar por los canales establecidos toda la documentación necesaria para este tipo de certificados que no estuviera en posesión de la ACCV o no estuviera en vigor.

- Documentación asociada al organismo

- Documentación asociada a las credenciales personales para la solicitud y gestión en nombre de dicho organismo.

La Autoridad de registro comprueba la documentación y valida los datos utilizando registros accesibles al público para dicha verificación (3.2.2). Una vez comprobados todos los datos, ACCV acreditará al solicitante para la solicitud de certificados de sede electrónica administrativa, durante 13 meses a partir de la aprobación sin necesidad de aportar documentación adicional. En el caso de

identificación con certificado de empleado público no existe limitación temporal mientras el certificado esté en vigor.

Ademas de validar las credenciales personales y de la entidad, ACCV verifica en los registros autorizados la posesión del dominio o dominios asociados a la solicitud, de forma que no haya dudas en la existencia de esta posesión tal y como se ha detallado en los apartados 3.2.2 y 3.2.3 de esta política. ACCV proporciona registros de esas búsquedas garantizando que pueden reproducirse en cada paso. Para todas estas validaciones se utilizan las direcciones de correo y telefoneó proporcionados en el proceso de registro, siendo necesario una conexión directa entre estos datos y los dominios incluidos en al solicitud.

Como parte de este proceso, ACCV comprueba que la solicitud de certificado no incluye dominios que puedan ser usados para phising u otros usos fraudulentos, utilizando listas y mecanismos de uso público y de confianza.

4.2.2. Aprobación o rechazo de la solicitud de certificado

En caso de aceptación, la Autoridad de Registro notificará al solicitante por medio de un correo electrónico firmado digitalmente a la dirección de correo que figura en el perfil del usuario en la aplicación NPSC.

El solicitante debe acceder a NPSC con su certificado personal cualificado. Si el solicitante esta en condiciones técnicas y administrativas de llevar a cabo esta generación, la correspondiente opción le aparecerá habilitada en la aplicación.

En caso de denegación, la Autoridad de Registro lo notificará al solicitante mediante el envío de un correo electrónico firmado a la dirección que figure en la solicitud. La solicitud se cancelara y no podrá reutilizarse, aunque es posible reutilizar la documentación suministrada que haya sido verificado por un periodo no superior a 13 meses.

Este proceso es llevado a cabo por un miembro de ACCV diferente al que ha llevado a cabo la validación de los datos. La diferenciación de roles se consigue usando las capacidades incluidas en la aplicación de gestión y registro.
ACCV utilizará esta información para decidir sobre nuevas solicitudes.

4.2.3. Plazo para resolver la solicitud

El tiempo máximo para resolver la solicitud es de cinco días laborables.

4.3. Emisión de certificados

ACCV no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, éste puede ser revocado.

4.3.1. Acciones de la CA durante el proceso de emisión

La emisión del certificado tiene lugar una vez que la Autoridad de Registro ha realizado las comprobaciones necesarias para validar la solicitud. El mecanismo que determina la naturaleza y forma de realizar estas comprobaciones es esta Política de Certificación.

Cuando el solicitante recibe el correo electrónico de aprobación, debe entrar de nuevo en NPSC, identificándose con un certificado personal cualificado para generar y descargar el certificado.

La organización responsable del certificado de sede electrónica puede solicitar a la ACCV que añada otros usuarios con capacidad para realizar las transacciones que están asociadas al ciclo de vida de los certificados. La Autoridad de Registro comprobará la solicitud de credencial y notificará al solicitante la autorización o denegación del permiso, a través de un correo electrónico firmado.

ACCV podrá realizar esta autorización de oficio en el caso de que el responsable del sitio web pierda su capacidad de gestión y no exista otra persona autorizada.

ACCV realizará revisiones frecuentes de las muestras de los certificados de sede electrónica para garantizar la exactitud de los datos y el efecto. Si en el transcurso de estos muestreos se confirma un cambio de datos que pueda implicar la pérdida de la posesión del dominio, la ACCV revocará los certificados implicados. En caso de inexactitud de los datos que figuran en el certificado o de su inaplicabilidad se aplicará el mismo proceso. ACCV dejará constancia documental de todas estas revisiones y actuaciones.

4.3.2. Notificación de la emisión al suscriptor

ACCV notifica al suscriptor sobre la emisión del certificado, a través de un correo electrónico firmado a la dirección de correo proporcionada en el proceso de solicitud.

4.4. Aceptación de certificados

4.4.1. Conducta que constituye aceptación del certificado

La aceptación de los certificados por parte de los suscriptores se produce en el momento de la firma del contrato de certificación asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El Contrato de Certificación es un documento que debe ser firmado por el solicitante, y cuyo fin es vincular a la persona que solicita el certificado de sede electrónica, con el conocimiento de las normas de uso y con la veracidad de los datos presentados. El formulario del Contrato de Certificación se recoge en el Anexo I de esta Política de Certificación.

El usuario debe aceptar el contrato antes de la emisión del certificado.

4.4.2. Publicación del certificado por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.4.3. Notificación de la emisión a terceros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.5. Uso del par de claves y del certificado.

4.5.1. Uso del certificado y la clave privada del suscriptor

Los usos de la clave vienen definidos en el contenido del certificado en las extensiones: keyUsage, extendedKeyUsage y basicConstraints. Estas extensiones se detallan en el apartado *7.1.2 Extensiones del certificado*.

4.5.2. Uso de la clave pública y del certificado por la parte que confía

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6. Renovación de certificados.

La renovación de certificados debe ser realizada utilizando los mismos procedimientos y métodos de identificación que los establecidos para realizar la solicitud inicial.

4.6.1. Circunstancia para la renovación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.2. Quién puede solicitar renovación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.3. Procesamiento de solicitudes de renovación de certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.4. Notificación de nueva emisión de certificado al suscriptor
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.5. Conducta que constituye la aceptación de un certificado de renovación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.6. Publicación del certificado de renovación por la CA
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.6.7. Notificación de emisión de certificado por la CA a otras entidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7. Renovación de claves
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.1. Circunstancia para la renovación de claves (re-key) certificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.3. Procesamiento de solicitudes de cambio de claves del certificado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.4. Notificación de nueva emisión de certificado al suscriptor
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.5. Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed)
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.6. Publicación del certificado con renovación de claves (re-keyed) por la CA
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.7.7. Notificación de emisión de certificado por la CA a otras entidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8. Modificación de certificados.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.1. Circunstancia para la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.2. Quién puede solicitar la modificación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.3. Procesamiento de solicitudes de modificación de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.4. Notificación de nueva emisión de certificado al suscriptor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.5. Conducta que constituye la aceptación de un certificado modificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.6. Publicación del certificado modificado por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.8.7. Notificación de emisión de certificado por la CA a otras entidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9. Revocación y suspensión de certificados.

4.9.1. Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.2. Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.3. Procedimiento de solicitud de revocación

La Agencia de Tecnología y Certificación Electrónica acepta solicitudes de revocación por los siguientes procedimientos.

4.9.3.1. Telemático

Accediendo al Área de Gestión de certificados no personales (NPSC) ubicada en https://npsc.accv.es:8450/npsc el usuario puede revocar los certificados que ha solicitado o de los que tiene permiso para ello.

4.9.4. Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.5. Tiempo dentro del cual CA debe procesar la solicitud de revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.6. Requisitos de comprobación de CRLs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.7. Frecuencia de emisión de CRLs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.8. Máxima latencia de CRL
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.9. Disponibilidad de comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.10. Requisitos de la comprobación on-line de la revocación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.11. Otras formas de divulgación de información de revocación disponibles
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.12. Requisitos especiales de revocación por compromiso de las claves
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.13. Circunstancias para la suspensión
ACCV no soporta la suspensión de certificados como operación independiente sobre sus certificados.

4.9.14. Entidad que puede solicitar la suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.15. Procedimiento para la solicitud de suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.9.16. Límites del período de suspensión
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10. Servicios de comprobación de estado de certificados.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.1. Características operacionales
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.2. Disponibilidad del servicio
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.10.3. Características opcionales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

4.11. Finalización de la suscripción.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

ACCV informará al responsable del certificado de sede, mediante correo electrónico firmado digitalmente, en un momento previo anterior a la publicación del certificado en la Lista de Certificados Revocados, acerca de la suspensión o revocación de los certificados en los cuales aparezca como suscriptor o responsable, especificando los motivos, la fecha y la hora en que su certificado quedará sin efecto, y comunicándole que no debe continuar utilizándolo.

4.12. Depósito y recuperación de claves.

4.12.1. Política y prácticas clave de custodia y recuperación

ACCV no realiza el depósito de certificados y claves de ningún tipo asociadas a este tipo de certificados.

4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión

La recuperación de las claves de sesión no esta soportado.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de Seguridad Física

5.1.1. Ubicación y construcción
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.2. Acceso físico
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.3. Alimentación eléctrica y aire acondicionado
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.4. Exposición al agua
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.5. Protección y prevención de incendios
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.6. Sistema de almacenamiento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.7. Eliminación de residuos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.1.8. Backup remoto
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2. Controles de procedimientos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.1. Papeles de confianza
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.2. Número de personas requeridas por tarea
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.3. Identificación y autenticación para cada papel
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.2.4. Roles que requieren separación de tareas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3. Controles de seguridad de personal
Este apartado refleja el contenido del documento *Controles de Seguridad del Personal* de ACCV.

5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.2. Procedimientos de comprobación de antecedentes
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.3. Requerimientos de formación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.4. Requerimientos y frecuencia de actualización de la formación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.5. Frecuencia y secuencia de rotación de tareas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.6. Sanciones por acciones no autorizadas
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.7. Requerimientos de contratación de personal
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.8. Documentación proporcionada al personal
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.9. Controles periódicos de cumplimiento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.3.10. Finalización de los contratos
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4. Procedimientos de Control de Seguridad

5.4.1. Tipos de eventos registrados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.2. Frecuencia de procesado de logs
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.3. Periodo de retención para los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.4. Protección de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.5. Procedimientos de backup de los logs de auditoría
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.6. Sistema de recogida de información de auditoría (interno vs externo)
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.7. Notificación al sujeto causa del evento
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.4.8. Análisis de vulnerabilidades
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5. Archivo de informaciones y registros

5.5.1. Tipo de informaciones y eventos registrados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.2. Periodo de retención para el archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.3. Protección del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.4. Procedimientos de backup del archivo.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.5. Requerimientos para el sellado de tiempo de los registros.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.6. Sistema de recogida de información de auditoría (interno vs externo).
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.5.7. Procedimientos para obtener y verificar información archivada
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.6. Cambio de Clave

No estipulado.

5.7. Recuperación en caso de compromiso de una clave o de desastre

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.1. Alteración de los recursos hardware, software y/o datos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.2. La clave pública de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.3. La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

5.8. Cese de una CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6. Controles de seguridad técnica

6.1. Generación e Instalación del par de claves

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.1 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

6.1.1. Generación del par de claves

El par de claves para el certificado emitido bajo el ámbito de la presente Política de Certificación se generan en HSM del usuario y nunca abandonan el mismo.

6.1.2. Entrega de la clave privada a la entidad

La clave privada para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentra contenida en el HSM y se generan por el subscriptor del certificado.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior del HSM y es entregada a la Autoridad de Certificación por la Autoridad de Registro mediante el envío de una solicitud de certificación en formato PKCS#10, firmada digitalmente por el solicitante.

Si se detecta que la clave pública de la solicitud no cumple los requisitos (clave débil, etc.) será rechazada.

6.1.4. Entrega de la clave pública de la CA a los usuarios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.1.5. Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es:

- Para las claves RSA de al menos 2048 bits.
- Para las claves ECDSA de al menos NIST ECC P-256.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

Se utilizan los parámetros definidos en el documento ETSI TS 119 312 “Electronic Signatures and Infraestructures (ESI); Cryptographic Suites”.

Los parámetros utilizados son los siguientes:

Signature Suite	**Hash Function**	**Padding Method**	**Signature algorithm**
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
sha2-with-ecdsa	SHA-256, SHA-384 or SHA-512		ecdsa

ACCV lleva a cabo la validación de las claves ECC siguiendo el procedimiento definido en NIST SP 800-89

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509v3)

Los certificados emitidos bajo la presente política contienen los atributos"KEY USAGE" y "EXTENDED KEY USAGE", tal como se define en el estándar X.509v3.

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento 1.3 Comunidad de usuarios y ámbito de aplicación.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento *"Perfiles de certificado y listas de certificados revocados"*.

6.1.8. Hardware/software de generación de claves

La generación de las claves se realiza en HSM.

Los requisitos mínimos para estos dispositivos son los especificados por el Ministerio correspondiente que tenga las competencias, y acorde a la normativa técnica europea.

6.2. Protección de la Clave Privada

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la Agencia de Tecnología y Certificación Electrónica.

Se recomienda utilizar sistemas para almacenar las claves privadas que cumplan una serie de requisitos de seguridad físicos y lógicos. ACCV puede solicitar a su discreción que el subscriptor describa los mecanismos utilizados para bastionar dichos sistemas.

ACCV aconseja utilizar las guiás del Centro Criptlógico Nacional (Serie STIC del CCN) para asegurar la seguridad de los sistemas de información y comunicaciones involucrados.

6.2.1. Estándares para los módulos criptográficos

Este punto está siempre referido a las claves que se generan para los certificados emitidos bajo el ámbito de la Política de Certificación vigente. La información sobre los estándares y controles del módulo criptográfico de las entidades que componen las Autoridades de Certificación se encuentra en el apartado 6.2.1 de la Declaración de Prácticas de Certificación (DPC) de la ACCV.

Los dispositivos HSM empleados en la emisión de los certificados adscritos a esta Política de Certificación deben disponer de certificación ITSEC E5 high, FIPS 140-2 nivel 3 o equivalente y soportan los estándares PKCS#11 y CSP.

También se aceptan los HSM certificados por la agencia acreditada para ello a nivel nacional (OC-CCN https://oc.ccn.cni.es/index.php/es/).

La generación de claves se realiza en los HSM.

Los requisitos mínimos para estos dispositivos son los especificados por el Organismo correspondiente que tenga las competencias, y según la normativa técnica europea.

Estos HSMs deben tener la acreditación como Dispositivo Seguro de Creación de Firma / Dispositivo Seguro de Creción de Sellos según la normativa eIDAS (QsigCD/QsealCD).

6.2.2. Control multipersona de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos.

6.2.3. Custodia de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.4. Copia de seguridad de la clave privada

No se custodian claves privadas de los suscriptores de los certificados definidos por la presente política, por lo que no es aplicable.

6.2.5. Archivo de la clave privada.

No se archivan las claves privadas.

6.2.6. Introducción de la clave privada en el módulo criptográfico.

La generación de las claves vinculadas al certificado se realiza en el HSM y nunca la abandonan.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. El almacenamiento de la clave privada dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.8. Método de activación de la clave privada.

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La activación dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.9. Método de desactivación de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La desactivación dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.10. Método de destrucción de la clave privada

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. La destrucción dependerá de los mecanismos del HSM elegido para generar y almacenar las claves.

6.2.11. Clasificación de los módulos criptográficos

Se deben cumplir los requisitos establecidos en la sección 6.2.1.

6.3. Otros Aspectos de la Gestión del par de claves.

6.3.1. Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.3.2. Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de 12 meses como máximo.

La clave utilizada para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de 12 meses como máximo. Esa es la fecha máxima de validez que se admite en la solicitud de los certificados emitidos en virtud de esta Política.

El certificado de ACCVCA-120 es válido desde el día 27 de enero de 2015 hasta el 1 de enero de 2027.

El certificado de ACCV RSA1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

El certificado de ACCV ECC1 TLS es válido desde el día 27 de febrero de 2024 hasta el 23 de febrero de 2039.

6.4. Datos de activación

6.4.1. Generación y activación de los datos de activación

La clave privada es generada por el solicitante y nunca está en posesión de la Agencia de Tecnología y Certificación Electrónica. Los datos de activación dependerán de los mecanismos del HSM elegido para generar y almacenar las claves.

6.4.2. Protección de los datos de activación

El responsable del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.4.3. Otros aspectos de los datos de activación

No hay otros aspectos a considerar.

6.5. Controles de Seguridad Informática

6.5.1. Requerimientos técnicos de seguridad informática específicos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.5.2. Valoración de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6. Controles de Seguridad del Ciclo de Vida.

6.6.1. Controles de desarrollo del sistema

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.2. Controles de gestión de la seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.6.3. Evaluación de la seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.7. Controles de Seguridad de la Red

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

6.8. TimeStamping

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7. Perfiles de certificados y CRL y OCSP

7.1. Perfil de Certificado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.1.1. Número de versión

ACCV utiliza certificados X.509 versión 3 (X.509 v3).

Esta política de certificación especifica el uso de un certificado con dos usos distintos; firma digital, y cifrado de clave.

7.1.2. Extensiones del certificado

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

Campo	**Valor**
Subject	
SerialNumber	NIF de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada la sede.
CommonName	Denominación de nombre de dominio (DNS) donde residirá el certificado. Si aparece debe coincidir con un DNSName del SAN. (OPCIONAL no recomendado)
OrganizationIdentifier (2.5.4.97)	NIF de la entidad, tal como figura en los registros oficiales. Codificado Según la Norma Europea ETSI EN 319 412-1
Organization	Denominación (nombre “oficial”) de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada la sede
Locality	Ciudad
State	Provincia
Country	ES Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
Version	V3
SerialNumber	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	ACCVCA-120 sha256withRSAEncryption ACCV RSA1 TLS sha256withRSAEncryption ACCV ECC1 TLS ecdsa-with-SHA384
Issuer (Emisor)	DN de la CA que emite el certificado (ver punto 7.1.4)
Válido desde	Fecha de Emisión
Válido hasta	Fecha de Caducidad
Clave Pública	Octet String conteniendo la clave pública del certificado de sede
Extended Key Usage	
	Server Authentication

	Client Authentication
CRL Distribution Point	
	ACCVCA-120: http://www.accv.es/fileadmin/Archivos/certificados/accvca120_der.crl ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crl ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crl
SubjectAlternativeName	
	Nombre Dominio DNS de la Sede (si se incluye commonName debe tener el mismo valor)
Opcional	Nombre Dominio DNS de la Sede
Opcional	Nombre Dominio DNS de la Sede
Opcional	Nombre Dominio DNS de la Sede
Opcional	Nombre Dominio DNS de la Sede
Certificate Policy Extensions	
Policy OID	{itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp(7)} 0.4.0.2042.1.7
Policy OID	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)certificate-policies(1) baseline-requirements(2) organization-validated(2)} 2.23.140.1.2.2
Policy OID	2.16.724.1.3.5.5.1
Policy OID	QCP-w Certificado cualificado de sitio web acorde al Reglamento UE 910/2014 itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qncp-web (5)
Policy OID	1.3.6.1.4.1.8149.3.14.6.0
Policy CPS Location	http://www.accv.es/CERT-CUALIFICADO-WEB_ACCV-ISTEC_CIF-A40573396_SPAIN
Authority Information Access	
Access Method	Id-ad-ocsp
Access Location	http://ocsp.accv.es
Access Method	Id-ad-calssuers

Access Location	ACCVCA-120: http://www.accv.es/gestcert/ACCVCA120SHA2.cacert.crt ACCV RSA1 TLS: http://www.accv.es/gestcert/accv_rsa1_tls.crt ACCV ECC1 TLS: http://www.accv.es/gestcert/accv_ecc1_tls.crt	
Fingerprint issuer	Fingerprint del certificado de la CA que emite el certificado (ver CPS)	
Algoritmo de hash	RSA: SHA-256 ECC: SHA-384	
KeyUsage (críticos)		
	RSA: Digital Signature Key Encipherment	ECC: Digital Signature
SCT List ***1.3.6.1.4.1.11129.2.4.2***	Signed Certificate Timestamp List	
QcStatement	**Campos QC (Qualified Certificate)**	
QcCompliance		El certificado es cualificado
QcType	web	Tipo particular de certificado cualificado
QcRetentionPeriod	15y	Periodo de retención de la información material
QcPDS	https://www.accv.es/fileadmin/Archivos/Practicas_de_certificacion/ACCV-PDS-V1.1-EN.pdf	Ubicación de PKI Disclosure Statement
QcSCD		Dispositivo seguro de creación de firma (SSCD)
CA/Browser Forum Organization Identifier Field	cabfOrganizationIdentifier (OID: 2.23.140.3.1) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	
	registrationSchemeIdentifier	3 character Registration Scheme identifier (VAT)
	registrationCountry	2 character ISO 3166 country code (ES)
	registrationStateOrProvince	State or Province (optional)
	registrationReference	Registration Reference allocated in accordance with the identified Registration Scheme (CIF)

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSA (1.2.840.113549.1.1.5)
- SHA256withRSA (1.2.840.113549.1.1.11)
- ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (1.2.840.10045.4.3.3)

7.1.4. Formatos de nombres

Los certificados emitidos por ACCV contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

Los Issuer names admitidos para certificados emitidos bajo esta politica son:

cn=ACCVCA-120,ou=PKIACCV,o=ACCV,c=ES

cn=ACCV RSA1 TLS,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

cn=ACCV ECC1 TLS,2.5.4.97=VATES-A40573396,o=ISTEC,l=BURJASSOT,s=VALENCIA,c=ES

Todos los campos del certificado del Subject y del Subject Alternative Name, exceptuando los que se refieren a nombre DNS o direcciones de correo, se cumplimentan obligatoriamente en mayúsculas, prescindiendo de acentos.

El campo subjectAlternativeName contiene al menos una entrada. Cada entrada en el campo subjectAlternativeName debe ser del tipo dNSName conteniendo el nombre completo cualificado de un sistema.

Subject:

commonName (opcional). Si se incluye debe coincidir con uno de los campos DNSName del subjectAlternativeName

serialNumber (obligatorio). NIF de la entidad, definido en Real Decreto 1065/2007, de 27 de Julio.

OrganizationIdentifier (obligatorio) Identificador de la entidad, siguiendo el formato definido en el estándar europeo ETSI EN 319 412-1

Organization (obligatorio) Designación (nombre oficial) de la Administración, organismo o entidad en nombre de la cual actúa el subscriptor del certificado y propietario del dominio.

locality (obligatorio) Ciudad

state (obligatorio) Estado o provincia

country (obligatorio) Código de país ISO 3166-1

7.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, no ambiguos, descriptivos y diferenciables por suscriptor en el ámbito de la política de emisión.

No hay restricciones definidas por extensión para los certificados emitidos bajo la presente política.

7.1.6. Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por ACCV para identificar la presente política es el siguiente:

1.3.6.1.4.1.8149.3.14.6.0

En este caso se añade un OID para identificar el tipo de entidad que se representa según la definición de los perfiles por la Administración General del Estado.

2.16.724.1.3.5.5.1 Certificado de sede electrónica de nivel alto

En este caso se añade un OID para identificar el tipo de entidad que se representa según la normativa ETSI EN 319 411-2

0.4.0.194112.1.5 **Política de certificación para certificados cualificados EU emitidos a sitios web**

En este caso se añade un OID para identificar el tipo de entidad que se representa según las guiás del CAB/Forum

2.23.140.1.2.2 **Certificates issued in accordance with the CA/Browser Forum's Baseline Requirements - Organization identity asserted**

En este caso se añade un OID para identificar el tipo de entidad que se representa según el estándar ETSI EN 319 411-1

0.4.0.2042.1.7 **Organizational Validation Certificate Policy (OVCP)**

7.1.7. Uso de la extensión "Policy Constraints"

No se hace uso de la extensión "*Policy Constraints*" en los certificados emitidos bajo la presente Política de Certificación.

7.1.8. Sintaxis y semántica de los cualificadores de política

La extensión *CertificatePolicy* puede incluir un campo Calificador de Política,opcional:

CPS Pointer: Contiene la URL donde se publica la Política.

7.1.9. Tratamiento semántico para la extensión "Certificate Policy"

La extensión *CertificatePolicy* identifica la política que define las prácticas que ACCV asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

7.1.10. Lista de Signed Certificate Timestamp (SCT)

Respuestas de logs cualificados conocidos que complan con la política de Transparencia de Certificados de Chrome.

Extensión OID: 1.3.6.1.4.1.11129.2.4.2

RFC 6962 (Certificate Transparency): https://tools.ietf.org/html/rfc6962

Para los certificados con un valor notBefore mayor o igual al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

Certificate lifetime	# of SCTs from separate logs	Maximum # of SCTs per log operator which count towards the SCT requirement
180 days or less	2	1
181 to 398 days	3	2

Para los certificados con un valor notBefore inferior al 21 de abril de 2021 (2021-04-21T00:00:00Z), el número de SCT incrustados se basa en la vida útil del certificado:

Lifetime of Certificate	Number of SCTs from distinct logs
< 15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4

Lifetime of Certificate	Number of SCTs from distinct logs
> 39 months	5

7.2. Perfil de CRL

7.2.1. Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.2.2. CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3. Perfil de OCSP

7.3.1. Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.3.2. Extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8. Auditoría de conformidad

8.1. Frecuencia de los controles de conformidad para cada entidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.2. Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.3. Relación entre el auditor y la entidad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.4. Tópicos cubiertos por el control de conformidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.5. Acciones a tomar como resultado de una deficiencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.6. Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

8.7. Auto auditorias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

Los precios para la emisión inicial y la renovación de los certificados a los que se refiere la presente política de certificación se recogen en la Lista de Tarifas de la Agencia de Tecnología y Certificación Electrónica. Esta Lista se publica en la página web de la ACCV www.accv.es

9.1.2. Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.3. Tarifas de acceso a la información de estado o revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.4. Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.1.5. Política de reintegros

No se prevén reintegros de las cantidades entregadas para el pago de este tipo de certificados.

9.2. Capacidad financiera

9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACCV.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.2.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3. Política de Confidencialidad

9.3.1. Información confidencial.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.2. Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.3.3. Divulgación de información de revocación /suspensión de certificados
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4. Protección de datos personales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.1. Plan de Protección de Datos Personales.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.2. Información considerada privada.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.3. Información no considerada privada.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.4. Responsabilidades.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.5. Prestación del consentimiento en el uso de los datos personales.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.4.7. Otros supuestos de divulgación de la información.
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.5. Derechos de propiedad Intelectual
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6. Obligaciones y Responsabilidad Civil

9.6.1. Obligaciones de la Entidad de Certificación
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.2. Obligaciones de la Autoridad de Registro
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.3. Obligaciones de los suscriptores
Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACCV

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.6.5. Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.7. Renuncias de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8. Limitaciones de responsabilidad

9.8.1. Garantías y limitaciones de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

No obstante no existen límites económicos asociados a las transacciones que se realicen con este tipo de certificados por parte de los suscriptores.

9.8.2. Deslinde de responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.8.3. Limitaciones de pérdidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.9. Indemnizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10. Plazo y finalización.

9.10.1. Plazo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.2. Finalización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.10.3. Supervivencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.11. Notificaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

Todos los correos que la ACCV envíe a los suscriptores de los certificados emitidos bajo esta Política de Certificación, en el ejercicio de la prestación del servicio de certificación, serán firmados digitalmente para garantizar su autenticidad e integridad.

9.12. Modificaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.1. Procedimientos de especificación de cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.2. Procedimientos de publicación y notificación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.12.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13. Resolución de conflictos.

9.13.1. Resolución extrajudicial de conflictos.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.13.2. Jurisdicción competente.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.14. Legislación aplicable

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.15. Conformidad con la Ley aplicable.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16. Cláusulas diversas.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.1. Acuerdo completo

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.2. Asignación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.3. Separabilidad

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.4. Cumplimiento (honorarios de abogados y exención de derechos)

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.16.5. Fuerza mayor

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

9.17. Otras cuestiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

10. Anexo I

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.14
Sección 1 – Datos del solicitante *Apellidos*: *Nombre*: NIF: Tel.: Puesto o cargo: Administración-Organización: CIF de la Organización: *Dirección correo electrónico*: Dirección postal:
Sección 2 – Datos de la sede electrónica Nombre cualificado: Alias (si el certificado no se emite al nombre cualificado): Nombre descriptivo de la sede electrónica: Dirección de correo de contacto:
Sección 3 – *Fecha y Firma* *Suscribo el presente contrato de certificación asociado a la Política de Certificación de Certificados Cualificados de Sede Electrónica Administrativa en dispositivo seguro con código 1.3.6.1.4.1.8149.3.14, emitido por la Agencia de Tecnología y Certificación Electrónica. Declaro conocer y aceptar las normas de utilización de este tipo de certificados que se encuentran expuestas en http://www.accv.es. Declaro, asimismo, que los datos puestos de manifiesto son ciertos.* *Firma del solicitante* Firmat/*Firmado*:

CONTRATO DE CERTIFICACIÓN – CÓDIGO 1.3.6.1.4.1.8149.3.14
Condiciones de utilización de los certificados

1.Los certificados asociados a la Política de Certificación para Certificados Cualificados de Sede Electrónica Administrativa en dispositivo seguro, emitidos por la ACCV son del tipo X.509v3 y se rigen por la Declaración de Prácticas de Certificación de la ACCV, en tanto que Prestador de Servicios de Certificación, así como por la Política de Certificación referida. Ambos documentos se deben interpretar según la legislación de la Comunidad Europea, el Ordenamiento Jurídico Español y la legislación propia de la Generalitat.

2.El solicitante de los certificados debe ser una persona física, en posesión de un certificado reconocido de la Agencia de Tecnología y Certificación Electrónica, y deben estar empleados en una Administración Pública, Ente Instrumental de la Administración o Entidad Corporativa

3.El solicitante de los certificados, especialmente habilitado para la gestión de éstos por parte de una Administración o Entidad pública determinada, es responsable de la veracidad de los datos aportados en todo momento a lo largo del proceso de solicitud y registro. Será responsable de comunicar cualquier variación de los datos aportados para la obtención del certificado.

4.El suscriptor del certificado es responsable de la custodia de su clave privada y de comunicar a la mayor brevedad posible cualquier pérdida o sustracción de esta clave.

5.El suscriptor del certificado es responsable de limitar el uso del certificado a lo dispuesto en la Política de Certificación asociada, que es un documento público y que se encuentra disponible en http://www.accv.es.

6. La Agencia de Tecnología y Certificación Electrónica, no se responsabiliza del contenido de los documentos firmados haciendo uso de los certificados por ella emitidos.

7.La Agencia de Tecnología y Certificación Electrónica, es responsable del cumplimiento de las legislaciones Europea, Española y Valenciana, por lo que a Firma Electrónica se refiere. Es, asimismo, responsable del cumplimiento de lo dispuesto en la Declaración de Prácticas de Certificación de la ACCV y en la Política de Certificación asociada a este tipo de certificados.

8.El periodo de validez de estos certificados es de 12 meses como máximo. Para su renovación deberán seguirse el mismo procedimiento que para la primera solicitud o bien los procedimientos previstos en la Política de Certificación asociada.

9.Los certificados emitidos perderán su eficacia, además de al vencimiento del periodo de validez, cuando se produzca una revocación, cuando se inutilice el soporte del certificado, ante resolución judicial o administrativa que ordene la pérdida de eficacia, por inexactitudes graves en los datos aportados por el solicitante y por fallecimiento del suscriptor del certificado. Otras condiciones para la pérdida de eficacia se recogen en la Declaración de Prácticas de Certificación y en la Política de Certificación asociada a este tipo de certificados.

10.La documentación a aportar para la identificación de la persona física solicitante del certificado será el Documento Nacional de Identidad, NIE o Pasaporte válido y vigente. El solicitante deberá aportar los datos relativos a su relación con la Administración Pública , Ente Instrumental de la Administración o Entidad Corporativa de Derecho Público.

11.En cumplimiento de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Carácter Personal, se informa al solicitante de la existencia de un fichero automatizado de datos de carácter personal, creado bajo la responsabilidad de la Agencia de Tecnología y Certificación Electrónica. La finalidad de este fichero es servir a los usos relacionados con los servicios de certificación que presta la Agencia de Tecnología y Certificación Electrónica. El suscriptor autoriza expresamente el uso de sus datos personales que contiene el fichero, en la medida en que sean necesarios para llevar a cabo las acciones previstas en la Política de Certificación.

12.La Agencia de Tecnología y Certificación Electrónica se compromete a poner los medios a su alcance para evitar la alteración, pérdida o acceso no autorizado a los datos de carácter personal contenidos en el fichero.

13.El solicitante podrá ejercer sus derechos de acceso, rectificación o cancelación sobre sus datos de carácter personal dirigiendo escrito a la Agencia de Tecnología y Certificación Electrónica, a través de cualquiera de los Registros de Entrada de la Generalitat indicando claramente esta voluntad.

Motivos de revocación

Estos son los motivos que podrá utilizar para revocar su certificado:

Sin motivo o sin especificar

El suscriptor no está obligado a proporcionar un motivo de revocación, a menos que su clave privada se haya visto comprometida.

Cambio de los datos de filiación

Se DEBERÍA elegir este motivo de revocación cuando el nombre de su organización u otra información de la organización en el certificado haya cambiado.

Reemplazo

Se DEBERÍA elegir este motivo de revocación cuando se solicita un nuevo certificado para reemplazar un certificado existente.

Cambio de la propiedad de los dominios

Se DEBERÍA elegir este motivo de revocación cuando ya no sea propietario de todos los nombres de dominio en el certificado o cuando ya no vaya a utilizar el certificado porque el sitio web vaya a dejar de estar operativo.

Compromiso de la clave

Se DEBE elegir este motivo de revocación cuando el suscriptor tenga conocimiento o tenga motivos para creer que la clave privada de su certificado se ha visto comprometida. Por ejemplo si una persona no autorizada ha tenido acceso a la clave privada de su certificado. Si se selecciona este motivo SE REVOCARÁN TODOS LOS CERTIFICADOS DEL ORGANISMO EMITIDOS CON LAS MISMAS CLAVES y la ACCV puede contactar con el solicitante para recabar mas información y requerir evidencias adicionales.

Privilegio retirado

La CA detecta que ha habido una infracción del lado del suscriptor que no ha resultado en compromiso de clave, como que el suscriptor del certificado proporcionó información engañosa en su solicitud de certificado o no ha cumplido con sus obligaciones materiales bajo el acuerdo del suscriptor o los términos de uso.

14.Los certificados con el uso de clave serverAuthentication están sujetos a lo definido por el CA/Browser Forum en https://cabforum.org/working-groups/server/baseline-requirements/documents/. Entre la condiciones establecidas se encuentra la obligatoriedad de revocar los certificados si se detecta que la emisión u operación no cumple con lo definido en la normativa. Esta revocación se debe hacer en un plazo máximo de entre uno (1) y cinco (5) días naturales dependiendo del tipo de incidente y no es posible aplazamiento de ningún tipo. Si no es posible cumplir esta condición no se deben utilizar nunca certificados emitidos bajo esta normativa.

Con la firma del presente documento se autoriza a la Agencia de Tecnología y Certificación Electrónica a consultar los datos de identidad que consten en el Ministerio de Interior, evitando que el ciudadano aporte fotocopia de su documento de identidad.