Consorci
Administració Oberta
de Catalunya

Declaració de Pràctiques de Certificació
Entitat de Certificació Ciutadania
(EC-CIUTADANIA)

Referència:	D1111_E0650_N-DPC EC-CIUTADANIA
Versió:	2.0
Data:	09/05/2018

Índex

1. Introducció

1.1. Presentació

1.1.1. Tipus i classes de certificats

El Consorci AOC ha definit una tipologia de serveis de certificació que permeten, a l'EC-CIUTADANIA, emetre certificats digitals per a diversos usos i usuaris finals diferents.

- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que actua en nom i representació del subscriptor o titular del certificat (que pot ser ell mateix o una persona jurídica a la qual estigui vinculat)

D'altra banda, els certificats d'empleat públic són certificats corporatius, caracteritzats pel fet que el posseïdor de la clau privada està vinculat al subscriptor o titular del certificat, que és una organització del sector públic.. La persona física posseïdora de la clau privada estarà identificada en el certificat. Típicament, l'EC-CIUTADANIA emet certificats d'empleat públic pels operadors de la infraestructura (operadors de registre, etc).

El registre de les dades per a l'emissió dels certificats d'empleat públic el realitza l'entitat subscriptora del mencionat certificat, actuant com a entitat de registre interna.

La resta de certificats seran certificats de persona vinculada, emesos en concurrència amb el lliure mercat, i habitualment en règim d'actuació subsidiària, quan no existeixin prestadors que ofereixin el servei o el nombre dels mateixos resulti insuficient per a garantir la seva distribució efectiva als usuaris finals (ciutadans, empreses, profesionals).

El registre de les dades per a l'emissió dels certificats de persona vinculada el realitza una entitat de registre, sota la responsabilitat de l'Entitat de Certificació.

Els certificats de persona vinculada poden ser individuals (quan s'expedeixin a una persona física, actuant en el seu propi nom - com per exemple, als ciutadans per a relacionar-se per mitjans electrònics amb les entitats del sector públic de Catalunya) .

1.1.1.1. Certificats personals

L'EC-CIUTADANIA podrà emetre els següents tipus de certificats personals:

- idCAT certificat: és un certificat qualificat de conformitat amb allò establert a la legislació aplicable, descrita a la secció 9.15 d'aquesta DPC. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permet la generació de la "signatura electrònica avançada"

1.1.1.2. Certificats de proves

De qualsevol dels tipus de certificats que recull la present política es poden emetre, en determinades circumstàncies, certificats de proves.

1.1.2. Relació entre la Declaració de Pràctiques de Certificació (DPC) i altres documents

Aquest document conté la declaració de pràctiques de certificació de l'EC-CIUTADANIA.

L'EC-CIUTADANIA emet certificats dintre de la jerarquia de certificació operada pel Consorci AOC, per tant ha de disposar d'una declaració de pràctiques de certificació, d'acord amb la política general de certificació del Consorci AOC.

Aquesta Declaració de Pràctiques de Certificació (DPC) inclou els procediments que aplica l'EC-CIUTADANIA en la prestació dels seus serveis, en compliment dels requisits establerts per les polítiques que gestiona i la legislació aplicable..

Aquesta DPC és coherent amb allò establert en la Política General de Certificació i fins i tot inclou múltiples referències a aquesta, per a evitar duplicitats allà on la DPC no introdueix informació addicional.

1.2. Nom del document i identificació

1.2.1. Identificació d'aquest document

Aquest document es denomina "Declaració de Pràctiques de Certificació (DPC) de l'EC-CIUTADANIA".

Aquesta Declaració de Pràctiques de Certificació s'identifica amb el següent OID:

1.3.6.1.4.1.15096.1.2.11

1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC

L'EC-CIUTADANIA emet i gestiona certificats d'acord amb les següents polítiques:

Certificats personals:

- **CPISA-2 idCAT** – Certificat de persona física d'identificació, i signatura electrònica avançada, emès per l'EC-CIUTADANIA. Aquests certificats no es podran emetre a partir de l'entrada en vigor de la versió 2.0 d'aquest document.

  OID: 1.3.6.1.4.1.15096.1.3.1.86.2

- **CPISA-2 idCAT adaptat a eIDAS** (REGLAMENT (UE) No 910/2014 DEL PARLAMENT EUROPEU I DEL CONSELL, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i per la qual es deroga la Directiva 1999/93/CE) – Certificat de persona física d'identificació, i signatura electrònica avançada, emès per l'EC-CIUTADANIA

  OID: 1.3.6.1.4.1.15096.1.3.2.86.2

Els documents descriptius d'aquests perfils de certificats es publiquen al web del Consorci AOC.

1.3. Comunitat d'usuaris de certificats

Aquesta declaració de pràctiques de certificació regula una comunitat d'usuaris que obtenen certificats per a poder portar a terme relacions administratives per mitjans electrònics, d'acord amb la llei aplicable i la normativa administrativa corresponent, que es recullen a l'apartat 9.15 Conformitat amb la llei aplicable

L'EC-CIUTADANIA emet certificats idCAT al públic, destinats a ciutadans i ciutadanes catalans majors d'edat, així com a altres persones (col·lectivament anomenats subscriptors) que necessiten relacionar-se amb les entitats que integren el Sector Públic de Catalunya i amb altres institucions.

El certificat idCAT és un certificat qualificat d'acord amb allò establert a la legislació aplicable, descrita a la secció 9.15 d'aquesta DPC.

1.3.1. Prestadors de serveis de certificació

Un prestador de serveis de certificació és una persona física o jurídica que produeix certificats i presta altres serveis en relació amb la signatura electrònica, d'acord amb la Llei aplicable, descrita a 9.15. Conformitat amb la llei aplicable.

El Consorci AOC serà el prestador de serveis de certificació de l'EC-CIUTADANIA.

Conforme a aquesta funció, el Consorci AOC serà responsable per l'actuació de l'EC-CIUTADANIA davant els usuaris finals i els tercers verificadors de certificats i signatures electròniques.

1.3.2. Entitat de Certificació Arrel

El Consorci AOC disposa d'una autoritat de certificació principal, que és l'arrel de la jerarquia pública de certificació de Catalunya: l'EC-ACC, la finalitat de la qual és integrar altres entitats de certificació en el sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

1.3.3. EC-CIUTADANIA

L'EC-CIUTADANIA és l'Entitat de Certificació per a dotar de certificats digitals als ciutadans i ciutadanes catalanes majors d'edat, així com a altres persones (col·lectivament anomenats subscriptors) que necessiten relacionar-se amb les entitats que integren el Sector Públic de Catalunya i amb altres institucions.

L'EC-CIUTADANIA està vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya i emet els certificats indicats en el punt 1.1.1.

1.3.4. Entitats de Registre

Conforme a allò establert a la Política General de Certificació, les Entitats de Registre assisteixen a les Entitats de Certificació Vinculades en determinats procediments i relacions

amb els sol·licitants i subscriptors de certificats, especialment en els tràmits d'identificació, registre i autenticació dels subscriptors dels certificats i dels posseïdors de claus.

El Consorci AOC és responsable del procés de creació d'entitats de registre de l'EC-CIUTADANIA: exigeix la formalització de l'instrument jurídic pertinent; i verifica que l'Entitat de Registre compta amb els recursos materials i humans necessaris; i que ha designat i ha format al personal que serà responsable de l'emissió de certificats (els denominats operadors de l'entitat de registre). Així mateix, el Consorci AOC és responsable de l'emissió dels certificats d'operador que aquests necessitaran per a poder operar (típicament seran CIPISQ); i validarà les peticions de certificats per a operadors de les Entitats de Registre examinant la sol·licitud i fent les comprovacions necessàries per al compliment de la Política General de Certificació i d'aquesta Declaració de Pràctiques de Certificació.

1.3.5. Usuaris finals

Els usuaris finals són les persones (físiques o jurídiques) que obtenen i/o utilitzen els certificats personals emesos per l'EC-CIUTADANIA; concretament, podem distingir els següents usuaris finals:

- Els sol·licitants de certificats: són persones majors d'edat que sol·liciten els certificats. Poden fer-ho:
    a) Les persones que seran els futurs subscriptors dels certificats
    b) Altres persones autoritzades - documentalment – pels futurs subscriptors (representants)
- Els subscriptors o titulars de certificats: per tractar-se de certificats individuals personals, són les persones físiques identificades en el camp "Subject" dels certificats. Tenen llicència d'ús del certificat
- Els posseïdors de claus: són els subscriptors dels certificats, de conformitat amb allò establert a la Política General de Certificació
- Els verificadors dels certificats: són les persones que reben signatures electròniques i/o certificats digitals i han de verificar-los, com a pas previ a confiar en ells, de conformitat amb allò establert a la Política General de Certificació

1.4. Ús dels certificats

Aquesta secció llista les aplicacions per a les quals pot utilitzar-se cada tipus de certificat, establint limitacions, i prohibeix algunes aplicacions dels certificats.

1.4.1. Usos típics dels certificats

Els certificats idCAT de signatura avançada són certificats qualificatsd'acord amb allò establert a la legislació aplicable, tal com es descriu a la secció 9.15 d'aquesta DPC, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Els certificats idCAT no funcionen necessàriament amb dispositius qualificats de creació de signatura electrònica d'acord amb dita legislació aplicable.

Els certificats idCAT garanteixen la identitat del subscriptor, resultant idonis per a oferir suport a la signatura electrònica avançada.

Encara que la signatura electrònica avançada no s'equipara directament a la signatura escrita, aquesta equiparació es pot produir igualment en virtut d'un contracte de signatura electrònica o d'una norma jurídica específica (per exemple l'"ORDRE HAC/1181/2003, de 12 de maig, per la que s'estableixen normes específiques sobre l'ús de la signatura electrònica en les relacions tributàries per mitjans electrònics, informàtics i telemàtics amb l'Agència Estatal d'Administració Tributària"), que establirà les condicions addicionals necessàries perquè es produeixi aquesta equiparació.

A més, es poden utilitzar per a diversos usos, entre els que es poden indicar els següents:

- Identificació remota, basada en presentació de la credencial
- Autenticació per mitjans electrònics davant sistemes de control d'accés

1.4.2. Aplicacions prohibides

1.4.2.1. Informacions per a tots els tipus de certificats

Els certificats no s'han dissenyat, no es poden destinar i no s'autoritza el seu ús o revenda com a equips de control de situacions perilloses o per a usos que requereixen actuacions a prova d'errors, com el funcionament d'instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error podria directament comportar la mort, lesions personals o danys mediambientals severs.

1.4.2.2. Certificats personals

Els certificats personals emesos per l'EC-CIUTADANIA – els perfils dels quals es relacionen a l'apartat *Identificació de polítiques de certificació cobertes per aquesta DPC* – no podran utilitzar-se per als fins descrits a la Política General de Certificació, apartat *Aplicacions prohibides*.

1.5. Administració de la Declaració de Pràctiques

1.5.1. Organització que administra l'especificació

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2. Dades de contacte de l'organització

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

Adreça postal comercial: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Web del Consorci AOC: `www.aoc.cat`

Web del Servei SCD del Consorci AOC:

http://web.aoc.cat/blog/serveis/catcert-er-idcat/

Web del servei idCAT del Consorci AOC: www.idcat.cat

Servei d'Atenció a l'Usuari: 902 901 080, en horari 24x7 per a la gestió de suspensions de certificats.

1.5.3. Persona que determina la conformitat d'una Declaració de Pràctiques de Certificació (DPC) amb la política

La persona que determina la conformitat d'una DPC amb la Política General de Certificació és el/la Responsable del Servei SCD del Consorci AOC,

1.5.4. Procediment d'aprovació

El sistema documental i d'organització de l'EC-CIUTADANIA garanteix, mitjançant l'existència i l'aplicació dels corresponents procediments, el correcte manteniment de la Declaració de pràctiques de certificació i de les especificacions de servei relacionades amb ella.

Això inclou el procediment de modificació d'especificació del servei i el procediment de publicació d'especificacions de servei.

La versió inicial d'aquesta Declaració de pràctiques és aprovada per la Comissió Executiva del Consorci AOC, que és l'òrgan col·legiat de direcció executiva del Consorci.

El Director Gerent del Consorci AOC és competent per a aprovar les successives modificacions d'aquesta Declaració de pràctiques.

2. Publicació d'informació i directori de certificats

2.1. Directori de certificats

Conforme a allò establert a la Política General de Certificació.

2.2. Publicació d'informació de l'EC-CIUTADANIA

Conforme a allò establert a la Política General de Certificació.

2.3. Freqüència de publicació

La informació de l'EC-CIUTADANIA es publica quan es troba disponible i, en especial, de forma immediata quan s'emeten les mencions relatives a la vigència dels certificats.

Els canvis en aquest document es regeixen per allò establert a la secció 9.12.1 *Procediment per a les modificacions.*

Passats 15 (quinze) dies des de la publicació de la nova versió, es retira la referència al canvi de la pàgina principal i s'insereix en el directori.

Les versions antigues de la documentació són conservades per un període de 15 (quinze) anys per l'EC-CIUTADANIA, podent ésser consultades pels interessats.

La informació d'estat de revocació de certificats es publica d'acord amb allò establert a la secció 4.9.7 *Freqüència d'emissió de llistes de revocació de certificats (CRL's).*

2.4. Control d'accés

Conforme a allò establert a la Política General de Certificació.

3. Identificació i autenticació

3.1. Gestió de noms

En aquesta secció s'estableixen requisits relatius als procediments d'identificació i autenticació que s'utilitzen durant les operacions de registre que realitzen, amb anterioritat a l'emissió i al lliurament de certificats, les Entitats de Registre.

3.1.1. Tipus de noms

Conforme a allò establert a la Política General de Certificació.

3.1.2. Significat dels noms

Conforme a allò establert a la Política General de Certificació.

3.1.3. Utilització d'anònims i pseudònims

No es poden utilitzar anònims ni pseudònims.

3.1.4. Interpretació de formats de noms

Sense estipulació addicional.

3.1.5. Unicitat dels noms

Conforme a allò establert a la Política General de Certificació.

3.1.6. Resolució de conflictes relatius a nom

Conforme a allò establert a la Política General de Certificació.

Referent al tractament de marques registrades, veure l'apartat 9.5.3.

3.2. Validació inicial de la identitat

3.2.1. Prova de possessió de clau privada

Conforme a allò establert a la Política General de Certificació.

3.2.2. Autenticació de la identitat d'una organització

3.2.2.1. Entitats de Registre

Conforme a allò establert a la Política General de Certificació.

3.2.2.2. Les entitats subscriptores de certificats

No aplica, donat que l'EC-CIUTADANIA no emet certificats corporatius.

3.2.3. Autenticació de la identitat d'una persona física

Aquesta secció conté informacions per a la comprovació de la identitat d'una persona física identificada en un certificat.

L'acreditació de la identitat es pot realitzar directament davant les Entitats de Registre, mitjançant el procés de pre-validació, en el que el sol·licitant consigna les dades directament als operadors, els quals les validen, contrastant-los amb els documents originals aportats (NIF, NIE, passaport o DNI d'altres països) i, si són correctes, els introdueixen en el sistema i procedeixen a emetre el certificat.

El sol·licitant també pot consignar les seves dades identificatives a la web idCAT del Consorci AOC. Posteriorment, el sol·licitant es persona davant una Entitat de Registre, que pot ser la més propera al seu domicili, i presenta la documentació identificativa que ha indicat a la sol·licitud (NIF, NIE, passaport o DNI d'altres països) a un operador de registre, aportant també, en els casos que sigui necessari una fotocòpia d'aquest document i, si ho desitja, una còpia impresa del formulari de confirmació de dades que li va mostrar la web al final del procés de sol·licitud.

Els documents identificatius que aporti el sol·licitant han d'estar en vigor. Quan estiguin en procés de renovació, haurà d'aportar el resguard de renovació; i si aquest no conté fotografia, podrà completar-se la verificació de la identitat utilitzant el document caducat.

L'operador de l'Entitat de Registre valida, mitjançant la fotografia, que el document identificatiu aportat pertany al sol·licitant; també comprovarà que aquest és major d'edat.

Seguidament, es dona al titular el document de compareixença o full de lliurament, que inclou les dades de la sol·licitud del certificat, perquè el sol·licitant el signi.

L'operador comprovarà també que la signatura que el subscriptor acaba de realitzar en la sol·licitud de certificat correspongui a la signatura que consta en el document identificatiu (NIF, NIE, passaport o DNI d'altres països).

Si totes aquestes comprovacions són satisfactòries, es valida la sol·licitud en el sistema informàtic, enviant-la electrònicament i de forma segura a l'EC-CIUTADANIA.

3.2.3.1. Necessitat de presència personal

Conforme a allò establert a la Política General de Certificació.

3.2.4. Informació no verificada

L' idCAT Certificat inclou informació del subscriptor no verificada, com l'adreça de correu electrònic d'aquest.

3.3. Identificació i autenticació de sol·licituds de renovació

3.3.1. Validació per a la renovació de certificats

Tant si es tracta d'una renovació ordinària, com si és posterior a la revocació del certificat a renovar, el procés a seguir per a la renovació d'un certificat serà el mateix que per a l'emissió de certificats nous: l'EC-CIUTADANIA haurà de comprovar – mitjançant la intervenció d'una Entitat de Registre - que la informació utilitzada per a verificar la identitat i la resta de dades del subscriptor continuen sent vàlides.

Si qualsevol informació del subscriptor o del posseïdor de la clau ha canviat, es registrarà adequadament la nova informació, d'acord amb allò establert a la secció 3.2 *Validació inicial de la identitat*.

4. Característiques d'operació del cicle de vida dels certificats

Nota: el terme "notificació" s'utilitza en aquest document com equivalent de "comunicació", a excepció de les tramitacions documentals amb altres organismes públics exigibles per la legislació aplicable.

4.1. Sol·licitud d'emissió de certificat

La sol·licitud és el primer pas que ha de fer el subscriptor per a aconseguir els certificats per al seu ús personal.

Els ciutadans que desitgin obtenir unidCAT certificat poden visitar la web del servei idCAT del Consorci AOC o personar-se directament en les oficines de qualsevol de les entitats de registre (Ajuntaments, Diputacions, etc.) que ofereixen aquesta possibilitat, emplenar el formulari de sol·licitud i seguir les instruccions que allà s'indiquen.

4.1.1. Legitimació per a sol·licitar l'emissió

Conforme a allò establert a la Política General de Certificació.

4.1.2. Procediment d'alta; Responsabilitats

L'EC-CIUTADANIA, mitjançant la participació de les Entitats de Registre, s'assegura que les sol·licituds de certificats són completes, precises i estan degudament autoritzades.

Un cop que l'operador de registre ha comprovat favorablement la identitat del sol·licitant, ha verificat la documentació acreditativa presentada per ell i aquest ha signat el document de compareixença, l'operador signa la sol·licitud autoritzant-la i la remet a l'EC-CIUTADANIA.

Per a les sol·licituds emplenades via web, prèviament a la personació del sol·licitant davant una Entitat de Registre: si durant l'acte de personació l'operador de registre detecta algun error en les dades introduïdes – al comparar-les amb la documentació identificativa que es presenta – l'operador podrà introduir els canvis que siguin necessaris, sempre que quedi constància documentada de l'origen del canvi; per a això demanarà al sol·licitant que signi un document de rectificació de dades.

4.2. Processament de la sol·licitud de certificació

Quan l'EC-CIUTADANIA rep una sol·licitud de certificat autoritzada per una Entitat de Registre, recupera la corresponent sol·licitud de la taula de sol·licituds, l'emmagatzema en l'estructura de certificats i la signa, completant així la generació del certificat.

4.2.1. Accions de l'EC-CIUTADANIA durant el procés d'emissió

Nota: Els procediments establerts en aquesta secció també s'apliquen en cas de renovació de certificats, ja que la renovació implica l'emissió d'un nou certificat.

Per a cada sol·licitud de certificat tramesa, l'EC-CIUTADANIA actuarà conforme a allò establert a l'efecte en la Política General de Certificació – apartat 4.3.1 *Accions de l'Entitat de Certificació durant els processos d'emissió i renovació.*

4.2.2. Comunicació de l'emissió al subscriptor

L'EC-CIUTADANIA comunicarà al sol·licitant l'aprovació o denegació de la sol·licitud de certificat cursada.

En cas que hagi estat aprovada, també comunicarà – quan correspongui - al futur posseïdor de claus, per correu electrònic, que s'ha generat el certificat, que es troba disponible i la forma d'obtenir-lo.

Per a obtenir el certificat, el subscriptor ha d'accedir a la pàgina web que s'indica en el correu electrònic mencionat i seguir les instruccions que aquest detalla per a descarregar el certificat.

4.3. Acceptació del certificat

En determinats casos, l'EC-CIUTADANIA és responsable de crear el parell de claus criptogràfiques dels certificats idCAT Certificat que emet; i sempre és responsable de generar el certificat digital corresponent.

L'EC-CIUTADANIA generarà el full de sol·licitud d'emissió del certificat, perquè sigui signat pel futur posseïdor de claus, conforme a allò establert a la Política General de Certificació. De manera que, en el mateix acte, quedi constància documentada:

- de la seva compareixença
- de la veracitat i correcció de les dades que consten en la sol·licitud
- de la seva acreditació mitjançant documentació identificativa
- que ha sigut informat de la política de protecció de dades del Consorci AOC en relació als certificats que emet l'EC-CIUTADANIA
- de la seva conformitat amb la Declaració de Pràctiques de Certificació de l'EC-CIUTADANIA
- i de la seva acceptació del certificat que sol·licita

4.3.1. Responsabilitats de l'Entitat de Registre

4.3.1.1. Per a Certificats personals

L'EC-CIUTADANIA delega en les entitats de registre(més concretament en la figura del responsable d'aquestes entitats de registre) algunes de les seves responsabilitats referents al procés de lliurament i acceptació dels certificats digitals que emet.

Concretament, el responsable de l'entitat de registre haurà de:

- informar al posseïdor de les claus de les seves obligacions i responsabilitats en relació al certificat que li lliura
- recollir del posseïdor de les claus el reconeixement de l'acceptació del certificat, mitjançant la signatura del full de sol·licitud descrita anteriorment

- custodiar durant 15 anys un exemplar del full de sol·licitud i acceptació del certificat, degudament signada pel posseïdor de les claus

4.3.2. Conducta que constitueix acceptació del certificat

El certificat s'accepta mitjançant la signatura, per part del posseïdor de claus, del full de sol·licitud i acceptació del certificat.

També es considera la possibilitat d'acceptar el certificat mitjançant un mecanisme telemàtic d'activació del certificat.

4.3.3. Publicació del certificat

Conforme a allò establert a la Política General de Certificació.

4.3.4. Notificació de l'emissió a tercers

No aplicable.

4.4. Ús del parell de claus i del certificat

4.4.1. Ús per part dels posseïdors de claus

Conforme a allò establert a la Política General de Certificació.

4.4.2. Ús pel tercer que confia en certificats

Conforme a allò establert a la Política General de Certificació.

D'altra banda, donat que els usos previstos del certificat idCAT són administratius (en els quals el tercer que confia és una entitat pública), quan el tercer verificador que vulgui permetre l'ús de l'idCAT en els seus sistemes no sigui una d'aquestes entitats, haurà de signar un conveni específic d'extensió de l'ús del certificat, que permetrà al Consorci AOC assumir el risc corresponent.

4.5. Renovació de certificats sense renovació de claus

No es permet la renovació de certificats sense renovació de claus.

4.6. Renovació de certificats amb renovació de claus

Conforme a allò establert a la Política General de Certificació.

4.7. Renovació telemàtica

Conforme a allò establert a la Política General de Certificació.

4.8. Modificació de certificats

El subscriptor d'un certificat emès per l'EC-CIUTADANIA solament pot modificar les dades de contacte associades al certificat que el Consorci AOC utilitza per a enviar-li informació relativa a la gestió d'aquest (com per exemple, l'adreça de correu electrònic en què vol rebre els avisos de pròxima caducitat del certificat). Però en cap cas es pot modificar la informació continguda en el certificat; a tots els efectes, la modificació d'aquesta comporta la revocació i l'emissió d'un nou certificat.

Per a poder canviar les dades de contacte, el posseïdor de les claus ha de sol·licitar-ho a través de la web del servei idCAT, seleccionant el certificat i introduint les dades noves.

4.9. Revocació i suspensió de certificats

4.9.1. Causes de revocació de certificats

Conforme a allò establert a la Política General de Certificació.

4.9.2. Legitimació per a sol·licitar la revocació

Pot sol·licitar la revocació d'un certificat:

- El subscriptor a nom del qual es va emetre el certificat
- L'Entitat de Registre que va intervenir en l'emissió
- L'EC-CIUTADANIA

4.9.3. Procediments de sol·licitud de revocació

La sol·licitud de revocació ha d'incloure la informació suficient per a poder identificar raonablement, a criteri de l'EC-CIUTADANIA, d'una banda el certificat que se sol·licita revocar i, de l'altra, l'autenticitat i l'autoritat del sol·licitant. Com a mínim, les dades de contacte del posseïdor de claus, número de NIF o d'altre document identificatiu acceptat, la data i el motiu de la petició, així com el número de sèrie del certificat.

La sol·licitud de revocació ha de ser lliurada personalment, enviada per correu electrònic signat o per correu postal certificat signat.

La petició de revocació, amb la documentació necessària, és recollida, registrada i comunicada per l'Entitat de Registre. Es comprova que la documentació sigui suficient i s'autentica i autoritza al sol·licitant.

Si tot és correcte, un operador de registre porta a terme la revocació efectiva, mitjançant l'aplicació informàtica corresponent. I a continuació, de forma automàtica i immediata, s'indica aquesta revocació en l'estat del certificat en la llista de revocacions.

La sol·licitud i la documentació adjunta s'arxiven.

4.9.4. Termini temporal de sol·licitud de revocació

Conforme a allò establert a la Política General de Certificació.

4.9.5. Termini màxim de processament de la sol·licitud de revocació

Conforme a allò establert a la Política General de Certificació.

4.9.6. Obligació de consulta d'informació de revocació de certificats

Conforme a allò establert a la Política General de Certificació.

4.9.7. Freqüència d'emissió de llistes de certificats revocats (LCRs)

Conforme a allò establert a la Política General de Certificació.

4.9.8. Període màxim de publicació d'LRCs

Conforme a allò establert a la Política General de Certificació.

4.9.9. Disponibilitat de serveis de comprovació d'estat de certificats

Conforme a allò establert a la Política General de Certificació.

4.9.10. Obligació de consulta de serveis de comprovació d'estat de certificats

Conforme a allò establert a la Política General de Certificació.

4.9.11. Altres formes d'informació de revocació de certificats

Sense estipulació addicional.

4.9.12. Requeriments especials en cas de compromís de la clau privada

Conforme a allò establert a la Política General de Certificació.

4.9.13. Causes de suspensió de certificats

A més de per les causes previstes a la Política General de Certificació, l'EC-CIUTADANIA pot suspendre un certificat quan no hagi estat descarregat des de la web en la qual l'EC el deixa a disposició del subscriptor en un termini de 90 dies, comptats des de la seva data d'emissió.

També quan se superin els 10 intents fallits de descàrrega des d'aquesta mateixa web.

4.9.14. Efecte de la suspensió de certificats

Conforme a allò establert a la Política General de Certificació.

4.9.15. Qui pot sol·licitar la suspensió

Pot sol·licitar la suspensió d'un certificat:

- El subscriptor a nom del qual s'ha emès el certificat
- L'EC-CIUTADANIA
- Un tercer interessat legitimat per actuar en defensa dels interessos del subscriptor.

4.9.16. Procediments de sol·licitud de suspensió

L'EC-CIUTADANIA determina a continuació els procediments i els mecanismes d'accés als sistemes de suspensió, informant en tot cas al subscriptor d'acord amb allò previst a la lei aplicable descrita a l'apartat 9.15. Conformitat amb la legislació aplicable.

1) En un primer cas, el subscriptor d'un certificat idCAT fa una trucada al telèfon del Centre d'Atenció a l'Usuari (CAU) del Consorci AOC. El subscriptor s'identifica davant l'operador del CAU indicant-li el número del document identificatiu (NIF, NIE, passaport o DNI d'altres països) amb el qual va sol·licitar el certificat.

   Per a iniciar la suspensió es requereix la següent informació:

   - Data i hora de la sol·licitud de la suspensió
   - Identitat del subscriptor que sol·licita la suspensió
   - Informació de contacte de l'entitat que sol·licita la suspensió
   - Nom i cognoms del posseïdor de claus a qui se li ha de suspendre el certificat digital
   - DNI del posseïdor de claus a qui se li ha de suspendre el certificat digital
   - Número de sèrie (serial number) del certificat digital que se sol·licita suspendre
   - Raó detallada de la petició de suspensió
   -

2) L'operador introdueix aquest número de document identificatiu en la corresponent aplicació informàtica i, apareixent-li totes les dades del titular del certificat que pot comprovar amb la persona que va realitzar la trucada, li planteja la pregunta de desafiament que el subscriptor va fer i va respondre en el moment de realitzar la

sol·licitud del certificat. Si respon correctament, l'operador considera validada la sol·licitud de suspensió.

3) El titular del certificat rep un correu electrònic pel qual se li comunica que s'ha suspès el seu certificat; les passes a seguir per a habilitar-lo de nou; i que, si no l'habilita en els 120 dies següents, el seu certificat serà revocat automàticament.

4.9.17. Període màxim de suspensió

Conforme a allò establert a la Política General de Certificació.

4.9.18. Habilitació d'un certificat suspès

El subscriptor o una persona legitimada per sol·licitar la suspensió, podrà sol·licitar l'habilitació del certificat que roman suspès, personant-se i identificant-se davant d'una Entitat de Registre i signant el corresponent document de sol·licitud d'habilitació comunicant que s'ha extingit el motiu que va provocar la suspensió.

4.10. Serveis de comprovació d'estat de certificats

4.10.1. Característiques d'operació dels serveis

Les CLR's es publiquen als servidors dell Consorci AOC i en les URLs indicades en els certificats emesos.

De forma alternativa, els verificadors podran consultar els certificats publicats en el directori de l'EC-CIUTADANIA.

4.10.2. Disponibilitat dels serveis

Conforme a allò establert a la Política General de Certificació.

4.10.3. Altres funcions dels serveis

Sense estipulació addicional.

4.11. Finalització de la subscripció

Conforme a allò establert a la Política General de Certificació.

4.12. Dipòsit i recuperació de claus

No es practica.

5. Controls de seguretat física, de gestió i d'operacions

5.1. Controls de seguretat física

Conforme a allò establert a la Política General de Certificació.

5.1.1. Localització i construcció de les instal·lacions

Conforme a allò establert a la Política General de Certificació.

5.1.2. Accés físic

Conforme a allò establert a la Política General de Certificació.

5.1.3. Electricitat i aire condicionat

Conforme a allò establert a la Política General de Certificació.

5.1.4. Exposició a l'aigua

Conforme a allò establert a la Política General de Certificació.

5.1.5. Advertència i protecció d'incendis

Conforme a allò establert a la Política General de Certificació.

5.1.6. Emmagatzematge de suports

Conforme a allò establert a la Política General de Certificació.

5.1.7. Tractament de residus

Conforme a allò establert a la Política General de Certificació.

5.1.8. Còpia de seguretat fora de les instal·lacions

Conforme a allò establert a la Política General de Certificació.

5.2. Controls de procediments

L'EC-CIUTADANIA garanteix que els seus sistemes s'operen de forma segura i, per això, estableix i implanta procediments per a les funcions que afecten a la provisió dels seus serveis.

El personal al servei de l'EC-CIUTADANIA realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'EC-CIUTADANIA. Aquesta política de seguretat ofereix suport a rols amb diferents privilegis.

5.2.1. Funcions fiables

Conforme a allò establert a la Política General de Certificació.

Les funcions i obligacions fiables es defineixen a la secció 5.3 d'aquest document.

5.2.2. Nombre de persones per tasca

Conforme a allò establert a la Política General de Certificació.

5.2.3. Identificació i autenticació per a cada funció

Conforme a allò establert a la Política General de Certificació.

5.2.4. Rols que requereixen separació de tasques

Conforme a allò establert a la Política General de Certificació.

5.3. Controls de personal

L'EC-CIUTADANIA té en compte els següents aspectes:

- Es manté confidencialitat de la informació, posant els mitjans necessaris i mantenint una actitud adequada en el desenvolupament de les seves funcions i, fora de l'àmbit laboral, en allò referent a la seguretat de les infraestructures
- Ésser diligent i responsable en el tractament, manteniment i custòdia dels actius de la infraestructura identificats a la política, en els plans de seguretat o en aquest document
- No es revela informació no pública fora de l'àmbit de la infraestructura, ni s'extreuen suports d'informació a nivells de seguretat inferiors
- Es reporta al Responsable de Seguretat, el més aviat possible, qualsevol incident que es consideri que afecta a la seguretat de la infraestructura o que limiti la qualitat de servei
- S'utilitzen els actius de la infraestructura per a les finalitats que els han sigut encomanades
- S'exigeixen manuals o guies d'usuari dels sistemes que utilitza, que permeten desenvolupar la seva funció correctament
- S'exigeix documentació escrita que marqui les seves funcions i mesures de seguretat a les que està sotmès

- El responsable de seguretat vetlla perquè el punt anterior sigui executat, proveint als responsables d'àrea de tota la informació que sigui necessària
- No s'instal·len en cap dels sistemes de la infraestructura, software o hardware que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació
- No s'accedeix voluntàriament, ni s'elimina o altera informació no destinada a la seva persona o perfil professional

El personal afectat per aquesta normativa és:

- el Responsable del Servei de Certificació Digital
- el Responsable de l'EC-CIUTADANIA
- el Responsable de Seguretat
- el Responsable d'Operacions
- l'Operador de Cerimònies de Claus
- l'Equip tècnic d'administració, operació i explotació
- els Administradors de la xarxa
- i els Operadors de les Entitats de Registre

A més, es veu afectat el següent personal del Consorci AOC:

- qui fa les peticions dels certificats
- qui fa l'aprovació i validació de les peticions de certificats
- qui fa la generació / personalització de certificats
- qui custodia les claus o tokens criptogràfiques
- qui custodia les claus o combinacions de seguretat d'accés a la sala d'operacions
- qui accedeix a informació classificada
- el personal de comunicacions i operacions
- el personal de seguretat (física i lògica) involucrats en l'operació
- el responsable del servei

5.3.1. Requisits d'historial, qualificacions, experiència i autorització

Conforme a allò establert a la Política General de Certificació.

5.3.2. Requisits de formació

Conforme a allò establert a la Política General de Certificació.

El Consorci AOC, a més, proporciona a tot el personal involucrat en les operacions de les Entitats de Registre de l'EC-CIUTADANIA, una informació adequada, que inclou els procediments de treball i els de seguretat.

També es realitza instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències al personal intern.

5.3.3. Requisits i freqüència d'actualització formativa

Conforme a allò establert a la Política General de Certificació.

5.3.4. Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5. Sancions per accions no autoritzades

Conforme a allò establert a la Política General de Certificació.

5.3.6. Requisits de contractació de professionals

Conforme a allò establert a la Política General de Certificació.

5.3.7. Subministrament de documentació al personal

Conforme a allò establert a la Política General de Certificació.

5.4. Procediments d'auditoria de seguretat

5.4.1. Tipus d'esdeveniments registrats

Conforme a allò establert a la Política General de Certificació.

5.4.2. Freqüència de tractament de registres d'auditoria

Conforme a allò establert a la Política General de Certificació.

5.4.3. Període de conservació de registres d'auditoria

Conforme a allò establert a la Política General de Certificació.

5.4.4. Protecció dels registres d'auditoria

Conforme a allò establert a la Política General de Certificació.

5.4.5. Procediments de còpies de seguretat

Conforme a allò establert a la Política General de Certificació.

Amb la finalitat de conservar correctament les còpies de seguretat s'han implantat els següents punts:

- Es guarden en armaris ignífugs
- Només persones autoritzades disposen d'accés a les còpies de seguretat
- Les còpies estan identificades

- Si un material ha contingut còpies de seguretat (usb,, dvd's...) i es volen reutilitzar, s'assegura que les dades que ha contingut siguin totalment esborrades, fent impossible la seva recuperació
- S'autoritza expressament l'extracció de les còpies de seguretat fora de l'Entitat de Registre, emplenant una fitxa al respecte i anotant el corresponent detall en un llibre de registre
- Es procura anar dipositant còpies de seguretat periòdicament fora de l'Entitat de Registre

5.4.6. Localització del sistema d'acumulació de registres d'auditoria

Conforme a allò establert a la Política General de Certificació.

5.4.7. Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment

Conforme a allò establert a la Política General de Certificació.

5.4.8. Anàlisi de vulnerabilitats

Conforme a allò establert a la Política General de Certificació.

5.5. Arxiu d'informacions

Conforme a allò establert a la Política General de Certificació.

5.5.1. Tipus d'esdeveniments registrats

L'EC-CIUTADANIA guarda registres de tots els esdeveniments que tinguin lloc durant el cicle de vida d'un certificat, incloent la renovació d'aquest.

L'EC-CIUTADANIA guarda un registre del següent:

Documents originals:

- Formulari de sol·licitud de certificats
- Full de lliurament de subscriptor de certificats

5.5.2. Període de conservació de registres

L'EC-CIUTADANIA guarda els registres especificats a la secció 5.5.1 durant 15 anys, comptats des del moment d'expedició del certificat.

5.5.3. Protecció de l'arxiu

Conforme a allò establert a la Política General de Certificació.

5.5.4. Procediments de còpia suport

Es fan còpies de seguretat dels logs d'accés lògic al sistema operatiu de l'LRA. S'encarrega un tècnic de comunicacions del Consorci AOC.

Aquestes còpies de seguretat es realitzen amb una periodicitat mensual i es guarden en format CD, i aquests discos en una caixa forta present a la mateixa sala.

Es realitzen també còpies de seguretat de les personalitzacions per al Consorci AOC de les aplicacions que donen suport a la PKI. Aquestes còpies les guarda el Consorci AOC a les seves instal·lacions.

5.5.5. Requisits de segellat de data i hora

Conforme a allò establert a la Política General de Certificació.

5.5.6. Localització del sistema d'arxiu

L'EC-CIUTADANIA té un sistema d'emmagatzemament de dades d'arxiu fora de les seves pròpies instal·lacions, així com s'especifica a la secció 5.1.8.

5.5.7. Procediments d'obtenció i verificació d'informació d'arxiu

Conforme a allò establert a la Política General de Certificació.

5.6. Renovació de claus

Els certificats de l'EC-CIUTADANIA renovats es comuniquen als usuaris finals, mitjançant la seva publicació a la pàgina web del Servei SCD del Consorci AOC.

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromisos

L'EC-CIUTADANIA estableix els procediments que aplica en la gestió de les incidències que afecten les seves claus i, molt especialment, en els compromisos de la seguretat de les claus.

5.7.2. Corrupció de recursos, aplicacions o dades

Quan tingui lloc un esdeveniment de corrupció de recursos, aplicacions o dades, l'EC-CIUTADANIA inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per a fer que el sistema torni al seu estat normal de funcionament.

5.7.3. Compromís de la clau privada de l'Entitat

El pla de continuïtat de negoci de l'EC-CIUTADANIA (o pla de recuperació de desastres) considera el compromís o la sospita de compromís de la clau privada de l'EC-CIUTADANIA com un desastre.

En cas de compromís, l'EC-CIUTADANIA:

- Informa a tots els subscriptors i verificadors del compromís
- Indica que els certificats i la informació de l'estat de revocació lliurats usant la clau de l'EC-CIUTADANIA ja no són vàlids

5.7.4. Desastre sobre les instal·lacions

L'EC-CIUTADANIA desenvolupa, manté, prova i, si és necessari, executa un pla d'emergència en cas de desastre, ja sigui per causes naturals o causat per l'home, sobre les instal·lacions, que indica com es restauren els serveis dels Sistemes d'Informació. La ubicació dels sistemes de recuperació de desastre disposa de les proteccions físiques de seguretat detallades en el Pla de Seguretat.

L'EC-CIUTADANIA és capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, podent, com a mínim, executar-se les següents accions:

- Revocació de certificats
- Publicació d'informació de revocació

La base de dades de recuperació de desastres utilitzada per l'EC-CIUTADANIA està sincronitzada amb la base de dades de producció, dintre dels límits temporals especificats en el Pla de Seguretat. Els equips de recuperació de desastres de l'EC-CIUTADANIA té les mesures de seguretat físiques especificades en el Pla de Seguretat.

5.8. Finalització del servei

5.8.1. EC-CIUTADANIA

Conforme a allò establert a la Política General de Certificació.

En cas de finalització del servei, l'EC-CIUTADANIA:

- Comunicarà el cessament de la seva activitat a les entitats afectades, amb una antelació mínima de dos mesos
- Informarà a les entitats afectades sobre el tractament dels certificats emesos que encara no hagin expirat i, especialment, sobre el mecanisme de consulta de l'estat d'aquests que s'oferirà
- Transferirà les obligacions de l'EC-CIUTADANIA a altres persones jurídiques, sota el seu consentiment

Es preveu que l'EC-CIUTADANIA transfereixi els certificats, en els termes previstos a la legislació aplicable, descrita a la secció 9.15 d'aquesta DPC.

5.8.2. Entitat de Registre

Les Entitats de Registre hauran de conservar i custodiar diligentment tota la informació generada en la seva activitat com a Entitat de Registre durant 15 anys després de finalitzar les activitats relacionades amb l'Entitat de Registre.

6. Controls de seguretat tècnica

L'EC-CIUTADANIA utilitza sistemes i productes fiables que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i criptogràfica dels processos de certificació als que serveixen de suport.

6.1. Generació i instal·lació del parell de claus

6.1.1. Generació del parell de claus

6.1.1.1. Requisits per a tots els certificats

El parell de claus podrà ser generat pel futur posseïdor de claus o per l'Entitat de Registre.

6.1.1.2. Informació per als certificats idCAT CPISA

Les claus pública i privada dels certificats idCAT les pot generar el Consorci AOC i enviar-les al posseïdor de claus de forma segura. També poden ser generades pel futur posseïdor de claus, qui remetrà la corresponent prova de possessió de clau privada (PKCS#10) a l'EC-CIUTADANIA.

Aquestes claus no s'emmagatzemen, de manera que, en cas de suspensió, revocació o expiració del certificat, el Consorci AOC no respondrà per la pèrdua d'informació que hagués estat xifrada amb elles.

6.1.2. Enviament de la clau privada al subscriptor

6.1.3. Enviament de la clau pública a l'emissor del certificat

Conforme a allò establert a la Política General de Certificació.

6.1.4. Distribució de la clau pública del Prestador de Serveis de Certificació

La clau de l'EC-CIUTADANIA i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya són comunicades als verificadors, assegurant la integritat de la clau i autenticant-ne l'origen.

La clau pública de l'EC-CIUTADANIA es publica en el directori de l'EC-CIUTADANIA, en forma de certificat CIC signat per l'EC-ACC. Els usuaris poden accedir al directori per a obtenir les claus públiques de l'EC-CIUTADANIA.

Aquest mateix certificat també es publica a la web del Consorci AOC.

Addicionalment, en aplicacions S/MIME, el missatge de dades conté una cadena de certificats, incloent els certificats CIC amb les claus públiques de les Entitats de Certificació

de la jerarquia (en aquest cas, de l'EC-CIUTADANIA i de l'EC-ACC) que, d'aquesta forma, són distribuïdes als usuaris.

6.1.5. Mides de claus

Les claus de l'EC-CIUTADANIA són de 2.048 bits.

Les claus de tots els certificats emesos per l'EC-CIUTADANIA són de 2.048 bits.

6.1.6. Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7. Comprovació de qualitat de paràmetres de clau pública

Conforme a allò establert a la Política General de Certificació.

6.1.8. Generació de claus en aplicacions informàtiques o en béns d'equip

Conforme a allò establert a la Política General de Certificació.

La generació de claus per als certificats idCAT emesos per l'EC-CIUTADANIA es realitza mitjançant aplicacions informàtiques.

6.1.9. Propòsits d'ús de claus

L'EC-CIUTADANIA inclou l'extensió KeyUsage en tots els certificats, indicant els usos permesos de les corresponents claus privades.

6.2. Protecció de la clau privada

6.2.1. Mòduls de protecció de la clau privada

6.2.1.1. Estàndards dels mòduls criptogràfics

Conforme a allò establert a la Política General de Certificació.

6.2.2. Control per més d'una persona (n de m) sobre la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.3. Dipòsit de la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.4. Còpia de seguretat de la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.5. Arxiu de la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

Conforme a allò establert a la Política General de Certificació.

6.2.7. Emmagatzematge de la clau privada en el mòdul criptogràfic

Conforme a allò establert a la Política General de Certificació.

6.2.8. Mètode d'activació de la clau privada

La clau privada del subscriptor s'activa mitjançant la introducció del PIN en la corresponent aplicació de generació de signatura.

Aquesta aplicació en els sistemes informàtics basats en windows és el Cryptographic Service Provider. La web del servei idCAT ofereix la possibilitat, en la secció "abans de fer la sol·licitud", d'actualitzar el sistema de l'usuari amb aquesta aplicació, mitjançant un enllaç a la web de Microsoft.

Els sistemes basats en Netscape, poden utilitzar l'aplicació PKCS #11.

6.2.9. Mètode de desactivació de la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.10. Mètode de destrucció de la clau privada

Conforme a allò establert a la Política General de Certificació.

6.2.11. Classificació dels mòduls criptogràfics

Els mòduls de l'EC-CIUTADANIA (EJBCA Enterprise) estan certificats Common Criteria EAL 4+.

6.3. Altres aspectes de gestió del parell de claus

6.3.1. Arxiu de la clau pública

L'EC-CIUTADANIA arxiva les seves claus públiques, d'acord amb allò establert a la secció 6.2.

6.3.2. Períodes d'utilització de les claus pública i privada

Conforme a allò establert a la Política General de Certificació.

6.4. Dades d'activació

6.4.1. Generació i instal·lació de les dades d'activació

La generació i instal·lació de les dades d'activació es basa en el Cryptographic Service Provider.

6.4.2. Protecció de les dades d'activació

L'usuari és responsable de cuidar la seva clau privada amb una paraula de pas tan completa com sigui possible, a través de l'aplicació (Cryptographic Service Provider).

S'aconsella que aquesta paraula de pas no sigui massa curta i estigui formada per números i lletres.

El subscriptor ha de recordar aquesta paraula de pas.

6.4.3. Altres aspectes de les dades d'activació

Sense estipulació addicional.

6.5. Controls de seguretat informàtica

6.5.1. Requisits tècnics específics de seguretat informàtica

Conforme a allò establert a la Política General de Certificació.

6.5.2. Avaluació del nivell de seguretat informàtica

L'aplicació d'autoritat de certificació, mitjançant la qual opera l'EC-CIUTADANIA (EJBCA Enterprise), és fiable, donat que va obtenir la certificació Common Criteria EAL 4+.

6.6. Controls tècnics del cicle de vida

6.6.1. Controls de desenvolupament de sistemes

Conforme a allò establert a la Política General de Certificació.

6.6.2. Controls de gestió de seguretat

Conforme a allò establert a la Política General de Certificació.

A més, l'EC-CIUTADANIA garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures; en particular, existeixen instruccions per a:

a) Operar els mòduls de forma correcta i segura
b) Instal·lar els mòduls minimitzant el risc de fallida dels sistemes
c) Protegir els mòduls contra virus i software maliciós, per a garantir la integritat i validesa de la informació que processen.

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7. Controls de seguretat de xarxa

Es garanteix que l'accés a les diferents xarxes de l'EC-CIUTADANIA és limitat a individus degudament autoritzats. En particular:

- S'implementen controls (com per exemple tallafocs) per a protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de forma que s'impedeixin accés i protocols que no siguin necessaris per a l'operació de l'EC-CIUTADANIA.
- Les dades sensibles (incloent les dades de registre del subscriptor) es protegeixen quan s'intercanvien a través de xarxes no segures.
- Es garanteix que els components locals de xarxa (com enrutadors/routers) es troben ubicats en entorns segurs; també es garanteix l'auditoria periòdica de les seves configuracions.

6.8. Segell de temps

Sense estipulació addicional.

7. Perfils de certificats i llistes de certificats revocats

7.1. Perfil de certificat

Conforme a allò establert a la Política General de Certificació.

Els documents descriptius dels diversos perfils de certificats digitals que expedeix l'EC-CIUTADANIA es publiquen a la web del Consorci AOC.

7.2. Perfil de la llista de revocació de certificats

Conforme a allò establert a la Política General de Certificació.

8. Auditoria de conformitat

L'EC-CIUTADANIA realitza periòdicament una auditoria de conformitat per a provar que compleix els requisits de seguretat i d'operació necessaris per a formar part de la jerarquia pública de certificació de Catalunya.

L'EC-CIUTADANIA pot delegar l'execució de les auditories en una tercera entitat contractada pel Consorci AOC. En aquests casos, l'EC-CIUTADANIA coopera completament amb el personal que porta a terme la investigació.

8.1. Freqüència de l'auditoria de conformitat

Conforme a allò establert a la Política General de Certificació.

8.2. Identificació i qualificació de l'auditor

L'EC-CIUTADANIA s'adreça a auditors independents externs per a la realització de les auditories anuals de conformitat. Aquests han de demostrar experiència en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de Certificació i dels elements relacionats.

8.3. Relació de l'auditor amb l'entitat auditada

Les auditories externes de conformitat executades per tercers són realitzades per entitats independents de l'EC-CIUTADANIA.

8.4. Relació d'elements objecte d'auditoria

Conforme a allò establert a la Política General de Certificació.

8.5. Accions a emprendre com a resultat d'una falta de conformitat

Conforme a allò establert a la Política General de Certificació.

8.6. Tractament dels informes d'auditoria

Els informes de resultats de les auditories seran lliurats al Consorci AOC, en tant que és el Prestador de Serveis de Certificació, en un termini màxim de 15 dies després de l'execució de l'auditoria, per a la seva avaluació i gestió diligent.

9. Requisits comercials i legals

9.1. Tarifes

9.1.1. Tarifa d'emissió o renovació de certificats

El Consorci AOC estableix les tarifes que aplica l'EC-CIUTADANIA en la prestació dels seus serveis. Les tarifes es poden consultar a la web del Consorci AOC.

9.1.2. Tarifa d'accés a certificats

No es pot establir una tarifa per l'accés als certificats.

9.1.3. Tarifa d'accés a informació d'estat de certificat

No es pot establir una tarifa per l'accés a la informació d'estat dels certificats.

9.1.4. Tarifes d'altres serveis

Sense estipulació addicional.

9.1.5. Política de reintegrament

El Consorci AOC no practicarà reemborsaments. En cas de productes defectuosos, es procedirà a substituir el producte defectuós per un altre en bon estat.

9.2. Capacitat financera

9.2.1. Assegurança de responsabilitat civil

El Consorci AOC disposa d'una garantia de cobertura de la seva responsabilitat civil suficient, en els termes previstos a la legislació aplicable, descrita a la secció 9.15. Conformitat amb la llei aplicable, excepte quan es trobi eximida per Llei d'aquesta obligació. Aquesta assegurança cobreix les actuacions del Consorci AOC com a prestador de serveis de certificació.

9.2.2. Altres actius

Sense estipulació addicional.

9.2.3. Cobertura d'assegurament per a subscriptors i tercers que confien en certificats

En cas d'ús incorrecte o no autoritzat dels certificats, el Consorci AOC (o l'EC-CIUTADANIA) no actuarà com a agent fiduciari front a subscriptors i terceres

persones, que hauran d'adreçar-se contra l'infractor de les condicions d'ús dels certificats establertes pel Consorci AOC (o l'EC-CIUTADANIA).

9.3. Confidencialitat

9.3.1. Informacions confidencials

Conforme a allò establert a la Política General de Certificació.

9.3.2. Informacions no confidencials

Conforme a allò establert a la Política General de Certificació.

9.3.3. Responsabilitat per a la protecció d'informació confidencial

Conforme a allò establert a la Política General de Certificació.

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

Conforme a allò establert a la Política General de Certificació.

9.4.2. Dades de caràcter personal no disponibles a tercers

Conforme a allò establert a la Política General de Certificació.

9.4.3. Dades de caràcter personal disponibles a tercers

Conforme a allò establert a la Política General de Certificació.

9.4.4. Responsabilitat corresponent a la protecció de dades personals

Conforme a allò establert a la Política General de Certificació.

9.4.5. Gestió d'incidències relacionades amb les dades de caràcter personal

Conforme a allò establert a la Política General de Certificació.

9.4.6. Prestació del consentiment per al tractament de les dades personals

Conforme a allò establert a la Política General de Certificació.

9.4.7. Comunicació de dades personals

Conforme a allò establert a la Política General de Certificació.

9.5. Drets de propietat intel·lectual

9.5.1. Propietat dels certificats i informació de revocació

Conforme a allò establert a la Política General de Certificació.

9.5.2. Propietat de la Política de Certificació i Declaració de Pràctiques de Certificació

Conforme a allò establert a la Política General de Certificació.

9.5.3. Propietat de la informació relativa a noms

Conforme a allò establert a la Política General de Certificació.

9.5.4. Propietat de claus

Conforme a allò establert a la Política General de Certificació.

9.6. Obligacions i responsabilitat civil

9.6.1. Entitats de Certificació

9.6.1.1. Obligacions generals de l'EC-CIUTADANIA

Conforme a allò establert a la Política General de Certificació.

9.6.1.2. Requisits específics per als certificats personals

Conforme a allò establert a la Política General de Certificació.

9.6.1.3. Garanties oferides a subscriptors i verificadors

Conforme a allò establert a la Política General de Certificació.

9.6.2. Obligacions i altres compromisos de les Entitats de Registre

9.6.2.1. Obligacions i altres compromisos

L'EC-CIUTADANIA pot delegar algunes funcions a Entitats de Registre que, en aquest cas, queden obligades al seu compliment, en les mateixes condicions que l'Entitat de Certificació.

L'Entitat de Registre actua en el seu propi nom, sense perjudici de la responsabilitat de l'EC- CIUTADANIA.

L'Entitat de Registre queda obligada a registrar les dades del certificat i la seva aprovació en cas de ser correctes, així com al registre de les dades d'aquest certificat, pel qual realitza les comprovacions que consideri necessàries en relació a la identitat i la resta de dades personals i complementàries dels subscriptors i, si fos necessari, dels posseïdors de claus.

Aquestes comprovacions inclouen la justificació documental aportada pel sol·licitant i, si l'Entitat de Registre ho considerés necessari, qualsevol altre document i informació rellevant, facilitats pel subscriptor, pel posseïdor de claus o per terceres persones.

Si l'Entitat de Registre detectés errors en les dades que estan incloses en els certificats, o en els documents, que justifiquessin aquestes dades, està obligada a realitzar els canvis que consideri necessaris abans de l'emissió del certificat, o a la paralització del procés d'emissió i a gestionar amb el subscriptor la incidència corresponent.

En cas que l'Entitat de Registre corregeixi les dades sense gestió prèvia de la incidència corresponent amb el subscriptor, queda obligada a notificar les dades que finalment se certifiquin al subscriptor en el moment del lliurament.

L'Entitat de Registre es reserva el dret a no aprovar la sol·licitud d'emissió del certificat, quan la justificació documental aportada pel sol·licitant sigui insuficient per a la correcta identificació i/o autenticació del subscriptor.

9.6.3. Garanties oferides a subscriptor i verificadors

9.6.3.1. Garantia del Consorci AOC per als serveis de certificació digital

Conforme a allò establert a la Política General de Certificació.

9.6.3.2. Exclusió de la garantia

El Consorci AOC no garanteix cap software utilitzat pel subscriptor o per qualsevol altra persona, per a generar, verificar o utilitzar de forma distinta, cap signatura electrònica o certificat digital emès pel Consorci AOC, a excepció dels casos en què existeixi una declaració escrita d'aquest en sentit contrari.

9.6.4. Subscriptors

9.6.4.1. Obligacions i altres compromisos

9.6.4.1.1. Informacions per a tots els tipus de certificats

A més d'allò establert a la Política General de Certificació, l'EC-CIUTADANIA obliga al subscriptor a:

1. Utilitzar el parell de claus exclusivament per a signatures electròniques i conforme a qualsevol altra limitació que li sigui notificada.
2. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu qualificat de creació de signatura, amb la finalitat d'evitar usos no autoritzats.
3. El subscriptor genera les seves pròpies claus, per tant, s'obliga a:
    i. Generar les seves claus de subscriptor utilitzant un algoritme qualificat com acceptable per a la signatura electrònica qualificada.
    ii. Crear les claus dintre del dispositiu qualificat de creació de signatura.
    iii. Utilitzar longituds i algoritmes de clau qualificats com acceptables per a la signatura Electrònica qualificada.
4. Notificar a l'EC, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu qualificat de creació de signatura.

9.6.4.1.2. Informacions específiques per als certificats de signatura electrònica qualificada

No aplica.

9.6.4.2. Garanties oferides pel subscriptor

Conforme a allò establert a la Política General de Certificació.

9.6.4.3. Protecció de la clau privada

Conforme a allò establert a la Política General de Certificació.

9.6.5. Verificadors

9.6.5.1. Obligacions i altres compromisos

Conforme a allò establert a la Política General de Certificació.

9.6.5.2. Garanties oferides pel verificador

Conforme a allò establert a la Política General de Certificació.

9.6.6. Altres participants

9.6.6.1. Obligacions i garanties del directori

Conforme a allò establert a la Política General de Certificació.

9.6.6.2. Garanties oferides pel directori

L'EC-CIUTADANIA té la responsabilitat civil del directori de certificació.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de l'EC-CIUTADANIA

Conforme a allò establert a la Política General de Certificació.

9.8. Limitacions de responsabilitat

9.8.1. Limitacions de responsabilitat de l'EC-CIUTADANIA

Més enllà de les limitacions dels prestadors de serveis de certificació establertes a la legislació aplicable, descrita a l'apartat 9.15. Conformitat amb la llei aplicable , l'EC-CIUTADANIA limita la seva responsabilitat restringint el servei a l'emissió i la gestió de certificats i, en el seu cas, de parells de claus de subscriptors.

L'EC-CIUTADANIA limita la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat i límits de valor de les transaccions per a les que pot utilitzar-se el certificat.

9.8.2. Cas fortuït i força major

L'EC-CIUTADANIA inclou clàusules per a limitar la seva responsabilitat en cas fortuït i en cas de força major, en els instruments jurídics amb els subscriptors.

9.9. Indemnitzacions

9.9.1. Clàusula d'indemnitat de subscriptor

No s'establirà clàusula d'indemnitat del subscriptor.

9.9.2. Clàusula d'indemnitat de verificador

No s'establirà clàusula d'indemnitat del verificador.

9.10. Termini i finalització

9.10.1. Termini

L'EC-CIUTADANIA estableix, en els seus instruments jurídics amb els subscriptors, una clàusula que determina el període de vigència de la relació jurídica en virtut de la qual els subministra certificats.

9.10.2. Finalització

L'EC-CIUTADANIA estableix, en els seus instruments jurídics amb els subscriptors, una clàusula que determina les conseqüències de la finalització de la relació jurídica en virtut de la qual els subministra certificats.

9.10.3. Supervivència

Conforme a allò establert a la Política General de Certificació.

9.11. Notificacions

Conforme a allò establert a la Política General de Certificació.

9.12. Modificacions

9.12.1. Procediment per a les modificacions

Conforme a allò establert a la Política General de Certificació.

9.12.2. Termini i mecanismes per a notificacions

Les modificacions d'aquest document seran aprovades pel Consorci AOC, conforme a allò que s'estableix a l'apartat 1.5.

9.12.3. Circumstàncies en les que un OID ha de ser canviat

Sense estipulació addicional.

9.13. Resolució de conflictes

9.13.1. Resolució extrajudicial de conflictes

Conforme a allò establert a la Política General de Certificació.

9.13.2. Jurisdicció competent

Conforme a allò establert a la Política General de Certificació.

9.14. Llei aplicable

Conforme a allò establert a la Política General de Certificació.

9.15. Conformitat amb la llei aplicable

Conforme a allò establert en la Política General de Certificació.

9.16. Clàusules diverses

9.16.1. Acord íntegre

Conforme a allò establert a la Política General de Certificació.

9.16.2. Subrogació

Conforme a allò establert en la Política General de Certificació.

9.16.3. Divisibilitat

Conforme a allò establert a la Política General de Certificació.

9.16.4. Aplicacions

Sense estipulació addicional.

9.16.5. Altres clàusules

Sense estipulació addicional.

ANNEX – Control documental

Projecte:	**Informe creació del document DPC EC-CIUTADANIA**
Entitat de destí:	**Servei SCD - Consorci AOC**
Codi de referència:	**Revisió 1er semestre 2018**
Versió:	**2.0**
Data de l'edició:	**09/05/2018**

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
1.0	Tot el document	Redacció inicial de la Declaració de Pràctiques de Certificació de l'EC-CIUTADANIA	Servei CATCert del Consorci AOC	18/09/2014
1.1	Tot el document	Revisió ortogràfica del document	Servei SCD del Consorci AOC	20/01/2016
2.0	Tot el document	Revisió global per adaptació a eIDAS	Servei SCD del Consorci AOC	09/05/2018