Consorci
Administració Oberta
de Catalunya

Declaració de Pràctiques de Certificació
Entitat de Certificació IdCAT
(EC-IDCAT)

Referència:	D1111_E0650_N-DPC EC-IDCAT
Versió:	4.0
Data:	05/08/2016

Control documental

Estat formal	**Elaborat per:** Servei de Certificació Digital	**Aprovat per:** Direcció del Consorci AOC
Data de creació	26/09/2006	
Control de versions	**Data:**	05/08/2016
	Descripció:	Revisió global – integració de CATCert a Consorci AOC
Nivell accés informació	pública	
Títol	Declaració de Pràctiques de Certificació – Entitat de Certificació IdCAT	
Fitxer	D111 E0650 N-DPC EC-AL v4r0 CAT	
Control de còpies	Només les còpies disponibles a https://www.aoc.cat/ garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'Autor	 	

Índex

1. Introducció

Aquest document és la Declaració de Pràctiques de Certificació de l'Entitat de Certificació 'IdCAT' (d'ara endavant, EC-IDCAT), Entitat de Certificació per a les entitats locals de Catalunya.

En aquesta DPC es regulen tècnicament i operativament els serveis de certificació de l'EC-IDCAT.

Els apartats amb el contingut "Sense estipulació addicional" indiquen que s'ha de consultar la Política General de Certificació del Consorci AOC.

1.1 Presentació

Quan es va desenvolupar el pacte institucional signat el 23 de juliol del 2001 pels grups parlamentaris del Parlament de Catalunya, la Generalitat de Catalunya i el Consorci d'Ens Locals de Catalunya (Localret), per al desenvolupament de polítiques que permetin afrontar el canvi fonamental en les estructures socials i econòmiques derivat de la confluència de les noves tecnologies de la informació i de la comunicació en l'àmbit de les administracions públiques catalanes, es va decidir establir sistemes d'interrelació entre les esmentades administracions, i entre les administracions i els ciutadans, per via telemàtica i electrònica, en les condicions de seguretat necessàries i, especialment, fent ús de certificats digitals d'identitat i signatura electrònica.

En compliment de l'esmentat pacte institucional i per tal de desenvolupar el programa Catalunya en Xarxa, Localret i la Generalitat de Catalunya van acordar la creació del Consorci per a l'Administració Oberta Electrònica de Catalunya, amb la finalitat de desenvolupar polítiques públiques en matèria de serveis electrònics a les administracions públiques i d'exercir la condició d'autoritat (tècnica) de certificació de signatura electrònica per garantir el secret, la integritat, la identitat i l'autenticitat en les comunicacions i documents electrònics que es produeixen en l'àmbit de les administracions públiques catalanes.

El 25 de febrer del 2002 va tenir lloc la sessió constitutiva del Consorci per a l'Administració Oberta Electrònica de Catalunya, una sessió en la qual el Consell General va adoptar, d'entre altres, l'acord de constituir un ens de gestió directa sota la forma d'organisme autònom de caràcter comercial amb la denominació d'Agència Catalana de Certificació (CATCert) i amb l'objectiu de gestionar certificats digitals i prestar altres serveis relacionats amb la signatura electrònica en l'àmbit públic català.

CATCert es va crear per acord de la Comissió Executiva del Consorci de l'Administració Oberta Electrònica de Catalunya, de 29 d'abril del 2002, com a organisme autònom de caràcter comercial, els estatuts de la qual van ser publicats al Diari Oficial de la Generalitat de Catalunya el 30 de maig del 2003, per Resolució PRE/1574/2003, de 15 de maig.

Per tant, l'Agència Catalana de Certificació es constitueix en l'entitat principal del sistema públic català de certificació que regula l'emissió i la gestió dels certificats que s'emeten per a les institucions d'autogovern de Catalunya, les institucions que integren el món local i la resta d'entitats públiques i privades que integren el sector públic català; així com l'admissió i l'ús dels certificats emesos a ciutadans i empreses per altres prestadors de serveis de certificació i que sol·licitin la corresponent classificació.

Aquestes institucions emetran certificats per mitjà d'una infraestructura tècnica proporcionada per CATCert, denominada "jerarquia pública de certificació de Catalunya", i

podran admetre i utilitzar certificats d'altres prestadors mitjançant els serveis de classificació i validació de CATCert.

En aquest sentit, CATCert va crear el 8 de gener del 2003, una jerarquia d'entitats de certificació, l'arrel de la qual és la pròpia Agència.

L'Entitat de certificació de CATCert (denominada EC-ACC) és l'arrel de la jerarquia de confiança, i certifica les Entitats de Certificació que es creen dins del marc de les administracions públiques catalanes.

Actualment existeixen nou entitats de certificació vinculades a la jerarquia pública de certificació de les administracions públiques catalanes: EC-GENCAT, EC-SAFP, EC-AL, EC-idCAT, EC-UR, EC-URV, EC-Parlament, EC-SectorPublic i EC-Ciutadania.

L'EC-IDCAT és l'Entitat de Certificació Vinculada a la jerarquia pública de certificació de Catalunya encarregada d'emetre certificats als ciutadans catalans que necessiten relacionar-se amb les administracions i d'altres institucions.

L'Acord de Govern de 16 d'octubre de 2013 assigna la prestació de serveis de certificació al Consorci Administració Oberta de Catalunya (AOC), com a mesura de racionalització del sector públic, que es concreta en la integració de l'Agència Catalana de Certificació en el Consorci AOC, en el qual revertiran totes les marques, drets, deures i serveis gestionats fins a la data per CATCert.

La integració es va fer efectiva mitjançant l'esmentat acord amb efectes comptables i jurídics el 30 de juny de 2013, data en la qual el Consorci AOC assumeix els drets i obligacions així com la prestació del servei, incloent el Servei de Certificació Digital, responsable de l'emissió i gestió del cicle de vida dels certificats digitals. En endavant, el Consorci Administració Oberta de Catalunya és el prestador dels serveis de certificació (TSP) públics de Catalunya i el propietari de la infraestructura de clau pública (PKI) que abans era titularitat de CATCert.

1.1.1 Tipus i classes de certificats

L'EC-IdCAT ha definit una tipologia de serveis de certificació, que li permeten emetre certificats digitals per a diversos usos i usuaris finals diferents.

L'EC-idCAT emet certificats idCAT, que són certificats reconeguts d'identificació i signatura electrònica avançada, destinats a ciutadans i ciutadanes catalanes majors d'edat, així com a altres persones (col·lectivament anomenats subscriptors) que necessiten relacionar-se amb les Administracions públiques i altres institucions.

El certificat idCAT és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 17 a 20 de la Llei esmentada.

El procediment de validació de la identitat requereix la compareixença personal de la persona física que obté el certificat davant d'una oficina de registre col·laboradora del Consorci AOC.

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-IdCAT.

L'EC-IDCAT emet certificats dins de la Jerarquia pública de certificació del Consorci AOC. Per tant, disposa d'una Declaració de Pràctiques de Certificació (DPC) d'acord amb la Política General de Certificació del Consorci AOC.

Aquesta DPC inclou els procediments que aplica l'EC-IDCAT en la prestació dels seus serveis, en compliment dels requisits establerts per les polítiques que gestiona i l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Aquesta DPC es relaciona amb documentació auxiliar, entre la qual es troben els instruments jurídics reguladors de la prestació del servei, de la documentació i de les polítiques de seguretat, així com de la documentació d'operacions.

1.2 Nom del document i identificació

1.2.1 Identificació d'aquest document

Aquest document s'anomena "Declaració de Pràctiques de Certificació (DPC) de l'EC-IDCAT".

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

1.3.6.1.4.1.15096.1.2.6

1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

L'EC-IdCAT ha definit i aprovat la següent especificació de política per als certificats idCAT:

CIPISR – Certificat d'infraestructura d'operador

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16

CIDS-1 – Certificat de infraestructura de servidor segur, emès per la EC-IdCAT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.17

CIDA-1 – Certificat d'infraestructura d'aplicació, emès per la EC-IdCAT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.18

CIO-1 – Certificat d'infraestructura de servidor d'estat de certificats en línia, emès per la EC-IdCAT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.19

CIV-1 – Certificat d'infraestructura d'entitat de validació, emès per la EC-IdCAT

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.20

CIT-1 - Certificat d'infraestructura d'entitat de segells de temps, emès per la EC-IdCAT

Classe 1. 1.3.6.1.4.1.15096.1.3.1.111

idCAT basat en certificat CPIXSA - Certificat de persona física ciutadà d'identificació, xifrat i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.1

idCAT-CEX basat en certificat CPIXSA - Certificat de persona física de nacionalitat estrangera d'identificació, xifrat i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.2

idCAT-T basat en certificat CPIXSA - Certificat de persona física ciutadà d'identificació,

xifrat i signatura electrònica avançada, amb suport targeta o *token*

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.3

Els documents descriptius d'aquests perfils de certificats es publiquen en el 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 diverses relacions administratives i privades, d'acord amb la Llei 59/2003 i la normativa administrativa corresponent.

Els certificats idCAT sempre s'emeten al públic.

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 59/2003, de 19 de desembre, de signatura electrònica.

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

Conforme a aquesta funció,el Consorci AOC serà responsable per l'actuació de l'EC-IdCAT,davant els usuaris finals i els tercers verificadors de certificats i signatures electròniques, per l'actuació de les autoritats de certificació que operen en nom de les diferents entitats de certificació.

1.3.2 Entitat de Certificació Arrel

L'Entitat de Certificació Arrel, que és el Consorci AOC, disposa d'una autoritat de certificació principal, denominada "Arrel de la jerarquia pública de certificació de Catalunya" i té la finalitat d'integrar altres entitats de certificació en el sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

L'esmentada vinculació tècnica s'aconsegueix mitjançant l'emissió de certificats d'infraestructura d'entitat de certificació vinculada (CIC).

1.3.3 EC-idCAT

L'EC-idCAT és l'Entitat de Certificació habilitada per emetre certificats als ciutadans de Catalunya, vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya, que emet els certificats indicats en el punt 1.1.1.

La petjada digital del certificat de L'EC-idCAT és:

```
50 49 88 bd b7 df e0 dd a8 eb f6 98 e0 b5 c4 65 02 fb 41 fc
```

1.3.4 Entitats de Registre

Són Entitats de Registre per a certificats idCAT, totes aquelles entitats que s'hagin adherit a les Condicions del Servei de Certificació Digital del Consorci AOC.

El procés de creació d'entitats de registre és responsabilitat de l'administrador de l'Entitat de Certificació. Mitjançant conveni signat entre la Institució i el Consorci AOC es constitueix l'entitat de registre. El Consorci AOC verifica que l'Entitat de Registre compti amb els recursos materials i humans necessaris, i de la designació del personal responsable. Tanmateix, és responsable, en tot cas, de la formació del personal que emeti els certificats com a operadors de l'entitat de registre i, a tal efecte, de l'emissió dels certificats d'operador corresponents (típicament, CIPISR). El Consorci AOC validarà les peticions de certificats de les Entitats de Registre examinant la sol·licitud i fent les comprovacions necessàries per al compliment la Política General de Certificació i de la Declaració de Pràctiques de Certificació.

1.3.5 Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats emesos per l'EC-IDCAT. En concret, es poden distingir els usuaris finals següents:

- Els sol·licitants de certificats.
- Els subscriptors o titulars de certificats.
- Els verificadors de signatures i certificats.

1.3.5.1 Sol·licitants de certificats

Els certificats idCAT són sol·licitats per persones majors d'edat, en el seu propi nom.

Poden ser sol·licitants:

a) La persona que serà el futur subscriptor.

b) Una persona autoritzada pel futur subscriptor (representant)

L'autorització s'ha de realitzar de forma expressa mitjançant document públic.

1.3.5.2 Subscriptors de certificats

Els subscriptors dels certificats són les institucions i les persones, físiques o jurídiques, que s'identifiquen en el camp "Subject" del certificat.

El subscriptor té llicència d'ús del certificat.

1.3.5.3 Usuaris de certificats

Els usuaris dels certificats són els verificadors.

1.3.5.4 Verificadors de certificats

Els verificadors són les persones físiques i jurídiques que reben signatures electròniques i han de verificar-los, com pas previ a confiar-hi.

1.4 Ús dels certificats

Aquesta secció llista les aplicacions per a les que es pot utilitzar 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 reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, 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 segurs de creació de signatura electrònica d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els certificats idCAT garanteixen la identitat del subscriptor resultant idonis per 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 qual 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 l'esmentada equiparació.

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

- Identificació distribuïda, basada en presentació de la credencial
- Autenticació en sistemes de control d'accés, de sistema operatiu o centralitzats.

Els certificats idCAT tenen la possibilitat de rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge, utilitzant la clau pública del subscriptor indicada al certificat.

El subscriptor utilitza la seva clau privada per desxifrar el missatge o document.

1.4.2. Aplicacions prohibides

Els certificats només es podran utilitzar dins dels límits d'ús recollits d'una manera expressa en la seva llicència d'ús i les seves corresponents Condicions d'Ús. Qualsevol altre ús fora dels descrits en els esmentats documents, queden exclosos expressament de l'àmbit contractual i prohibits formalment.

Els certificats idCAT (a excepció del CIPISR) no es poden utilitzar per signar peticions d'emissió, renovació, suspensió o revocació de certificats, ni per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats (LRC), ni per realitzar cap tipus de transaccions econòmiques.

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

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 de certificació digitaldel Consorci AOC:

www.aoc.cat/catcert

Servei d'Atenció al'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 de Certificació Digital del Consorci AOC, basant-se en els resultats d'una auditoria a l'efecte, realitzada per un tercer, bianualment.

1.5.4 Procediment d'aprovació

El sistema documental i d'organització de l'EC-IdCAT 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

El servei de Directori de certificats està disponible durant les 24 hores dels 7 dies de la setmana i, en cas d'error del sistema fora de control de l'EC-IDCAT aquesta darrera realitza els seus millors esforços perquè el servei es trobi disponible de nou en el termini establert a la secció 5.7.4 d'aquesta DPC.

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

L'EC-IDCAT publica les següents informacions, en el web del Consorci AOC (http://www.aoc.cat/catcert/):

a) Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.

b) La política general de certificació

c) Els perfils dels certificats i de les llistes de revocació dels certificats.

d) La Declaració de Pràctiques de Certificació.

e) Els instruments jurídics vinculants amb subscriptors i verificadors.

Tot canvi en les especificacions o condicions del servei es comunica als usuaris per part de l'EC-IDCAT, a través del dipòsit.

En tots els casos es fa una referència explícita als canvis a la pàgina principal del Web del servei.

No es retira la versió anterior del document objecte del canvi, però s'indica que ha estat substituït per la versió nova.

2.3. Freqüència de publicació

La informació de l'EC-IDCAT 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 l'establert a la secció 9.12.1.

La informació d'estat de revocació de certificats es publica d'acord amb l'establert a la secció 4.9.7.

Al cap de 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-IDCAT, podent ser consultada, per causa raonada pels interessats.

La informació d'estat de revocació de certificats es publica d'acord amb allò establert a la secció 4.10.7.

2.4. Control d’accés

Sense estipulació addicional.

3. Identificació i autenticació

3.1. Gestió de nom

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 lliurament de certificats, les Entitats de Registre.

3.1.1. Tipus de noms

Sense estipulació addicional.

3.1.1.1 Estructura sintàctica

Sense estipulació addicional.

3.1.1.2 Perfils dels certificats

Els perfils dels certificats emesos per l'EC-IDCAT es publiquen al web del Consorci AOC (http://www.aoc.cat/catcert/).

3.1.2. Significat dels noms

Sense estipulació addicional.

3.1.3. Utilització d'anònims i pseudònims

No es poden fer servir pseudònims per a identificar una organització.

3.1.4. Interpretació de formats de noms

Sense estipulació addicional.

3.1.5. Unicitat dels noms

Sense estipulació addicional

3.1.6. Resolució de conflictes relatius a noms

Sense estipulació addicional.

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

Sense estipulació addicional.

3.2.2. Autenticació de la identitat

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

Per acreditar la identitat del subscriptor, aquest es persona davant d'una Entitat de Registre que elegeix i que pot ser la més propera al seu domicili.

Recordem que en el darrer pas de la sol·licitud del certificat, la web ofereix al sol·licitant la possibilitat de cercar l'Entitat de Registre, per província, comarca o població.

L'acreditació de la identitat es pot realizar directament davant de les Entitats de Registre, segons el qual el sol·licitant consigna les dades directament als operadors, que els contrasten amb els documents originals aportats (DNI, NIE, passaport). Una vegada recollides les dades es procedeix a emetre el certificat

El sol·licitant també pot consignar les dades d'identitat en la web del Consorci AOC. Seguidament, el sol·licitant es persona davant l'Entitat de Registre de la seva elecció. Una vegada el sol·licitant es trobi a les dependències de l'Entitat de Registre es presenta amb el document que l'identifica i que ha indicat a la sol·licitud (DNI, NIF, NIE o passaport, depenent del cas), amb una fotocòpia de l'esmentat document i, si així ho desitja, una còpia impresa del formulari de confirmació de dades que li mostra la web just al final del procés de sol·licitud.

L'encarregat de rebre l'esmentada documentació a l'Entitat de Registre, comprova visualment que la fotografia del document que identifica el sol·licitant sigui exactament la corresponent al subscriptor i la majoria d'edat.

Seguidament imprimeix el document de compareixença amb les dades de la sol·licitud del certificat perquè el sol·licitant el firmi.

L'encarregat comprova també que la signatura que el subscriptor acaba de realitzar a la sol·licitud de certificat correspon a la signatura que hi ha al document que l'identifica.

Fetes totes aquestes comprovacions es valida la sol·licitud en el sistema informàtic enviant-lo electrònicament i de forma segura a l'EC-idCAT

Tots els documents que aporti el subscriptor han d'estar vigents. En el seu cas, haurà d'aportar el comprovant de renovació. Si aquest no conté fotografia, es podrà completar la verificació de la identitat usant el document caducat.

3.2.2.1 Necessitat de presència personal

La identificació de la persona física que obté un certificat idCAT pot realitzar-se

- Mitjançant la seva presència davant dels encarregats de verificar la seva identitat.
- Es pot prescindir de la presència si la signatura continguda a la sol·licitud d'expedició d'un certificat ha estat legitimada notarialment, i en els casos previstos per l'article 13.4 de la Llei 59/2003, de 19 de desembre.
- Mitjançant el procediment que estableix la normativa administrativa, quan la presència es realitzi davant de les Administracions Públiques.

3.2.2.2 Informacions addicionals per a subscriptores de nacionalitat espanyola

El subscriptor s'identifica obligatòriament amb el seu Document Nacional d'Identitat.

3.2.2.3 Informacions addicionals per a subscriptors de nacionalitat no espanyola residents a Catalunya.

El subscriptor s'identifica obligatòriament amb el seu DNI, la seva targeta de residència o document NIE (ciutadans comunitaris i d'altres estats, exempts de la targeta de residència).

3.2.3 Informació de subscriptor no verificada

Els certificats inclouen informació del subscriptor no verificada, com l'adreça electrònica.

3.3 Identificació i autenticació de sol·licituds de renovació

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

3.3.1 Validació per a la renovació rutinària de certificats

El sistema de certificació comunica al subscriptor la data de la finalització de la vigència del certificat amb una antelació de 60 dies, i en cas de no haver tramitat la renovació, també amb una antelació de 30 dies.

La renovació s'inicia quan el subscriptor del certificat idCAT, encara en vigor, demana la renovació seguint la ruta indicada en el missatge electrònic.

En cas que en el moment de la renovació no hagin passat 5 anys respecte la darrera identificació del ciutadà a una Entitat de Registre, el subscriptor no s'ha de personar davant les entitats de registre. El sistema no permetrà modificar cap dada respecte les validades en la primera emissió. Si alguna d'aquestes dades ja no és vàlida, el subscriptor haurà de sol·licitar una nova emissió identificant-se, amb el nou document, a l'Entitat de Registre.

En cas que ja hagin passat més de 5 anys respecte la darrera identificació (per exemple, en casos de segona renovació), el subscriptor s'haurà de personar novament davant l'Entitat de Registre, o aportar l'acta notarial corresponent, per a que es procedeixi a la nova emissió.

3.3.2 Validació per a la renovació de certificats després de la revocació

La renovació de certificats després de la seva revocació no és possible.

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

Nota: el terme "notificació" s'utilitza en aquest document com a 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

4.1.1 Legitimació per sol·licitar l'emissió

Abans de l'emissió i lliurament d'un certificat, existeix una sol·licitud de certificat.

Tots aquells que desitgen convertir-se en subscriptors realitzen una sol·licitud de certificat idCAT, a través del web http://www.idcat.cat, o directament presentant-se davant de qualsevol de les entitats de registre idCAT (Ajuntaments, Diputacions, etc.) que ofereixen aquesta possibilitat, seguint els passos que allà s'indiquen.

4.1.2 Procediment d'alta; Responsabilitats

L'EC-idCAT s'assegura que les sol·licituds de certificats són completes, precises i estan degudament autoritzades.

Per realitzar la sol·licitud prèvia, cal accedir a la pàgina web de presentació d'aquest servei (www.idcat.cat) que conté un menú amb les passes a seguir per realitzar la sol·licitud.

El primer pas de necessària execució és carregar en el nostre sistema informàtic les claus públiques de la jerarquia pública de certificació.

El següent pas consisteix en el deure de visualització del text divulgatiu de la política de certificació idCAT i la declaració d'intencions d'ús de les dades personals i la seva protecció.

A continuació trobem el formulari on introduïm les nostres dades personals i de contacte. És molt important emplenar el formulari amb les dades exactament com estan escrites als documents que ens identifiquen, que l'operador de l'Entitat de Registre que ens atengui pugui comprovar i validar posteriorment les esmentades dades.

Seguidament ens apareix una pantalla amb les dades que hem introduït que les puguem visualitzar i si són correctes, enviar-les a l'EC-idCAT activant la casella corresponent (típicament, fent clic en el botó "Enviar dades").

Per acabar ens apareix una pantalla amb les dades introduïdes on se'ns demana que l'imprimim per tenir una còpia escrita de la nostra sol·licitud, i se'ns informa de les Entitats de Registre més properes al domicili indicat a la sol·licitud.

4.2 Processament de la sol·licitud de certificació

Després que l'Entitat de Registre comprovi la identitat del sol·licitant, verifiqui la documentació presentada, s'envia la sol·licitud d'emissió de certificat a l'EC-idCAT i el ciutadà signa el document de compareixença corresponent.

Si alguna de les comprovacions és errònia, s'introdueixen els canvis, s'envia l'esmentada sol·licitud a l'EC-idCAT i es signa pel sol·licitant el document de compareixença amb les dades modificades.

L'EC-idCAT rep l'autorització de l'Entitat de Registre, recupera la corresponent sol·licitud de la taula de sol·licituds, l'emmagatzema en l'estructura de certificats, la signa, i es completa així la generació del certificat.

A partir d'aquest moment el sol·licitant ja pot descarregar des del web el seu certificat i començar a utilitzar-lo.

A més l'EC-idCAT té en compte els següents aspectes:

- Genera els certificats vinculant-los de forma segura amb la informació que el futur subscriptor indica al formulari de registre.
- Protegeix el secret i la integritat de les dades de registre.
- Inclou al certificat les informacions establertes a l'article 11 de la Llei 59/2003, d'acord amb l'establert a la secció 7 d'aquest document.
- Garanteix la data i l'hora en què s'expedeix un certificat
- Utilitza sistemes i productes fiables que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport.
- S'assegura que el certificat és emès per sistemes que utilitzin protecció contra falsificació.

En el cas de certificats emesos en dispositiu (clauers, targetes criptogràfiques), l'emissió i lliurament del certificat es realitza en l'acte de personació davant l'entitat de registre.

4.3 Emissió de certificat

4.3.1 Accions de l'EC-IDCAT 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.

Després de l'aprovació de la sol·licitud de certificació es procedeix a l'emissió del certificat, de forma segura i es posa el certificat a disposició del subscriptor en el suport corresponent

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

L'EC-idCAT ha de:

- Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent-hi la clau pública certificada
- En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de

generació de claus i, que la clau privada és lliurada de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus en cas de certificats d'organització.

- Protegir la confidencialitat i integritat de les dades de registre, especialment en cas de que siguin intercanviats amb el subscriptor, en cas de certificats individuals, amb el posseïdor de claus, en cas de certificats d'organització o amb el tercer sol·licitant, en el seu cas.
- Incloure en el certificat les informacions establertes en l'art. 11.2 de la Llei 59/2003, d'acord amb allò establert la secció corresponent d'aquesta política.
- Indicar la data i l'hora en les que es va expedir un certificat.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.
- Prendre mesures contra la falsificació de certificats i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus.

4.3.2 Notificació de l'emissió al subscriptor

L'EC-idCAT comunica per correu electrònic al sol·licitant, una vegada l'emissió ha finalitzat, satisfactòriament i les instruccions per a iniciar l'ús del certificat

Per a que el subscriptor obtingui el certificat idCAT (en cas d'emissió en programari) cal que accedeixi a la pàgina web que se li indica al correu electrònic i que procedeixi a descarregar el certificat.

4.4. Acceptació del certificat

4.4.1. Responsabilitats del Prestador de Serveis de Certificació

L'EC-idCAT proporciona accés al certificat al subscriptor.

4.4.2. Conducta que constitueix acceptació del certificat

El subscriptor accepta el certificat i les condicions d'ús del mateix en signar el document emès per l'Entitat de Registre.

En el cas de certificat emesos en dispositiu, el certificat es descarrega en la pròpia oficina de l'Entitat de Registre.

4.4.3. Publicació del certificat

La publicación de los certificados idCAT requereix sempre el consentimient previ dels subscriptors.

4.4.4. Notificació de l'emissió a tercers

No aplicable.

4.5. Ús del parell de claus i del certificat

4.5.1. Ús del parell de claus pels subscriptors

El certificat idCAT serveix per als ciutadans i ciutadanes catalanes i altres persones físiques majors d'edat que necessitin relacionar-se amb les Administracions públiques catalanes, realitzant els corresponents tràmits telemàtics entre ambdues parts amb totes les garanties jurídiques i tècniques recollides en les normes vigents

A més es pot utilitzar pel subscriptor en les seves relacions telemàtiques amb altres persones físiques o jurídiques que ho acceptin, sempre que el seu ús no impliqui una transferència de valor econòmic directe o indirecte.

També permet enviar correu electrònic segur (signat i xifrat) amb altres ciutadans o organitzacions.

4.5.2. Ús pel tercer que confia en certificats

El certificat idCAT serveix per a ús administratiu (quan el tercer és una Administració pública) o privat (quan el tercer no és Administració pública). El tercer verificador que vulgui permetre l'ús professional de l'IdCAT en els seus sistemes haurà de signar un conveni específic d'extensió de l'ús del certificat, que permeti al Consorci AOC assumir el risc corresponent.

4.6. Renovació de certificats sense renovació de claus

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

4.7. Renovació de certificats amb renovació de claus

Quan se sol·liciti la renovació d'un certificat amb renovació del parell de claus, el ciutadà només podrà renovar-lo de forma no presencial en cas que no hagin transcorregut 5 anys des de la darrera identificació davant de l'Entitat de Registre, i a més, les dades associades al certificat no podran ser modificades, de la forma com s'especifica a la secció corresponent d'aquesta política.

Si les condicions jurídiques de prestació del servei han variat des de l'emissió del certificat, serà necessari que l'Entitat de Certificació o bé l'Entitat de Registre informin d'aquest fet al sol·licitant.

La renovació d'un certificat s'inicia 60 dies abans de la data d'expiració del certificat, quan el subscriptor rep un correu electrònic on se l'informa dels passos a seguir per a executar la renovació del certificat. Aquest correu electrònic es torna a enviar 30 dies abans de l'expiració, en cas que el subscriptor no hagi sol·licitat encara la nova emissió.

4.8. Modificació de certificats

El subscriptor només pot modificar les dades de contacte associades al certificat però no les dades identificatives del mateix. Per canviar les dades de contacte cal que ho sol·liciti a través del web www.idcat.cat, seleccionant el seu certificat i introduint les noves dades.

4.9. Revocació i suspensió de certificats.

4.9.1. Causes de revocació de certificats

L'EC-idCAT revoca un certificat per les següents causes:

1. Circumstàncies que afecten la informació continguda al certificat
    - Modificació d'alguna de les dades contingudes al certificat.
    - Descobriment que alguna de les dades aportades a la sol·licitud de certificat és incorrecte, així com l'alteració o modificació de les circumstàncies verificades per a l'expedició del certificat.
    - Descobriment que alguna de les dades contingudes al certificat és incorrecte.
2. Circumstàncies que afecten la seguretat de la clau o del certificat
    - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-idCAT, sempre que afecti la fiabilitat dels certificats emesos a partir d'aquest incident.
    - Infracció, per l'EC-idCAT, dels requisits previstos en els procediments de gestió de certificats, establerts en aquest document.
    - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
    - Accés o utilització no autoritzats, per un tercer, de la clau privada del subscriptor.
    - L'ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el subscriptor.
    - Acabament de la relació entre l'EC-idCAT i subscriptor.
    - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor.
    - Infracció pel sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
    - Infracció pel subscriptor, de les seves obligacions, responsabilitat i garanties, establertes a l'eina jurídica corresponent o en aquest document.
    - La incapacitat sobrevinguda o la mort del subscriptor.
    - Sol·licitud del subscriptor de revocació del certificat, d'acord amb l'establert a la secció 3.4 d'aquesta política.
4. Altres circumstàncies

- La suspensió del certificat digital per un període superior a 120 dies.
- El final del servei de l'EC-idCAT, d'acord amb l'establert a la secció 5.8 d'aquest document.
- La finalització de prestació de serveis per part de CATCert, d'acord amb el que estableix la Política General de Certificació.
- Resolució judicial o administrativa que ho ordeni (Art. 8.1 de la Llei 59/2003, de signatura electrònica).
- Revocació d'ofici per error en la generació del certificat, ja sigui per una incidència tècnica o per error de l'operador en la introducció de les dades del subscriptor.

Si l'entitat a què es dirigeix la sol·licitud de revocació no disposa de tota la informació necessària per determinar la revocació d'un certificat, però té indicis del seu compromís, pot decidir la suspensió.En aquest cas es considera que les actuacions realitzades durant el període de suspensió no són vàlides, sempre que el certificat finalment sigui revocat. Són vàlides si s'aixeca la suspensió, a través de l'habilitació, i el certificat torna a passar a l'estat de vigència.

L'eina jurídica que vincula l'EC-idCAT amb el subscriptor estableix que el subscriptor sol·licita la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

4.9.2. Legitimació per a sol·licitar la revocació

Poden sol·licitar la revocació d'un certificat:

- El subscriptor a nom del qual el certificat va ser emès.
- L'Entitat de Registre idCAT que va intervenir a l'emissió.
- L'EC-idCAT

4.9.3. Procediments de sol·licitud de revocació

Per procedir a la sol·licitud de revocació, el subscriptor es persona a l'Entitat de Registre. La sol·licitud de revocació ha de ser lliurada presencialment, enviada per correu electrònic signat o per correu certificat convencional. S'ha d'incloure la informació suficient per poder identificar raonablement, a criteri de l'EC-idCAT, d'una banda, el certificat que se sol·licita revocar i, d'altra banda, l'autenticitat i autoritat del sol·licitant.

Aquesta informació suficient ha d'estar composta per les dades de contacte del posseïdor de claus inclòs el seu DNI o equivalent, i de l'entitat que demana la revocació, la data i la raó de la petició, així com el número de sèrie del certificat.

La petició de revocació amb la documentació necessària és recollida, registrada i notificada per l'Entitat de Registre.

S'arxiva i es comprova la documentació, s'autentica i s'autoritza el sol·licitant. Finalment es realitza la revocació en l'aplicació informàtica corresponent i, a continuació i de forma automàtica i immediata, s'indica l'esmentada revocació en l'estat del certificat en la llista de

revocacions. S'informa el subscriptor i, en el seu cas, el posseïdor de claus, sobre el canvi d'estat de revocació del certificat d'acord amb l'art. 10.2 de la Llei de signatura electrònica.

L'EC-idCAT no pot reactivar el certificat una vegada revocat.

Nota: Un certificat revocat no es pot tornar a utilitzar; això vol dir que no pot alçar-se la revocació, ni no anul·lar-se de cap altra forma: és un estat definitiu del certificat.

4.9.4. Període temporal de sol·licitud de revocació

Les sol·licituds de revocació es remeten de forma immediata quan es té coneixement de la causa de revocació.

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

La sol·licitud de revocació es processada en el mínim termini possible, sempre dins dels horaris d'oficina de l'Entitat de Certificació.

En cas de trobar-se fora d'hores d'oficina, el subscriptor pot sol·licitar la suspensió cautelar del certificat.

4.9.6. Obligació de consulta de informació de revocació de certificats

Els verificadors comproven l'estat d'aquells certificats en què desitgen confiar.

Un mètode pel qual es verifica l'estat dels certificats és consultant la llista de revocació de certificats o LRC més recent emesa per l'EC-idCAT. L'estat de vigència també es pot comprovar online mitjançant el protocol OCSP.

L'EC-idCAT subministra informació als verificadors sobre com i on trobar la LRC corresponent.

4.9.7. Freqüència d'emissió de llistes de revocació de certificats (LRCs)

L'EC-IDCAT emet una LRC almenys cada 24 hores. A més s'emet una nova LRC després de cada suspensió o revocació.

S'indica en la LRC el moment programat d'emissió d'una nova LRC, si bé es pot emetre una LRC abans del termini indicat en la LRC anterior.

Els certificats revocats o suspesos són retirats de la LRC transcorreguts seixanta dies des de l'expiració.

4.9.8. Període màxim de publicació de LRCs

Les LRCs es publiquen immediatament en el web del Servei de Certificació Digital del Consorci AOC.

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

Els verificadors de certificats digitals poden consultar un servei en línia que respongui sobre l'estat de certificats (servei *OCSP responder* o d'altres serveis de validació de certificats) operat per un prestador de serveis de validació en qui es confia.

El Consorci AOC ofereix de manera gratuïta un servei *OCSP responder* per a la comprovació en línia de l'estat dels certificats emesos per les Entitats de Certificació que integren la jerarquia pública de certificació de Catalunya.

La URL en la que es troba disponible l'esmentat servei s'indica en el contingut dels certificats emesos. La informació relativa al perfil OCSP i, en general, al funcionament del servei es pot trobar a http://www.aoc.cat/catcert .

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

El verificador que no utilitza LRC per comprovar la validesa d'un certificat, ho pot fer en el Dipòsit de l'EC-IDCAT, al qual s'haurà de poder accedir directament a través de la pàgina web del Servei de Certificació Digital del Consorci AOC.

Els verificadors comproven l'estat d'aquells certificats en els que desitgen confiar.

Una forma per la qual es verifica l'estat dels certificats és consultant la LRC més recent de l'EC-IDCAT.

L'EC-IDCAT subministra informació als verificadors referent a com i on trobar la LRC corresponent.

4.9.11. Altres formes d'informació de revocació de certificats

L'EC-IDCAT també informarà sobre la revocació dels certificats, mitjançant el protocol OCSP, que permet conèixer l'estat de vigència dels certificats on-line.

En la petició de consulta de vigència d'un certificat en línia s'ha de consignar un numero de sèrie del certificat sobre el qual es fa la petició i les dades identificatives de l'autoritat de certificació emissora.

Si la petició no està vàlidament realitzada o si el servei no pot donar una resposta en el moment de la sol·licitud, el servei OCSP retornarà una resposta que identifiqui el motiu pel qual no es torna aquesta resposta (sol·licitant no autoritzat, error en la resposta o inoperabilitat temporal del prestador requerit).

Si la petició està vàlidament realitzada i els serveis no tenen cap disfunció, es respondrà a la petició amb la consignació que el certificat és vàlid o que està revocat (en aquest cas es consignarà també el moment de la finalització de la vigència del certificat).

Aquesta resposta serà signada per l'Entitat de certificació amb el certificat corresponent (en aquest cas, el certificat d'infraestructura de servidor d'estat de certificats en línia –que rep l'acrònim CIO). Aquesta resposta serà emmagatzemada.

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

El compromís de la clau privada de l'EC-IDCAT és notificat, en la mesura possible, a tots els participants en la jerarquia pública de certificació de Catalunya, mitjançant el Directori del Servei de Certificació Digital del Consorci AOC.

4.9.13. Causes de suspensió de certificats

Els certificats es poden suspendre:

- Quan ho sol·liciti el posseïdor de claus o el subscriptor o un tercer autoritzat (art. 9.1.a de la Llei 59/2003)
- En els casos legals previstos a l'article 9.1 de la Llei de Signatura Electrònica, és a dir, en cas que una resolució judicial o administrativa ho ordeni.
- Quan la documentació requerida a la sol·licitud de revocació sigui suficient però no es pugui identificar raonablement el posseïdor de claus.
- Si el subscriptor no utilitza el certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest cas, l'EC-IDCAT ha d'assegurar-se que el certificat no està suspès durant més temps del necessari per consignar el seu compromís.
- Quan no s'activa el certificat en un termini de 120 dies a partir de la data d'emissió del certificat.

4.9.14. Legitimitat per sol·licitar la suspensió

1. El subscriptor que va demanar l'emissió de certificats (Sol·licitant de l'Entitat de Registre).
2. L'EC-IdCAT.

4.9.15. Procediments de sol·licitud de suspensió

La suspensió dels certificat digitals es pot realitzar de les formes que es detallen a continuació, tot informant al subscriptor d'acord amb els termes establerts a l'article 10.2 de la Llei de Signatura Electrònica:

1. La suspensió pot ser sol·licitada pel posseïdor de les claus i es pot dur a terme per mitjà d'una trucada al 902 90 10 80.
2. La suspensió pot ser sol·licitada per l'Entitat de Registre. En cas que l'Entitat de Registre disposi d'autorització del Consorci AOC, pot realitzar ella mateixa el procés de suspensió. En cas contrari, realitza la tramitació de la suspensió a través del Consorci AOC.
3. La suspensió pot ser realitzada per l'EC-IDCAT directament, a través del component LRA o des de la web de consulta avançada de certificats.

El procediment de suspensió es tramita de la mateixa manera que el procediment de revocació.

Per 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 (en cas que no sigui el mateix posseïdor)
- Informació de contacte la Institució que demana 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.
- Organisme i departament a què pertany el posseïdor de claus.
- Número de sèrie (serial number) del certificat digital que se sol·licita suspendre.
- Raó detallada per a la petició de suspensió.
- Codi de suspensió associat al certificat.

Un cop suspesa la vigència d'un certificat s'informarà al subscriptor i, en el seu cas, al posseïdor de claus, sobre el canvi d'estat de suspensió i que el termini màxim de la mateixa serà de 120 dies (arts. 10.2 i 10.4 de la llei 59/2003).

4.9.16. Període màxim de suspensió

El termini màxim de suspensió serà de cent vint dies naturals.

4.9.17. Habilitació d'un certificat suspès

El subscriptor podrà habilitar el certificat que roman suspès, personant-se i identificant-se davant l'Entitat de Registre, 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 LCRs es publiquen a la web del 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-IDCAT.

4.10.2. Disponibilitat dels serveis

Els verificadors de certificats digitals poden consultar un servei en línia que respongui sobre l'estat de certificats (servei *OCSP responder* o d'altres serveis devalidació de certificats) operat per un prestador de serveis de validació en qui es confia.

El Consorci AOC ofereix de manera gratuïta un servei *OCSP responder* per a la comprovació en línia de l'estat dels certificats emesos per les Entitats de Certificació que integren la jerarquia pública de certificació de Catalunya.

La URL en la que es troba disponible l'esmentat servei s'indica en el contingut dels certificats emesos. La informació relativa al perfil OCSP i, en general, al funcionament del servei es pot trobar a http://www.aoc.cat/catcert

4.10.3. Altres funcions dels serveis

Sense estipulació addicional.

4.11. Acabament de la subscripció

L'acabament de la subscripció no implica la revocació dels certificats que hagin estat emesos, sinó que aquests es poden utilitzar fins que expirin.

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

Sense estipulació addicional.

5.1.1 Localització i construcció de les instal·lacions

Sense estipulació addicional.

5.1.2 Accés físic

Sense estipulació addicional.

5.1.3 Electricitat i aire condicionat

Sense estipulació addicional.

5.1.4 Exposició a l'aigua

Sense estipulació addicional.

5.1.5 Advertència i protecció d'incendis

Sense estipulació addicional.

5.1.6 Emmagatzematge de suports

Sense estipulació addicional.

5.1.7 Tractament de residus

Sense estipulació addicional.

5.1.8 Còpia de seguretat fora de les instal·lacions

Sense estipulació addicional.

5.2 Controls de procediments

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

El personal al servei de l'EC-IdCAT realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'EC-IdCAT.

5.2.1 Funcions fiables

Sense estipulació addicional.

5.2.2 Nombre de persones per tasca

Sense estipulació addicional.

5.2.3 Identificació i autenticació per a cada funció

Sense estipulació addicional.

5.2.4 Rols que requereixen separació de tasques

Sense estipulació addicional.

5.3 Controls de personal

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

- Es manté la 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 en 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'extrauen 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 limitar la qualitat del 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 quals està sotmès

- El responsable de seguretat vetlla perquè el punt anterior sigui executat, proveint als responsables d'àrea tota la informació que fos 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-IdCAT

- 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

- 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 criptogràfics

- 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

Sense estipulació addicional.

5.3.2 Requisits de formació

Sense estipulació addicional.

5.3.3 Requisits i freqüència d'actualització formativa

Sense estipulació addicional.

5.3.4 Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5 Sancions per accions no autoritzades

Sense estipulació addicional.

5.3.6 Requisits de contractació de professionals

Sense estipulació addicional.

5.3.7 Subministrament de documentació al personal

Sense estipulació addicional.

5.4 Procediments d'auditoria de seguretat

5.4.1 Tipus d'esdeveniments registrats

Sense estipulació addicional.

5.4.2 Freqüència de tractament de registres d'auditoria

Sense estipulació addicional.

5.4.3 Període de conservació de registres d'auditoria

Sense estipulació addicional.

5.4.4 Protecció dels registres d'auditoria

Sense estipulació addicional.

5.4.5 Procediments de còpies de seguretat

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

- Es guarden en armaris ignífugues
- Solament persones autoritzades disposen d'accés a les còpies de seguretat
- Les còpies estan identificades
- Si un material ha contingut còpies de seguretat (disquets, dvd's...) ies 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

Sense estipulació addicional.

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

Sense estipulació addicional.

5.4.8 Anàlisi de vulnerabilitats

Sense estipulació addicional.

5.5 Arxiu d'informacions

Sense estipulació addicional.

5.5.1 Tipus d'esdeveniments registrats

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

L'EC-IdCAT guarda registre del següent:

Documents originals:

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

L'EC-IdCAT guarda, en relació amb els certificats Extended Validation:

- LOG i pistes d'auditoria
- Documentació relativa a peticions, verificacions i revocacions de certificats Extended Validation

5.5.2 Període de conservació de registres

L'EC-IDCAT 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

Sense estipulació addicional.

5.5.4 Procediments de generació de còpies de seguretat

Sense estipulació addicional.

5.5.5 Requisits de segellat de data i hora

Sense estipulació addicional.

5.5.6 Localització del sistema d'arxiu

L'EC-IdCAT 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

Sense estipulació addicional.

5.6 Renovació de claus

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

5.7 Compromís de claus i recuperació de desastre

5.7.1 Procediment de gestió d'incidències i compromisos

L'EC-IdCAT 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, EC-IdCAT inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per afer 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 EC-IdCAT (o pla de recuperació de desastres) considera el compromís, o la sospita de compromís, de la clau privada de EC-IdCAT com un desastre.

En cas de compromís, l'EC-IDCAT:

- 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-IDCAT ja no són vàlids

5.7.4 Desastre sobre les instal·lacions

L'EC-IDCAT 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 indiqui 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-IdCAT 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 (excepte en el mes d'agost)
- Publicació d'informació de revocació

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

5.8 Finalització del servei

5.8.1 EC-IDCAT

Sense estipulació addicional.

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 Entitat de Registre durant 15 anys després de finalitzar les activitats relacionades amb l'Entitat de Registre.

6. Controls de seguretat tècnica

L'EC-IdCAT 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

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

6.1.2. Tramesa de la clau privada al subscriptor

La clau privada és generada pel subscriptor en el seu sistema informàtic o al clauer i no ha de sortir sota cap concepte de l'esmentat sistema, per tant no hi ha cap tramesa de la clau privada, en cap direcció.

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

El mètode de tramesa de la clau pública a l'EC-IDCAT és PKCS #10.

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

La clau de l'EC-IDCAT i les claus de les Entitats de Certificació anteriors de la jerarquia pública de certificació de Catalunya estan a disposició als verificadors, assegurant la integritat de la clau i autenticant l'origen.

La clau pública de l'EC-ACC, que és l'arrel de la jerarquia, es publica en el directori de l'EC-IDCAT, en forma de certificat auto-signat, al costat d'una declaració referent a que la clau permet autenticar a l'EC-IDCAT.

S'estableixen mesures addicionals per confiar en el certificat auto-signat, com ara la comprovació de l'empremta digital del certificat.

La clau pública de l'EC-IDCAT es publica en el directori de l'EC-IDCAT, en forma de certificat CIC signat per l'EC-ACC.

Els usuaris accedeixen al Directori per obtenir les claus públiques de l'EC-IDCAT.

Una vegada que el subscriptor ha generat el parell de claus del certificat ambdues claus seran emmagatzemades al reposador de claus del sistema operatiu instal·lat a la màquina del Subscriptor o al clauer però a més, la clau pública junt amb les dades de la sol·licitud del certificat s'inseriran en un arxiu PKCS#10 (signat per la clau privada). Aquest arxiu és, en definitiva, la petició de certificació que s'envia a l'EC-idCAT.

Aquest enviament s'efectua mitjançant una comunicació segura a través del protocol SSL versió 2 amb autenticació exclusiva del servidor, i aquesta es emmagatzemada a la Taula de Sol·licituds de l'EC-idCAT.

6.1.4. Mides de claus

Les claus de l'EC-IDCAT són almenys de 2.048 bits.

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

6.1.5. Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.6. Comprovació de qualitat de paràmetres de clau pública

Es realitza d'acord amb l'informe especial de l' ETSI TS 101 276, que indica la qualitat dels algoritmes de signatura electrònica.

6.1.7. Generació de claus en aplicacions informàtiques o en bens d'equip

Els parells de claus de l'EC-IDCAT són generats utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica CEN CWA 14167 o equivalent.

Els parells de claus dels subscriptors de certificats reconeguts i certificats de nivell alt, s'han de generar al component d'Autoritat de Registre Local i en targetes intel·ligents, o en dispositius criptogràfics que compleixen els requisits establerts per les especificacions tècniques CEN CWA 14169 i CWA 14170 o equivalent.

L'EC-IDCAT o l'Entitat de Registre comprova l'autenticitat i el nivell de seguretat de les targetes o dispositius criptogràfics adquirits als proveïdors, abans d'autoritzar-ne l'ús.

La generació de claus per a la resta de certificats poden realitzar-se mitjançant aplicacions informàtiques.

6.1.8. Propòsits d'ús de claus

L'EC-IDCAT inclou l'extensió KeyUsage a 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

Les claus privades de les Entitats de Certificació es protegeixen utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica FIPS 140-2 Nivell 3 o superior.

Els parells de claus dels subscriptors de certificats reconeguts i de certificats de nivell alt estan protegits per targetes intel·ligents o altre maquinari que compleixen els requisits establerts per l'especificació tècnica CEN CWA 14169 o equivalent.

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

Les targetes amb circuit integrat (altrament, targetes intel·ligents) es lliuren per l'emissió de cada nou certificat per l'Entitat de Registre,o bé directament pel Consorci AOC quan actua com a Entitat de Registre Virtual.

Per cada nova emissió o renovació dels certificats es lliura una targeta nova, és a dir, no es carrega certificats en targetes ja usades.

Quan el Consorci AOC detecti errors o defectes en les targetes, podrà retirar d'ofici les targetes afectades. En cas de detectar defectes o errors en casos puntuals, es substituirà la targeta afectada, prèvia revocació del certificat i s'emetrà un nou certificat que es lliurarà en una targeta nova sense cost addicional per al subscriptor.

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

Dels 5 possibles dispositius criptogràfics que existeixen l'EC-IDCAT requereix el concurs d'al menys 2 de forma simultània.

Cada un d'aquests dispositius és responsabilitat d'una persona concreta, única coneixedora de la clau d'accés al mateix. La clau d'accés és coneguda únicament per una persona responsable d'aquest dispositiu. Cap d'elles no en coneix més que una de les claus d'accés.

Els dispositius criptogràfics queden emmagatzemats a les dependències de l'EC-IDCAT, i per al seu accés és necessària una persona addicional.

6.2.3. Dipòsit de la clau privada

Les claus privades de l'EC-IDCAT s'emmagatzemen en espais ignífugs i protegits per controls d'accés físic doble.

Les claus privades dels certificats de xifrat sí es podran emmagatzemar a l'EC-IDCAT.

6.2.4. Còpia de seguretat de la clau privada

Existeix còpia de seguretat de la clau privada de l'EC-IDCAT i dels mitjans necessaris per accedir, en lloc independent d'aquella on s'emmagatzema habitualment.

6.2.5. Arxiu de la clau privada

La clau privada de l'EC-IDCAT compta amb una còpia de seguretat realitzada, emmagatzemada, i recuperada quan convingui, per personal subjecte a la política de confiança del personal. Aquest personal està expressament autoritzat per a aquestes finalitats, i es limita a aquell que necessiti fer-ho en les pràctiques de l'EC-IDCAT.

Els controls de seguretat a aplicar en còpies de seguretat de l'EC-IDCAT són d'igual o superior nivell a les que s'apliquin a les claus habitualment en ús.

Quan les claus s'emmagatzemen en un mòdul maquinari de procés dedicat, es proveeixen els controls oportuns perquè aquestes mai no puguin abandonar el dispositiu.

No s'emmagatzemen còpies de les claus privades dels certificats, excepte en el cas dels certificats de xifrat, per garantir la recuperació de les dades.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

Les claus privades de l'EC-IDCAT queden emmagatzemades en fitxers xifrats amb claus fragmentades i en targetes intel·ligents (de les quals no poden ser extretes).

Aquestes targetes són utilitzades per introduir la clau privada en el mòdul criptogràfic.

6.2.7. Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generen directament en els mòduls criptogràfics.

6.2.8. Mètode d'activació de la clau privada.

Es requereixen almenys dues persones per activar la clau privada de l'EC-IDCAT.

Per a certificats personals i d'entitat, la clau privada del subscriptor s'activa mitjançant la introducció del PIN a la targeta intel·ligent.

6.2.9. Mètode de desactivació de la clau privada

No aplicable.

6.2.10. Mètode de destrucció de la clau privada

Les claus privades són destruïdes de manera que s'impedeixi el seu robatori, modificació, divulgació no autoritzada o ús no autoritzat.

6.2.11. Classificació dels mòduls criptogràfics

Els mòduls de l'EC-IDCAT obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) amb els augments que determinen a l'especificació tècnica CEN CWA 14167.

Els mòduls dels subscriptors de certificats reconeguts i certificats de nivell alt obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) o FIPS 140-2 nivell 3 amb els augments que determinen a l'especificació tècnica CEN CWA 14169 o equivalent.

6.3. Altres aspectes de gestió del parell de claus

6.3.1. Arxiu de la clau pública

L'EC-IDCAT arxiva les seves claus públiques, d'acord amb l'establert a la secció 5.5.

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

Els períodes d'utilització de les claus són les determinades per la durada del certificat, i una vegada transcorregut no es poden continuar utilitzant.

Com a excepció, la clau privada de desxifrat es pot continuar utilitzant fins després de l'expiració del certificat.

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

El subscriptor és responsable de tenir cura de la seva clau privada, amb una contrasenya el més completa possible, a través de l'aplicació (Cryptographic Service Provider).

S'aconsella que l'esmentada contrasenya no sigui massa curta i formada per números i lletres.

El subscriptor ha de recordar l'esmentada contrasenya.

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

Es garanteix que l'accés als sistemes és limitat a individus degudament autoritzats. En particular:

- L'EC-IDCAT garanteix una administració efectiva del nivell d'accés dels usuaris (operadors, administradors, així com de qualsevol usuari amb accés directe al sistema) per mantenir la seguretat del sistema, incloent la gestió de comptes d'usuari, auditoria i modificacions o denegacions d'accés oportunes.

- L'EC-IDCAT garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada en les pràctiques de l'EC-IDCAT, incloent la separació de funcions d'administració dels sistemes de seguretat i dels operadors. En concret, l'ús de programes d'utilitats del sistema està restringit i estretament controlat.

- El personal de l'EC-IDCAT està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.

- El personal de l'EC-IDCAT és responsable i pot justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.

- Ha d'evitar-se la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que quedin accessibles a usuaris no autoritzats.

- Els sistemes de seguretat i monitoratge permeten una ràpida detecció, registre i actuació davant d'intents d'accés irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).

- L'accés als dipòsits públics de la informació de l'EC-IDCAT (per exemple, certificats o informació d'estat de revocació) conta amb un control d'accessos per a modificacions o esborrament de dades.

6.5.2. Avaluació del nivell de seguretat informàtica

Les aplicacions de EC i ER són fiables, d'acord amb l'especificació tècnica CEN CWA 14167-1, avaluant-se el grau de compliment mitjançant una auditoria de seguretat informàtica conforme amb l'especificació tècnica CEN CWA 14172-3 i un perfil de protecció adequat, d'acord amb la norma ISO 15408 o equivalent.

6.6. Controls tècnics del cicle de vida

6.6.1. Controls de desenvolupament de sistemes

Es realitza una anàlisi de requisits de seguretat durant les fases de disseny i especificació de requisits de qualsevol component utilitzat en les aplicacions d'Autoritat (tècnica) de certificació i d'Autoritat (tècnica) de Registre, per garantir que els sistemes són segurs.

S'utilitzen procediments de control de canvis per a les noves versions, actualitzacions i pegats d'emergència, dels esmentats components.

6.6.2. Controls de gestió de seguretat

L'EC-IDCAT garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures i, en particular, ha d'assegurar que existeixen instruccions per:

a. Operar els mòduls de forma correcta i segura.

b. Instal·lar els mòduls minimitzant el risc de fallada dels sistemes.

c. Protegir els mòduls contra virus i programari maliciós, per garantir la integritat i validesa de la informació que processen.

L'EC-IDCAT manté un inventari de tots els actius informàtics i realitza una classificació dels mateixos d'acord amb les seves necessitats de protecció, coherent amb l'anàlisi de riscs efectuada.

La configuració dels sistemes s'audita de forma periòdica, d'acord amb l'establert a la secció 8.1.

Es realitza un seguiment de les necessitats de capacitat, i es planificaran procediments per garantir suficient disponibilitat electrònica i d'emmagatzematge per als actius informatius.

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-IDCAT és limitat a individus degudament autoritzats. En particular:

- S'implementen controls (com per exemple tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'EC-IDCAT.

- Les dades sensibles es protegeixen quan s'intercanvien a través de xarxes no segures (incloent les dades de registre del subscriptor).

- Es garanteix que els components locals de xarxa (com direccionadors) es troben ubicats en entorns segurs, així com 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

Els documents descriptius dels diversos perfils de certificats digitals que expedeix l'EC-IdCAT es publiquen a la web del Consorci AOC http://www.aoc.cat/catcert/.

7.2 Perfil de la llista de revocació de certificats

L'accés a la informació relativa a la llista de revocació de certificats es publica al web del Consorci AOC http://www.aoc.cat/catcert/.

8. Auditoria de conformitat

EC-IDCAT 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.

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

8.1 Freqüència de l'auditoria de conformitat

Sense estipulació addicional.

8.2 Identificació i qualificació de l'auditor

L'EC-idCATAL acut 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-IDCAT.

8.4 Relació d'elements objecte d'auditoria

Sense estipulació addicional.

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

Sense estipulació addicional.

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 EC-IdCAT en la prestació dels seus serveis. Les tarifes es poden consultar a la web del servei de certificació digital 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 reembossaments. 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 l'article 20.2 de la Llei 59/2003, de 19 de desembre, excepte quan es trobi eximit 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 confiïn en certificats

En cas d'ús incorrecte o no autoritzat dels certificats, el Consorci AOC (o l'EC-IDCAT) no actuarà com a agent fiduciari davant 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-IDCAT).

9.3 Confidencialitat

9.3.1 Informacions confidencials

Sense estipulació addicional.

9.3.2 Informacions no confidencials

Sense estipulació addicional.

9.3.3 Responsabilitat per a la protecció d'informació confidencial

Sense estipulació addicional.

9.4 Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

Sense estipulació addicional.

9.4.2. Dades de caràcter personal no disponibles a tercers

Sense estipulació addicional.

9.4.3. Dades de caràcter personal disponibles a tercers

Sense estipulació addicional.

9.4.4. Responsabilitat corresponent a la protecció de dades personals

Sense estipulació addicional.

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

Sense estipulació addicional.

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

Sense estipulació addicional.

9.4.7. Comunicació de dades personals

Sense estipulació addicional.

9.5 Drets de propietat intel·lectual

9.5.1 Propietat dels certificats i informació de revocació

Sense estipulació addicional.

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

Sense estipulació addicional.

9.5.3 Propietat de la informació relativa a noms

Sense estipulació addicional.

9.5.4 Propietat de claus

Sense estipulació addicional.

9.6 Obligacions i responsabilitat civil

9.6.1 Entitats de Certificació

9.6.1.1 Obligacions generals de l'EC-IDCAT

Sense estipulació addicional.

9.6.1.2 Garanties oferides a subscriptors i verificadors

Sense estipulació addicional.

9.6.2 Obligacions i altres compromisos de les Entitats de Registre

9.6.2.1 Obligacions i altres compromisos

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

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

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 que realitza les comprovacions que considera necessàries sobre la identitat i la resta de dades personals i complementàries dels subscriptors.

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

Si l'Entitat de Registre detecta errors en les dades que estan incloses als certificats, o als documents que justifiquen 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 el 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 subscriptors i verificadors

9.6.3.1 Garantia del Consorci AOC pels serveis de certificació digital

Sense estipulació addicional.

9.6.3.2 Exclusió de la garantia

Sense estipulació addicional.

9.6.4 Subscriptors

9.6.4.1 Obligacions i altres compromisos

Sense estipulació addicional.

9.6.4.2 Garanties oferides pel subscriptor

Sense estipulació addicional.

9.6.4.3 Protecció de la clau privada

Sense estipulació addicional.

9.6.5 Verificadors

9.6.5.1 Obligacions i altres compromisos

Sense estipulació addicional.

9.6.5.2 Garanties oferides pel verificador

Sense estipulació addicional.

9.6.6 Altres participants

9.6.6.1 Obligacions i garanties del directori

Sense estipulació addicional.

9.6.6.2 Garanties oferides pel directori

EC-IDCAT té la responsabilitat civil del directori de certificació.

9.7 Renúncies de garanties

9.7.1 Rebuig de garanties de l'EC-IDCAT

EC-IDCAT pot rebutjar totes les garanties del servei que no es trobin vinculades a obligacions establertes per la Llei 59/2003, de 19 de desembre, incloent especialment la garantia d'adaptació per a un propòsit particular o garantia d'ús mercantil del certificat.

9.8 Limitacions de responsabilitat

9.8.1 Limitacions de responsabilitat de l'EC-IDCAT

EC-IdCAT limita la seva responsabilitat restringint el servei a l'emissió i gestió de certificats i, en el seu cas, de parells de claus de subscriptors i dipòsits criptogràfics (de signatura i verificació de signatura, així com de xifrat o desxifrat).

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

9.8.2 Cas fortuït i força major

L'EC-IDCAT 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

EC-IDCAT 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

EC-IDCAT 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

Sense estipulació addicional.

9.11 Notificacions

Sense estipulació addicional.

9.12 Modificacions

9.12.1 Procediment per a les modificacions

Sense estipulació addicional.

9.12.2 Termini i mecanismes per a notificacions

Les modificacions d'aquest document seran aprovades pel Consorci AOC, conforme 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

Sense estipulació addicional.

9.13.2 Jurisdicció competent

Sense estipulació addicional.

9.14 Llei aplicable

Sense estipulació addicional.

9.15 Conformitat amb la llei aplicable

EC-IDCAT manifesta, en aquest document i en els instruments jurídics amb subscriptors, el compliment de la Llei 59/2003, de 19 de desembre, de signatura electrònica. La prestació de serveis s'ajusta a la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic.

9.16 Clàusules diverses

9.16.1 Acord íntegre

Sense estipulació addicional.

9.16.2 Subrogació

Sense estipulació addicional.

9.16.3 Divisibilitat

Sense estipulació addicional.

9.16.4 Aplicacions

Sense estipulació addicional.

9.16.5 Altres clàusules

Sense estipulació addicional.

ANNEX – Control documental

Control de versions DPC EC-IDCAT 1er semestre 2016

Projecte:	**Informe modificació del document DPC EC-IDCAT**
Entitat de destí:	**Consorci AOC**
Codi de referència:	**Revisió 1er semestre 2016**
Versió:	**Canvis de la v3.8 a la v4.0 en català i en castellà**
Data de l'edició:	**05/08/2016**

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
4.0	Totes	Revisió global - Integració de CATCert a Consorci AOC	Servei de Certificació Digital - Consorci AOC	05/08/2016