Consorci
Administració Oberta
de Catalunya

Declaració de Pràctiques de Certificació
Entitat de Certificació GENCAT
(EC-GENCAT)

Referència:	D1111_E0650_N-DPC EC-GENCAT
Versió:	2.0
Data:	05/08/2016

Control documental

Estat formal	**Elaborat per:** Servei de Certificació Digital - AOC	**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 GENCAT	
Fitxer	D111 E0650 N-DPC EC-GENCAT v2r0 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	 Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.cao envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

Índex

1. Introducció

Aquest document és la Declaració de Pràctiques de Certificació de l'Entitat de Certificació 'GENCAT (d'ara endavant, EC-GENCAT.

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

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 GENCAT (denominada EC-GENCAT) es va crear per satisfer les necessitats de l'Administració de la Generalitat de Catalunya. Posteriorment, es va crear l'Entitat de Certificació de Secretaria d'Administració i Funció Pública, sota la jerarquía de l'EC-GENCAT. L'EC-SAFP és l'entitat de certificació que emet certificats a l'usuari final, de tal manera que l'EC-GENCAT es manté operativa per garantir el funcionament de la jerarquía, però no emet certificats a usuaris finals, emetent només els certificats d'infraestructura corresponents.

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

Els certificats d'infraestructura són aquells que s'emeten per gestionar i operar la infraestructura de clau pública (PKI), que és el sistema tècnic, jurídic, de seguretat i d'organització que ofereix suport als serveis de certificació i de signatura electrònica.

L'EC-GENCAT emet els següents tipus de Certificats d'infraestructura:

1) Certificat d'infraestructura d'entitat de certificació vinculada (CIC), que s'expedeix a les Entitats de Certificació que es vinculen a la jerarquia.

   Les Entitats de Certificació vinculades poden, al seu torn, emetre certificats d'infraestructura o certificats d'entitat final (personals, d'entitat i de dispositiu), segons la classe del certificat CIC que posseeixin, des del moment en el qual hagin obtingut un certificat CIC vàlid, i mentre l'esmentat certificat sigui vigent.

2) Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR), que s'empra per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.

3) Certificat d'infraestructura de dispositiu servidor segur (CIDS), que utilitza una aplicació informàtica servidor de SSL o de TLS d'infraestructura per identificar-se davant les aplicacions client que s'hi connecten i per protegir el secret de les comunicacions entre el client i el servidor, com per exemple els servidors de les entitats de certificació.

4) Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA), que s'utilitza per aplicacions informàtiques de la infraestructura que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i que reben documents i missatges xifrats, com per exemple les aplicacions de notificació de missatges de les entitats de certificació.

5) Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO), que utilitza un servidor OCSP Responder per signar les seves respostes sobre l'estat de validesa dels certificats.

6) Certificat d'infraestructura d'entitat de segells de temps (CIT), que utilitza una entitat per signar els segells de temps que emet.

7) Certificat d'infraestructura d'entitat de validació (CIV), que utilitzat un servidor d'entitat de validació per signar els seus informes.

1.1.1.1 Certificat d'infraestructura d'entitat de certificació vinculada (CIC)

Els certificats CIC són aquells certificats d'infraestructura emesos únicament a altres Entitats de Certificació que, d'aquesta forma, queden vinculades a la jerarquia pública de certificació de Catalunya.

Els certificats CIC s'expedeixen per oferir serveis a una comunitat d'usuaris concreta dins de la jerarquia pública de certificació de Catalunya i poden ser de diferents nivells (nivell 1, 2 o successius).

Amb aquests certificats, es faculta a les Entitats de Certificació a emetre certificats a usuaris finals o a altres Entitats de Certificació dins de la seva pròpia comunitat d'usuaris, en funció de les seves necessitats concretes i sempre que tècnicament no afecti el funcionament, plataformes, sistemes i aplicacions emprats habitualment pels usuaris finals.

Cada certificat CIC rep un nivell, adequat al seu període de durada, que s'utilitzarà per a la programació de la renovació periòdica de la infraestructura de certificació.

Aquests certificats permeten que les Entitats de Certificació subscriptores puguin expedir certificats a altres usuaris, ja siguin altres Entitats de Certificació de nivell inferior dins de la jerarquia, com entitats finals (personals, d'entitat, de dispositiu i d'objecte), des del moment en què hagin obtingut un certificat CIC vàlid i mentre aquest certificat sigui vigent.

Aquests certificats generalment són emesos pel Consorci AOC, com a Entitat de Certificació Arrel, a organitzacions que operen una Entitat de Certificació dins de la seva jerarquia per a diferents usos, segons la seva classe.

Aquests certificats CIC s'obtenen després d'un procés d'admissió de l'EC Vinculada als serveis de certificació del Consorci AOC, procés descrit a la Política General de Certificació del Consorci AOC.

La futura EC Vinculada no podrà sol·licitar el Certificat CIC fins que no hagi completat el seu procediment d'admissió en la Jerarquia d'Entitats de Certificació de Catalunya d'acord amb la Política General de Certificació del Consorci AOC.

1.1.1.2 Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR)

Els CIPISR són certificats d'infraestructura emesos a operadors d'Entitats de Registre per als treballs d'emissió i gestió del cicle de vida de certificats d'una Entitat de Certificació.

Per consegüent, aquests certificats s'utilitzen únicament per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació, i no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

Els CIPISR s'emeten en dues modalitats: de classe 1 i de classe 2. Els CIPISR de classe 1 s'expedeixen a operadors d'Entitats de Registre en l'àmbit de les institucions integrants del sector públic català, mentre que els CIPISR de classe 2 s'expedeixen a operadors d'entorns tancats d'usuaris en l'àmbit privat.

La durada de la llicència dels CIPISR, de classe 1 i 2, és de quatre (4) anys, a comptar des de la data de la seva emissió.

1.1.1.3 Certificat d'infraestructura de dispositiu servidor segur (CIDS)

Els CIDS són certificats d'infraestructura emesos a Entitats de Certificació responsables de l'operació de servidors segurs SSL o TLS amb la finalitat d'identificar-se davant de les aplicacions client que es connecten i la protecció del secret de les comunicacions entre el client i el servidor.

Els certificats CIDS es caracteritzen pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat del subscriptor del certificat.

Els certificats CIDS són certificats destinats a ser utilitzats exclusivament en un servidor del subscriptor identificat en el propi certificat, que l'identifiquen electrònicament i protegeixen la informació entre el client i el servidor. Per això, és condició essencial per a la validesa del certificat CIDS l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

La durada de la llicència dels CIDS és de quatre (4) anys, a comptar des de la data de la seva emissió.

1.1.1.4 Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA)

Els certificats CIDA són certificats d'infraestructura, emesos a Entitats de Certificació responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, signen electrònicament *webservices* o altres protocols i reben documents i missatges xifrats.

Com a certificat de dispositiu, els certificats CIDA es caracteritzen pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza les operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat del subscriptor del certificat.

Els certificats CIDA són certificats destinats a ser utilitzats exclusivament en un dispositiu del subscriptor identificat en el propi certificat i, per tant, en els sistemes del subscriptor del certificat.

La durada de la llicència dels CIDA és de quatre (4) anys, a comptar des de la data de la seva emissió.

1.1.1.5 Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO)

Els certificats CIO són aquells certificats d'infraestructura, emesos per gestionar els serveis de certificació, que s'expedeixen a Entitats responsables de l'operació de servidors OCSP Responder, per signar les seves respostes sobre l'estat de validesa dels certificats.

Els certificats CIO són certificats destinats a ser utilitzats exclusivament en un servidor OCSP Responder de l'Entitat subscriptora, servidor que es troba identificat en el propi certificat. Per això, és condició essencial per a la validesa del certificat CIO l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

La durada de la llicència dels CIO és de quatre (4) anys, a comptar des de la data de la seva emissió.

1.1.1.6 Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet

Els certificats CIT són certificats expedits a les Entitats responsables de l'operació d'autoritats de segellat de temps i hora (d'ara endavant, TSA) que s'utilitzen per signar els segells de temps que emeten aquestes autoritats.

Els CIT són certificats ordinaris que serveixen per gestionar els serveis de certificació i per garantir la data i l'hora d'un acte determinat.

La durada de la llicència dels CIT és de quatre (4) anys, a comptar des de la data de la seva emissió.

Els certificats CIT són emesos exclusivament perquè les Entitats subscriptors signin els segells de temps que emeten.

1.1.1.7 Certificat d'infraestructura d'entitat de validació (CIV)

Els certificats CIV són certificats d'infraestructura, emesos per gestionar els serveis de certificació, que s'expedeixen a Entitats de Validació perquè signin els informes de validació que emeten.

El certificat CIV ofereix, respecte dels Informes de Validació signats amb aquest certificat, les garanties següents:

- Garantia de verificació dels certificats o signatures respecte dels quals s'hagi realitzat la sol·licitud de l'Informe de Validació.
- Garantia del contingut dels esmentats certificats o signatures prèviament verificats.
- Garantia de la data i hora de l'informe.

La durada de la llicència dels CIV és de quatre (4) anys, a comptar des de la data de la seva emissió.

Addicionalment, en funció dels requeriments tècnics i de les necessitats dels usuaris, és possible que els esmentats tipus de certificats puguin incorporar altres funcionalitats que, en tot cas, s'identificaran a cada política específica de certificació que haurà de ser aprovada pel 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-GENCAT.

L'EC-GENCAT emet certificats dins de la Jerarquia pública de certificació de l'Agència Catalana de Certificació. 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-GENCAT 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-GENCAT".

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

1.3.6.1.4.1.15096.1.2.3

1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIC.-** Certificat d'infraestructura d'entitat de certificació vinculada:

- Els CIC de nivell 2 s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.12.
    - **Certificat d'Infraestructura de l'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP)**

- **CIPISR.- Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors**

  Els certificats CIPISR de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.15.

  Els certificats CIPISR de classe 2 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.16.

- **Certificat d'infraestructura de dispositiu servidor segur (CIDS)**

  Els certificats CIDS de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.17.

- **Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA)**

  Els certificats CIDA de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.18.

- **Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO)**

  Els certificats CIO de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.19.

- **Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet.**

  Els certificats CIT de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.111.

- **Certificat d'infraestructura d'entitat de validació (CIV).**

  Els certificats CIV de classe 1 emesos per l'EC-GENCAT s'identifiquen amb l'identificador d'objecte (OID): 1.3.6.1.4.1.15096.1.3.1.20.

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

1.3 Comunitat d'usuaris de certificats

Aquesta DPC regula una comunitat d'usuaris, que obtenen certificats per a diverses relacions administratives i privades, d'acord amb la Llei 59/2003, de 19 de desembre, de signatura electrònica i la normativa administrativa corresponent.

Els certificats d'infraestructura de l'EC-GENCAT no s'expedeixen al públic, sinó a:

- L'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP).

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 prestador de serveis de certificació genera els certificats digitals mitjançant l'operació d'entitats de certificació de la seva titularitat que signen els certificats.

El Consorci AOC és el prestador de serveis de certificació de l'EC-GENCAT.

En la seva funció de prestador de serveis de certificació, el Consorci AOC és responsable de la actuació de l'EC-GENCAT davant dels usuaris finals i en especial dels 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-GENCAT

L'EC-GENCAT és l'Entitat de Certificació del sector públic 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-GENCAT és:

```
f0 b7 5b b7 93 11 b0 e5 d0 10 f1 ed 8d c7 e5 8f 15 be 68 fd
```

1.3.4 Entitats de Registre

Les Entitats de Registre són les persones físiques o jurídiques que assisteixen a les Entitats de Certificació Vinculades a determinats procediments i relacions amb els sol·licitants i subscriptors de certificats, especialment als tràmits d'identificació, registre i autenticació dels subscriptors dels certificats i dels posseïdors de claus.

1.3.5 Usuaris finals

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

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

1.3.5.1 Sol·licitants de certificats

Els sol·licitants dels certificats indicats en aquesta DPC són les persones autoritzades per les Entitats de Certificació subscriptora.

Poden ser sol·licitants:

- La persona que serà el futur posseïdor de claus.
- Una persona autoritzada per:
    - L'Entitat de Certificació de la Secretaria d'Administració Pública (EC-SAFP).
    - L'entitat de Certificació SectorPúblic (EC-SectorPublic)
    - L'Entitat de Certificació Ciutadania (EC-CIUTADANIA)
    - L'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP)
    - L'Entitat de Certificació de Ciutadans (EC-idCAT).
    - L'Entitat de Certificació de l'Administració Local (EC-AL).
    - L'Entitat de Certificació d'Universitats i Recerca (EC-UR)
    - L'Entitat de Certificació del Parlament de Catalunya (EC-PARLAMENT)

L'autorització es podrà realitzar de forma expressa o tàcita i, en aquells casos en els quals l'EC-GENCAT ho consideri convenient, s'haurà de formalitzar documentalment.

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 dels certificats d'infraestructura és:

- L'Entitat de Certificació de la Secretaria d'Administració Pública (EC-SAFP).
- L'entitat de Certificació SectorPúblic (EC-SectorPublic)
- L'Entitat de Certificació Ciutadania (EC-CIUTADANIA)
- L'Entitat de Certificació de la Secretaria d'Administració i Funció Pública (EC-SAFP)
- L'Entitat de Certificació de Ciutadans (EC-idCAT).
- L'Entitat de Certificació de l'Administració Local (EC-AL).
- L'Entitat de Certificació d'Universitats i Recerca (EC-UR)
- L'Entitat de Certificació del Parlament de Catalunya (EC-PARLAMENT)

1.3.5.3 Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus de signatura digital de certificats personals o d'entitat, de classe 1 o 2 d'organització, que estan degudament autoritzades per això pel subscriptor i degudament identificades al certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim (aquesta última possibilitat s'aplica únicament als certificats de classe 2).

1.3.5.4 Usuaris de certificats

Els ls suaris dels certificats són els verificadors

1.3.5.5 Verificadors de certificats

Els verificadors són les persones (s'inclouen les persones físiques, institucions, persones jurídiques i altres organitzacions i entitats) que reben signatures digitals i certificats digitals i han de verificar-los com a pas previ per 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 Ús típic dels certificats

1.4.1.1 Certificat d'infraestructura d'entitat de certificació vinculada (CIC) que s'expedeix a les Entitats de Certificació que es vinculen a la jerarquia

Aquests certificats permeten que les Entitats de Certificació subscriptores puguin expedir certificats a altres usuaris, ja siguin altres Entitats de Certificació de nivell inferior dins de la jerarquia, com entitats finals (personals, d'entitat, de dispositiu i d'objecte), des del moment en què hagin obtingut un certificat CIC vàlid i mentre aquest sigui vigent.

Aquests certificats generalment són emesos pel Consorci AOC, com a EC Arrel, a organitzacions que operen una EC dins de la seva jerarquia, per a diferents usos, segons la seva classe:

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC.
- Emissió i signatura de certificats CIC, CIPISR, CIDS, CIDA, CIO, CIT i CIV.
- Emissió i signatura de llistes de revocació de certificats (LRC).

a. Certificat d'Infraestructura d'Entitat de Certificació

Els usos permesos del certificat CIC de l'EC-GENCAT són:

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC.
- Emissió i signatura de certificats CIC, CIPISR, CIDS, CIDA, CIO, CIT i CIV.
- Emissió i signatura de llistes de revocació de certificats (LRC).

1.4.1.2 Certificat d'infraestructura personal de signatura electrònica reconeguda d'operadors (CIPISR)

Aquests Certificats permeten que els operadors d'Entitats de Registre realitzin els treballs d'emissió i de gestió del cicle de vida de certificats d'una Entitat de Certificació.

Per consegüent, aquests certificats s'utilitzen únicament per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació, i no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

1.4.1.3 Certificat d'infraestructura de dispositiu servidor segur (CIDS)

Aquests Certificats permeten que les Entitats de Certificació responsables de l'operació de servidors segurs SSL o TLS:

- S'identifiquin davant de les aplicacions client que es connectin,
- Protegeixin el secret de les comunicacions entre el client i el servidor.

Els Certificats CIDS estan destinats a ser utilitzats exclusivament en un servidor del subscriptor identificat en el propi certificat, que l'identifiquen electrònicament i protegeixen la informació entre el client i el servidor. Per això, és condició essencial per a la validesa del certificat CIDS l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

1.4.1.4 Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA)

Aquests Certificats permeten que les Entitats de Certificació responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment signin electrònicament *webservices* o altres protocols i rebin documents i missatges xifrats.

Els Certificats CIDA estan destinats a ser utilitzats exclusivament en un dispositiu del subscriptor identificat en el propi certificat i, per tant, en els sistemes del subscriptor del certificat.

1.4.1.5 Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO)

Aquests Certificats permeten que les Entitats responsables de l'operació de servidors OCSP Responder signin les seves respostes sobre l'estat de validesa dels certificats.

Els certificats CIO són certificats destinats a ser utilitzats exclusivament en un servidor OCSP Responder de l'Entitat subscriptora, servidor que es troba identificat en el propi

certificat. Per això, és condició essencial per a la validesa del certificat CIO l'especificació dels sistemes del subscriptor en els quals s'utilitzaran els certificats.

1.4.1.6 Certificat d'infraestructura d'entitat de segells de temps (CIT)

Aquests Certificats permeten que les Entitats responsables de l'operació d'autoritats de segellat de temps i hora (d'ara endavant, TSA) signin els segells de temps que aquestes Entitats emeten.

Els CIT són certificats ordinaris que serveixen per gestionar els serveis de certificació i per garantir la data i l'hora d'un acte determinat.

1.4.1.7 Certificat d'infraestructura d'entitat de validació (CIV)

Aquests Certificats permeten que les Entitats de Certificació, actuant com a Entitats de Validació, signin els informes de validació que emeten.

1.4.2 Aplicacions prohibides

1.4.2.1 Informacions per a tots els tipus de certificats

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 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 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 Requisits específics per als CIC

Els certificats CIC s'atendran a allò que es disposa en aquesta DPC i, en tot cas, les limitacions estaran delimitades per la classe de certificat CIC i per la política del certificat en qüestió.

1.4.2.3 Requisits específics per als CIPISR

Els CIPISR no es poden utilitzar per a cap altre ús que no sigui el d'operador d'Entitat de Registre.

1.4.2.4 Requisits específics per als CIDS, CIDA, CIO, CIT i CIV

Els CIDS, CIDA, CIO, CIT i CIV no es poden utilitzar en sistemes diferents dels d'Entitat de Certificació.

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-GENCAT 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-GENCAT, 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-GENCAT

L'EC-GENCAT publica les informacions següents al seu web (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 i, quan sigui convenient, les polítiques específiques.

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.

Qualsevol canvi en les especificacions o en les condicions del servei es comunica als usuaris per l'EC-GENCAT a través del directori.

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-GENCAT 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.*

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-GENCAT, podent ser consultades pels interessats.

La informació d'estat de revocació de certificats es publica d'acord amb allò establert a la secció 4.7.10.

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

3.1.1.1 Estructura sintáctica

Tots els certificats contenen un nom diferenciat X.501 en el camp Subject, incloent un component Common Name (CN=).

L'estructura sintàctica i el contingut dels camps de cada certificat, així com els seu significat semàntic, es troben descrits en el document "perfil de certificat" corresponent que el Consorci AOC publica al seu web (http://www.aoc.cat/catcert/).

3.1.1.2 Perfils dels certificats

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

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 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

L'EC-GENCAT emet diferents tipus de certificats. Els noms dels subscriptors de certificats són únics per a cada servei de generació de certificats operat per l'EC-GENCAT i per a cada tipus de certificat, és a dir, una mateixa persona només pot tenir al seu nom certificats de tipus diferents emesos per l'EC-GENCAT.

No es pot tornar a assignar un nom de subscriptor que ja hagi estat ocupat a un subscriptor diferent.

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 d'una organització

Aquesta secció conté els requisits per a la comprovació de la identitat d'una organització identificada en el certificat.

En general, l'EC-GENCAT no haurà de determinar que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat. Tampoc actuarà com àrbitre o mediador, ni haurà de resoldre cap disputa concernent a la propietat de noms de persones o organitzacions, noms de domini, marques o noms comercials (per exemple, relatius a direccions electròniques).

3.2.2.1 Entitats de Certificació Vinculades

No es requereix realitzar procediment d'autenticació de les Entitats de Certificació Vinculades a la jerarquia pública de certificació del Consorci AOC, ja que aquestes es creen en el si de la jerarquia mitjançant un procediment aprovat per la pròpia EC-GENCAT denominat "Cerimònia de Claus", descrit a la secció corresponent d'aquesta DPC.

3.2.2.2 Entitats de Registre

L'EC-GENCAT autentica, prèviament a l'emissió i al lliurament d'un certificat CIPISR, per a qualsevol dels components d'una Entitat de Registre, la identitat de l'Entitat de Registre i de l'operador conforme a la secció corresponent d'aquesta DPC.

3.2.2.3 Subscriptors de Certificats

No es requereix realitzar procediment d'autenticació de l'organització titular del certificat, ja que es tracta de certificats corporatius, en els quals l'organització subscriptora del certificat i l'Entitat de Registre coincideixen.

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.

3.2.3.1 Elements d'identificació

El número i tipus de documents necessaris per a acreditar la identitat del posseïdor de claus són els que admet l'EC-GENCAT,, tal com es recull en la seva normativa reguladora.

En tot cas, aquests documents identificatius contindran com a mínim:

- Nom i cognoms de la persona
- Número d'identitat reconegut legalment (DNI, NIF o NIE dels països signants de l'Acord de Schengen; passaport en el cas dels certificats d'estranger)
- Data i lloc de naixement.
- Qualsevol altra informació que pugui ser utilitzada per a diferenciar a una persona d'altra, dintre de l'àmbit de la Institució (per exemple: fotografia, correu-e, categoria, càrrec, etc.).

3.2.3.2 Validació dels elements d'identificació

Sense estipulació addicional.

3.2.3.3 Necessitat de presència personal

Sense estipulació addicional.

3.2.3.4 Vinculació de la persona física amb l'organització

- Requisits per a certificats de classe 1

Com que es tracta de certificats corporatius, en els quals l'Entitat de Registre i el subscriptor coincideixen, no és necessari obtenir una justificació documental específica de la vinculació del posseïdor de la clau amb l'Entitat de Registre, sinó que s'utilitzen els registres interns de la Institució.

- Requisits per a certificats de classe 2

L'EC-GENCAT ha d'obtenir una justificació documental de la vinculació de la persona física amb l'organització, mitjançant qualsevol mitjà admès en dret.

L'EC-GENCAT pot utilitzar Entitats de Registre per a aquesta tasca.

3.2.4 Informació no verificada

L'EC-GENCAT es responsabilitza que tota la informació inclosa en la sol·licitud del certificat sigui exacta i completa per a la finalitat del certificat; i que té dret al seu ús (per exemple, dret a utilitzar cert nom en l'adreça de correu electrònic o la legitimitat en l'ús d'un servidor web).

No obstant això, els certificats poden incloure informació no verificada, com per exemple l'adreça de correu electrònic, sempre que s'indiqui als usuaris finals en el propi certificat o en els instruments jurídics corresponents.

3.3 Identificació i autenticació de sol·licituds de renovació

3.3.1 Validació per a la renovació de certificats

Abans de renovar un certificat, l'Entitat de Certificació haurà de comprovar - mitjançant la intervenció d'una Entitat de Registre - que la informació utilitzada pera verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau continuen essent 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 en la secció corresponent.

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

4.1.1.1 Requisits generals

Únicament poden sol·licitar certificats d'infraestructura les Entitats de Certificació Vinculades a la jerarquia pública de certificació de Catalunya, operada pel Consorci AOC.

4.1.1.2 Requisits específics per al Certificat CIC

La futura Entitat de Certificació no podrà sol·licitar el Certificat CIC fins que no hagi completat el seu procediment d'admissió, a la Jerarquia d'Entitats de Certificació del Consorci AOC.

4.1.2 Procediment d'alta; Responsabilitats

L'EC-GENCAT, amb caràcter previ a l'emissió d'un certificat, s'assegura que les sol·licituds de certificats estiguin completes, precises i degudament autoritzades.

Abans de l'emissió i lliurament d'un certificat, l'EC-GENCAT informarà el subscriptor o, en el seu cas, el posseïdor de claus dels termes i condicions aplicables al certificat. Aquest requisit es compleix mitjançant el lliurament de l'instrument jurídic que vincula l'EC-GENCAT amb el subscriptor o el full de lliurament al posseïdor de claus, en el qual s'inclourà l'esmentada informació. Aquesta informació es comunicarà en suport perdurable, en paper o electrònicament, i en llenguatge fàcilment comprensible.

4.2 Processament de la sol·licitud de certificació

4.2.1 Requisits per a tot tipus de certificats

Un cop ha tingut lloc una petició de certificat, l'EC-GENCAT, a través d'una persona autoritzada, verifica la informació proporcionada conforme als requisits previstos en aquesta DPC.

- Si la verificació no és correcta, l'EC-GENCAT denega la petició. En el supòsit que les irregularitats no es puguin corregir, l'EC-GENCAT denega la sol·licitud definitivament.
- Si la verificació és correcta, l'EC-GENCAT:
  - Aprova la sol·licitud.
  - Genera, en el seu cas, el parell de claus i el certificat.

4.2.2 Requisits addicionals per al Certificat CIC

Quan l'Entitat de Certificació que sol·licita ser vinculada a la jerarquia pública de certificació de Catalunya no estigui operada pel Consorci AOC, es comprovarà, abans d'emetre el certificat, que el prestador de serveis de certificació corresponent pugui demostrar la fiabilitat necessària dels seus serveis.

L'EC-GENCAT comprovarà, en el procés d'admissió de l'Entitat de Certificació, els aspectes següents:

- Que les polítiques i procediments operats per l'Entitat de Certificació no són discriminatoris.
- Que l'Entitat de Certificació oferirà els seus serveis a tots els seus sol·licitants, les activitats de les quals entren en l'àmbit d'operació declarat a la seva DPC, d'acord amb l'establert a la secció 1.3 de la Política General de Certificació.
- Que l'Entitat de Certificació és una entitat legal, d'acord amb l'establert a la secció 1.3.1 de la Política General de Certificació, dada que s'autenticarà d'acord amb l'establert a la secció corresponent la Política General de Certificació.
- Que l'Entitat de Certificació disposa de sistemes de gestió de la qualitat i la seguretat adequats per a la prestació del servei, dada que es comprovarà en l'auditoria de conformitat prevista a la secció 8 de la Política General de Certificació.
- Que l'Entitat de Certificació utilitza personal qualificat i amb l'experiència necessària per a la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments adequats de seguretat i de gestió.
- Que l'Entitat de Certificació compleix els requisits de capacitat financera establerts a la secció 9.2 de la Política General de Certificació.
- Que l'Entitat de Certificació compleix els requisits relatius als procediments de resolució de disputes, establerts a la secció 9.13 de la Política General de Certificació.
- Que l'Entitat de Certificació ha documentat de manera adequada les relacions jurídiques en virtut de les que externalitza part o la totalitat dels seus serveis.

4.3 Emissió de certificat

4.3.1 Accions de l'EC-GENCAT durant el procés d'emissió

Per a cada sol·licitud de certificat tramitada, l'EC-GENCAT:

- Utilitza un procediment de generació de certificats X.509 v3 que vincula de forma segura el certificat amb la informació de registre, incloent la clau pública certificada, mitjançant la signatura digital de l'EC-GENCAT.
- Protegeix la confidencialitat i la integritat de les dades de registre.
- Inclou als certificats personals les informacions establertes a l'article 11.2 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, d'acord amb l'establert a la secció 3 d'aquesta DPC.
- Compleix les obligacions establertes pels articles 12, 18, 19, 20 i altres aplicables, de la Llei 59/2003, de 19 de desembre, de signatura electrònica, en la generació de certificats reconeguts.
- Compleix els controls establerts per aquesta Declaració de Pràctiques de Certificació.

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 certificat nou.

4.3.2 Notificació de l'emissió al subscriptor

L'EC-GENCAT notifica al Consorci AOC l'emissió del certificat, o la incidència corresponent. Així mateix, s'indicarà la disponibilitat del certificat i la forma d'obtenir-lo.

4.4 Acceptació del certificat

4.4.1 Responsabilitats del Prestador de Serveis de Certificació

L'EC-GENCAT:

- Si no ho ha fet abans, i quan resulti necessari, acreditarà la identitat del subscriptor.

- Proporcionarà al subscriptor accés al certificat.

- Lliurarà, en el seu cas, el dispositiu criptogràfic de signatura, verificació de signatura, xifrat o desxifrat.

- Proporcionarà la informació següent:

  - Informació bàsica sobre la política i l'ús del certificat, incloent especialment informació sobre l'Entitat de Certificació Vinculada i la Declaració de Pràctiques de Certificació aplicable, així com les seves obligacions, facultats i responsabilitats.
  - Informació sobre el certificat i el dispositiu criptogràfic.
  - Reconeixement del posseïdor de rebre el certificat i, en el seu cas, el dispositiu criptogràfic, i acceptació dels esmentats elements.
  - Obligacions del posseïdor de claus.
  - Responsabilitat de posseïdor de claus.
  - Mètode d'imputació exclusiva al posseïdor de la seva clau privada i de les seves dades d'activació del certificat i, en el seu cas, del dispositiu criptogràfic, d'acord amb l'establert a les seccions corresponents d'aquesta política.
  - La data de l'acte de lliurament i acceptació.

4.4.2 Conducta que constitueix acceptació del certificat

El certificat es pot acceptar mitjançant la signatura del full de posseïdor o responsable de la custòdia de claus.

També es pot acceptar el certificat mitjançant un mecanisme telemàtic d'activació del certificat.

4.4.3 Publicació del certificat

Els certificats es poden publicar sense el consentiment previ dels posseïdors de claus.

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 per part dels posseïdors de claus

Sense estipulació addicional.

4.5.1.1 Requisits addicionals per als certificats CIC

Els certificats CIC només poden ser utilitzats per a funcions d'Entitat de Certificació, en conjunció amb un dispositiu segur de generació de signatura, d'acord amb els requisits establerts a la Política General de Certificació del Consorci AOC.

4.5.2 Ús pel tercer que confia en certificats

Sense estipulació addicional.

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

Sense estipulació addicional.

4.8 Renovació telemàtica

Sense estipulació addicional.

4.9 Modificació de certificats

Sense estipulació addicional.

4.10 Revocació i suspensió de certificats

4.10.1 Causes de revocació de certificats

Sense estipulació addicional.

4.10.2 Legitimació per a sol·licitar la revocació

Sense estipulació addicional.

4.10.3 Procediments de sol·licitud de revocació

La sol·licitud de revocació ha de ser tramesa telemàticament. Excepcionalment es podrà trametre per correu electrònic signat o per correu certificat convencional. S'ha d'incloure la informació suficient per a poder identificar raonablement, a criteri de l'EC-GENCAT, per una banda, el certificat que es sol·licita revocar i, per altra, l'autenticitat i autoritat del sol·licitant.

Aquesta informació suficient ha d'estar formada 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.

Qui faci la sol·licitud de revocació pot demanar a l'Entitat de Registre més informació sobre aquest procediment.

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

Les Entitats de Registre atenen les sol·licituds de revocació dintre del seu horari d'oficina. Fora d'aquest horari, quan sigui urgent deixar sense efecte un certificat, es pot sol·licitar la suspensió cautelar del certificat mitjançant trucada telefònica al Centre d'Atenció a l'Usuari del Consorci AOC, l'horari d'atenció del qual és 24x365.

L'acció de revocació la porta a terme un dels operadors de l'Entitat de Registre, qui accedeix a l'aplicació web a l'efecte, autenticant-se mitjançant un certificat digital d'operador (CIPISR, de classe 1 si és operador de l'Entitat de Registre o de classe 2 quan sigui un operador del Centre d'Atenció a l'Usuari) emès per l'EC-GENCAT.

Una vegada registrat el canvi d'estat del certificat en el sistema de l'EC-GENCAT, de forma automàtica i a la major brevetat possible, es genera i publica una nova Llista de Certificats Revocats (LCR o CRL) en la qual constarà la referència d'aquest certificat.

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

4.10.4 Termini temporal de sol·licitud de revocació

Sense estipulació addicional.

4.10.5 Termini màxim de processament de la sol·licitud de revocació

Sense estipulació addicional. Sense estipulació addicional.

4.10.6 Obligació de consulta d'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-GENCAT.

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

4.10.7 Freqüència d'emissió de llistes de revocació de certificats (LRCs)

Sense estipulació addicional.

4.10.8 Període màxim de publicació de LRCs

Sense estipulació addicional.

4.10.9 Disponibilitat de serveis de comprovació d'estat de certificats

Sense estipulació addicional.

4.10.10 Obligació de consulta de serveis de comprovació d'estat de certificats

Sense estipulació addicional.

4.10.11 Altres formes d'informació de revocació de certificats

Sense estipulació addicional.

4.10.12 Requeriments especials en cas de compromís de la clau privada

Sense estipulació addicional.

4.10.13 Causes de suspensió de certificats

Sense estipulació addicional.

4.10.14 Efecte de la suspensió de certificats

Sense estipulació addicional.

4.10.15 Qui pot sol·licitar la suspensió

Sense estipulació addicional.

4.10.16 Procediments de sol·licitud de suspensió

Sense estipulació addicional.

4.10.17 Període màxim de suspensió

Sense estipulació addicional.

4.10.18 Habilitació d'un certificat suspès

Sense estipulació addicional.

4.11 Serveis de comprovació d'estat de certificats

4.11.1 Característiques d'operació dels serveis

Les LRCs 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-GENCAT.

4.11.2 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 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

4.11.3 Altres funcions dels serveis

Sense estipulació addicional.

4.12 Finalització de la subscripció

Sense estipulació addicional.

4.13 Dipòsit i recuperació de claus

4.13.1 Política i pràctiques de dipòsit i recuperació de claus

No es practica recuperació de claus.

4.13.2 Política i pràctiques d'encapsulament i recuperació de claus de sessió

Sense estipulació addicional.

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-GENCAT 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-ACC realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'EC-ACC. Aquesta política de seguretat ofereix suport a rols amb diferents privilegis.

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-GENCAT 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-GENCAT

- 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 Usuaris de l'EC-GENCAT

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

Sense estipulació addicional.

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

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

5.4.8 Anàlisi de vulnerabilitats

5.5 Arxiu d'informacions

Sense estipulació addicional.

5.5.1 Tipus d'esdeveniments registrats

- Sense estipulació addicional

5.5.2 Període de conservació de registres

L'EC-GENCAT guarda els registres especificats a la secció 5.5.1 durant 15 anys, comptats des del moment d'expedició del certificat. Tota la informació relativa als Certificats d'Infraestructura de Certificació es guarda de forma permanent

L'EC-GENCAT guarda els registres especificats a la secció 5.5.1 en relació amb els certificats Extended Validation per un període de 7 anys, comptats des del moment de l'expedició del certificat.

5.5.3 Protecció de l'arxiu

Sense estipulació addicional.

5.5.4 Procediments de còpia suport

Sense estipulació addicional.

5.5.5 Requisits de segellat de data i hora

Sense estipulació addicional.

5.5.6 Localització del sistema d'arxiu

Sense estipulació addicional.

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-GENCAT 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-GENCAT 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-GENCAT 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 l'EC-GENCAT (o pla de recuperació de desastres) considera el compromís, o la sospita de compromís, de la clau privada de l'EC-GENCAT com un desastre.

En cas de compromís, l'EC-GENCAT:

- 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-GENCAT ja no són vàlids

5.7.4 Desastre sobre les instal·lacions

L'EC-GENCAT 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-GENCAT 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 l'EC-GENCAT 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 l'EC-GENCAT tenen les mesures de seguretat físiques especificades en el Pla de Seguretat.

5.8 Finalització del servei

5.8.1 EC-GENCAT

Sense estipulació addicional.

5.8.2 Entitat de Registre

Sense estipulació addicional.

6. Controls de seguretat tècnica

L'EC-GENCAT 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'EC-GENCAT.

6.1.2 Enviament de la clau privada al subscriptor

Sense estipulació addicional.

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

Sense estipulació addicional.

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

EC-GENCATEC-GENCAT

La clau de l'EC-GENCAT i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya es comuniquen als verificadors, i així s'assegura la integritat de la clau i se n'autentica l'origen.

La clau pública de l'EC-GENCAT, que és l'arrel de la jerarquia, es publica al directori de l'EC-GENCAT en forma de certificat auto-signat juntament amb una declaració que fa referència al fet que la clau permet autenticar a l'EC-GENCAT.

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-GENCAT es publica al directori de l'EC-GENCAT en forma de certificat CIC signat pel Consorci AOC.

Els usuaris accedeixen al directori per obtenir les claus públiques de l'EC-GENCAT.

6.1.5 Mides de claus

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

Les claus de tots els certificats emesos per l'EC-GENCAT 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

Sense estipulació addicional.

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

Sense estipulació addicional.

6.1.9 Propòsits d'ús de claus

L'EC-GENCAT 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

Sense estipulació addicional.

6.2.1.2 Cicle de vida de les targetes amb circuit integrat

Sense estipulació addicional.

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

Sense estipulació addicional.

6.2.3 Dipòsit de la clau privada

Sense estipulació addicional.

6.2.4 Còpia de seguretat de la clau privada

Sense estipulació addicional.

6.2.5 Arxiu de la clau privada

Sense estipulació addicional.

6.2.6 Introducció de la clau privada en el mòdul criptogràfic

Sense estipulació addicional.

6.2.7 Emmagatzematge de la clau privada en el mòdul criptogràfic

Sense estipulació addicional.

6.2.8 Mètode d'activació de la clau privada

Es requereixen almenys dues persones per a activar la clau privada de l'EC-GENCAT

Per a certificats CIPISR, la clau privada del posseïdor de claus s'activa mitjançant la introducció del PIN en la targeta intel·ligent.

6.2.9 Mètode de desactivació de la clau privada

Sense estipulació addicional.

6.2.10 Mètode de destrucció de la clau privada

Sense estipulació addicional.

6.2.11 Classificació dels mòduls criptogràfics

Sense estipulació addicional.

6.3 Altres aspectes de gestió del parell de claus

6.3.1 Arxiu de la clau pública

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

6.3.2 Períodes d'utilització de les claus pública i privada

Sense estipulació addicional.

6.4 Dades d'activació

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

Sense estipulació addicional.

6.4.2 Protecció de les dades d'activació

Sense estipulació addicional.

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

Sense estipulació addicional.

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, i s'avalua el grau de compliment mitjançant una auditoria de seguretat informàtica conforme a l'especificació tècnica CWA 14172-2 i un perfil de protecció adient, 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

Sense estipulació addicional.

6.6.2 Controls de gestió de seguretat

Conforme a allò establert a la Política General de Certificació.

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-GENCAT 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 manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'EC-GENCAT.
- 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

Sense estipulació addicional.

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

7.2 Perfil de la llista de revocació de certificats

Sense estipulació addicional.

8. Auditoria de conformitat

L'EC-GENCAT 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-GENCAT pot delegar l'execució de les auditories en una tercera entitat contractada pel Consorci AOC. En Aquests casos l'EC-GENCAT 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-GENCAT 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-GENCAT.

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 l'EC-GENCAT 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

La cobertura la aporta el seguro previsto en el apartado 9.2.1, por los daños previstos por la Ley 59/2003, de 19 de diciembre, excluidas las exoneraciones legales de responsabilidad que prevé su artículo 23.

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.

9.4.1. Responsabilitat corresponent a la protecció de dades personals

Sense estipulació addicional.

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

Sense estipulació addicional.

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

Sense estipulació addicional.

9.4.4. 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-GENCAT

Sense estipulació addicional.

9.6.1.2 Garanties oferides a subscriptors i verificadors

Sense estipulació addicional.

9.6.2 Entitats de Registre

9.6.2.1 Obligacions i altres compromisos

Sense estipulació adicional, exceptuant l'obligació d'emmagatzemar els fulls de lliurament de certificat durant un període de 15 anys, que és assumida per les entitats subscriptores dels certificats corporatius que emet l'EC-GENCAT.

En quant al nombre d'operadors de l'autoritat de registre que aquesta ha de nomenar:per a l'EC-GENCAT hauran de ser quatre o més dels empleats que treballin per a ella.

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

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

9.7 Renúncies de garanties

9.7.1 Rebuig de garanties de l'EC- GENCAT

L'EC-GENCAT 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- GENCAT

La EC-GENCAT limita la seva responsabilitat restringint el servei a l'emissió i gestió dels dertificats i, en el seu cas, de parells de claus de subscriptors i depòsits criptogràfics (de signatura i verificació de signatura, així com de xifrat o desxifrat) subministrats per aquest

.

9.8.2 Cas fortuït i força major

L'EC-GENCAT 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-GENCAT 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 als subscriptors.

9.10.2 Finalització

L'EC-GENCAT 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'apartat1.5.

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

L'EC-GENCAT 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-GENCAT 1er semestre 2016

Projecte:	**Informe modificació del document DPC EC-GENCAT**
Entitat de destí:	**Consorci AOC**
Codi de referència:	**Revisió 1er semestre 2016**
Versió:	**Canvis de la v1.4 a la v2.0 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
2.0	Totes	Revisió global – Integració de CATCert a Consorci AOC	Servei de Certificació Digital - Consorci AOC	05/08/2016