



**Consorci
Administració Oberta
de Catalunya**

**PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA PRESTACIÓ DEL
SERVEI DE SIGNATURA REMOTA BASADA EN CERTIFICATS
QUALIFICATS DEL CONSORCI AOC AOC 2014 17**



Realitzat per: Consorci AOC

Versió:1.1

Data: 2023

Arxiu: PPT_SSR_2023_v.1.1.docx

1 Índex

2	OBJECTE.....	6
3	ABAST	7
4	MARC NORMATIU	8
5	DESCRIPCIÓ DE LA SITUACIÓ ACTUAL.....	10
5.1	El servei de certificació digital del Consorci AOC	10
5.1.1	Model de registre	11
5.2	Els serveis de identificació i signatura electrònica	12
5.2.1	Bus d'integració de mecanismes d'identificació i signatura electrònica (Servei VALid)	12
5.2.2	Signador	12
5.2.3	Mecanismes d'autenticació per a treballadors públics	12
5.3	Els servei Signador Centralitzat	12
6	DESCRIPCIÓ DELS SERVEIS OBJECTE DEL CONTRACTE	14
6.1	Obligacions essencials del contracte	14
6.2	Obligacions relatives al procés de registre	15
6.3	Catàleg de serveis objecte del contracte	16
6.3.1	Serveis a tant alçat	16
6.3.2	Serveis a preu unitari i manteniment d'aplicacions informàtiques	17
6.3.3	Gestió de les claus d'entitat final i jerarquia	17
6.4	El Servei de Signatura Remota (SSR) del Consorci AOC	18
6.4.1	Servei de signatura electrònica en remot per a la ciutadania	18
6.4.2	Servei de signatura electrònica en remot per als empleats i treballadors del sector públic	18
6.4.3	Servei de signatura electrònica en remot amb certificats de segell electrònic qualificat pel sector públic	19
6.5	Aplicació PKI	20
6.5.1	Emissió de Llistes de Revocació de Certificats (CRL)	20
6.5.2	Servei de Consulta d'Estat de Certificats en Línia (OCSP)	21
6.6	Model de registre de serveis del Consorci AOC	21
6.6.1	Registre àmbit de l'empleat públic i segells electrònics	22
6.6.2	Registre àmbit ciutadania	23
6.7	Infraestructura tecnològica	23
6.7.1	Entorns	23
6.7.2	Centres de Processament de Dades	24
6.7.3	Maquinari i programari dedicat.....	25
6.8	Governament de la Seguretat	25
6.8.1	Gestió de traces	25

6.8.2	Comunicacions segures d'accés a les aplicacions objecte de la licitació	25
6.8.3	Arquitectura, proves de recuperació de desastres i proves de recuperació de backups	25
6.8.4	Seguretat de les instal·lacions des de les quals es presta el servei	26
6.8.5	Seguretat en el cloud.....	26
6.8.6	La gestió de la seguretat i el compliment normatiu	26
6.8.7	La gestió de la continuïtat i la disponibilitat	28
6.8.8	Cessament de l'activitat.....	29
6.8.9	Auditories a les Entitats de Registre vinculades	29
6.8.10	Auditories del Prestador de Serveis de Certificació Consorci AOC	29
6.9	El servei de suport.....	30
6.9.1	El servei de Suport del Consorci AOC	30
6.9.2	Àmbits d'atenció i suport a prestar per l'adjudicatari:.....	30
6.9.3	Canals d'entrada de peticions	30
6.9.4	Horari d'atenció	31
6.10	Servei de Manteniment Evolutiu.....	31
6.10.1	Metodologia	31
6.10.2	Manteniment correctiu	35
6.10.3	Manteniment tècnic – legal.....	35
6.10.4	Manteniment evolutiu	36
6.10.5	Tasques en l'àmbit del manteniment evolutiu	36
6.11	Serveis organitzatius i de compliment.....	36
6.11.1	Serveis de formació.....	37
6.11.2	Serveis de facturació	38
7	Acords de nivell de servei	39
7.1	Model de mesura del nivell de servei	40
7.1.1	Indicadors	41
7.1.2	Fonts d'informació per a l'obtenció dels nivells de servei	41
7.1.3	Aplicació dels acords de nivell de servei.....	41
7.2	ANS d'Explotació del Servei.....	42
7.2.1	ANS del Servei d'emissió o canvi d'estat de certificats T-CAT	42
7.2.2	ANS de disponibilitat	43
7.2.3	ANS de capacitat	43
7.2.4	ANS de continuïtat.....	44
7.2.5	ANS de qualitat del servei d'emissió i gestió de certificats	44
7.2.6	ANS del Servei de Suport.....	44
7.3	ANS dels Serveis de Programació	45
7.3.1	Acords de nivell de servei del desenvolupament	45

7.3.2	Requeriments de nivell de servei en el manteniment correctiu i resolució d'incidències	46
7.3.3	Temps de resposta en el manteniment evolutiu	46
7.3.4	Desviacions en el manteniment evolutiu	47
8	FASES D'EXECUCIÓ DEL CONTRACTE	48
8.1	Creació i explotació del servei signatura remota qualificada basada en certificats qualificats del Consorci AOC	49
8.2	Transició de l'operació del servei actual	49
8.3	Devolució del servei	49
9	SEGUIMENT DEL SERVEI	51
9.1	Governament i millora del servei	51
9.2	Estructura de responsabilitats de l'adjudicatari	51
9.3	Estructura de responsabilitats del Consorci AOC	54
9.4	Gestió d'incidències i problemes	54
9.5	Òrgans de Gestió	55
9.5.1	Reunions de direcció.	55
9.5.2	Reunions de seguiment.	55
9.6	Model de relació en la fase de Transició de l'operació	56
9.6.1	Governament de la fase de transició de l'operació	57
10	REFERÈNCIES	59
11	Annex – Situació actual	60
11.1	Catàleg actual de certificats del Consorci AOC	60
11.2	Situació actual de subsistemes i components del Servei	61
11.3	El Servei de Registre de certificats personals i de segell electrònic pel Sector Públic (T-CAT) 62	
11.3.1	Model de Registre T-CAT	62
11.3.2	Topologia de la xarxa d'Entitats de Registre T-CAT	64
11.3.3	Rols del sistema de registre T-CAT	65
11.3.4	Diagrama de relacions dels procediments d'emissió	67
11.3.5	Gestió documental del Servei de Certificació T-CAT	70
11.3.6	Taula de relació entre rols i històries d'usuari del component ASCD	70
11.3.7	Històries d'usuari de les operacions de sol·licitud i gestió del cicle de vida dels certificats dins d'EACAT	71
11.3.8	Altres operacions	74
11.4	El servei de Registre de certificats personals per Ciutadania (idCAT)	74
11.4.1	La web del ciutadà	75
11.4.2	La Web dels Operadors de Registre	75
11.4.3	La Web dels Operadors de Certificació o d'administració	75
11.4.4	Procediment de sol·licitud i emissió idCAT	76

11.4.5 Serveis per l'ús de certificats de segell electrònic centralitzats : el Servei Signador Centralitzat.....	77
11.4.6 Actius de programari, codi i dades del servei actual a disposició de l'adjudicatari.....	77
11.5 Serveis d'auditoria d'ER	78
11.6 Serveis evolutius i de personalització de programari actuals	78
11.7 ANS actual del servei de certificació	79
11.8 Formació i divulgació.....	79

2 OBJECTE

El Consorci d'Administració Oberta de Catalunya (Consorci AOC) és l'òrgan competent en relació a la prestació de serveis d'identitat digital i signatura electrònica, d'acord amb la Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya i amb els seus estatuts. D'acord amb aquesta competència, com a Prestador de Serveis de Confiança, ofereix al conjunt de les Administracions Públiques Catalanes serveis d'emissió de certificats qualificats, tant de persona física, per als empleats públics i la ciutadania, com de segells electrònics.

L'objecte d'aquest plec és la contractació d'un servei tecnològic de signatura i segell electrònics remots, en modalitat de *Platform as a Service* (PaaS), així com la seva operació, per donar cobertura a la signatura electrònica de documents, i que permeti la custòdia i l'ús de segells electrònics en l'exercici de l'actuació administrativa automatitzada, així com de certificats qualificats d'empleat públic i de la ciutadania.

3 ABAST

El present plec té com objecte la contractació del servei de custòdia de certificats qualificats de segell electrònic, empleat públic i ciutadania, com a base per a la prestació d'un servei de signatura remota per al conjunt de les Administracions Públiques Catalanes. El Consorci AOC requereix contractar la infraestructura, posada en marxa i operació, així com el suport necessari per assolir la qualificació dels certificats custodiats, tant de persona física com segells electrònics, d'acord a les condicions fixades en els plecs de prescripcions tècniques i administratius particulars que regulen aquesta licitació.

En concret, l'adjudicatari haurà de posar en marxa i operar una infraestructura que permeti:

- Custodiar i emprar certificats de segell electrònic qualificats de les Administracions Públiques Catalanes, que sigui integrable amb les seves aplicacions a través de les solucions comunes de signatura electrònica del Consorci AOC, per al seu ús en l'àmbit de l'actuació administrativa automatitzada.
- Un sistema de signatura remota que permeti custodiar i emprar certificats qualificats de treballador públic i que es pugui integrar amb les aplicacions de les Administracions Públiques Catalanes, a través de les solucions comunes de signatura electrònica que el Consorci AOC ofereix.
- Un sistema de signatura remota que permeti custodiar i emprar certificats qualificats de persona física orientat a la ciutadania, sigui integrable amb les aplicacions de les Administracions Públiques Catalanes a través del servei VALid del Consorci AOC. Tenint en compte l'ús esporàdic que acostumen a tenir aquest tipus de certificats, el sistema haurà de permetre la possibilitat que aquests siguin d'un sol ús.

En tots aquests casos, els sistemes contractats i operats per l'adjudicatari seran els dispositius qualificats de creació de signatura i segell electrònics remots que empraran els certificats qualificats d'empleat públic i treballador públic (TCAT), els segells electrònics qualificats i els certificats de persona física (idCAT) que el Consorci AOC emet com a Prestador Qualificat de Serveis de Confiança. Per tal de facilitar aquesta emissió, l'empresa adjudicatària del contracte objecte d'aquest plec operarà dues arrels intermèdies, una per ciutadania i l'altra per segells electrònics i certificats d'empleat i treballador públic.

Estem davant d'un servei d'alta criticitat, amb un consum elevat i una gran quantitat d'usuaris concurrents, així com una important dependència estratègica amb els serveis digitals dels ens i organismes públics de l'àmbit català.

4 MARC NORMATIU

L'Article 7 de la Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya estableix, entre d'altres, que L'Administració de la Generalitat i els ens locals, sens perjudici d'altres fórmules de col·laboració, cooperen i col·laboren, ordinàriament i voluntàriament, per mitjà del Consorci Administració Oberta Electrònica de Catalunya, en la definició i l'execució de les estratègies comunes per l'extensió dels mitjans electrònics per a garantir la identitat i per a acreditar la voluntat en les actuacions dels ciutadans i el personal del sector públic. Per altra banda, el mateix article estipula que l'Agència Catalana de Certificació, integrada actualment en el Consorci AOC, presta serveis de signatura electrònica al sector públic de Catalunya per a garantir la confidencialitat, la integritat, la identitat i el no-rebuig en les comunicacions electròniques que duen a terme les entitats del sector públic de Catalunya.

La prestació dels serveis de serveis de certificació, com a servei de confiança, queda regulada pel Capítol III del Reglament (UE) 910/2014 del Parlament i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior i que deroga la Directiva 1999/93/CE (en endavant ReIDAS). Pel que fa als certificats qualificats de signatura electrònica, al seu Annex II sobre els requisits dels dispositius qualificats de signatura electrònica, obre la porta a que els prestadors qualificats de serveis de confiança puguin gestionar les claus de signatura en nom del signatari quan diu, al seu punt 4, que aquests només les podran duplicar amb l'objectiu de fer-ne una còpia de seguretat.

Per la seva banda, la Llei 6/2020, de l'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, i que és d'aplicació als prestadors establerts a l'Estat Espanyol, al seu article 9 especifica que un prestador no podrà "emmagatzemar ni copiar, per si mateix o a través d'un tercer, les dades de creació de signatura, segell o autenticació de lloc web de la persona física o jurídica a què hagin prestat els seus serveis, excepte en cas de la seva gestió en nom del titular. En aquest cas, utilitzaran sistemes i productes fiables, inclosos els canals de comunicació electrònica segurs, i s'aplicaran procediments i mecanismes tècnics i organitzatius i adequats, per garantir que l'entorn sigui fiable i s'utilitzi sota el control exclusiu del titular del certificat. A més, hauran de custodiar i protegir les dades de creació de signatura, segell o autenticació de lloc web davant de qualsevol alteració, destrucció o accés no autoritzat, així com garantir-ne la contínua disponibilitat."

Amb l'objectiu de complir amb els requisits de seguretats establerts, s'han definit dues normes tècniques aplicables a les aplicacions de signatura en servidor, als mòduls d'activació de signatura i als mòduls criptogràfics, que són respectivament:

- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

Per altra banda, existeixen especificacions tècniques que defineixen requisits de seguretat per als prestadors de serveis de confiança aplicables a l'operació de dispositius remots de signatura i segell electrònics, així com un protocol per al seu ús:

- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation

Finalment, cal tenir en compte les normes europees aprovades per garantir els requisits que han de complir els prestadors qualificats de serveis de confiança en general, i els que emeten certificats qualificats de signatura i segell electrònic, i que són:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles

Pel que fa a la prestació de serveis de certificació en l'àmbit de les administracions públiques, tractant-se de serveis que treballen amb dades de caràcter personal, caldrà tenir en compte i complir amb el que estableix Reglament (UE) 2016/679, de 27 d'abril del 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals. Per altra banda, sent el Consorci AOC part del sector públic de Catalunya, es requerirà que l'empresa adjudicatària estigui certificada en l'Esquema Nacional de Seguretat, regulat actualment pel Real Decret 311/2022, de 3 de maig.

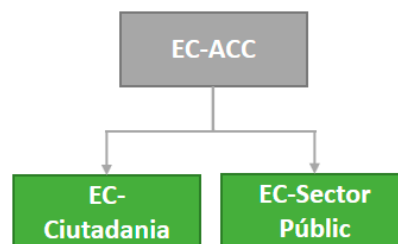
La normativa interna del Consorci AOC en matèria de seguretat i del servei objecte de licitació.

5 DESCRIPCIÓ DE LA SITUACIÓ ACTUAL

5.1 El servei de certificació digital del Consorci AOC

El Consorci AOC és el prestador qualificat de serveis de confiança de les Administracions Públiques Catalanes, emetent certificats de segell electrònic, d'empleat públic i de persona física per a la ciutadania. Com a tal, disposa d'una jerarquia formada per una Entitat de Certificació arrel (root CA), que és l'EC-ACC, i 2 Entitats de Certificació subordinades i englobant de la següent manera els àmbits de prestació dels serveis:

- **EC-SectorPublic:** que concentra l'emissió de certificats pel Sector Públic de Catalunya. És la entitat subordinada que emet els certificats:
 - **TCAT i TCAT-P** com a certificats qualificats de signatura qualificada i signatura avançada respectivament.
 - **TCAT de representant** d'administració pública
 - **TCAT i T-CAT P de pseudònim**
 - **Certificats de segells electrònic**
 - **Certificats de dispositiu Aplicació (CDA) i Segell Electrònic**
- **EC-Ciutadania:** que emet certificats digitals a la ciutadania coneguts com idCAT.



Actualment, el Consorci AOC està ampliant aquesta jerarquia per incloure autoritats de certificació subordinades pels següents àmbits concrets:

- SubCA SECTOR PÚBLIC Q (G3) A.1: per a l'emissió de certificats electrònics qualificats per al sector públic de Catalunya, en substitució de l'EC-SECTORPÚBLIC.
- SubCA CIUTADANIA Q (G3) A.2: per a l'emissió de certificats electrònics qualificats per a ciutadania, en substitució de l'EC-CIUTADANIA.
- SubCA SECTOR PÚBLIC R Q (G3) A.3: per a l'emissió de certificats electrònics qualificats de signatura remota per al sector públic de Catalunya.
- SubCA CIUTADANIA R Q (G3) A.4: per a l'emissió de certificats electrònics qualificats de signatura remota per a ciutadania.
- SubCA Q TSA (G3) A.5: per a l'emissió de certificats electrònics qualificats per a serveis de segells de temps qualificat.
- SubCA TSA noQ (G3) A.6: per a l'emissió de certificats electrònics qualificats per a serveis de segells de temps no qualificat.
- SubCA noQ (G3) A.7: per a l'emissió de certificats electrònics no qualificats.

Amb l'objectiu permetre a l'adjudicatari del contracte objecte de la present licitació poder emetre certificats de signatura i segell electrònic remots, aquest s'encarregarà de l'operació de les següents entitats subordinades:

- SubCA SECTOR PÚBLIC R Q (G3) A.3.
- SubCA CIUTADANIA R Q (G3) A.4.

Les claus privades d'aquestes subCAs es van generar al 2022 en una sessió auditada, es van protegir amb unes targetes d'Operació (OCS) en propietat exclusiva del Consorci AOC i es mantenen sense operació des d'aquell moment fins a l'adjudicació del contracte objecte d'aquesta licitació.

La prestació dels serveis de certificació del Consorci AOC està regulat per un document de Declaració de Pràctiques, unes polítiques de certificació, uns textos de divulgació i uns documents de perfils disponibles a <https://epscd.aoc.cat/regulacio>. El contingut final d'aquest conjunt de documents dependrà de la solució oferta per l'adjudicatari, tot i que estarà basat en les best practices recomanades per la norma aplicable. El Consorci AOC facilitarà a l'adjudicatari la inclusió de les seves propostes de canvi en aquest conjunt documental per reflectir les característiques del servei.

S'adjunta més detall sobre la situació actual dels serveis oferts pel Consorci AOC al punt 11 ([Annex I](#)) d'aquest mateix document

5.1.1 Model de registre

Sector Públic

Per tal de poder emetre certificats d'empleat i treballador públic i segells electrònic per al seu personal, aplicacions i serveis, les administracions públiques catalanes s'estableixen com a entitats subscriptores del Servei TCAT, des d'on es porten a terme les tasques de verificació de la identitat i registre previ. En concret, les entitats subscriptores verifiquen la identitat del subjecte dels certificats, gestionen la seva emissió i el seu lliurament i custòdia. Si s'escau, també gestionen la seva revocació o renovació.

Les persones operadores de les entitats subscriptores s'identifiquen i sol·liciten l'emissió de certificats a través de pantalles disposades a l'efecte a la plataforma EACAT, que enviarà les peticions al programari de l'Entitat de Certificació, encarregada de la seva gestió i execució. La resta d'operacions relatives al cicle de vida dels certificats (petició, aprovació, lliurament i revocació) es porten a terme a través de l'aplicació web de registre de l'Entitat de Certificació.

Les entitats subscriptores del servei TCAT actuen d'acord amb el corresponent document de [condicions específiques](#) disponible des del lloc web del Consorci AOC.

Ciutadania

De mateixa manera, el Consorci AOC disposa també d'una xarxa d'Entitats de Registre distribuïdes per tot el territori que s'encarreguen de identificar i registrar a les persones que demanen un certificat de persona física idCAT de forma presencial. El portal de suport del Consorci AOC ofereix una [llista de les entitats](#) on es pot adreçar la ciutadania a l'hora obtenir un certificat idCAT.

Com en el cas de les entitats subscriptores del servei TCAT, les entitats de registre idCAT operen amb acord al corresponent document de [condicions específiques](#). Tot i això, en el cas de idCAT l'aplicació web per gestionar les operacions d'una entitat de registre idCAT no està integrada a la plataforma EACAT, i el programari de l'Entitat de Certificació que les fa efectives és també independent.

Per la seva banda, el Consorci AOC posa a disposició de la ciutadania un portal (<https://www.idcat.cat/>) des d'on es poden demanar i descarregar els certificats idCAT, així com gestionar la resta d'operacions del seu cicle de vida.

Actualment el Consorci AOC està desenvolupant el sistema que permetrà emetre els certificats idCAT mitjançant un procés de videoidentificació, complint amb els requisits establerts a l'efecte a l'Orde ETD/465/2021, de 6 de maig, per la qual es regulen els mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.

5.2 Els serveis de identificació i signatura electrònica

5.2.1 Bus d'integració de mecanismes d'identificació i signatura electrònica (Servei VALid)

Per tal de facilitar al conjunt de les Administracions Públiques Catalanes la integració dels sistemes d'identificació i signatura electrònica, el Consorci AOC posa a la seva disposició el servei VALID com a bus d'integració d'aquest tipus de mecanismes. Com a servei d'identificació electrònica, VALID implementa és una implementació del protocol OAuth 2.0 que inclou un servei de consulta de les dades de la persona identificada. Actualment els mecanismes d'identificació electrònica que el servei admet són:

- idCAT Mòbil com a mecanisme d'autenticació basat en l'enviament de contrasenyes d'un sol ús al telèfon mòbil de les persones usuàries.
- Autenticació amb certificats qualificats
- Les credencials admeses per la plataforma Cl@ve, incloent l'accés als mecanismes d'identificació notificats pels diferents Estats membre de la Unió Europea d'acord amb el que especifica el Capítol II del ReIDAS

5.2.2 Signador

Per altra banda, el Consorci AOC ofereix un servei per facilitar al conjunt de les aplicacions web de les Administracions Públiques Catalanes la funcionalitat de signatura electrònica amb certificats personals en local anomenat **Signador**. Les aplicacions que integren aquest servei poden redirigir la signatura de documents al servei, que permetrà a les persones usuàries signar amb els certificats que gestionin a la seva màquina en local, ja sigui emprant el magatzem de claus del navegador o el sistema operatiu. L'operació concreta de signatura actualment es pot portar a terme o bé emprant una aplicació nativa instal·lable a l'ordinador de les persones usuàries, o bé executant un fitxer de Java Web Start (jnlp).

5.2.3 Mecanismes d'autenticació per a treballadors públics

Finalment, les aplicacions de cada administració pública, com per exemple els gestors d'expedients i portesignatures, autèntiquen la identitat dels seus treballadors públics emprant els seus propis sistemes. Per exemple, els treballadors de la Generalitat de Catalunya autèntiquen a la seva identitat per accedir a les diferents aplicacions de negoci a través d'una plataforma anomenada GICAR.

Des del Consorci AOC es disposa d'un servei de federació d'aquests mecanismes d'autenticació, amb l'objectiu de poder donar un accés unificat a serveis comuns a totes les administracions.

5.3 Els servei Signador Centralitzat

Actualment, el Consorci AOC ofereix al conjunt d'Administracions Públiques Catalanes un servei, anomenat **Signador Centralitzat**, com a plataforma tecnològica de **signatura electrònica desatesa** que dona cobertura a la signatura electrònica de documents. Com a servei permet custodiar i fer servir segells electrònics en l'exercici de l'actuació administrativa automatitzada.



Figura 1. Custòdia de certificats de segell electrònic

Quan un ens demana un segell electrònic de nivell mig al Consorci AOC a través d'una entitat subscriptora pot decidir que aquest sigui custodiat en exclusivitat pel Consorci AOC i a aplicacions (per a ús propi i per a eines de l'AOC), tant serveis que ofereix el propi Consorci AOC com externs, a fer-ne ús.

El servei comprèn les següents funcionalitats:

- Custòdia de certificats de segell electrònic de nivell mig (o substancial), emesos pel Consorci AOC
- Suport dels formats de signatura avançada XML (XAdES), ASN.1 (CAAdES) i sobre PDF (PAdES).
- Creació de signatures electròniques en format avançat a partir de les claus associades als certificats electrònics custodiats.
- Registre de totes les accions realitzades a la plataforma pels usuaris d'aquesta per tal de deixar-ne constància i traça a efectes d'auditoria i a instància o requeriment judicial.

6 DESCRIPCIÓ DELS SERVEIS OBJECTE DEL CONTRACTE

6.1 Obligacions essencials del contracte

- [R1] L'adjudicatari haurà de proporcionar al Consorci AOC una infraestructura per hostatjar les claus privades de certificats de treballador públic, empleat públic, ciutadania i segell electrònic en remot.
- [R2] Operar les Entitats de Certificació SubCA SECTOR PÚBLIC R Q (G3) A.3. i SubCA CIUTADANIA R Q (G3) A.4 del Consorci AOC per tal d'emetre els certificats de signatura electrònica d'empleat públic, segells electrònics i ciutadania en remot.
- [R3] Oferir al Consorci AOC i al conjunt de les administracions Públiques Catalanes un servei de signatura electrònica remota que es pugui emprar amb certificats qualificats de signatura electrònica i segell electrònics, i que sigui integrable amb les aplicacions de les Administracions Públiques Catalanes
- [R4] L'adjudicatari queda obligat a l'adequació i la plena conformitat dels seus serveis al ReIDAS, i a les normes tècniques que aprovades per a la seva aplicació, ja descrites en el [marc normatiu](#) d'aquest plec. En aquest sentit, el contractista haurà d'obtenir a la seva costa i en el menor espai de temps possible, l'avaluació periòdica de la conformitat i complir amb la resta d'obligacions corresponents a la seva condició de prestador de serveis de confiança qualificat, així com assumir qualsevol canvi que en cada moment exigeixi el supervisor nacional o que en derivin de la normativa espanyola que es dicti per donar compliment o per aplicar el ReIDAS. En cap cas aquesta obligació d'adequació es considerarà modificació del contracte.
- [R5] Les claus dels certificats personals de signatura i de segell electrònic qualificats seran custodiades i emprades en dispositius certificats Common Criteria EAL 4+ amb els perfils de protecció definits per les normes CEN EN 419 241-2 i CEN EN 419 221-5 o similars i hauran d'aparèixer a la llista de dispositius qualificats de creació de signatura electrònica i segell electrònic que publica la Comissió Europea d'acord amb els punts 32 i 23 de l'article 3 del ReIDAS.
- [R6] L'empresa adjudicatària haurà de garantir que els serveis de confiança digital compleixen amb el que indica la Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, el Reial Decret 311/2022, del 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, el Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica, i les seves normes tècniques i de seguretat de desenvolupament, i la Llei 40/2015, de l'1 d'octubre, de Règim Jurídic del Sector Públic, especialment pel que fa a l'admissió i interoperabilitat dels certificats i els sistemes de signatura o segell en l'àmbit de les administracions públiques. Tanmateix haurà de complir amb la Declaració de Pràctiques de Certificació de l'Entitat de Certificació del Consorci AOC i les Polítiques de certificació corresponents. Aquesta normativa és l'aplicada en el moment de la redacció del plec però es pot veure modificada durant l'execució.
- [R7] Facturar electrònicament els imports dels certificats digitals en un termini de 10 dies laborals a comptar des del mes següent al de l'emissió, d'acord amb els requeriments del Consorci AOC.
- [R8] Sotmetre's i superar les auditories periòdiques establertes al ReIDAS i a la Llei 6/2020, d'11 de novembre o al normativa aplicada en cada moment.
- [R9] Emetre, lliurar, administrar, revocar i renovar certificats quan ho sol·liciti l'entitat de registre, en els casos excepcionals i pels motius descrits a la a les respectives Polítiques de Certificació.
- [R10] Notificar a l'ens subscriptor en el cas de certificats d'empleats públics, o al titular del certificat, pel cas dels certificats de ciutadans, com a mínim amb 2 mesos d'antelació

- a la data d'expiració del certificat, la possibilitat de renovar-los, així com revocació dels certificats, quan es produeixin.
- [R11] Comunicar als tercers que ho sol·licitin l'estat dels certificats, d'acord amb el que s'estableix a la Declaració de Pràctiques de Certificació de l'Entitat de Certificació del Consorci AOC per als diferents serveis de verificació de certificat.
- [R12] Oferir un tercer nivell de suport als usuaris.
- [R13] Elaborar el material comunicatiu i divulgatiu necessari per a la formació al personal de les Entitats de Registre que hagi d'executar les tasques, d'acord amb els estàndards del Consorci AOC. Aquest material divulgatiu i formatiu sempre haurà d'estar actualitzat.
- [R14] Garantir que les claus privades de les Entitats de Certificació gestionades per l'adjudicatari no han estat compromeses.
- [R15] Aplicar amb una diligència raonable per a Disposar de mecanismes per garantir que cada sistema d'autenticació i signatura subministrat en execució del servei objecte d'aquesta licitació compleixi amb els requisits de qualitat i seguretat i la normativa de protecció de dades .
- [R16] Pel que fa als usos d'identificació i signatura, els serveis objecte d'aquest contracte s'hauran d'integrar com a proveïdor de identitat i signatura amb el servei VALid del consorci AOC, en els termes que es descriuen en les Condicions específiques del servei. Per a la funcionalitat de VALid de la generació de signatures, els serveis objecte del contracte s'hauran d'oferir a través de l'element Signador (<https://signador.aoc.cat/signador/init>). VALid i Signador estan àmpliament integrats amb processos d'identificació i signatura que ofereix el sector públic de Catalunya i és estratègic poder oferir els serveis objecte d'aquest contracte a través dels mateixos.

6.2 Obligacions relatives al procés de registre

- [R17] L'adjudicatari haurà de registrar les dades dels ens i dels usuaris amb l'objectiu de gestionar les credencials d'accés, d'acord a la normativa tècnica i legislativa aplicable per poder oferir el servei amb el nivell de seguretat necessari.
- [R18] L'adjudicatari serà responsable de publicar i mantenir un procediment i un mecanisme per a l'alta al servei on figurin tots els participants del servei de l'ens sol·licitant amb el seu rol i tota la documentació que sigui necessària per mantenir l'alta al servei. Per a la primera alta, per exemple, podrà ser un formulari d'alta en format pdf que permeti la inclusió com a evidència de la signatura del sol·licitant del servei. Les dades caldrà mantenir-les permanentment actualitzades. La documentació de les altes es mantindrà en un espai segur compartit amb el Consorci AOC.
- [R19] En relació als mecanismes d'autorització d'accés, l'adjudicatari en podrà proposar diversos en funció del nivell de seguretat de la instància a la que s'accedeix (servei qualificat o no qualificat) però en cap cas sense comprometre la seguretat del servei. Per l'accés a l'entorn qualificat es sol·licita que, com a mínim, la solució suporti mecanismes d'autorització d'accés de serveis web estàndard i amb suport a certificats (p.ex. JWT i API Key). Modalitats com la filtrada per IP origen i paraula de pas, malgrat que no permeten identificar unívocament a una aplicació, s'han de permetre en la fase inicial i pel servei no qualificat. L'adjudicatari haurà de garantir el compliment de les normes tècniques de gestió dels secrets i, en particular, compliment polítiques de seguretat d'AOC en relació a la gestió d'aquests.
- [R20] Aquesta interfície d'accés als serveis haurà de disposar de serveis per garantir la continuïtat del servei i evitar atacs de denegació de servei com s'estableix en el punt "6.8.6 La gestió de la seguretat i el compliment normatiu" i "6.8.7 La gestió de la continuïtat i la disponibilitat" d'aquest mateix document. Addicionalment, també haurà de mantenir el comptatge i anotació del consum de cada client per poder mantenir-ne un control i eventualment, establir quotes de consum o denegar l'accés al servei per mal ús del mateix.

- [R21] Oferir i mantenir una aplicació web des d'on les persones operadores de les entitats subscriptores TCAT puguin portar a terme les tasques relatives al cicle de vida (emissió, i revocació) dels certificats en remot de la SubCA SECTOR PÚBLIC R Q (G3) A.3 , tant d'empleat o treballador públic, com de segells electrònics.
- [R22] Oferir APIs que permetin integrar la funció de sol·licitud de certificats de tots els perfils objecte d'aquesta licitació.
- [R23] Emetre, lliurar, administrar, revocar i renovar certificats en els casos i pels motius descrits a la Declaració de Pràctiques de Certificació de l'Entitat de Certificació del Consorci AOC i la corresponent Política de Certificació.
- [R24] Emetre un certificat per a cada operador nomenat per l'ens usuari després de l'aprovació de la sol·licitud del certificat corresponent, sempre que tingui la formació realitzada i superada satisfactòriament. Aquest certificat té una validesa d'un màxim de quatre anys.

6.3 Catàleg de serveis objecte del contracte

El catàleg de serveis inclosos en l'àmbit d'aquesta licitació estarà format, principalment, pels següents:

6.3.1 Serveis a tant alçat

Al llarg de la fase inicial de transició de l'operació del servei, que es portarà a terme durant el primer d'execució del contracte (finalitza a final del 2024), s'inclouen totes les despeses generals necessàries per garantir la posada en marxa i bon funcionament del servei.

Concretament:

- El finançament de les despeses en maquinari i programari durant la fase de transició, prestació i de devolució del servei. Entre d'altres:
 - La provisió de dispositius criptogràfics HSM dedicats a la generació, custòdia i ús de les claus de signatura pels entorns de producció i contingència, tal i com s'especifica en el present document.
 - També les targetes d'operació remota que calguin pel canvi de titularitat de claus a l'adjudicatari.
 - La provisió de les eines d'observació en temps real dels Acords de Nivell de Servei, detallats en el present document.
- Durant tota la vigència del contracte, el manteniment i evolució de la solució de signatura i segell electrònic remots, interfícies i gestió de credencials d'accés al servei.
- Les despeses de funcionament ordinari, de gestió operativa i explotació del servei, incloent específicament l'adequació al marc normatiu i tècnic vigent a cada moment.
- El servei de suport de tercer nivell, d'acord amb els acords de nivell de servei del Consorci AOC
- Adequació de la documentació del servei al marc normatiu vigent en cada moment així com les traduccions necessàries. La documentació del servei inclou: manuals, material de suport, procediments, etc..
- Les auditories i altres avaluacions periòdiques a que s'hagi de sotmetre, en l'àmbit d'aplicació d'aquest plec.

- Els serveis “Serveis organitzatius i de compliment” descrits al present document i que inclouen l'emissió i control de les factures enviades als organismes finals, d'acord amb les directrius del Consorci AOC i el servei de formació a operadors de registre.

Els següents serveis no són objecte d'aquest contracte:

- El servei de suport de primer nivell.

6.3.2 Serveis a preu unitari i manteniment d'aplicacions informàtiques

Un cop iniciada la fase de prestació del servei, es considera un cost unitari pel seu consum sota demanda, associat a les modalitats indicades a continuació.

Pels evolutius que es requereixin durant l'execució del contracte, els serveis de programació tindran un cost associat.

Sota aquestes categories s'inclou el següent catàleg de serveis amb els preus i volumetries previstes per any que s'indiquen al Plec de Clàusules Administratives:

Concepte	Descripció breu
Emissió de certificat remot per a la ciutadania	Emissió de certificat qualificat en repositori remot no qualificat per a la ciutadania
Emissió de certificat remot Qualificat per signatura qualificada pel sector públic	Emissió de certificat personal qualificat amb vigència de 5 anys en repositori remot qualificat pel sector públic.
Emissió de certificat personal remot pel sector públic	Emissió de certificat personal qualificat amb vigència de 5 anys en repositori remot no qualificat pel sector públic.
Emissió de Segell Remot pel sector públic	Emissió de certificat de segell qualificat amb vigència de 3 anys en repositori remot no qualificat pel sector públic.
Serveis de programació	Preu/hora programador

6.3.3 Gestió de les claus d'entitat final i jerarquia

- [R25] Les claus dels certificats d'entitat final del servei de signatura remota es generaran, utilitzaran i custodiaran en dispositius criptogràfics (HSM) d'acord a la normativa aplicable i condicions definides en el present plec de prescripcions tècniques. Els HSMs per allotjar les claus del SSR hauran de ser proveïts per l'adjudicatari i dedicats al servei del Consorci AOC. En el punt “6.4 El Servei de Signatura Remota (SSR) del Consorci AOC” es defineixen les condicions en relació als àmbits, nivells de confiança, etc., requerits per a la prestació del servei.
- [R26] Les claus de la jerarquia emissora dels certificats d'entitat final es lliuraran a l'adjudicatari durant la fase de transició. Es transferiran a l'adjudicatari mitjançant el lliurament dels fitxers de claus i els fitxers del security world associat. S'ampliarà el conjunt de targetes d'Operació dels dispositius criptogràfics i es lliuraran a l'adjudicatari les targetes addicionals. L'adjudicatari podrà proposar altres opcions

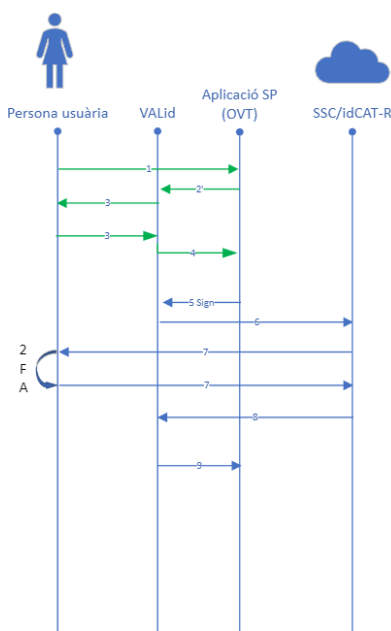
de traspàs de la operació mentre aquesta segueixi essent segura i conforme al marc normatiu. L'adjudicatari les operarà tenint en les condicions indicades al present document, i també s'encarregarà de reconèixer aquestes subCAs davant de terceres parts.

6.4 El Servei de Signatura Remota (SSR) del Consorci AOC

6.4.1 Servei de signatura electrònica en remot per a la ciutadania

[R27] Integrat amb VALid com a mecanisme d'autenticació de la identitat de les persones usuàries.

Un exemple de funcionament del procés de signatura remota per a la ciutadania seria el mostrat pel següent esquema, on "Aplicació SP" seria una carpeta ciutadana d'un Ajuntament, per exemple:



[R28] L'adjudicatari oferirà una API per produir signatures electròniques amb els certificats generats que el Consorci AOC integrarà amb el servei Signador per oferir la funcionalitat de signatura electrònica amb certificat qualificat.

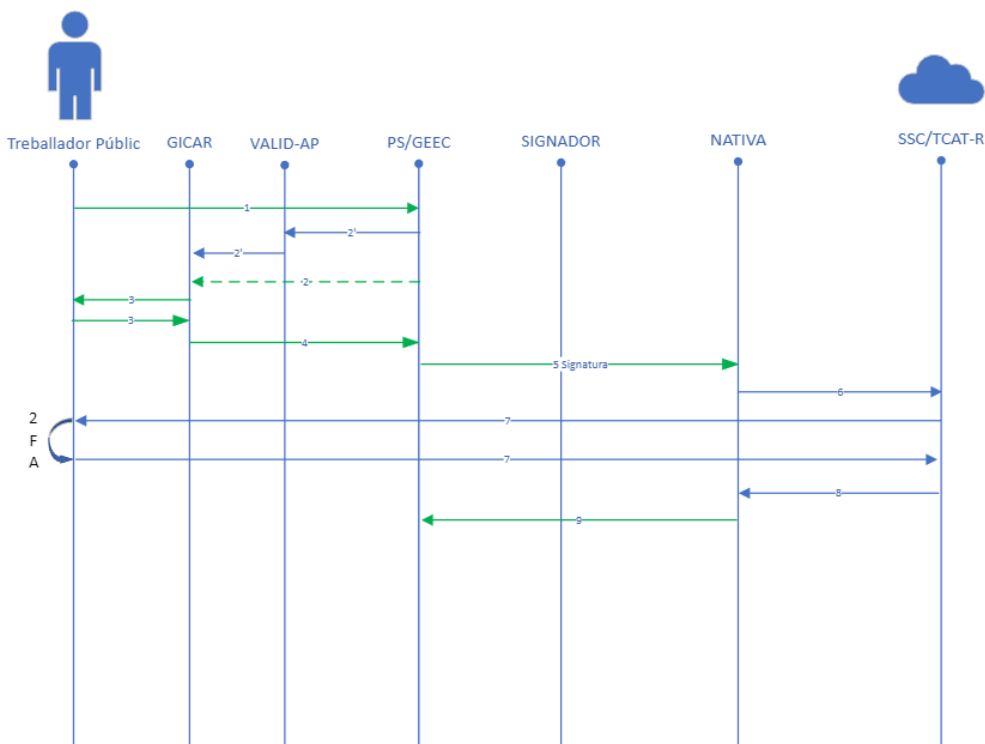
El procés de registre i emissió dels certificats de signatura electrònica en remot per a la ciutadania serà el mateix que ja s'utilitza actualment per a l'emissió dels certificats idCAT en programari. L'emissió dels certificats es gestionarà mitjançant les APIs que l'adjudicatari proporcionarà a l'efecte.

6.4.2 Servei de signatura electrònica en remot per als empleats i treballadors del sector públic

[R29] Pel que fa als usos d'identificació i signatura, els serveis objecte d'aquest contracte s'hauran d'integrar, com a proveïdor de identitat i signatura de les Administracions Públiques Catalanes, a través d'un servei comú ofert pel Consorci.

[R30] Pel que fa a les funcionalitats de generació de signatura electrònica, els serveis objecte del contracte s'hauran d'oferir a través de l'element Signador (<https://signador.aoc.cat/signador/init>).

Exemple de funcionament, on GICAR és un exemple de mecanisme d'identificació d'una administració, i "PS/GEEC" és una aplicació exemple que requereix que els usuaris signin :

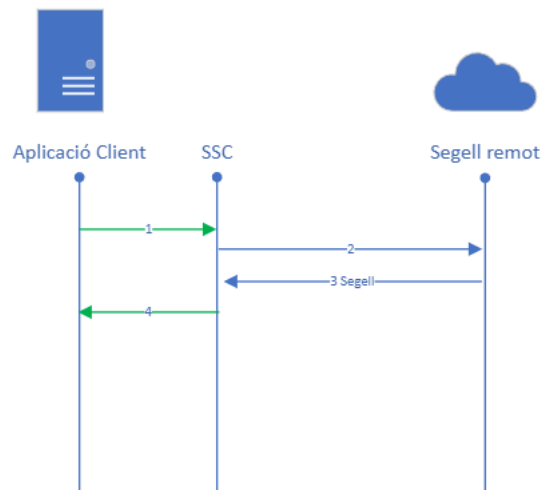


6.4.3 Servei de signatura electrònica en remot amb certificats de segell electrònic qualificat pel sector públic

- [R31] Oferir el servei de custòdia de certificats qualificats de segell electrònic.
- [R32] Custodiar els certificats de segell electrònic que actualment estan hostatjats al servei Signador Centralitzat del Consorci AOC descrit al punt 4.3 d'aquest document.
- [R33] Oferir una API per integrar les funcions de segellat electrònic en els formats qualificats XAdES, CAdES i PAdES. Caldrà proporcionar un descriptor en WSDL per tal de facilitar la integració de les aplicacions que seran usuàries.
- [R34] L'adjudicatari haurà de prestar aquestes funcionalitats ajustant-se a l'Acord de Nivell de Servei descrit en aquest plec.
- [R35] Actualment els sistemes i dispositius de signatura i segell electrònics que el Consorci AOC ofereix treballen amb algorismes de signatura RSA i de resum criptogràfic SHA1, SHA256 i SHA512. En tot cas, el servei de signatura electrònica en remot haurà de treballar amb els algorismes recomanats a la darrera versió de l'especificació ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

Si cal canviar la missatgeria sencera per algun motiu evolutiu, de seguretat, etc., caldrà planificar-ho al llarg del contracte. Si aquest és el cas, el Consorci AOC definirà una missatgeria pròpia, alineada amb els estàndards vigents, per evitar canvis en futurs canvis d'aplicacions de signatura.

Exemple de funcionament, on “SSC” és el bus d’integració de mecanismes d’identificació que l’AOC ofereix a les administracions públiques catalanes, i que serà l’encarregat de cridar, via API, a les funcions de segellat electrònic que proporcionarà l’adjudicatari:



6.5 Aplicació PKI

- [R36] L'aplicació de gestió de la infraestructura de clau pública (PKI) que l'adjudicatari porti per allotjar i fer ús de les claus de jerarquia, cal que estigui certificada Common Criteria EAL 4+ i estigui configurada per aproximar-se tant com sigui possible a la política de seguretat CIMC (Certificate Issuing and Management Components Protection Profile).
- [R37] La solució d'infraestructura de clau pública (PKI) aportada per l'adjudicatari haurà de ser mantinguda en termes de suport i actualitzacions de seguretat al llarg de tota la vigència del contracte. Addicionalment, haurà de permetre la devolució del servei a la finalització del contracte i no impedir que un futur es requereixi transferir el servei a un nou adjudicatari.
- [R38] En cas d'incapacitat per proveir el servei, desaparició o cessament de les activitats de l'adjudicatari, aquest haurà de lliurar al Consorci AOC el codi font del programari de la PKI emprat per a l'operació de les ECs que formen part de la jerarquia de certificació del Consorci AOC.
- [R39] La nova solució PKI haurà d'incorporar serveis de publicació de l'estat dels certificats emesos que, com a mínim, ofereixin les funcionalitats i el rendiment dels sistemes requerits a l'apartat d'ANS i segons es defineixen a continuació.

6.5.1 Emissió de Llistes de Revocació de Certificats (CRL)

- [R40] Per a cada Entitat de Certificació (en endavant EC), l'adjudicatari generarà i allotjarà les corresponents llistes de revocació de certificats, d'acord a les condicions (de periodicitat, vigència, etc.) establertes a la Declaració de Pràctiques de Certificació,

publicada a: <http://epsd.aoc.cat/regulacio>. El Consorci AOC definirà amb l'adjudicatari un nom DNS del domini aoc.cat per a l'accés al servei.

6.5.2 Servei de Consulta d'Estat de Certificats en Línia (OCSP)

- [R41] Per a cada EC, l'adjudicatari gestionarà un servei de respostes OCSP. Aquest servei NO podrà respondre l'estat desconegut (UNKNOWN) pels certificats que no hagi emès. El Consorci AOC definirà amb l'adjudicatari, un nom DNS del domini aoc.cat per a l'accés al servei.
- [R42] Transferència de les claus de jerarquia: les claus privades de les Entitats de Certificació objecte d'aquesta licitació es van generar al 2022 en una sessió auditada i s'han inclòs en l'abast d'auditoria EIDAS i, per tant, a la Declaració de Pràctiques de Certificació del Consorci AOC. Aquestes claus es van generar amb tecnologia Entrust de dispositius HSMs model nCipher i es van protegir amb unes targetes d'operació (OCS) en una configuració 2/5 i amb totes les targetes en propietat exclusiva del Consorci AOC.
- [R43] Durant la fase de transició, el Consorci AOC ofereix la possibilitat de transferir a l'adjudicatari la custòdia d'aquestes claus mitjançant el procediment previst pel fabricant dels dispositius criptogràfics on es van generar les claus. És a dir, mitjançant la recuperació del Security World d'AOC als dispositius criptogràfics HSMs que proveeixi i canviant el conjunt OCS per un nou conjunt amb titularitat de operadors que l'adjudicatari defineixi.
- [R44] L'adjudicatari podrà utilitzar altres fabricants de HSMs o altres mecanismes de transferència sempre i quan no comprometin la seguretat de les claus ni les operacions associades durant el procés de la migració i usos posteriors.

6.6 Model de registre de serveis del Consorci AOC

- [R45] Pel compliment dels punts relatius al registre de dades d'ens i rols del sistema, en les condicions indicades a l'apartat "Obligacions relatives al procés de registre", l'adjudicatari haurà de configurar els sistemes objecte del contracte amb els rols del sistema del Servei de Certificació Digital que opera el consorci AOC.
- [R46] El Consorci AOC lliurarà a l'adjudicatari la informació de ens i rols en vigor i que l'adjudicatari haurà d'aplicar com a configuració inicial del nou servei que operarà. Addicionalment, les credencials d'operadors que es configuraran inicialment al sistema seran, per tant, també les mateixes que existeixen en la fase de transició. A partir de la primera sincronització, per cada canvi en les dades dels ens o operadors, l'adjudicatari configurarà les mateixes al sistema segons els ANS existents i relacionats a aquesta tasca.
- [R47] Els operadors de tot el sistema de registre actualment operen amb certificats no qualificats EIDAS però generats en targeta criptogràfica. D'aquesta manera es garanteix l'accés multi-factor al sistema de registre. La provisió d'aquestes targetes quedarà fora de l'abast d'aquest contracte.
- [R48] El compliment de la gestió de les altes en relació a l'auditoria externa EIDAS, recaurà en el sistema de l'adjudicatari, ja que és en aquest sistema on es configuren els accessos als serveis oferts i els elements aquí descrits només conformen el canal d'entrada de les mateixes fins a l'adjudicatari.
- [R49] Pel compliment de les obligacions relatives al procediment administratiu de qualsevol de les sol·licituds de dades del sistema o d'emissió de certificats,

- l'adjudicatari haurà de registrar d'entrada les peticions a través del servei de Registre Unificat (MUX) del Consorci AOC.
- [R50] Pel compliment de les obligacions relatives a la custòdia electrònica segura de qualsevol de les sol·licituds de dades del sistema o d'emissió de certificats, l'adjudicatari haurà d'integrar els seus processos amb el servei de custòdia DESA'L del Consorci AOC.
- [R51] L'adjudicatari haurà d'oferir i una aplicació per dur a terme la generació de les evidències derivades del cicle de vida dels certificats objecte d'aquest contracte, d'acord amb els procediments i manuals del Consorci AOC. A mode d'exemple, caldrà resoldre la signatura de múltiples operadors en l'aprovació i generació d'un certificat d'empleat públic. El format d'evidència generada ha de permetre garantir la seva retenció, validació i consulta durant quinze anys des de la data de caducitat del certificat, o segons el termini normatiu aplicable a cada moment durant la vigència del contracte.
- [R52] L'adjudicatari haurà d'oferir a través d'una interfície automàtica de programari (API) l'accés a totes les dades i processos de l'entitat de registre. En concret, ha de permetre l'accés a les dades d'usuaris, ens, rols, productes i també als processos de registre. L'objectiu és garantir el desacoblament dels components interns de les interfícies d'usuari. També per facilitar la integració en altres sistemes que pugui desenvolupar el Consorci AOC i que requereixin dades del registre de certificats.

6.6.1 Registre àmbit de l'empleat públic i segells electrònics

El Servei de Certificació Digital T-CAT es compon de tres elements principals::

- Connector AOC: canal d'entrada per a l'alta de serveis i per fer la tramitació de sol·licituds i modificació de dades de ens i rols en el servei de forma digital, segura i amb mecanismes per fer el seguiment del tràmit.
- Solució web per a la gestió de peticions, emissió i cicle de vida: per a les operacions de registre de dades de subscriptors, emissió de certificats, documentació i gestió del cicle de vida del certificat digital per mitjans web i també mitjançant connectors automàtics.
- Solució web per gestionar lliurament i codis d'activació : per fer el lliurament dels certificats de forma segura i enviant els codis d'activació per correu electrònic

El funcionament actual està exposat amb detall a l'annex d'aquest document.

- [R53] L'adjudicatari haurà de gestionar les sol·licituds de certificats rebudes pel Consorci AOC, a través dels diversos canals que aquest ofereixi als seus ens usuaris.
- [R54] L'adjudicatari haurà de proveir una solució web que permeti als operadors gestionar les peticions dels certificats, així com el seu cicle de vida, un cop emesos (revocació, consulta), d'acord als procediments i experiència d'usuari del Consorci AOC.
- [R55] Aquesta solució web de gestió ha de permetre la càrrega individual o massiva de peticions de certificats, des de la pròpia web o via "connector AOC". Haurà de disposar d'opcions per recuperar dades de l'històric de certificats.
- [R56] Disposar d'un mòdul de gestió d'estats dels certificats (cicle de vida). Aquest mòdul ha de poder ser utilitzat via web o bé via connector automàtic. En aquest punt és important destacar que la gestió dels certificats s'ha de poder fer per part d'un operador i per part del titular del certificat. Pel que fa a la solució web per gestionar lliuraments i codis d'activació, l'adjudicatari haurà de proveir una solució web que permeti als responsables dels ens usuaris lliurar els certificats als titulars, així com la generació dels codis d'activació corresponents, tants cops com sigui necessari, d'acord als procediments i experiència d'usuari del Consorci AOC,

- [R57] En els components que interaccionen directament amb l'usuari final, cal que aquests permetin l'acceptació digital i generació d'evidència corresponent per part de l'usuari. Per exemple, l'acceptació de les condicions a l'emissió del certificat en el moment del lliurament.
- [R58] Aquesta mateixa solució ha de disposar de connectors de consulta d'estat de certificats. En concret, les consultes, a mode d'informe, poden ser sobre un certificat en particular o múltiples (p.e.: els associats a una Entitat de Registre,) i es poden consumir de forma síncrona o asíncrona (p.e. informes diaris).

6.6.1.1 ER vinculades

- [R59] D'acord amb el que s'ha exposat fins ara, les ER vinculades no han de tenir necessitat de disposar de cap maquinari específic per fer la seva funció dins el Servei de Certificació Digital, a través de la solució web de gestió de lliuraments i codis d'activació.

6.6.1.2 L'ER centralitzada del Consorci AOC

- [R60] L'adjudicatari crearà una ER a les seves oficines des d'on podrà oferir els serveis d'acord amb les característiques de prestador públic que té el Consorci AOC. El Consorci AOC opera una ER que és la que centralitza les peticions de certificats digitals de tots els ens que no estan vinculats a una altra ER o que, puntualment, demanen emissions de trameses concretes de certificats, revocacions d'ofici, i la gestió dels operadors i rols en el sistema.

6.6.2 Registre àmbit ciutadania

- [R61] L'adjudicatari disposarà d'un sistema per emetre els certificats digitals en remot per a la ciutadania, a partir del registre dut a terme mitjançant el sistema de videoidentificació proveït pel Consorci AOC.
- [R62] La solució s'ocuparà de gestionar l'enviament de les comunicacions electròniques necessàries a la persona titular per a l'obtenció del certificat, així com d'oferir-li el mecanisme que li permeti signar l'evidència corresponent a la recepció del certificat.
- [R63] La responsabilitat de l'allotjament i custòdia de les evidències de registre del procés d'obtenció dels certificats recaurà en l'adjudicatari d'aquest contracte mentre no les dipositi als sistemes del Consorci AOC per custòdia segons el període normatiu de retenció.

6.7 Infraestructura tecnològica

6.7.1 Entorns

Per complir amb els requisits normatius, garantint-ne la disponibilitat i continuïtat dels serveis prestats, l'adjudicatari haurà de desplegar la infraestructura en els següents entorns:

6.7.1.1 Producció

- [R64] Entorn complet amb característiques d'escalabilitat, balanceig de càrrega i alta disponibilitat. El dimensionament dels equips ha de garantir la capacitat de procés de la càrrega de peticions d'usuaris prevista.

- [R65] Els elements de seguretat perimètrics han de garantir l'accés controlat als usuaris del sistema.

6.7.1.2 Contingència

- [R66] A l'entorn de contingència, amb requisits de seguretat equivalents als de producció, l'adjudicatari haurà d'allotjar els sistemes necessaris per a garantir, la continuïtat de tots els serveis objecte d'aquest contracte que s'ofereixen a l'entorn de Producció.

6.7.1.3 Preproducció

- [R67] Desplegament d'un entorn estable complet, destinat a les proves funcionals i a la realització de proves de rendiment. Tota la seva activitat no tindrà impacte en el conjunt de dades reals ni afectarà al rendiment dels altres entorns.

6.7.1.4 Desenvolupament

- [R68] Desplegament d'un entorn dissenyat per a la realització de les activitats relacionades amb el desenvolupament i el manteniment dels sistemes que formen el servei. Sense requeriments especials d'estabilitat ni disponibilitat.
- [R69] L'entorn de desenvolupament pot estar diversificat sempre que es garanteixi la seguretat en el control d'accés i que no s'utilitzin dades reals.

6.7.2 Centres de Processament de Dades

- [R70] Donat que els custodis de les targetes d'administració (ACS) dels dispositius criptogràfics (HSMs) en els que s'allotjaran les claus de les ECs del Consorci AOC seran personal vinculat al mateix Consorci AOC i, amb l'objectiu de minimitzar els desplaçaments que aquests hagin de fer cada cop que calgui realitzar una intervenció sobre aquests dispositius, es requereix que el CPD principal (CPD-1) estigui ubicat a l'àrea metropolitana de Barcelona.
- [R71] La infraestructura tècnica dins del CPD principal ha de trobar-se en una cambra amb condicions de seguretat i nivell de protecció contra qualsevol agressió física que pugui afectar als equips informàtics o de telecomunicacions, i haurà de ser conforme als requisits que imposen les normes tècniques aplicables als prestadors de serveis de confiança que emeten certificats qualificats i ofereixen serveis de signatura remota, ja especificades en aquest plec.
- [R72] Al CPD de contingència (CPD-2), amb requisits de seguretat equivalents als del CPD principal, l'adjudicatari haurà d'allotjar els sistemes necessaris per garantir la continuïtat de tots els serveis objecte d'aquest contracte a l'entorn de Producció. Pels ANS d'activació del Pla de Recuperació de Desastres (PRD), es requereix que aquest CPD també estigui a la província de Barcelona i a una distància de seguretat mínima de 15 kms del CPD principal (CPD-1). El Consorci AOC acceptarà que el requisit de distància sigui superior, sempre dins del territori espanyol, si l'adjudicatari proposa l'ús de mecanismes d'administració i operació dels dispositius remotes que siguin segurs, sempre d'acord amb el que indiqui el propi fabricant dels dispositius criptogràfics.
- [R73] La resta de capes de serveis tecnològics poden estar allotjades al núvol (cloud), si el proveïdor ho considera. En aquest cas, haurà de garantir el compliment de les obligacions establertes pel marc normatiu del present plec, especialment al que especifica el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals, així com l'Acord de Nivell de Servei requerit.

6.7.3 Maquinari i programari dedicat

- [R74] Les claus criptogràfiques dels usuaris del servei de signatura remota i de les EC's del Consorci AOC s'hauran de generar i mantenir dins de dispositius criptogràfics (HSMs) d'ús exclusiu per al Consorci AOC. Les aplicacions de generació i gestió de certificats, així com de signatura electrònica remota també han de ser per a ús dedicat als serveis del Consorci AOC. La configuració serà en alta disponibilitat per a l'entorn de Producció i, si la capacitat ho permet, també per al de contingència.
- [R75] Al llarg de la vigència del present contracte, s'ha previst (en l'import a tant alçat) que anualment l'adjudicatari adquireixi i renovi els dispositius criptogràfics del servei, juntament amb els eventuais serveis de migració de claus entre els dispositius antics i els nous, si s'escau. La instal·lació d'aquests nous dispositius i les tasques crítiques de migració es duran a terme a les instal·lacions de l'adjudicatari per, en última instància, fer la seva posada en funcionament al llarg de l'execució del present contracte i les seves pròrrogues.
- [R76] Es preveu, per tant, que si s'executa tot el contracte fins a la seva duració màxima, es puguin renovar completament la plataforma criptogràfica. De cara a la correcta devolució del servei, aquests dispositius s'hauran de mantenir amb la garantia del fabricant durant tota la vigència del contracte per part de l'adjudicatari.

6.8 Governament de la Seguretat

6.8.1 Gestió de traces

- [R77] L'adjudicatari haurà de complir amb la norma de gestió de traces vigent, i haurà d'assegurar que emmagatzema totes les traces que li apliquen, d'acord a la classificació d'informació segons l'Esquema Nacional de Seguretat i als requisits establerts a les normes ETSI objecte d'auditoria.
- [R78] Les traces hauran de ser accessibles en mode lectura i s'assegurarà el marcatge de les traces amb requeriments específics de conservació segons la legislació aplicable.
- [R79] L'adjudicatari, tenint en compte el nivell de classificació de seguretat de l'aplicació exposat a l'apartat "Classificació de la informació", haurà de facilitar els mecanismes per a que les traces siguin accessibles i estiguin integrades amb el repositori de traces de seguretat que determini el Consorci AOC.
- [R80] L'adjudicatari haurà de dur a terme el retorn al Consorci AOC de les dades i traces generades com a molt en periodicitat anual.

6.8.2 Comunicacions segures d'accés a les aplicacions objecte de la licitació

- [R81] L'adjudicatari haurà de garantir que totes les aplicacions web objecte del contracte (tant internet com intranet) utilitzin canals de comunicació segurs HTTPS/TLS.

6.8.3 Arquitectura, proves de recuperació de desastres i proves de recuperació de backups

L'adjudicatari haurà de:

- [R82] Garantir que el disseny de l'arquitectura de la solució permet assolir els requeriments de disponibilitat/continuitat requerits.

- [R83] Participar en la preparació i execució de les proves de recuperació de desastres (PRDs) i en les proves de recuperació de backups, realitzant proves que certifiquin la capacitat de recuperació esperada.

6.8.4 Seguretat de les instal·lacions des de les quals es presta el servei

- [R84] L'adjudicatari vetllarà pel compliment de les mesures de seguretat exposades a les Condicions Generals de Prestació dels serveis i a la Declaració de Pràctiques de Certificació del Consorci AOC i podrà ser auditat de forma anual per valorar el grau de compliment i identificar riscos de seguretat.

6.8.5 Seguretat en el cloud

- [R85] En el cas que algun dels serveis o eines de suport a la prestació del mateix estiguin ubicats al núvol, l'adjudicatari haurà de garantir igualment el compliment dels requeriments de seguretat que estableix el marc normatiu indicat en aquest plec.

6.8.6 La gestió de la seguretat i el compliment normatiu

- [R86] L'adjudicatari, de forma coordinada amb l'àrea de seguretat del Consorci AOC, haurà de donar compliment al marc legal i normatiu vigent (definit al punt 3. Marc Normatiu).

En aquest apartat es remarquen aquells aspectes de seguretat considerats de major rellevància dins l'abast del servei i que caldrà tenir operatius per la posada en marxa del mateix.

6.8.6.1 Classificació dels sistemes d'informació

- [R87] L'adjudicatari haurà de tenir en compte el nivell de seguretat dels sistemes d'informació objecte del contracte, segons l'anàlisi de riscos realitzat pel Consorci AOC amb acord al que especifica l'Esquema Nacional de Seguretat, per aplicar correctament el marc normatiu i legal indicat anteriorment.

6.8.6.2 Compliment normatiu i legal

- [R88] L'adjudicatari haurà de complir amb tots els requeriments que siguin d'aplicació d'acord al marc normatiu de seguretat vigent i de totes les actualitzacions posteriors que es produeixin, així com a tot el marc legal en matèria de ciberseguretat que en sigui d'aplicació (per exemple, Esquema Nacional de Seguretat (ENS), el Reglament General de Protecció de dades (RGPD) i el Reglament Europeu d'identificació i serveis de confiança (eIDAS).
- [R89] L'adjudicatari haurà d'incorporar-se al model de compliment normatiu del Consorci AOC. En aquest model s'integren les possibles auditories que el Consorci AOC determini realitzar, així com el seguiment dels plans d'acció derivats de les mateixes. També s'inclou en aquest model el compliment per part de l'adjudicatari de plans d'acció relatius a normatives o estàndards que el Consorci AOC determini realitzar i el seu seguiment recurrent. L'adjudicatari haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en el model de compliment, donant resposta en els terminis marcats pel Consorci AOC.
- [R90] L'adjudicatari haurà de garantir l'accés del personal autoritzat del Consorci AOC a la informació de seguretat (procediments, registre d'incidents, traces, etc.). Tota la

informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. El Consorci AOC i l'adjudicatari establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat requerits .

6.8.6.3 Requisits de protecció de dades

- [R91] El licitador, en la seva oferta, haurà de detallar les mesures de seguretat i les mesures de privacitat des del disseny i per defecte que s'estableixen per donar compliment als requeriments establerts al Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i a Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. En aquest sentit, caldrà estar a les guies aprovades per l'Autoritat Catalana de Protecció de Dades, l'Agencia Española de Protección de Datos i el Comitè Europeu de Protecció de Dades (CEPD).
- [R92] L'adjudicatari haurà de revisar anualment, i quan es produeixi alguna modificació en el tractament de les dades, l'Anàlisi de Riscos pels drets i llibertats dels titulars de les dades i adoptar les mesures de seguretat que, si s'escau, calgui implantar per preservar-los

6.8.6.4 Auditoria externa

- [R93] L'adjudicatari haurà de disposar de la certificació de compliment, a partir de l'inici de la fase de transició i fins a la finalització del contracte, conforme a l'Esquema Nacional de Seguretat de nivell ALT, així com una auditoria sobre el compliment de la normativa de protecció de dades de caràcter personal..

S'adjunta informació de rellevància a tenir present per a l'assoliment d'aquest requeriment:

- Esquema Nacional de Seguretat (ENS):
 - o Per donar compliment amb els requisits en matèria d'integritat, disponibilitat, autenticitat, traçabilitat, confidencialitat de la informació, segons disposa l'ENS i d'acord als paràmetres aprovats pel Consorci AOC dins la categorització del servei en els dominis de l'ENS:

Sistema Servei de Certificació Digital						
Denominació de l'actiu essencial	C	I	D	A	T	DP
Subsistema repositori de jerarquia de claus de l'entorn principal	A	A	A	M	M	
Subsistema repositori de jerarquia de claus de l'entorn de contingència	A	A	A	M	M	
Subsistema d'emissió i revocació de certificats de l'entorn principal	M	M	A	M	B	M
Subsistema d'emissió i revocació de certificats de l'entorn de contingència	M	M	A	M	B	M
Subsistema d'Informació pública	B	B	A	M	M	
Subsistema repositori de claus remotes de l'entorn principal (SSR-QSCD)	A	A	A	M	A	M
Subsistema repositori de jerarquia de claus de l'entorn de contingència (SSR-QSCD)	A	A	A	M	A	M
Subsistema de suport	B	M	M	B	B	B
Subsistema serveis AOC (EACAT, MUX, DESAL, VO, VALID i Signador)	B	B	A	M	M	M
Valor màxim registrat	A	A	A	M	A	M
La valoració del subsistema es Alta (C=A, I=A, D=A, A=M, T=A, DP=M)						

- RTO i RPO segons definit al punt “7.2.4ANS de continuïtat”.
- Els subsistemes marcats en color verd, donat que es trobaran completament sota la responsabilitat de l'adjudicatari, seran objecte d'auditoria de actiu o subsistema d'acord a ENS per part de l'adjudicatari al llarg de la vigència del contracte. Els altres dos punts, donat que estan parcialment a AOC, l'auditoria es coordinarà amb AOC i s'executarà en també al llarg de la vigència del contracte.
- Accessibilitat:
 - Compliment normatiu normes accessibilitat aplicables.
- Pla de Seguretat del Consorci AOC:
 - Política de seguretat i normes derivades (veure punt “**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**”).
- Acreditació voluntària del PSC:
 - Auditoria interna del % de certificats emesos per part del propi adjudicatari.
 - A nivell de traces : de sol·licitud, aprovació, emissió, lliurament.
 - A nivell de producte amb certint o eines equivalents
 - Auditories periòdiques de les Entitats de Registre.

6.8.7 La gestió de la continuïtat i la disponibilitat

La finalitat de la gestió de la continuïtat i la disponibilitat se centra, principalment, en garantir la continuïtat dels serveis i processos davant de qualsevol situació adversa, evitant un impacte significatiu en l'organització, amb l'objectiu de garantir l'Acord de Nivell de Servei (en endavant ANS) especificat en aquest plec i complir amb els requisits a nivell normatiu.

Els objectius que es persegueixen són:

- Disposar de Plans de Continuïtat que permetin gestionar de forma eficient una situació d'emergència.
- Garantir la continuïtat dels processos i serveis considerats crítics, la indisponibilitat dels quals podria tenir un impacte irreversible.
- Provar els Plans de Continuïtat com a mesura de garantia de la seva efectivitat davant una situació real de contingència.
- Focalitzar l'esforç en la mitigació de riscos rellevants.
- Coordinar a totes les persones clau per fer front a una situació de contingència.
- Complir amb els requeriments legals / regulatoris en matèria de continuïtat de negoci.
- Alinear-se amb la metodologia del Consorci AOC i bones pràctiques del mercat (ISO 27002, BS25999/ISO22301, NIST sp 800-30,34, PAS 77, ITIL, ISO/PAS 22399:2007)

[R94] L'adjudicatari haurà de lliurar al Consorci AOC la seva política de continuïtat.

[R95] L'adjudicatari haurà de documentar, desenvolupar i implantar les mesures de disponibilitat necessàries per cobrir els indicadors de nivell de servei de disponibilitat especificats en aquest plec. Aquesta documentació s'haurà de lliurar al Consorci AOC.

[R96] L'adjudicatari haurà d'implantar mesures sobre els actius implicats que li permetin elaborar i lliurar al Consorci AOC un Pla de Continuïtat i de Recuperació davant Desastres del servei (en endavant, PRD) per garantir els nivells de servei establerts en aquest plec i que es deriven del document d'anàlisi de impacte de negoci (en anglès, Business Impact Analysis o BIA) elaborat pel Consorci AOC en relació a aquest servei i de la normativa aplicable.

- [R97] L'adjudicatari haurà de mantenir actualitzat el PRD davant canvis propis o per causes de tercers.
- [R98] L'adjudicatari haurà de proveir solucions tecnològiques que permetin assolir els objectius fixats al PRD, essent aquestes certificades mitjançant proves de recuperació periòdiques.
- [R99] L'adjudicatari participarà en les proves de recuperació i alta disponibilitat que el Consorci AOC planifiqui. Haurà d'elaborar el pla de proves i executar-les el dia de la prova, si s'escau, coordinadament amb els equips que realitzen les proves de continuïtat.
- [R100] Tota la informació del PRD haurà d'estar sempre disponible per al personal del Consorci AOC autoritzat i prèviament identificat. S'establiran els mecanismes per facilitar l'accés del personal autoritzat del Consorci AOC a aquesta informació, establint els controls de seguretat mínims exigits pel Consorci AOC.

6.8.8 Cessament de l'activitat

- [R101] En cas de cessament de l'activitat per part del Consorci AOC, l'adjudicatari col·laborarà amb el Consorci amb les tasques descrites per aquest en el seu Pla de Cessament de l'activitat. Aquestes tasques inclouen:
 - La notificació a les persones i organitzacions usuàries del servei, així com als òrgans supervisors i d'altres entitats implicades.
 - La transferència de les seves obligacions a un altre eventual prestador de serveis de confiança per mantenir el servei durant el període de temps definit al Pla.
 - La destrucció de les claus privades, tant de les entitats intermèdies com de les entitats i persones usuàries del servei, gestionades per l'adjudicatari.
 - En cas de cessament de l'activitat, el Consorci AOC revocarà les autoritzacions a l'adjudicatari per en el seu nom a l'hora de prestar els serveis objecte d'aquest plec.

6.8.9 Auditories a les Entitats de Registre vinculades

- [R102] Tal i com s'indica en el punt "11.5 Serveis d'auditoria d'ER", el Consorci AOC duu a terme auditories de control procedimental del compliment de les funcions i responsabilitats exercides per les ER que facin ús dels processos i aplicacions proveïdes per l'adjudicatari en el marc d'aquest contracte. Si s'escau, l'adjudicatari haurà d'aplicar les mesures derivades del resultat de les auditories a les ER en els seus processos i aplicacions.

6.8.10 Auditories del Prestador de Serveis de Certificació Consorci AOC

- [R103] Tal com s'estableix a les obligacions essencials del contracte, l'adjudicatari queda obligat a la adequació i plena conformitat dels serveis en l'àmbit del present contracte ReIDAS, i a les normes tècniques que aprovades per a la seva aplicació.
- [R104] En aquest sentit, el contractista haurà de complir, sense costos emergents pel Consorci AOC, amb la resta d'obligacions corresponents a la seva condició de prestador de serveis de confiança qualificat. Això inclou tant les avaluacions periòdiques i planificades, com les inspeccions que puguin sobrevenir.
- [R105] Més concretament: l'adjudicatari s'haurà de sotmetre a les auditories de compliment que facilitin els reconeixements dels certificats emesos. També s'haurà de sotmetre, si s'escau, a les inspeccions que el Supervisor Nacional d'acord a EIDAS requereixi, siguin rutinàries o extraordinàries. Sense costos emergents pel Consorci AOC,

- donat que aquests conceptes estan inclosos en els serveis que prestarà l'adjudicatari.
- [R106] L'àmbit de l'auditoria externa inclourà les subCAs i perfils que emeti i operi l'adjudicatari en l'àmbit del present contracte i, en cap cas, altres subCAs o perfils de la resta de jerarquia de Certificació del Consorci AOC.
- [R107] L'àmbit d'auditoria també inclourà l'aplicació de signatura remota emprada per l'adjudicatari, donat que és un dispositiu qualificat de signatura electrònica remota.

6.9 El servei de suport

6.9.1 El servei de Suport del Consorci AOC

Actualment el servei de suport del Consorci AOC s'estructura en 3 nivells:

- **1er nivell:** format per personal subcontractat, extern al Consorci AOC. Aquest nivell s'encarrega de resoldre incidències tipificades, documentades i d'acord a procediments definits al portal de suport i a la web del Consorci AOC i de resolució senzilla. Els seus ANS estan publicats a la web del Consorci AOC
- **2n nivell:** format per personal subcontractat, extern al Consorci AOC. S'encarrega de resoldre incidències que requereixen intervenció de personal amb certa qualificació tècnica i que no es troben documentades i ni disposen de procediments al portal de suport ni a la web del Consorci AOC.
- **3er nivell:** Aquelles incidències que no puguin ser resoltes al nivell 2 es deriven al tercer nivell. En el cas del servei objecte d'aquest contracte, es requereix a l'empresa adjudicatària la resolució d'incidències escalades a aquest nivell.

6.9.2 Àmbits d'atenció i suport a prestar per l'adjudicatari:

- [R108] L'adjudicatari haurà d'oferir el servei de suport de tercer nivell al Consorci AOC.
- [R109] També haurà de fer el manteniment del material de suport corresponent (FAQ's, alguns manuals tècnics i operatius, vídeos, etc). Aquests canvis caldrà realitzar-los amb la màxima celeritat. Es requerirà a l'adjudicatari que proveeixi i mantingui, sense costos emergents pel Consorci AOC, eines d'auto diagnòstic i d'autoservei adreçades als usuaris del servei, que millorin la capacitat de resposta dels primers nivells de suport i millorin la percepció del servei per part dels usuaris.

6.9.3 Canals d'entrada de peticions

Els usuaris formularan les seves peticions pels canals habituals:

- Servei d'atenció telefònica, per resolució de dubtes i incidències: 900 90 50 90
- Mitjançant formulari web habilitat a l'efecte.

El nivell 1 derivarà a l'adjudicatari les peticions referents al servei objecte d'aquest contracte, generant el tiquet corresponent amb l'eina de ticketing que empra el Consorci AOC pel suport a la resta dels seus serveis (què actualment és "ZENDESK") la qual assignarà un número identificador de la petició.

El Consorci AOC cedirà a l'adjudicatari les llicències d'usuaris de la eina de ticketing que siguin necessàries per tal que les pugui emprar el personal de l'empresa adjudicatària que

prestarà el servei de suport, en els casos que des de l'AOC se'ls hi sol·liciti intervenció per solventar alguna incidència.

6.9.4 Horari d'atenció

[R110] L'horari del servei de suport de 3er nivell a prestar per l'adjudicatari serà, com a mínim, de 8.00 a 17.00 hores, de dilluns a divendres, excepte festius del calendari laboral de Catalunya. De forma ocasional es podria ampliar aquest horari per alguna campanya especial.

6.10 Servei de Manteniment Evolutiu

[R111] En tractar-se d'un servei allotjat per l'adjudicatari, el mateix inclourà, dins del preu d'adjudicació del contracte, i durant tota la vigència del mateix, un servei de manteniment evolutiu per a adequacions del servei.

En aquest apartat es descriu tant la metodologia com la dedicació que es destinarà aquest servei, així com la tipologia de canvis i adequacions a aplicar.

L'abast d'aquest manteniment seran les aplicacions esmentades en els requisits objecte d'aquesta licitació. El codi d'aquests components s'allotjarà al gestor de codi GIT del Consorci AOC per al seu manteniment i evolució al llarg de tota la vigència del contracte. S'exclou el codi font i propietat intel·lectual del producte comercial ja desenvolupat que s'aportarà per oferir el servei i del qual únicament es guardaran al gestor de codi les configuracions i personalitzacions. Tota la gestió d'aquests canvis i intercanvis de documents relacionats es farà a través de l'eina JIRA del consorci AOC.

Per totes les situacions d'adequació del servei s'hauran de complir els següents requisits:

- Abans de portar a terme una tasca d'evolutiu, l'empresa adjudicatària portarà a terme un anàlisi de l'impacte que aquesta pot tenir en matèria de protecció de dades de caràcter personal i dur a terme un AARR
- Prèvia a l'aplicació de l'actualització del servei, l'adjudicatari es compromet a realitzar una còpia de seguretat de totes les dades, evitant la pèrdua d'informació.
- Abans d'executar l'actualització del servei en Producció, serà necessari disposar de la conformitat del Consorci AOC mitjançant un tiquet en l'eina de gestió de canvis (JIRA). En aquest tiquet es confirmaran els punts de control definits en els punts successius, així com la data i hora de quan serà realitzada la instal·lació de l'actualització.
- Les actualitzacions del servei, hauran de ser realitzades a la finestra temporal indicada pel Consorci AOC. En general, en l'entorn de Producció els dimecres a partir de les 15:00 i en l'entorn de Preproducció els dijous a partir de les 10:00.
- Si es produís una baixada en el rendiment del servei com a conseqüència de la posada en marxa d'algun canvi, l'adjudicatari haurà de tractar-lo com un error del servei.

Els acords de nivell de servei aplicables a les sol·licituds de Servei de manteniment evolutiu seran els definits per l'ANS descrit en aquest plec.

6.10.1 Metodologia

La proposta metodològica ha de preveure, com a mínim:

6.10.1.1 Presa de requeriments

L'objectiu d'aquesta fase és que l'adjudicatari disposi de la llista de tots els requisits a satisfer per tal de dur a terme l'evolutiú proposat.

El tipus de requisits a satisfer podrà ser de diversa índole. Els requisits més rellevants són:

- Requisits funcionals: tenen a veure amb les funcionalitats que es desitja incorporar o modificar a l'aplicació.
- Requisits tècnics: tenen a veure amb possibles millores no funcionals de caire tecnològic; per exemple, potser l'actualització d'una versió determinada d'una llibreria d'un tercer. Un altre cas, pot ser que una consulta en base de dades cal fer-la sobre una tecnologia determinada (com podria ser mysql).
- Requisits de calendari: tenen a veure amb terminis de lliurament de l'evolutiú.
- Requisits de context: tenen a veure amb la importància que pugui tenir l'evolutiú, el possible impacte sobre els clients, la prioritat de l'evolutiú respecte la resta de sol·licituds en curs i/o prèviament planificades, etc.
- Requisits de Seguretat: incorporar tots els controls de seguretat que, pel tipus d'informació tractada, ha d'incorporar l'evolutiú.
- Mesures de privacitat, des del disseny i per defecte, a implantar, si s'escau, i en funció de l'anàlisi de riscos dut a terme pels dret i llibertats dels titulars de les dades

Serà responsabilitat de l'adjudicatari vetllar i preocupar-se de recaptar tots i cadascun dels requeriments que afecten a la sol·licitud d'evolutiú.

Per tal de facilitar aquesta feina es durà a terme les següents accions:

- Es farà arribar a l'adjudicatari un document, l'anomenarem **fitxa d'inici d'evolutiú**, amb una descripció el més detallada possible de l'evolutiú que es desitja. Aquest document serà consensuat per ambdues parts.
- L'adjudicatari revisarà amb deteniment aquest document i gestionarà tots els dubtes que sorgeixin fins a obtenir tots els requeriments demanats. Si bé hi pot haver varies reunions a tal efecte es valorarà que l'adjudicatari obtingui els requeriments amb les mínimes reunions possibles.
- Resultat de l'exercici anterior l'adjudicatari elaborarà un document, l'anomenarem **"Document de requisits"**, on es recullin tots els requeriments per abordar l'evolutiú, agrupats segons la tipologia descrita anteriorment.
- El Consorci AOC revisarà aquest document i es gestionaran els canvis pertinents fins la seva formalització.

6.10.1.2 Fase de pre-anàlisi

L'objectiu d'aquesta fase és obtenir una estimació del impacte, tant econòmic com tècnic, de l'evolutiú desitjat.

En base al "Document de requisits", l'adjudicatari procedirà a fer un pre-anàlisi dels canvis que implicaria realitzar a l'aplicació per tal d'aconseguir l'evolutiú desitjat.

Del resultat d'aquest exercici es realitzarà un altre document, **"Document de pre-anàlisi"**, el qual contindrà com a mínim la següent informació:

- Descripció del pre-anàlisi.
- Descripció de la solució proposada: descripció del disseny tècnic, en línies generals, que es seguiria. En cas que l'adjudicatari vegi varies alternatives, explicar-les i indicar els avantatges i inconvenients de cadascuna.

- Estimació del cost en hores que implicarà l'evolutiú. Inclourà la suma de l'estimació de les hores de dedicació dels recursos humans que l'adjudicatari ha proposat per la prestació del servei que caldrà per realitzar l'evolutiú..
- Calendari amb la planificació estimada del projecte. Tot i estar en una fase de pre-anàlisi l'adjudicatari haurà de fer l'esforç d'elaborar un calendari, el més acurat possible, amb la planificació del projecte. Com a mínim, contindrà la informació referent a la fase d'anàlisi, disseny, construcció del sistema, i implantació i acceptació.

6.10.1.3 Fase d'anàlisi

L'objectiu d'aquesta fase es realitzar un anàlisi del canvi evolutiu a realitzar. Cal assegurar que la solució adoptada compleix tots i cada un dels requeriments recollits al document de requeriments, per la qual cosa serà imprescindible l'aprovació del document de pre-anàlisi abans d'iniciar aquesta fase.

L'adjudicatari haurà de realitzar un anàlisi exhaustiu, de com a mínim, els següents ítems:

- Anàlisi funcional i tècnic
- Definició de les Interfícies d'usuari
- Definició de les mesures de seguretat i mesures de privacitat des del disseny i per defecte a implantar quan s'escaigui
- Descripció de proves de validació: cal descriure les proves que es duren a terme per tal de validar el canvi evolutiu. Com a mínim, caldrà detallar el següent tipus de proves a realitzar:
 - Proves unitàries: consisteix en proves realitzades a nivell unitari (pe. sobre una única classe). La finalitat es detectar possibles mal funcionament d'una classe o component.
 - Proves d'integració: consisteix en proves d'interacció entre classes i/o components. Consisteixen en garantir la correcta integració de tots els components i classes del projecte.
 - Proves funcionals: l'objectiu d'aquestes proves és garantir que les funcionalitats de l'evolutiú tenen el comportament esperat. Cal descriure totes les proves funcionals que garanteixin haver testejat totes les funcionalitats de l'evolutiú. També cal definir proves per testejar l'aplicació davant d'un mal ús de l'usuari, i assegurar que el control d'errors de l'aplicació és correcte.
 - Proves de rendiment, si s'escauen.
 - Proves de seguretat: ús d'eines d'anàlisi dinàmic (OWASP) i anàlisi estàtic per la identificació de vulnerabilitats de seguretat en el codi.
 - Proves de regressió: l'objectiu és garantir que les funcionalitats existents abans de fer l'evolutiú segueixen funcionant correctament.

Com a resultat de l'exercici anterior l'adjudicatari elaborarà un document, l'anomenarem **"Document d'anàlisi funcional"**.

6.10.1.4 Fase de disseny

L'objectiu de la fase de disseny és detallar el disseny tècnic que es farà servir per tal de desenvolupar l'evolutiú desitjat.

- Les tasques que comportarà aquesta fase són:
- Definició de l'Arquitectura del Sistema
- Disseny tècnic
- Especificació Tècnica de Planificació de Proves

Com a resultat de l'exercici anterior l'adjudicatari elaborarà un document, l'anomenarem **"Document de disseny"**.

6.10.1.5 Fase de construcció del sistema

Les tasques que comportarà aquesta fase són:

- Generació del codi dels diversos components (p.e. classes): això és programar/tocar tot el codi necessari. Caldrà que tot el codi estigui comentat amb detall, per mitja del **"javadocs"**.
- Execució de proves unitàries
- Execució de proves d'integració
- Execució de proves funcionals i de regressió.
- Execució de proves de rendiment, si s'escau.
- Execució d'anàlisi dinàmic i estàtic de seguretat.
- Elaboració de documentació: pot variar segons l'evolutiu, però generalment es demanarà un manual d'usuari.
- Definició de la formació (si és necessari)

Com a resultat de l'exercici anterior l'adjudicatari elaborarà un document, l'anomenarem **"Document de pla de proves"**, el qual contindrà totes les proves definides en la fase d'anàlisi amb l'estat de la prova (superada o no superada). També s'indicarà el percentatge entre les proves superades respecte les totals.

El Consorci AOC, o en qui delegui, podrà executar qualsevol mena d'anàlisi (dinàmic, estàtic) que consideri oportú en qualsevol moment per determinar si el nivell de seguretat de l'evolutiu compleix els requisits de seguretat previ el pas a producció. En aquests casos l'adjudicatari haurà de proveir d'un usuari de prova per la completa execució de les anàlisis.

Com a mínim, es realitzarà una sessió conjunta entre el personal de l'adjudicatari i el Consorci AOC per verificar que el pla de proves està al 100% correcte. Cas que després de la sessió encara hi hagi proves de validació no superades caldrà tornar a planificar una altra sessió. Aquest procés s'iterarà fins que el 100% de les proves sigui satisfactori.

Per donar per tancada aquesta fase, l'adjudicatari haurà de lliurar la següent documentació:

- Lliurament de tot codi font i tots els components necessaris per implantar l'evolutiu . Caldrà que el codi estigui comentat amb detall, per mitja del **"javadocs"**.
- Lliurament del compilable.
- "Guia de d'implantació del canvi": aquest document contindrà el detall de totes i cada una de les instruccions tècniques que cal executar per tal d'implantar l'evolutiu en qüestió.

6.10.1.6 Fase d'implantació i acceptació

En base als lliuraments de la fase anterior es procedirà a realitzar la implantació de l'evolutiu sobre els diferents entorns. En primer terme, en l'entorn de desenvolupament. Procedirà a realitzar l'execució del pla de proves. Cas satisfactori procedirà a promocionar el canvi en l'entorn de pre-producció i posteriorment al de producció.

Cas que en aquest procés els resultats obtinguts no siguin els esperats (és a dir, els que es van obtenir en l'entorn de desenvolupament de l'adjudicatari) l'adjudicatari haurà de donar el suport necessari, si cal presencial, per solventar-ho.

Per exemple, caldrà corregir totes les vulnerabilitats de seguretat identificades per complir amb els llindars fixats pel Consorci AOC. Quan es superin aquests llindars d'acceptació, l'evolutiu podrà promocionar-se a producció.

Una vegada s'hagi realitzat l'execució del pla de proves amb el 100% de les proves funcionant en l'entorn de pre-producció i producció es donarà el projecte per tancat. A partir d'aquest instant entrarà en vigor el període de garantia de l'evolutiu.

A partir d'aquest moment ja ha d'entrar en vigor l'etapa de suport, és responsabilitat de l'adjudicatari realitzar les tasques necessàries de traspàs, formació i documentació de projecte, d'operació, i procedimental per tal que els nous desenvolupaments ja puguin ser objecte del servei de suport 24x7.

6.10.2 Manteniment correctiu

El programari desplegat requerirà serveis d'evolució i personalització. Aquests serveis es dediquen al manteniment evolutiu periòdic i a la resolució d'incidències derivades del dia a dia. Inclouen tasques com ara:

- Diagnòstic de problemes i incidències.
- Tercer nivell de resolució d'incidències.
- Millores menors de gestió.
- Suport a la prestació i seguiment del servei.
- Suport a integracions de clients.
- Altres peticions

El servei de manteniment correctiu inclourà la resolució d'aquells errors dels components tecnològics de la solució i el possible mal funcionament que hagin estat construïts pel licitador que hagi resultat adjudicatari i que formin part de la solució.

6.10.3 Manteniment tècnic – legal

El servei de manteniment tècnic-legal inclourà l'actualització de la documentació jurídica vinculada als serveis objecte d'aquesta licitació. L'adjudicatari haurà de garantir que la solució aportada es mantingui conforme a les normes i especificacions tècniques sobre la matèria objecte del contracte definides en el punt **¡Error! No se encuentra el origen de la referencia.** del present plec. Les prestacions incloses en l'àmbit i l'import dels serveis recurrents, en referència a aquest aspecte, hauran d'incloure com a mínim:

- L'actualització de versions que incloguin modificacions i/o ampliacions obligatòries dels protocols publicats i aprovats pels organismes citats anteriorment.
- Realitzar les adaptacions necessàries en el servei, a efectes de compliment de la normativa.
- Fer una proposta de canvis, en cas de ser necessari per modificacions normatives, en relació als fluxos de facturació electrònica definits inicialment, garantint en tot moment que els mateixos es trobin d'acord amb la normativa.
- En tot cas, tota modificació derivada d'un canvi normatiu ha d'estar implementada en un termini que asseguri l'alineament amb la legislació aplicable.
- L'actualització de versions que resultin de canvis introduïts per problemes d'interoperabilitat amb altres fabricants (Microsoft, Mozilla, Java, Google, Apple)
- L'actualització de versions degudes al manteniment correctiu del programari.
- Realitzar les explicacions i aclariments referents a aquestes actualitzacions, mitjançant l'eina de gestió d'evolutius (JIRA).

6.10.4 Manteniment evolutiu

El servei de manteniment evolutiu, inclourà aquelles modificacions sol·licitades pel Consorci AOC, al marge de les contemplades anteriorment en els punts anteriors.

6.10.5 Tasques en l'àmbit del manteniment evolutiu

Les tasques que es realitzaran dins l'abast d'aquest Servei de Manteniment Evolutiu es determinen en funció de la demanda dels usuaris dels serveis, dels responsables dels mateixos o de les diferents incidències que tenen lloc al llarg de la durada del contracte i que generen necessitats de millora. Per estimar les tasques i dedicacions previstes al pressupost base de licitació s'ha tingut en compte l'ús actual del servei de certificació digital del Consorci AOC i les necessitats detectades en el moment de redactar aquest plec.

Les tasques del tipus "Manteniment correctiu" i "Manteniment tècnic - legal", en cas que vinguin derivades de incidències o adequacions tècniques-legals d'obligat compliment per la prestació del servei, seran assumides per l'adjudicatari i, per tant, han d'estar previstes en l'import a tant alçat del contracte.

6.11 Serveis organitzatius i de compliment

Els serveis de caire organitzatiu no definits específicament fins ara i que intervenen en la prestació del servei de certificació digital són els següents:

- Serveis jurídics:
 - o Redacció i manteniment de la Documentació Jurídica (Política de certificació, Declaracions de pràctiques de certificació de cada EC, Condicions d'ús de cada perfil de certificat, etc) de forma coordinada amb la Responsable d'Assessorament Jurídic de Serveis del CAOC.
 - o Informes ad-hoc relatius a la prestació ordinària del servei.
- Suport a l'operativa de les Entitats de Registre
 - o Gestió de la xarxa de les ER's
 - o Gestió de la configuració de permisos al sistema
- Generació d'informes sobre de les dades d'activitat del servei i integració amb el sistema de Business Intelligence del Consorci AOC.
- Facturació a clients del servei: ens subscriptors i també intermediaris per tots els conceptes: consum de certificats, materials, manteniment de les ER's, formacions, auditories, projectes, etc.
- Expert en protecció de dades que garanteixi que, en tot el cicle de vida de les dades i per a totes les activitats de tractament, s'han adoptat les mesures de privacitat des del disseny i per defecte, les mesures de seguretat necessàries en atenció als riscos que es puguin derivar pels drets i llibertats dels titulars de les dades, així com la seva avaluació continuada i que en base al principi de responsabilitat proactiva es compleix. S'haurà de disposar de la documentació acreditativa del compliment esmentat.

Els serveis de caire organitzatiu que intervenen en la prestació del servei són els següents:

Implementació dels perfils segons els tipus de perfils requerits i propòsits i necessitats amb OIDs definits pels CAOC i proposarà les modificacions a les DPC i PC i perfils que seran aprovades i publicades per AOC, si procedeix.

En concret, la definició de tots els perfils i reconeixement amb el ministeri durant la primera auditoria del servei durant la fase de transició.

- Serveis jurídics:

- Redacció i manteniment de la Documentació Jurídica (Declaracions de pràctiques, condicions específiques de prestació del servei, etc) de forma coordinada amb la Responsable d'Assessorament Jurídic de Serveis del CAOC.
 - Informes ad-hoc relatius a la prestació ordinària del servei.
- Generació d'informes sobre de les dades d'activitat del servei i integració amb el sistema de Business Intelligence del Consorci AOC.
- Facturació

Dur a terme els anàlisi de riscos i disposar de la documentació acreditativa de les mesures aplicades, per preservar els drets i llibertats dels titulars de les dades objecte de tractament. El Consorci AOC és el propietari de tota la documentació elaborada per l'adjudicatari referent al servei prestat, i serà el responsable de la seva validació i aprovació.

[R112] Per la seva banda, l'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que el Consorci AOC proporcioni per tal efecte. Així mateix l'adjudicatari haurà de mantenir un registre de la documentació enviada al Consorci AOC amb el detall de les versions, dates i destinataris. Aquest registre estarà a disponible al repositori d'informació que el Consorci AOC hagi designat a tal efecte.

[R113] També es demana que es faci un registre de tots els fitxers que lliuri al Consorci AOC o que siguin generats per qualsevol petició concreta.

6.11.1 Serveis de formació

[R114] A demanda del Consorci AOC, l'adjudicatari haurà d'oferir els següents serveis de formació en relació als serveis objecte del present contracte:

Cursos virtuals:

- Cursos adreçats a usuaris finals, sobre els Usos i la difusió del certificat digital.
- Cursos dirigits als responsables del servei d'ens subscriptor per a processos de lliurament, manteniment, custòdia, etc...
- Cursos per formar operadors de les ER T-CAT o idCAT.

Aquests cursos es faran emprant la plataforma virtual del Consorci AOC, gestionada pel mateix Consorci AOC, amb els requeriments de la plataforma.

[R115] L'adjudicatari haurà de dur a terme la tutoria i la gestió de les inscripcions dels alumnes dels cursos virtuals, així com la resolució de les incidències que puguin aparèixer. El Consorci AOC posarà a disposició de l'adjudicatari els materials de que disposa, i que van ser elaborats per a les formacions que actualment està realitzant. Tot i que l'adaptació, el manteniment, i fins i tot la creació de nous materials formatius, l'haurà de fer l'adjudicatari, dins l'àmbit d'aquest contracte.

Pel que fa al servei de formació, es realitzen aquestes sessions amb aquests formats:

- 4 cursos virtuals per a operadors T-CAT.
- 14 cursos virtuals per a operadors idCAT.
- Curs virtual oberta per a ens subscriptor.
- De forma puntual cursos a mida presencials.

El servei de certificació digital porta a terme accions de formació i divulgació dirigides tant a usuaris finals (titulars dels certificats digitals) com a operadors i tècnics de suport a les Entitats de Registre.

6.11.2 Serveis de facturació

- [R116] El licitador descriurà a la seva oferta, més enllà de la seva proposta per a la generació i l'enviament de les factures adreçades als ens subscriptors i els mecanismes de reporting, la seva proposta de coordinació amb el Consorci AOC per tal que aquest pugui fer el seguiment i la resta de les activitats relatives a la gestió de la facturació; incloent la coordinació per a la gestió dels abonaments.
- [R117] A l'inici del contracte, l'enviament de les factures l'haurà de fer l'adjudicatari d'acord amb un extracte mensual i durant els 10 dies hàbils del mes següent a la generació del certificat.
- [R118] Les factures s'emetraran en format electrònic, sempre que sigui possible, a través d'una plataforma de facturació i contindran la informació especificada pel Consorci AOC per facilitar la gestió de la seva aprovació per part de l'ens destinatari. En cap cas s'hi inclouran dades de caràcter personal sense un tractament adequat per a la anonimització. S'ha de permetre identificar la comanda i cada element de la mateixa a partir de dades com ara:
- el nom del responsable del servei de l'ens destinatari.
 - un número de referència: codi de contractació intern, nº d'expedient o altra (si s'ha especificat en la sol·licitud)
- [R119] L'adjudicatari caldrà que realitzi un seguiment de la facturació enviada conjuntament amb el departament de gestió econòmica del Consorci AOC. La gestió del cobrament de les factures serà responsabilitat del Consorci AOC.

7 Acords de nivell de servei

El funcionament dels serveis objecte d'aquest contracte estarà subjecte a un sistema de control de qualitat exercit pel Consorci AOC, tot seguint els Acords de nivell de servei descrits i quantificats en aquest apartat. En tots els casos satisfan o excedeixen (per la naturalesa del servei) els ANS definits a les Condicions generals de prestació dels Serveis del Consorci AOC (publicades a <https://www.aoc.cat/condicions-prestacio-serveis-aoc/>). I els propis del servei de certificació digital, també publicat al web de l'AOC

A continuació es defineixen els àmbits i indicadors pels Acords de Nivell de Serveis (ANS) aplicables :

- ANS d'Explotació del Servei:
 - Indicadors de compliment dels nivells de servei recollits a les Declaracions de Pràctiques de Certificació¹ que apliquen a cada Entitat de Certificació en els següents àmbits:
 - Publicació d'informació i directori de certificats de les EC's
 - Procediments d'Identificació i autenticació previs a l'emissió de certificats
 - Compliment dels processos relatius a l'operació del cicle de vida dels certificats (p.ex. publicació de la CRL).
 - Alta d'usuaris al servei en menys de 7 dies
 - Disponibilitat del 99,9% del repositori de publicació d'informació i directori de certificats.
 - Acords de nivell de serveis relatius als procediments d'identificació i autenticació previs a la realització de la signatura remota.
 - ANS d'emissió i gestió dels certificats:
 - Terminis de lliurament en el servei d'emissió i renovació de certificats T-CAT pel sector públic pels dos nivells (ordinari i urgent i casos especials per eleccions o altres necessitats).
 - Terminis d'emissió en el servei d'emissió i renovació de certificats idCAT per la ciutadania.
 - El terminis per els certificats amb documentació addicional o no han de ser els mateixos, d'acord amb els publicats per part del Consorci AOC
 - Terminis de modificació de les fitxes d'ens subscriptor, Entitat de Registre, alta d'operadors, etc
 - Observat amb eines d'observació o a partir de traces del sistema d'emissió.
 - ANS de disponibilitat:
 - Disponibilitat continuada 24x7 dels serveis web
 - Nivell de disponibilitat superior al 99%.
 - Observat amb splunk o eina equivalent.
 - ANS de capacitat :
 - En transaccions per segon (tps) pels serveis web de signatura remota, OCSP, CRL i descàrrega dels certificats de la jerarquia (claus públiques).
 - Temps de resposta per sota de 3 segons en el 95% dels casos.
 - Observat amb splunk o eina equivalent.

¹Les Declaracions de Pràctiques de Certificació de les ECs del Consorci AOC es troben publicades a: <https://epsd.aoc.cat/regulacio>

- ANS de qualitat:
 - Auditories trimestrals del 3% de les sol·licituds d'emissió i gestió de certificats.
 - Evolució de les CRLs
 - Observat amb auditoria interna.
- ANS de Continuitat del Servei : Indicadors relatius a la gestió del pla de contingència, tal com es descriuen a l'apartat "La gestió de la continuïtat i la disponibilitat".
- ANS dels serveis relacionats:
 - Servei de suport a usuaris
 - Servei de facturació
 - Servei de formació a operadors de les ER
- ANS adequacions/evolutius (inclou documentació de les polítiques, contractes dels certificats, etc.)

La mesura dels ANS es farà amb eines d'AOC i/o amb eines proveïdes per l'adjudicatari per la monitorització contínua a partir de transaccions automàtiques o interaccions humanes simulades.

Els informes de Seguiment requerits inclouran els valors d'aquests indicadors definits pel període corresponent.

Es preveuen penalitats per incompliment d'aquests ANS al Plec de Clàusules Administratives.

7.1 Model de mesura del nivell de servei

Per tal de disposar de la informació necessària per a una gestió i governament homogenis del Servei, en els punts successius es defineix un Model de mesura del nivell de servei mínim que ha de permetre la valoració dels Acords dels Nivells de Servei (ANS) i la seva millora contínua.

El Model de Mesura del Nivell de Servei estructura un conjunt d'indicadors, organitzats de forma jeràrquica, que permeten mesurar els diferents aspectes d'un servei. Entre els quals (d'inferior a superior):

- Mètriques. Les mètriques seran mesures base del recompte de dades operatives. Poden ser merament informatives o afectar a un o varis dels indicadors de mesura.
- Indicadors de mesura (IM). Són indicadors calculats a partir dels valors de varies mètriques. Un indicador de mesura pot afectar a un o més indicadors de rendiment.
- Indicadors de rendiment (IR). Agrupen diferents indicadors de mesura i informen sobre determinats aspectes que componen el servei. Un indicador de rendiment només pot afectar a un indicador objectiu.
- Indicadors objectiu (IO). Agrupen diferents indicadors de rendiment relacionats amb un àmbit específic del servei. A priori s'han definit per tots els serveis els següents indicadors objectiu:
 - a. Cost
 - b. Temps
 - c. Recursos
 - d. Qualitat
 - e. Abast
- Indicador de nivell de servei (NS). Aquest indicador mesura de forma global el nivell d'acompliment del servei a provisionat, en base als indicadors objectiu.

El Model de mesura del nivell de servei s'implantarà de forma progressiva al llarg de l'execució del contracte. En el moment inicial de la seva implantació, es definiran únicament les Mètriques i els Indicadors de Mesura (IM). Serà sobre aquestes dues tipologies d'indicadors sobre les que es realitzarà la mesura del compliment dels ANS dels serveis prestats, i quan s'escaigui, l'aplicació de les penalitats associades al seu incompliment.

Al llarg del contracte, el Consorci AOC definirà i consensuarà amb els proveïdors la relació jeràrquica dels Indicadors de Mesura (IM) definits al model, respecte a la resta de nivells d'indicadors (Indicadors de rendiment [IR] i Indicadors objectiu [IO]), per tal d'assolir la mesura de l'Indicador de Nivell de Servei (NS).

Els licitadors hauran de descriure a les seves ofertes la seva proposta de Model de mesura del nivell de servei.

7.1.1 Indicadors

Es defineixen indicadors mínims per a mesurar el nivell de servei, de manera que el Consorci AOC pugui comprovar que s'acompleixen els nivells de servei establerts.

Aquests indicadors fan referència als àmbits de compliment indicats i han de permetre:

- Mesurar objectius concrets del servei
- Avaluar el grau de compliment del objectius
- Tenir una idea clara de l'impacte o importància de l'incompliment de l'objectiu

Les característiques a definir per cada indicador seran:

- Criticitat: determina si l'indicador de mesura és o no crític
- Fórmula d'obtenció/eina: fórmula a aplicar pel càlcul del valor de l'indicador de mesura, identificant les variables que intervenen al càlcul (mètriques) i, si s'escau, la referència a l'eina que permet l'automatització i extracció de les dades.
- Llindars de grau per a la definició dels trams: aquest trams permeten l'obtenció grau de l'indicador de mesura. Aquests llindars de grau poden tenir associats valors de millora en el temps.

Cal que els licitadors descriguin a les seves ofertes la seva proposta inicial d'indicadors per a la mesura del nivell de servei a partir del mínim proposat en aquest apartat.

7.1.2 Fonts d'informació per a l'obtenció dels nivells de servei

El Consorci AOC disposa d'un sistema d'informació per al càlcul dels indicadors de nivell de servei. El proveïdor haurà de proporcionar al Consorci AOC les dades que requereixi per aquest propòsit.

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei; el Consorci AOC conjuntament amb el proveïdor consensuaran i planificaran la introducció dels canvis corresponents en el Model de mesura del nivell de servei.

Algunes de les causes que poden comportar aquestes modificacions són: les variacions d'entorn tecnològic, d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, l'evolució de les transformacions, les innovacions i les millores del servei.

7.1.3 Aplicació dels acords de nivell de servei

Els Acords de Nivell de Servei definits per a cada àmbit del servei seran d'obligat compliment al llarg del contracte. Considerant els següents condicionants:

- En l'etapa de Transició de l'operació del servei, s'aplicaran a l'adjudicatari els ANS definits per aquest contracte a mesura que vagi prestant de forma efectiva els diferents serveis sobre els que apliquen i sempre i quan hi hagi acord mutu entre l'adjudicatari i el Consorci AOC.
- Al llarg de la fase de Transició de l'operació, els òrgans de gestió del servei faran una revisió de les mètriques i indicadors definits al plec, per tal d'adaptar-los a les necessitats del servei. Els ANS que resultin en la definició inicial i de les revisions successives seran aplicables en las fases de prestació ordinària del servei, adequació i en la fase de Devolució.
- Els Acords de Nivell de Servei es podran revisar i modificar semestralment sempre i quan hi hagi acord mutu entre l'adjudicatari i el Consorci AOC.
- Pel càlcul del nivell ofert per part de l'adjudicatari s'exclouran els increments de temps provocats per l'actuació ineludible d'una tercera part (p.ex. Interrupcions sobre sistemes depenents del Consorci AOC, suport a incidències per part d'empreses terceres, lliuraments d'informes per part d'un auditor, etc.).

7.2 ANS d'Explotació del Servei

Indicadors/valors de nivells de servei recollits a la futura Declaració de Pràctiques de Segell de temps en els següents àmbits derivats de les normes de negoci:

- Publicació d'informació i directori de certificats de les Entitats de Certificació.
- Procediments d'identificació i autenticació previs a l'emissió de certificats
- Compliment dels procediments relatius a l'operació del cicle de vida dels certificats.
- Emissió de la resta de CRLs cada 24 h, màxim 7 dies de vigència
- Alta d'usuaris al servei en menys de 7 dies.
- Acords de nivell de serveis relatius als procediments d'identificació i autenticació previs a la realització de signatura remota.

En general, són processos de criticitat alta pel servei i, per tant, de seguiment especial.

7.2.1 ANS del Servei d'emissió o canvi d'estat de certificats T-CAT

El període de lliurament dels certificats que emet l'entitat de registre del Consorci AOC és d'un màxim de 16 dies laborables a partir de la data d'arribada de la documentació correctament emplenada i signada, exceptuant per als certificats de pseudònim i representant que serà un màxim de 20 dies laborables. En el cas del servei urgent el termini serà de quatre dies laborables i es limita a cinc peticions per ens i setmana. En el cas dels certificats de pseudònim i representant la urgència només aplicarà a renovacions o en cas de pèrdua, robatori, etc.

Actualment, el servei ordinari d'emissió i renovació de certificats T-CAT ofert pel Consorci AOC té el compromís de lliurar els certificats en el termini de 16 dies naturals, que es compten a partir de la recepció de la documentació correctament emplenada i signada.

Tanmateix, es posa a disposició dels usuaris un servei d'emissió i renovació urgent de certificats per a tots aquells que, per motius d'urgència no puguin esperar al termini ordinari de 16 dies laborables. Donada la naturalesa del servei, aquest es limita a cinc certificats per ens i setmana que es lliuraran en el termini de 4 dies laborables, comptats a partir de la recepció correcta de la sol·licitud.

La mesura i obtenció es farà a través de eines de gestió de peticions del Consorci AOC o, en el seu defecte, de l'adjudicatari. Aquetes han de reflexar l'estat de la tramitació en cada moment de les trameses de certificats o sol·licituds de canvis d'estat. També s'hi inclouran les peticions de gestió de dades d'entitats o operadors del sistema.

7.2.2 ANS de disponibilitat

La disponibilitat dels serveis web objecte d'aquest contracte, d'acord a les condicions generals de prestació de serveis del Consorci AOC i a la categorització dels mateixos en el Pla de continuïtat del Consorci AOC, ha de ser continuada 24x7 i amb aquests nivells de disponibilitat:

- Serveis d'emissió/gestió de certificats: 99,9 %
 - Web operadors idCAT i T-CAT
 - Connectors de càrrega i consulta de peticions (LDAP)
- Serveis de càrrega i ús de certificats remots : 99,9%
 - Web gestió identitat remota.
 - Connectors de càrrega i ús del servei.
- Serveis de validació: 99,9%
 - Publicació CRL
 - OCSP
 - Web de documentació jurídica
 - Claus públiques.

Les excepcions al nivell de disponibilitat seran les actuacions d'operacions planificades i incidències de tercers que pugin afectar al servei.

Les eines per l'observació d'aquest ANS seran les pròpies del Consorci AOC (ISM) o una eina pel seguiment de la disponibilitat tipus Splunk proveïda per l'adjudicatari.

7.2.3 ANS de capacitat

El nivell de servei mínim de capacitat es quantifica mitjançant els indicadors de usuaris concurrents o transaccions per segon i es defineixen aquests valors per cada servei:

- Serveis d'emissió/gestió de certificats (usuaris concurrents) :
 - Web operadors idCAT : 5
 - Web operadors T-CAT : 5
 - Connectors de càrrega i consulta de peticions (LDAP) : 5
- Serveis de càrrega i ús de certificats remots (usuaris concurrents) :
 - Web gestió identitat remota: 5
 - Connectors de càrrega i ús del servei: 5
- Serveis de validació (transaccions per segon) :
 - CRL :
 - Mitjana dia: 2
 - Pics màxims : 60
 - OCSP :
 - Mitjana dia: 45
 - Pics màxims : 200
 - Descàrrega dels certificats de jerarquia (Claus públiques) :
 - Mitjana dia: 1
 - Pics màxims : 200

El temps de resposta haurà d'estar per sota del llindar dels 3 segons en el 95% dels casos.

L'eina per l'observació d'aquest ANS serà una eina pel seguiment de la disponibilitat tipus Splunk proveïda per l'adjudicatari.

7.2.4 ANS de continuïtat

Indicadors/valors de negoci RTO (Recovery Time Objective) i RPO (Recovery Point Objective) derivats del Pla de Continuïtat del Servei de Certificació Digital del Consorci tal com es descriuen al document d'Anàlisi d'Impacte en el negoci (en anglès BIA) en relació als Serveis d'emissió/gestió de certificats, els Serveis de Validació (OCSP i CRL) i la càrrega i ús :

- Servei d'emissió/gestió de certificats
 - o RTO: entre 24 i 4 h
 - o RPO: entre 24 i 4 h.
- Serveis de validació:
 - o RTO: entre 4 i 0 h
 - o RPO: entre 4 i 0 h.
- Servei de Signatura Remota:

Paràmetres de continuïtat resultants del BIA			
Procés	RTO	RPO	MTPD
Càrrega de segells	4 dies	1 setmana	2 setmanes
Ús de segells	24 hores		
Càrrega de certificats personals	24 hores	24 hores	
Ús de certificats personals	4 hores		

Maximum Tolerable Period of Disruption (MTPD), pel seu acrònim en anglès, que es defineix com el temps màxim que pot estar un procés o servei aturat sense comportar un impacte catastròfic que provoqui danys irreversibles a l'organització.

El compliment d'aquest ANS s'observarà a partir del resultat de les proves del Pla de Recuperació de Desastres (PRD) de periodicitat semestral i de les proves de recuperació de còpies de seguretat trimestrals d'acord a la política de còpies de seguretat definida al marc normatiu del Consorci AOC.

7.2.5 ANS de qualitat del servei d'emissió i gestió de certificats

El nivell de servei mínim de qualitat de la prestació serà:

- Pel servei d'emissió i gestió de certificats, es quantifica en el 98% de prestació correcta i s'obtindrà de l'auditoria de les traces del sistema i de la documentació generada en una mostra d'entre el 3% i 5% dels certificats generats.
- Per a l'adequació i correspondència dels certificats emesos als perfils definits corresponents a cada moment, quantificat en un 98%, mitjançant la comparació amb eines automàtiques, sobre una mostra d'entre el 3% i 5% dels certificats emesos en cada període objecte de seguiment. Es proposa utilitzar l'eina certlint (<https://github.com/aws-labs/certlint>) per a la comparació automàtica.

7.2.6 ANS del Servei de Suport

L'adjudicatari, en la prestació el servei de suport de 3er nivell, s'haurà d'alinear amb el Consorci AOC per tal que aquest pugui complir l'ANS compromès pel seu CAU. Aquest ANS és el que s'especifica a continuació:

Les incidències es catalogaran, segons la seva criticitat, en les categories que es descriuen a continuació:

- 0 (bloquejant): una incidència es catalogarà amb criticitat bloquejant (0), si impedeix la utilització total d'algun dels serveis del Consorci AOC.
- 1 (alta): una incidència es catalogarà amb criticitat alta (1) si impedeix la utilització d'una part concreta d'algun dels serveis del Consorci AOC i l'afectació pel negoci és elevada
- 2 (mitja): una incidència es catalogarà amb criticitat mitja (2) si impedeix la utilització d'una part concreta d'algun dels serveis del Consorci AOC, i l'afectació pel negoci és relativament baixa
- 3 (baixa): una incidència es catalogarà amb criticitat baixa (3) si no impedeix la utilització ni parcial ni total d'algun dels serveis del Consorci AOC

Es defineix el temps de resposta d'una incidència com el nombre d'hores que transcorren des de que l'usuari comunica una incidència al CAU i aquest l'accepta o bé l'escala al nivell superior. L'acceptació comportarà l'aprovació de procedir a resoldre la incidència, segons els acords de nivell de servei establerts.

El temps de resposta màxim permès d'una incidència dependrà del nivell de criticitat de la incidència. En la següent taula es mostren els temps de resposta i els temps de resolució màxims permesos en funció del nivell de criticitat de la incidència.

En la següent taula es mostren els temps màxims permesos per la resolució d'una incidència en funció del nivell de criticitat:

Criticitat Incidència	Temps de resposta (hores)	Temps de resolució (hores)	Horari	% de resolució dins del temps compromès
0 Bloquejant	0,5	2	horari supervisat (24x7)	95 %
1 Alta	1	16	horari garantit (de 8 a 15h)	95 %
2 Mitja	2	40	horari garantit (de 8 a 15h)	95 %
3 Baixa	4	64	horari garantit (de 8 a 15h)	95 %

Pel càlcul del temps de resolució d'una incidència s'exclouran els possibles increments de temps provocats per la intervenció inevitable en el procés de resolució per part de tercers.

7.3 ANS dels Serveis de Programació

Les condicions d'execució relatives als ANS que es defineixen en aquest apartat sobre els serveis de programació es troben a l'apartat 6.10.1 sobre la metodologia del manteniment evolutiu.

7.3.1 Acords de nivell de servei del desenvolupament

Els nivells mínims de prestació del servei hauran de ser:

- La data de lliurament planificada és de compliment obligatori un cop tancada i acordada l'ordre de treball. Un mínim del 95 % de les peticions acordades amb la

direcció funcional del projecte hauran de ser lliurades i ser acceptades per la direcció del projecte en la data de lliurament prevista.

- Percentatge d'evolutius sense errors. Un mínim del 95% dels evolutius lliurats dins del termini s'han de lliurar sense errors.
- Pla de proves de vulnerabilitats. Un mínim del 98% dels evolutius lliurats hauran de superar el pla de proves de vulnerabilitats sense errors.
- Pla de proves sense errors. Un mínim del 98% dels evolutius lliurats hauran de superar el pla de proves executat per personal del Consorci AOC sense errors.

Excepcionalment i amb previ avís, es podrà requerir l'execució de desenvolupaments evolutius urgents que no seguiran el procediment previ de valoració i que s'hauran de començar en el mateix dia o el dia següent.

7.3.2 Requeriments de nivell de servei en el manteniment correctiu i resolució d'incidències

Resolució d'incidències sense errors:

- Percentatge de la resolució d'incidències sense errors en el termini.
 - Càlcul: $(A/B) \times 100$
 - A: Número total d'incidències resoltes sense error en el termini
 - B: Total d'incidències resoltes en el termini
- Periodicitat: Mensual
- El percentatge d'incidències sense error en el termini establert haurà de ser com a mínim del 90%.
- El nivell ofert per qui resulti adjudicatari del servei constituirà un Acord de Nivell de Servei (ANS), el compliment del qual es mesurarà durant tota la durada de la prestació del servei.

7.3.3 Temps de resposta en el manteniment evolutiu

En relació al servei de manteniment evolutiu, es defineixen els següents temps:

- Temps de pressa de requeriments: és el nombre de dies laborables que transcorren des de que Consorci AOC lliura a l'adjudicatari el document "**Fitxa d'inici d'evolutiu**" i el moment en què l'adjudicatari lliura el "**Document de requeriments**".
 Els dies que no sigui possible realitzar les reunions oportunes per fer la pressa de requeriments per indisponibilitat de l'adjudicatari es tindran en compte per fer el càlcul dels temps de pressa de requeriments.
- Temps pre-anàlisi: és el nombre de dies laborables que transcorren des de que el Consorci AOC aprova el "**Document de requeriments**" i el moment en què l'adjudicatari lliura el "**Document de pre-anàlisi**".

En la següent taula es mostren els temps descrits anteriorment màxims permesos en funció del nivell de prioritat:

Nivell de prioritat	ANS: temps màxim permès pressa requeriments (en dies)	ANS: temps màxim permès fase pre-anàlisi (en dies)
Urgent	1	2
Normal	5	7

Baixa	10	10
-------	----	----

7.3.4 Desviacions en el manteniment evolutiu

En relació al servei de manteniment evolutiu, es defineix la desviació en el lliurament d'un evolutiu com el nombre de dies laborables que transcorren des de la data acordada entre Consorci AOC i l'adjudicatari per finalitzar la fase de construcció i la data en la que finalment finalitza aquesta fase.

La desviació en el lliurament d'un evolutiu no serà superior al 10% de l'estimació, realitzada en la fase de pre-anàlisi, de l'esforç (cost en hores o dies) necessari per realitzar la fase d'anàlisi, disseny i construcció de l'evolutiu. Per exemple, si la data acordada per finalitzar la fase de construcció és el 14 d'abril i l'esforç estimat de la fase d'anàlisi, disseny i construcció és de 10 dies laborables (80 hores), la desviació permesa serà d'1 dia (10% de 10 dies), i per tant, la data màxima permesa de lliurament serà el 15 d'abril.

8 FASES D'EXECUCIÓ DEL CONTRACTE

Es preveu que la planificació aproximada per a la prestació dels serveis objecte d'aquest contracte sigui, en l'escenari millor:

2024		2025	2026	2027
S1	S2			
Fase de transició de l'operació del Servei				
	Fase de prestació del Servei			
				Fase de devolució del Servei

- Transició de l'operació del servei: des de la signatura del contracte fins a 31 de desembre de 2024. Aquesta fase es descriu en detall en el punt "8.2 - Transició de l'operació del servei actual" del present document.
- Prestació del Servei de signatura remota: com a màxim, a partir de l'1 de setembre de 2024 i fins a la finalització del contracte. Com a punts clau a tenir en compte en aquest període, cal esmentar:
 - Inici de la prestació del servei de signatura remota no qualificat, basada en certificats personals i certificats de segell electrònic, com a màxim, a l'1 de juliol de 2024.
 - Com a màxim dotze mesos després de l'adjudicació del contracte, inici de la prestació del servei de signatura remota qualificada.
- Adequació del Servei: des de l'assoliment de l'autorització del supervisor nacional per a l'inici del servei de signatura remota qualificada i fins a la finalització del mateix, l'adjudicatari durà a terme les adequacions del servei previstes o sobrevingudes (normatives, de seguretat, tecnològiques, organitzatives, etc.) previstes en aquest plec o que es consideri convenient a cada moment per adequar-ne la prestació, previ acord amb el Consorci AOC sobre l'abast, la planificació, l'impacte en clients i el cost dels canvis – entre d'altres; sense que pugui suposar costos emergents per al Consorci AOC.
- Devolució del Servei: les tasques preparatòries s'iniciaran un any abans de la finalització del contracte. Aquesta fase es descriu en detall en el punt 8.3 del present document.

L'oferta dels licitadors ha de descriure la planificació que proposen detallant, entre d'altres, els següents aspectes:

- Descripció de les principals fites de cada fase.
- Pla de contingència/alternatiu, per a les fases que es considerin crítiques.
- Calendari previst per a cada fase i fita destacada.
- Si s'escau, avançaments o millores en el calendari d'alguna fase.

8.1 Creació i explotació del servei signatura remota qualificada basada en certificats qualificats del Consorci AOC

L'adjudicatari haurà de crear, allotjar, qualificar i operar el servei signatura remota qualificada basada en certificats qualificats, la titularitat del qual serà del Consorci AOC, com a Prestador de Serveis de Certificació per als ens del Sector Públic de Catalunya d'acord a EIDAS.

Per a l'emissió i gestió d'estat dels certificats del servei, el Consorci AOC posarà a disposició de l'adjudicatari unes claus d'Autoritat de Certificació subordinada i una proposta de perfils de certificat, tal i com s'exposa el punt **¡Error! No se encuentra el origen de la referencia.** del present plec. El sistema que realitzarà les funcions d'entitat de registre per aquests certificats els haurà de gestionar l'adjudicatari en el marc del present contracte.

Per a l'ús dels certificats, l'adjudicatari haurà de proveir els mecanismes per a l'activació del servei d'acord al definit punt 6.4 El Servei de Signatura Remota (SSR) del Consorci AOC.

8.2 Transició de l'operació del servei actual

Durant la fase de Transició de l'operació del servei actual, l'adjudicatari posarà en marxa la seva infraestructura i farà la transferència de l'operació dels sistemes que hauran de donar suport al servei de signatura remota del Consorci AOC, de manera que, a la finalització d'aquesta fase, la prestació efectiva del servei la dugui a terme, a tots els efectes, l'adjudicatari.

El calendari i fites de seguiment específic segons estableix el punt "9.69.6 Model de relació en la fase de Transició de l'operació" i "9.6.1 Governament de la fase de transició de l'operació" seran:

- Per la fase de revisió d'actius i documentació del servei actual del Consorci AOC, el nou adjudicatari disposarà d'un termini de 4 setmanes.
- Per l'inici de la prestació del servei de signatura remota no qualificat, el nou adjudicatari disposarà d'un termini de 6 mesos.
- Per l'inici de la prestació del servei de signatura remota qualificat, el nou adjudicatari disposarà d'un termini de 12 mesos.
- Per l'inici de l'auditoria d'ENS i de qualificació del servei, 6 mesos.

Durant la fase de Transició de l'operació l'adjudicatari haurà de mantenir l'ANS dels serveis actuals pels serveis que es vagin transferint.

8.3 Devolució del servei

L'adjudicatari haurà de garantir que es pugui dur a terme la transferència de l'operació del servei a un proveïdor alternatiu.

L'adjudicatari haurà de lliurar al Consorci AOC el codi font dels desenvolupaments realitzats pels seus serveis dins del marc d'aquest. També haurà de proveir la corresponent documentació relativa als desenvolupaments i control de versions.

L'adjudicatari haurà de proveir les llicències d'ús de la solució aportada.

L'adjudicatari haurà de proveir el maquinari dedicat i les màquines virtuals operatives, que siguin necessaris pel funcionament de la solució més enllà de la finalització del contracte. En cas que això suposi un cost addicional sobre el preu del contracte, el licitador l'haurà de desglossar en la seva oferta econòmica; altrament, s'entendrà que el preu de l'oferta del licitador inclou l'adquisició del maquinari dedicat necessari pel funcionament de la solució més

enllà de la finalització del contracte i que el cost d'aquest s'ha amortitzat durant el període de vigència del contracte.

L'adjudicatari prepararà i mantindrà actualitzats manuals d'operació detallats dels sistemes, què posarà a disposició del Consorci AOC durant la fase de Devolució del servei.

L'adjudicatari també haurà d'aportar la total col·laboració que sigui necessària per a la devolució o transferència del servei a l'Administració o al prestador que aquesta determini, durant el termini imprescindible, que no serà superior a tres mesos més enllà del termini fixat per a la prestació contractual: llevat de la manca de col·laboració pel contractista o l'aparició de factors imprevisibles, cas en que aquest termini quedarà automàticament ampliat fins a la total finalització de la devolució o transferència.

L'adjudicatari és responsable d'adoptar les mesures de seguretat necessàries per tal que les dades objecte de traspàs, fins que no estiguin en poder del Consorci o el nou adjudicatari, es mantinguin integres, exactes, disponibles, i s'adoptin les mesures de seguretat que determini el Consorci AOC

9 SEGUIMENT DEL SERVEI

L'objectiu d'aquest àmbit de seguiment és garantir la integració de la qualitat, seguretat i continuïtat, en tot el cicle de vida, dels processos, serveis i solucions, mitjançant la prescripció, seguiment, validació i verificació de l'eficax implantació dels controls definits.

9.1 Governament i millora del servei

L'adjudicatari és el responsable de generar i lliurar els informes i mètriques de reporting (en endavant informació) que es determinen en el punt "7 Acords de nivell de servei" i que apliquen als diferents àmbits del governament del servei objecte d'aquesta licitació. Aquests han de permetre al Consorci AOC governar, controlar i gestionar els serveis prestats per l'adjudicatari, tant des d'una òptica individual, com transversal i global.

El Consorci AOC podrà sol·licitar, durant la vigència del contracte canvis en l'estructura i contingut de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'adjudicatari haurà de proporcionar al Consorci AOC, a més dels informes periòdics de seguiments dels ANS, la informació (evidències) amb base a la qual s'hagin elaborat, per tal que el Consorci AOC la pugui incorporar a la seva eina de gestió.

El licitador proposarà els mecanismes necessaris per permetre al Consorci AOC comprovar que es mantenen els nivells de qualitat esperats.

A continuació es presenta una estructuració de les funcions i responsabilitats que el Consorci AOC trasllada a l'adjudicatari en el marc d'actuació comú, per a assegurar el compliment de les obligacions de cadascuna de les parts. És un marc de relació que permet acordar el contingut i nivell de la prestació dels serveis, així com el seguiment de la prestació real en els aspectes contractuals, estratègics, tàctics i operatius.

Els licitadors poden ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb el Consorci AOC, així com els mecanismes de control propis de cada servei i/o funció transversal.

El model de relació proposat en aquest contracte està sustentat en una estructura de competències i funcions que recauen sobre un esquelet de responsables de l'adjudicatari, els quals es relacionaran amb el Consorci AOC a 2 nivells: directiu i operatiu. Actuaran com a interlocutors amb el Consorci AOC, i seran el lligam entre l'estructura del Consorci AOC i l'organització interna del proveïdor.

9.2 Estructura de responsabilitats de l'adjudicatari

L'adjudicatari assignarà al Consorci AOC els responsables que sostindran el Model de Relació. L'equip haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les funcions i responsabilitats assignades.

L'estructura de responsabilitats i competències mencionada es concreta en els següents rols, tot i que una mateixa persona pot assumir-ne més d'un.

Per part de l'adjudicatari:

- **Responsable de compte:** Garant de l'existència dels mecanismes de relació par part de l'adjudicatari a l'hora de portar a terme els acords presos amb el Consorci AOC, serà la figura de referència en el marc del contracte i el darrer responsable de la prestació del conjunt de serveis i projectes. Aquesta figura es mantindrà durant tota la vida del contracte: en la gestió comercial, durant la provisió del servei i fins la devolució del mateix.

- **Responsable de serveis:** assignat pel proveïdor, les principals funcions del qual seran:
 - La gestió i seguiment diari del servei, així com la resolució de conflictes i redimensionament temporal o permanent del mateix.
 - Manteniment del registre de l'evolució del servei per a posteriorment poder elaborar els informes de servei i justificar el compliment dels ANS.
 - Seguiment i control dels recursos assignats al servei.
 - Realitzar el control de costos, l'estimació d'esforços i el seu seguiment.
 - Analitzar qualsevol desviació i situacions de gravetat dins la qualitat, terminis o abast del servei
 - Analitzar les modificacions en abast i cost del servei que es puguin derivar, i interpretar aquestes modificacions respecte el contracte vigent. En cas que no impliquin una modificació contractual, ha de tenir l'autoritat per formalitzar i implementar internament a la seva organització els acords presos.
 - Assegurar la bona col·laboració amb altres proveïdors del Consorci AOC amb qui s'ha de relacionar per tal de millorar el servei de negoci final.
- **Responsable de Control de Gestió:** Proporcionarà al Consorci AOC els informes de gestió acordats, tant amb indicadors econòmic-financers com d'altres, i portarà a terme el seguiment del model econòmic acordat amb l'adjudicatari. És la figura que consolidarà i aportarà al Consorci AOC les informacions objectives i també les subjectives, valorades (informació fiable i de qualitat i analitzada en base al coneixement del model) que permetin la presa de decisions operatives i estratègiques al llarg de la vida del contracte.
- **Responsable Jurídic:** Serà l'interlocutor principal amb el Consorci AOC en matèria jurídica pels serveis prestats per l'adjudicatari.
- **Expert en protecció de dades**, cas que no tingui obligació de disposar de Delegat de protecció de dades amb les atribucions especificades en l'apartat 6.8.6.3 Requisits de protecció de dades.
- **Responsable de Facturació:** Haurà de facilitar la informació relativa al procés de facturació, segons el model i format definit pel Consorci AOC, així com col·laborar en el procés de la conciliació. Vetllarà i assegurarà que el proveïdor:
 - Facilita la informació relativa al procés de facturació al Consorci AOC i també als subscriptors del Servei de Certificació Digital, segons els models i formats definits pel Consorci AOC:
 - Presentarà les factures i el detall per cada element / concepte dels imports facturats, adequant-se als següents criteris:
 - Detall complet de tots els elements de cost facturats, identificant les unitats de cost.
 - Tipificació i codificació dels elements de cost facturats.
 - El format de codificació i criteris de tipificació es validaran de forma conjunta.
 - Col·labora en el procés de la conciliació de la facturació al Consorci AOC.
- **Responsable d'Arquitectura i innovació:** Coordinarà l'aplicació de l'arquitectura corporativa en els sistemes d'informació i serveis a construir o mantenir pel proveïdor.
- **Responsable d'Operació de Suport i de Provisió del Servei:** És el responsable del compliment dels processos de gestió de peticions, incidències, problemes i esdeveniments (suport) i de gestió de configuració i inventari, canvis, versions i desplegaments (provisió). Com a principals funcions haurà de:
 - Assegurar la presa de decisió operativa directa entre el Consorci AOC i la seva organització.
 - Assegurar la coordinació amb el CAU (de 1er i 2n nivell, del Consorci AOC; i també del 3er nivell, de l'adjudicatari) per a tots el processos.
 - Assegurar una bona relació i coordinació entre els equips sota la seva responsabilitat per tal de complir les activitats associades a tots els processos de gestió definits, i amb responsabilitat sobre l'adjudicatari.

- **Responsable de Qualitat:** Garantirà l'existència d'un pla de qualitat pels serveis i aplicacions, així com la seva execució.
- **Responsable de Seguretat:** Serà responsable de:
 - Actuar com a enllaç entre l'adjudicatari i els diferents agents implicats (Consorti AOC, Agència de Ciberseguretat de Catalunya) quan es tractin temes de seguretat.
 - Garantir, liderar i impulsar el compliment del marc normatiu de seguretat del Consorci AOC dins la seva organització, assegurant la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives, i jurídiques); així com les directrius en matèria de seguretat establertes pel Consorci AOC.
 - Coordinar reunions de seguiment periòdiques amb el Consorci AOC i l'Agència de Ciberseguretat de Catalunya per informar del grau d'adequació de les aplicacions al model de seguretat establert, identificar-ne els riscos més rellevants i proposar plans d'acció per la seva mitigació.
 - Que tot el personal de l'adjudicatari que prestarà serveis al Consorci AOC, passi per un pla de formació en matèria de seguretat, focalitzant-se en el marc normatiu del Consorci AOC i els procediments de seguretat que li siguin d'aplicació.
 - Assegurar la informació regular al Consorci AOC segons els terminis marcats, de tot allò relacionat amb la seguretat (incidents, mesures correctores, riscos, nous projectes, iniciatives, etc...).
 - Coordinació operativa amb els equips operatius del Consorci AOC davant incidents o possibles amenaces de ciberseguretat (Lliurament d'evidències per la gestió i investigació d'incidents de seguretat, suport per l'aplicació ràpida de mesures de protecció i contenció davant amenaces o ciberincidents, disposar d'informació vinculada a l'aplicació (URLs, usuari d'aplicació, logs, etc..))
- **Responsable de Continuitat:** Serà el responsable de:
 - Garantir i liderar dins la seva organització la correcta implantació dels plans de continuïtat i disponibilitat (tant de serveis tecnològics com de negoci) acordats amb el Consorci AOC.
 - Que tot el personal de l'adjudicatari que prestarà serveis al Consorci AOC, passi per un pla de formació en matèria de continuïtat, focalitzant-se en el marc normatiu del Consorci AOC i els procediments de continuïtat que li siguin d'aplicació.
 - El desplegament de totes les mesures en aquest àmbit (tècniques, organitzatives, i jurídiques) necessàries per assolir el nivell de compliment exigint pel Consorci AOC.
 - Assegurar la informació regular al consorci AOC segons els terminis marcats, de tot allò relacionat amb la Continuitat i Disponibilitat (incidents, mesures correctores, riscos, nous projectes, iniciatives, etc...)
- **Programador:**
 - Liderar la fase de construcció dels canvis a realitzar: entre altres, realitzar les classes, interfícies i demés codi necessari per al desenvolupament de l'aplicació atenent als criteris fixats per cada desenvolupament (qualitat, robustesa, eficiència, etc.)
 - Execució exhaustiva del pla de proves definit pel projecte.
 - Col·laboració puntual, si així es creu convenient, en les fases de presa de requeriments, fase d'anàlisi i disseny i fase d'implantació.

- Escriure, depurar i mantenir el codi font realitzat, de manera que haurà de comentar correctament el codi, per a que aquest sigui mantenible. Els comentaris han de seguir les recomanacions de l'estàndard definit per java.
 - Generar la documentació (javadoc) a partir dels propis comentaris del codi (es pot utilitzar una eina de l'estil JavaDoc Tool).
 - En els casos d'incidències complexes haurà participar activament en el diagnòstic i execució del pla d'acció a seguir per la resolució de la incidència.
- **Tècnic:** Per portar a terme tasques de posada en marxa i operació del servei.

L'adjudicatari mantindrà una taula actualitzada amb les persones que tindran cadascun d'aquests rols.

9.3 Estructura de responsabilitats del Consorci AOC

Per part del Consorci AOC, els rols que participaran en la relació contractual:

- **Responsable de Transició de l'operació:** Presentarà la planificació, abast i metodologia d'execució dels diferents plans de transició del servei. Impulsarà i assegurarà l'execució d'aquests segons la direcció establerta pel Consorci AOC, de manera coordinada amb els responsables de la resta de proveïdors del Consorci AOC. Informarà del grau d'avenç, els riscos i plans de mitigació corresponents, i assegurarà l'acompanyament per part del proveïdor en la gestió del canvi. El Responsable de Transició desenvoluparà, alinearà, sincronitzarà i governarà de forma global els plans de transició de l'operació.
- **Responsable de Seguretat del Consorci AOC.**
- **Cap del Servei** Serà el responsable de la prestació dels serveis de cara a la ciutadania i entitats usuàries.
- **Cap de Projecte.** Serà el coordinador per part del Consorci AOC de les tasques tècniques relatives a la posada en marxa i operació dels serveis objecte d'aquest plec de prescripcions tècniques.
- **Responsable d'Assessorament Jurídic.** Es coordinarà amb el Responsable jurídic de l'adjudicatari per garantir el compliment normatiu i regulació del servei.
- **Responsable de Sistemes**
- **Representant de la Direcció** per garantir l'alineació del servei amb l'estratègia i missió del Consorci AOC.
- **Persona Delegada de Protecció de dades**

9.4 Gestió d'incidències i problemes

S'entén per a incidència qualsevol succés que no forma part de l'operativa normal d'un servei i que provoca, o pot provocar, la interrupció, el mal funcionament o la degradació en la qualitat del servei.

L'objectiu principal del procés de gestió d'incidències és restaurar el normal funcionament del servei tan aviat com sigui possible, minimitzant l'impacte advers sobre les operacions de negoci/clientes i organització, assegurant que el servei es mantingui en els millors nivells possibles de qualitat i disponibilitat.

El procés suporta tots els serveis que el Consorci AOC presta a l'usuari dins l'abast del plec i per tant el seu abast és la resolució de totes les incidències que puguin afectar a aquests serveis.

S'entén per problema qualsevol causa subjacent, encara no identificada, d'una sèrie d'incidents o d'un incident aïllat d'importància significativa.

L'objectiu principal de la Gestió de Problemes és minimitzar l'impacte negatiu que tenen les incidències sobre el negoci, i prevenir la recurrència d'incidències relacionades amb aquests errors. Per aconseguir aquesta fita, la Gestió de Problemes arriba fins a la causa arrel de les incidències i després inicia accions que corregeixen l'afectació de servei.

L'adjudicatari participarà activament en el procés de Gestió de Problemes sent el Responsable de tots els problemes que puguin sortir dels serveis que està prestant al Consorci AOC.

És responsabilitat de l'adjudicatari l'aplicació i seguiment dels procediments associats a la gestió de problemes sorgits dels serveis que presta, així com el seguiment i gestió de l'estat dels mateixos fins a la correcció de l'afectació de servei.

Davant la detecció de problemes greus i amb impacte directe a negoci, el proveïdor de servei haurà de notificar el problema al Cap del servei Consorci AOC.

El licitador descriurà la metodologia proposada per atendre:

- Registre d'incidències i problemes
- Classificació i assignació
- Investigació i diagnosi
- Seguiment i coordinació
- Resolució i recuperació
- Tancament d'incidències i problemes

9.5 Òrgans de Gestió

9.5.1 Reunions de direcció.

Les reunions de Direcció es realitzaran amb l'objectiu d'establir un control i una visió estratègica i àmplia sobre el desenvolupament global del servei.

Les reunions podran ser presencials i/o virtuals. En el cas de les presencials, poden realitzar-se tant a la seu del Consorci AOC, com de l'empresa adjudicatària. En tot cas, cal que l'adjudicatari disposi dels recursos necessaris en qualsevol de les modalitats de reunió previstes.

Les reunions de direcció es convocaran trimestralment, tot i que a petició del Consorci AOC i en circumstàncies concretes d'afectació crítica del servei, podran ser convocades en qualsevol moment durant la vigència del contracte, convocades amb una antelació mínima de 3 dies laborables, segons el calendari laboral aplicable al personal del Consorci AOC.

9.5.2 Reunions de seguiment.

El gestor del servei de l'adjudicatari i el Cap del Servei del Consorci AOC realitzaran una reunió de seguiment del servei, que serà periòdica i com a mínim de caràcter mensual, tot i que a petició del Consorci AOC i en circumstàncies concretes d'afectació crítica del servei, podran ser convocades en qualsevol moment durant la vigència del contracte, amb una antelació mínima de 1 dia laborable, segons el calendari laboral aplicable al personal del Consorci AOC.

Les reunions podran ser presencials i/o virtuals. En el cas de les presencials, poden realitzar-se tant a la seu del Consorci AOC com de l'empresa adjudicatària. En tot cas, cal que l'adjudicatari disposi dels recursos necessaris en qualsevol de les modalitats de reunió previstes.

Aquesta reunió es farà abans del desè dia laborable (de dilluns a divendres excepte festius) de cada mes. En aquesta reunió es revisarà l'informe mensual, el funcionament dels processos, es generaran propostes de millora del servei i es farà un seguiment de tot allò relacionat amb la prestació. A títol d'exemple s'indiquen alguns dels aspectes inclosos com a possible contingut de la reunió:

- Avaluar la situació d'execució del servei objecte del contracte a partir del seguiment de l'evolució dels objectius i indicadors formulats, així com el nivell d'acompliment dels acords de nivell de servei que estiguin vinculats.
- Seguiment de la seguretat i el compliment normatiu amb la prescripció, seguiment i verificació de la correcta implantació del model de seguretat d'acord amb els requisits enumerats en el punt "6.8.6 La gestió de la seguretat i el compliment normatiu".
- Seguiment de la continuïtat i la disponibilitat amb la prescripció, seguiment i verificació dels requisits, acords de nivell de servei i condicions definides en la present licitació.
- Revisar i posar en comú les incidències que s'hagin produït en el mes immediatament anterior, ja sigui en relació a la prestació efectiva del servei com en relació al model de gestió vinculat.
- Revisar i posar en comú novetats, jornades i/o documentació rellevant per a l'execució del servei, per tal de generar una dinàmica de participació que impacti de manera positiva en la gestió del coneixement i sigui aplicable a la pròpia prestació del servei.

Abans de cada reunió de seguiment i amb l'antelació establerta en el corresponent acord de nivell de servei establert el referent del servei de l'adjudicatari posarà a disposició del Cap del Servei del Consorci AOC l'informe de seguiment detallat que inclourà, com a mínim, informació sobre:

- Estat de compliment de les tasques en relació a les planificacions fetes i les possibles desviacions que s'hagin produït. Nombre d'actuacions realitzades d'acord amb l'objecte i abast del contracte.
- Millores aplicables al servei.
- Informació d'acompliments sobre els acords de nivell de servei establerts.

S'utilitzarà una eina de gestió del Consorci AOC que ha de permetre i facilitar la participació dels diferents actors implicats en l'execució del servei. Aquesta eina esdevé clau per mantenir coordinats tots els actors participants, detectar les necessitats a cobrir, així com detectar millores tant en la prestació del servei com en el model de gestió vinculat. El referent del servei és el principal responsable del manteniment de l'eina de gestió del servei i ha de reflectir tots els canvis, actualitzacions, documents, etc., amb el màxim rigor possible, per tal de tenir un accés immediat a la informació actualitzada de la prestació del servei i permetre una visió amb el major detall possible als diferents actors que participen en la gestió d'aquest lot.

Durant la fase de Transició de l'operació, la periodicitat i abast d'aquests comitès podrà ser modificada, i addicionalment s'establiran uns comitès específics executius i de seguiment, definits a l'apartat següent.

9.6 Model de relació en la fase de Transició de l'operació

Amb l'objectiu de minimitzar els riscos que puguin ocasionar incidències que afectin la continuïtat del servei, el model de relació en la fase de Transició de l'operació del servei serà diferenciat però coordinat amb el model de relació del seguiment del servei definit prèviament.

Es proposen els següents òrgans de gestió addicionals:

Òrgan de gestió	Principals activitats
Comitè de planificació i estratègia transició	• Establiment i seguiment del pla global de Transició.
Comitè de Transició de l'operació	• Interlocució, als efectes de la coordinació dels plans i activitats de transferència de serveis i coneixement, seguiment i coordinació del procés d'inventari. • Proposició d'accions relacionades amb la transició (fixació i canvi de prioritats, canvi de plans individuals, gestió de processos i criteris de traspàs de serveis, gestió del risc, etc).

La periodicitat d'aquests òrgans serà variable i es definirà a l'inici de la prestació del servei, essent revisable en funció dels plans i projectes de transició.

Els esmentats òrgans de gestió podran designar els grups de treball operatius que siguin necessaris per desenvolupar adequadament les seves funcions.

9.6.1 Governament de la fase de transició de l'operació

El Governament de la fase de Transició de l'operació té com a finalitat el govern i la direcció de la planificació, la coordinació, el seguiment, i la implantació de tots els processos que conformaran aquesta fase de cara a la prestació del nou servei per part de l'adjudicatari.

L'actuació del Responsable de transició del Consorci AOC serà transversal a totes les estructures organitzatives que estiguin implicades en els processos relacionats amb aquesta fase; assumint el lideratge del procés global de la transició de l'operació i exercint les responsabilitats de govern i control necessàries.

El Responsable de transició serà qui fixarà, en última instància, el calendari de desplegament dels diferents plans, d'acord amb l'adjudicatari; amb les necessitats i prioritats del Consorci AOC, i amb l'impacte en el Servei i/o les interrelacions entre els diferents serveis tecnològics que conformen el servei de negoci.

En l'àmbit operatiu, el Responsable de transició assegurarà, durant els diferents processos i activitats de les fases de Transició de l'operació, la interlocució i la coordinació tècnica i funcional de l'adjudicatari amb el Consorci AOC.

L'adjudicatari serà responsable de l'execució i l'assegurament de l'avenç segons la planificació i l'abast marcat pel Responsable de transició dels processos i activitats que haurà d'abordar. L'adjudicatari reportarà al Responsable de transició, qui serà l'únic òrgan de direcció i control de tot el pla de transició de l'operació.

L'adjudicatari serà el responsable d'identificar els possibles riscos associats als seus projectes de transició de l'operació; així com d'analitzar-los, i de proposar i executar els plans de mitigació corresponents; que reportarà al Responsable de transició. Aquest realitzarà el seguiment, avaluació, i gestió d'aquests riscos, i assegurarà la seva mitigació; tant dels riscos identificats individualment en cadascun dels processos i activitats de les fases, com dels riscos globals de tot el pla, la identificació dels quals és responsabilitat del Responsable de transició.

El Responsable de transició gestionarà els conflictes entre el Consorci AOC i l'adjudicatari, que poguessin causar impactes en els processos i activitats d'aquestes fases.

El Responsable de transició assegurarà la consecució de les tasques necessàries associades a la gestió del canvi relativa al procés de transició de l'operació. L'adjudicatari serà

responsable d'un pla d'acompanyament del canvi, i donarà suport al Responsable de transició en aquest àmbit.

Els licitadors han de proposar la definició, planificació i abast dels diferents plans de transició del servei objecte d'aquest contracte en base al que estableix el marc normatiu aplicable i, en concret, el punt "8.2 Transició de l'operació del servei actual" d'acord amb els requisits i condicions mínimes allà definits. El Consorci AOC realitzarà, dins l'àmbit dels processos d'aquestes fases, les accions de control necessàries per verificar l'assoliment de les fites marcades per a aquestes fases. Aquestes avaluacions es coordinaran mitjançant el comitè de planificació i estratègia de transició.

L'adjudicatari pot proposar eines per a la gestió de la transició de l'operació més enllà de les definides i requerides en aquest plec de prescripcions tècniques.

10 REFERÈNCIES

- Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i als serveis de confiança per les transaccions electròniques en el mercat interior i que deroga la Directiva 1999/93/CE.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i que deroga la Directiva 95/46/CE.
- Real Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Part 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

11 Annex – Situació actual

11.1 Catàleg actual de certificats del Consorci AOC

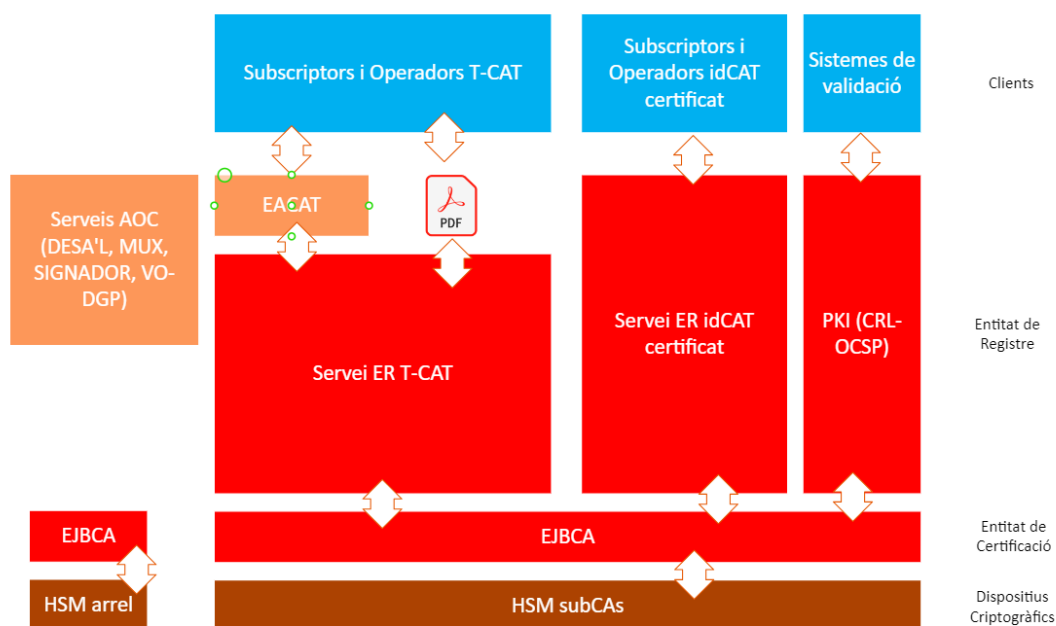
El Consorci AOC ofereix únicament certificats de signatura personal i segells electrònics que corresponen a les tipologies de serveis de Reglament EIDAS. A tal efecte, el [catàleg actual de certificats](#) que ofereix el Consorci AOC es pot consultar al web del Consorci AOC. S'adjunta una taula resum:

Certificats	Producte	Acrònims nous	Durada	Suport
idCAT: ciutadà	idCAT	CPISA2_idcat	4 anys	programari
T-CAT: Certificats electrònics qualificats d'empleat públic	T-CAT	CPI-1+CPSQ-1	4 anys	targeta
	T-CAT P	CPISA-1	4 anys	programari
T-CAT: Certificats electrònics qualificats de treballador públic	T-CAT	CPISQ-3	4 anys	targeta
	T-CAT P	CPISA-3	4 anys	programari
T-CAT: Certificats electrònics qualificats per al personal de l'administració pública	T-CAT Representant	CPRISQ-1	4 anys	targeta
	T-CAT Pseudònim	CPPI1+CPPSQ-1	4 anys	targeta
T-CAT: Certificats l'administració pública Certificats electrònics qualificats de segell electrònic de l'administració pública	Segell nivell mig	CDA-1_SGNM	3 anys	programari
T-CAT: Certificats aplicació	Dispositiu aplicació	CDA-1	3 anys	programari

El detall concret de cada perfil de certificat, així com el propòsit i modalitats de provisió i suport, es poden consultar als documents vigents de perfils, polítiques i declaració de pràctiques ubicades al web de regulació del servei a <https://epsd.aoc.cat/regulacio>.

11.2 Situació actual de subsistemes i components del Servei

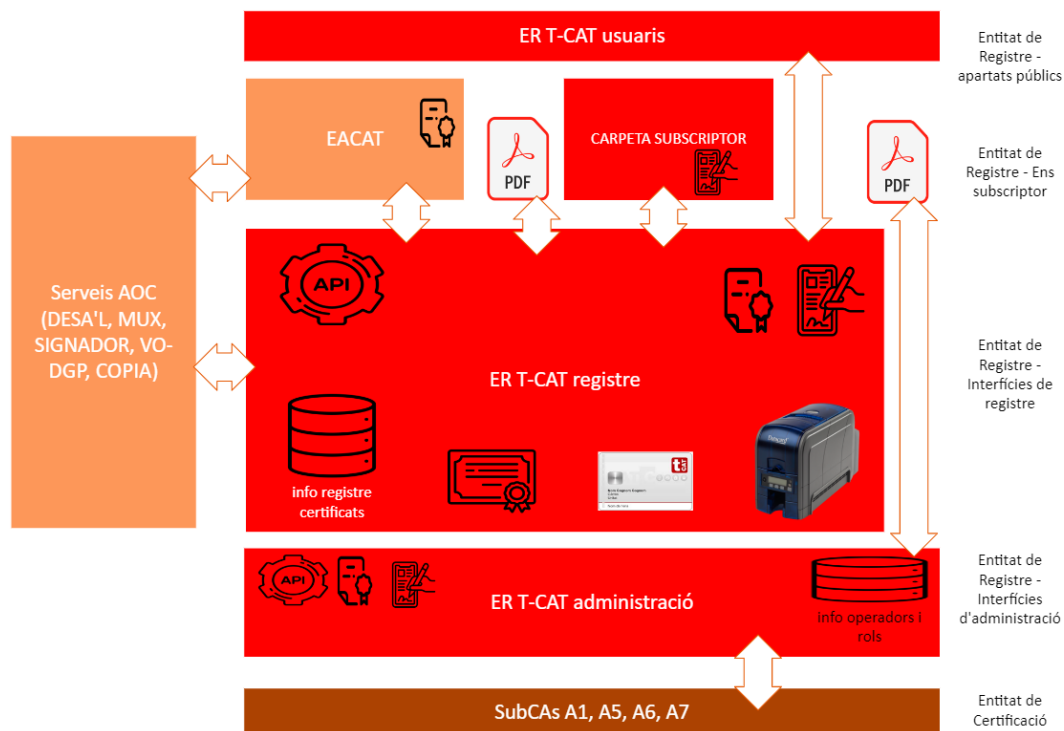
El següent esquema mostra l'estructura de sistemes que fa servir el Consorci AOC per a gestionar els serveis de certificació digital:



- En blau fosc es mostren clients agrupats per operadors del sistema de portals o com a clients i/o subscriptors.
- En vermell es mostren els components de l'SCD, ja siguin productes comercials o desenvolupats a mida :
 - Servei ER-T-CAT: portal, connectors i software de l'Entitat de Registre de Certificats T- CAT per a treballadors públics i de les Entitats de Certificació del Consorci AOC
 - Servei ER idCAT: portal i connectors d'idCAT
 - PKI-EPSCD : serveis de OCSP, CRL i informació pública (DPC, claus públiques, etc..)
- En marró: la capa criptogràfica (HSMs) de la EC arrel i subCA
- En taronja, integracions amb serveis del Consorci AOC:
 - EACAT (Extranet de les Administracions Públiques Catalanes) : canal d'entrada únic de la tramitació interadministrativa, inclosa la dels certificats digitals. Inclou tramitació en PDF de sol·licituds de certificats i operadors del sistema.
 - Serveis AOC: registre d'entrada/sortida (MUX), repositori documental (DESA'L), aplicacions de signatura (SIGNADOR), servei de digitalització (COPIA), accés a dades de la DGP (VO-DGP), etc..

11.3 El Servei de Registre de certificats personals i de segell electrònic pel Sector Públic (T-CAT)

El Servei de Certificació Digital per a treballador públic (en endavant, T-CAT) és el servei que s'ofereix per a l'emissió de certificats del sector públic català. Els certificats T-CAT són els que s'emeten des de les Entitat de Certificació de Sector Públic. Com a perfils de certificat s'hi inclouen els certificats de signatura electrònica i de segell electrònic.



11.3.1 Model de Registre T-CAT

Tot el procés de sol·licitud, emissió i lliurament dels certificats T-CAT actual es fa per mitjans digitals i emmagatzemant evidències documentals electròniques i segures en cada pas. Per dur a terme això, hi ha tres components lògics principals amb responsabilitats funcionals concretes assignades. Es descriuen a continuació en el mateix ordre que s'utilitzen en el cas d'una sol·licitud, emissió i lliurament d'un certificat T-CAT.

- 1) Mòdul ASCD d'EACAT : canal d'entrada de les sol·licituds de certificats T-CAT i de la documentació per a la gestió dels rols de tot el sistema de registre. Aquest mòdul està integrat dins del Servei EACAT ofert pel Consorci AOC. Per tant, s'utilitza per tots els ens adscrits a EACAT i susceptibles de sol·licitar un certificat digital T-CAT. Existeix un vídeo demostratiu del procés disponible [aquí](#). Les responsabilitats del component són:
 - a. Generar i arxivar la documentació electrònica de sol·licitud de certificats digitals (tramesa de certificats) amb la signatura de les persones autoritzades a fer aquest tràmit en l'ens sol·licitant.

- b. Canalitzar i arxivar la documentació electrònica de gestió dels rols del sistema de Registre de l'SCD T-CAT.
 - c. Assignació d'un número de referència únic per al seguiment del tràmit. Actualment és un número de registre assignat pel servei de registre unificat (MUX) del consorci AOC.
 - d. Notificació dels canvis d'estat de la tramitació. En particular de l'acceptació i de la finalització de la tramesa de certificats.
 - e. Arxiu de la documentació i les comunicacions generades pel tràmit en un Sistema de Gestió Documental (SGD). Actualment el gestor SGD utilitzat és el que disposa el Consorci AOC amb el servei propi DESA'L.
 - f. Control d'accés als tràmits de l'ASCD a través del sistema d'autenticació i autorització T-CAT amb els següents rols: editor de sol·licituds, sol·licitant de certificats personals, sol·licitant de certificats de dispositiu i certificador de dades.
- 2) Web operadors de registre: mòduls web i connectors de l'entitat de registre. És utilitzat per una vuitantena d'entitats que fan el rol d'Entitat de Registre de l'SCD T-CAT.
- a. Mòdul peticionari: mòdul de càrrega de peticions al sistema de registre. Disposa d'un canal d'entrada web i d'un canal d'entrada automàtic via connector REST que és el que utilitza el mòdul ASCD d'EACAT.
 - b. Mòdul aprovador: mòdul web per a l'aprovació de les sol·licituds.
 - c. Mòdul generador: mòdul basat en un programari instal·lat en un ordinador client per a la generació dels certificats. Si el suport del certificat T-CAT és una targeta criptogràfica, aquest mòdul interacciona amb una impressora de targetes. En cas que sigui de suport programari, aquest mòdul no intervé perquè aquella petició de certificat passa directament a estar llesta per lliurament a través de la carpeta del subscriptor (descriu a continuació).
 - d. Mòdul gestor de certificats: mòdul per a la gestió de l'estat del certificat (suspensió, habilitació i revocació). També disposa d'un canal d'entrada web i d'un canal d'entrada automàtic via un connector REST.
- 3) Carpeta del subscriptor : mòdul per a la gestió digital segura del procés de lliurament dels certificats T-CAT per part de l'ens sol·licitant dels certificats. El seu ús també és per part de tots els ens susceptibles de demanar un certificat digital T-CAT (uns 2.500).
- a. Aquest mòdul custodia els originals digitals no signats del contracte d'acceptació de les condicions del servei de certificació que signa el subscriptor del certificat T-CAT

- b. Custòdia dels codis d'activació (PIN i PUK en cas de targeta; contrasenya en cas de certificats en format p12) originals dels certificats T-CAT.
- c. La persona designada dins l'ens sol·licitant que fa ús d'aquest mòdul s'anomena Responsable del Servei i és un rol dins del sistema de certificació T-CAT.
- d. El Responsable del Servei és l'encarregat de fer signar els contractes d'acceptació de les condicions d'ús dels certificats T-CAT, lliurar els certificats (segons el procediment definit per a cada tipus de certificat T-CAT) i custodiar la documentació signada en l'arxiu en paper del seu Ens.
- e. El responsable també deixa evidència en el sistema de la signatura en paper i, amb aquest acte, genera l'enviament dels codis d'activació al subscriptor.
- f. Finalment, la carpeta del subscriptor també permet al subscriptor titular d'un certificat T-CAT, la recuperació dels codis d'activació originals a través d'una interfície web.
- g. També en aquest mòdul s'implementa la Cessió de certificats entre EERR que es defineix en el punt "11.3.4.3 Mòdul de cessió de certificats".

En els propers punts es descriuen més en detall cadascun dels components i mòduls esmentats.

11.3.2 Topologia de la xarxa d'Entitats de Registre T-CAT

Les Entitats de Registre T-CAT presenten les següents variants:

11.3.2.1 Ens subscriptors o Entitats de Registre Virtuals o vinculades

En l'entorn T-CAT, els Ens subscriptors o ERs virtuals o vinculades són tots els ens subscriptors del servei que no disposen de la impressora criptogràfica necessària per a gravar el xip i imprimir la personalització gràfica de les targetes. Les ER vinculades fan servir l'ASCD d'EACAT per a la certificació de dades de certificats T-CAT i el lliurament dels certificats T-CAT amb la carpeta del subscriptor.

El número d'Ens subscriptors o ERs Virtuals o vinculades (ens donats d'alta al sistema) actualment és de 2.482.

11.3.2.2 ERs Col·laboradores

En l'entorn T-CAT, s'entén per ER col·laboradora, una ER que disposa d'infraestructura per a l'emissió de certificats en suport targeta.

El número de ERs Col·laboradores és de 68 entitats de registre, de les quals n'hi ha que tenen varis punts d'atenció. El número total d'operadors de les ERs T-CAT és d'aproximadament : 747.

11.3.2.3 L'ER centralitzada del Consorci AOC

El Consorci AOC opera una ER que és la que centralitza les peticions de certificats digitals de tots els ens que no estan vinculats a una ER Col·laboradora o que, puntualment, demanen emissions de trameses concretes de certificats.

11.3.3 Rols del sistema de registre T-CAT

11.3.3.1 Rols de l'ASCD i Carpeta del Subscriptor

Aquests rols corresponen als components de l'ASCD i Carpeta del subscriptor descrits anteriorment. Estan definits a la web del Consorci AOC i es repliquen aquí per millor referència.

- Responsable del servei. Persones amb un rol de gestió i no un perfil d'elevat grau de responsabilitat, aquests actuen com a enllaç entre l'ens i la seva Entitat de Registre T-CAT. Entre les seves funcions, es responsabilitzen de lliurar els certificats digitals als titulars, de fer-los signar la documentació legal, d'arxivar-la convenientment i també d'informar-los de les seves obligacions i responsabilitats. Cal que hi hagi un mínim de dues persones amb el rol responsable del servei de certificació digital, però poden haver-hi tots els que es desitgin per tal de garantir la continuïtat del servei.
- Certificador de dades. Persones que es responsabilitzen de justificar la veracitat de les dades dels certificats. Recomanem que aquest rol sigui el perfil de l'ens amb capacitat per donar fe de les dades personals que ha de contenir el certificat digital. Per exemple: el/la secretari/ària d'un ajuntament, el/la cap de recursos humans o càrrecs similars. Cal que hi hagi un mínim de dues persones amb el rol de certificador, però poden haver-hi tots els que es desitgin per tal de garantir la continuïtat del servei.
- Sol·licitant de certificats personals. Persones amb autoritat dins de l'ens per sol·licitar l'emissió, renovació i revocació de certificats personals o d'entitat (p. ex. l'alcalde, tinent d'alcalde o un regidor a l'ajuntament, o el director de serveis d'un departament de la Generalitat). Cal que hi hagi un mínim de dues persones amb el rol de sol·licitant de certificats personals, però poden haver-hi tots els que es desitgin per tal de garantir la continuïtat del servei.
- Sol·licitant de certificats d'aplicació. Persones amb autoritat dins de l'ens per sol·licitar l'emissió, renovació i revocació de certificats de dispositiu (p. ex. el/la cap d'informàtica). Cal que hi hagi un mínim de dues persones amb el rol de sol·licitant de certificats de dispositiu, però poden haver-hi tots els que es desitgin per tal de garantir la continuïtat del servei.
- Editor de sol·licituds. Persones que poden emplenar, tot i que no signar, sol·licituds d'emissió, renovació i revocació de certificats digitals a través de l'EACAT, de forma que quedin preparades per a la signatura d'un usuari amb el rol de sol·licitant de certificats. Recomanem que els editors de sol·licituds siguin de perfil administratiu i que hi hagi un mínim de dues persones amb aquest rol, tot i que poden haver-hi tots els que es desitgin per tal de garantir la continuïtat del servei.

NOTA: els rols sol·licitant i certificador són incompatibles, i és recomanable què hi hagi un mínim de dues persones en cada rol.

Aquests rols són informats al Servei de Certificació Digital del Consorci AOC a través de la Fitxa d'Ens Subscriptor. Aquesta fitxa també incorpora les dades oficials de l'Ens en qüestió que, com a sol·licitant de certificats T-CAT, constaran als certificats que sol·liciti. La fitxa s'ha d'actualitzar cada dos anys i s'envia a través d'una tràmit ofert pel servei EACAT. S'adjunta un annex de mostra al present plec de prescripcions tècniques i un [enllaç](#) a un vídeo explicatiu del procés.

11.3.3.2 Rols web Operadors / Entitat de registre d'SCD

Hi ha establerts quatre rols d'operador (peticionari, aprovador, generador i gestor de certificats), un de coordinador del servei (responsable del servei) i tres figures associades (responsable de seguretat física, responsable de seguretat lògica i arxiver). Tot seguit s'explica la funció que realitza cadascun dels rols:

- Peticionari: persona encarregada d'introduir les dades de les sol·licituds de certificats a l'aplicació de petició de certificats. S'ha de tenir en compte que quan una petició entra per l'EACAT aquest rol desapareix i queda per a casos d'extraordinaris (nous ens o ens no donats d'alta a l'EACAT o problemes tècnics que impedeixin fer ús de la plataforma.)
- Aprovador: persona encarregada de revisar les dades de les sol·licituds introduïdes pel peticionari i aprovar (validar) o denegar (retornar al peticionari) la petició en conseqüència. En el cas de peticions introduïdes per l'EACAT, no es tractarà d'una tasca de revisió de la feina del peticionari, que no existeix, però si serà necessari comprovar que no hi ha errors evidents, proves dels ens que sol·liciten certificats, etc.
- Generador: persona encarregada de generar els certificats un cop aprovades les peticions
- Gestor de certificats: persona encarregada d'habilitar i revocar els certificats digitals durant el seu cicle de vida (la suspensió només és telefònica). S'ha de tenir en compte que, quan una petició entra per l'EACAT aquest rol desapareix i queda per a casos d'emergència (en que no sigui possible fer servir l'EACAT).
- Responsable del servei: el responsable del servei s'encarrega de la coordinació i bon funcionament de l'Entitat de Registre, en cas que arribin sol·licituds en paper o PDF signat, rep la documentació, valida la identitat i autoritat del sol·licitant, verifica la documentació, notifica al subscriptor l'inici de la tramitació, obre els expedients, arxiva la documentació i notifica al peticionari l'inici del procés. A més, actua com a enllaç entre l'organització i el Consorci AOC.
- Responsable de seguretat física: les funcions del responsable de seguretat física consisteixen en coordinar, controlar i revisar el conjunt de mesures contingudes a la política de seguretat i les normes i procediments de seguretat relacionats amb els aspectes físics. És a dir, tot allò que fa referència al control d'accés a la sala d'operacions,

la detecció i extinció d'incendis, la protecció de la informació i material a nivell físic, etc. Aquest rol queda englobat en el responsable de l'Entitat de Registre T-CAT.

- Responsable de seguretat lògica: les funcions del responsable de seguretat lògica consisteixen en coordinar, controlar i revisar el conjunt de mesures contingudes a la política de seguretat i les normes i procediments de seguretat relacionats amb els aspectes lògics de l'Entitat de Registre. És a dir, tot allò que fa referència a la seguretat informàtica (control d'accés a la xarxa, polítiques d'instal·lació de programari, configuració dels equips, etc.). Aquest rol queda englobat en el Responsable de l'Entitat de Registre T-CAT.
- Arxiver: l'arxiver o la persona que aquest designi s'encarregarà d'organitzar, classificar, descriure i vetllar per la salvaguarda de la documentació que es generi fruit de l'emissió i gestió dels certificats d'acord amb el sistema de gestió documental del seu organisme, o en la seva absència, segons les directrius que estableixi l'arxiver del Consorci AOC. Aquest rol queda englobat en el Responsable de l'Entitat de Registre T-CAT.

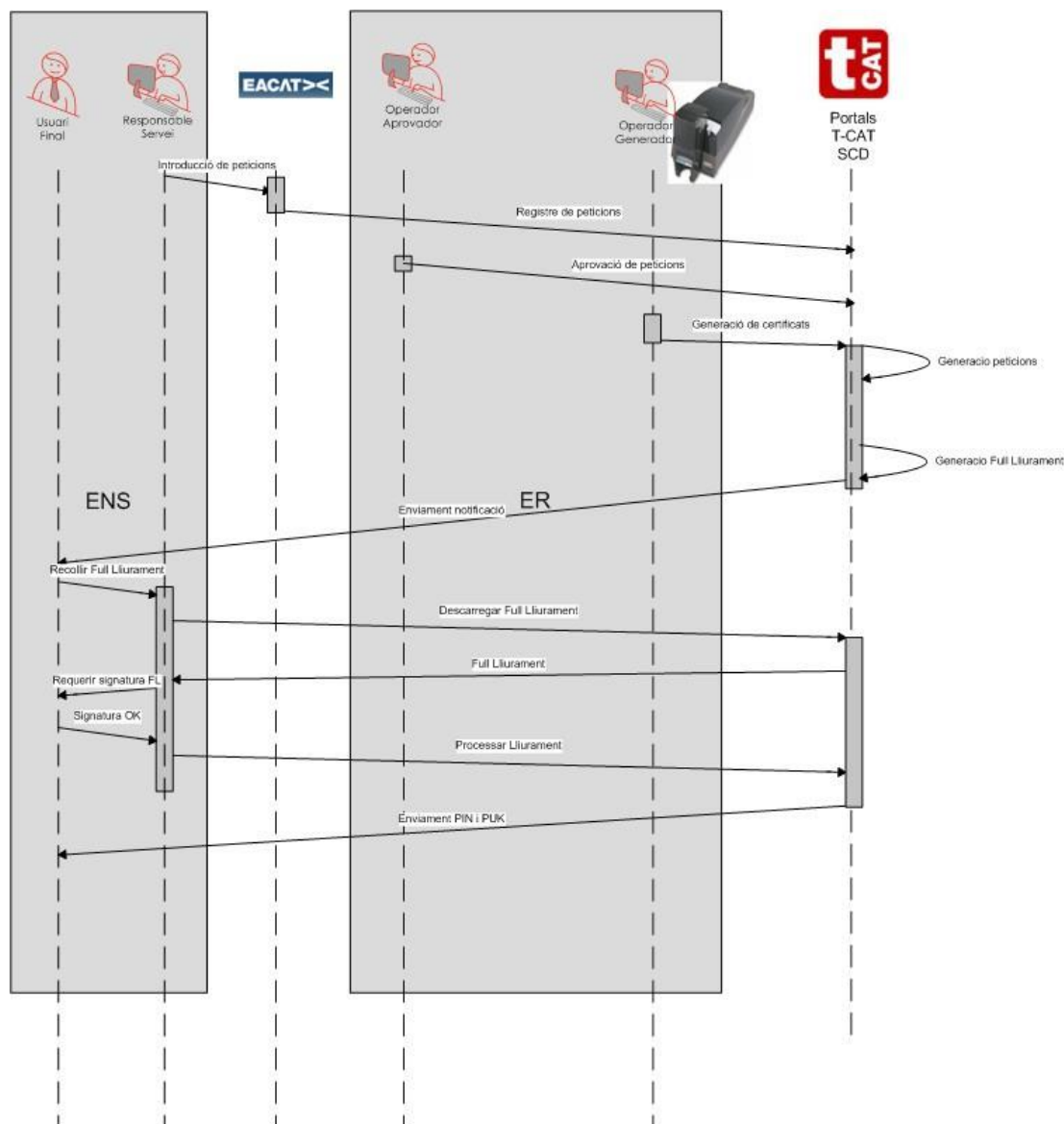
Aquests rols són informats al Servei de Certificació Digital del Consorci AOC a través de la Fitxa d'Entitat de Registre. La fitxa s'ha d'actualitzar cada dos anys i s'envia a través d'una tràmit ofert pel servei EACAT. S'adjunta un annex de mostra al present plec de prescripcions tècniques.

11.3.4 Diagrama de relacions dels procediments d'emissió

Mitjançant els següents diagrames de relacions, s'il·lustren els processos d'emissió de certificats digitals en suport targeta i programari. Els esquemes mostren els rols que intervenen al llarg del procés.

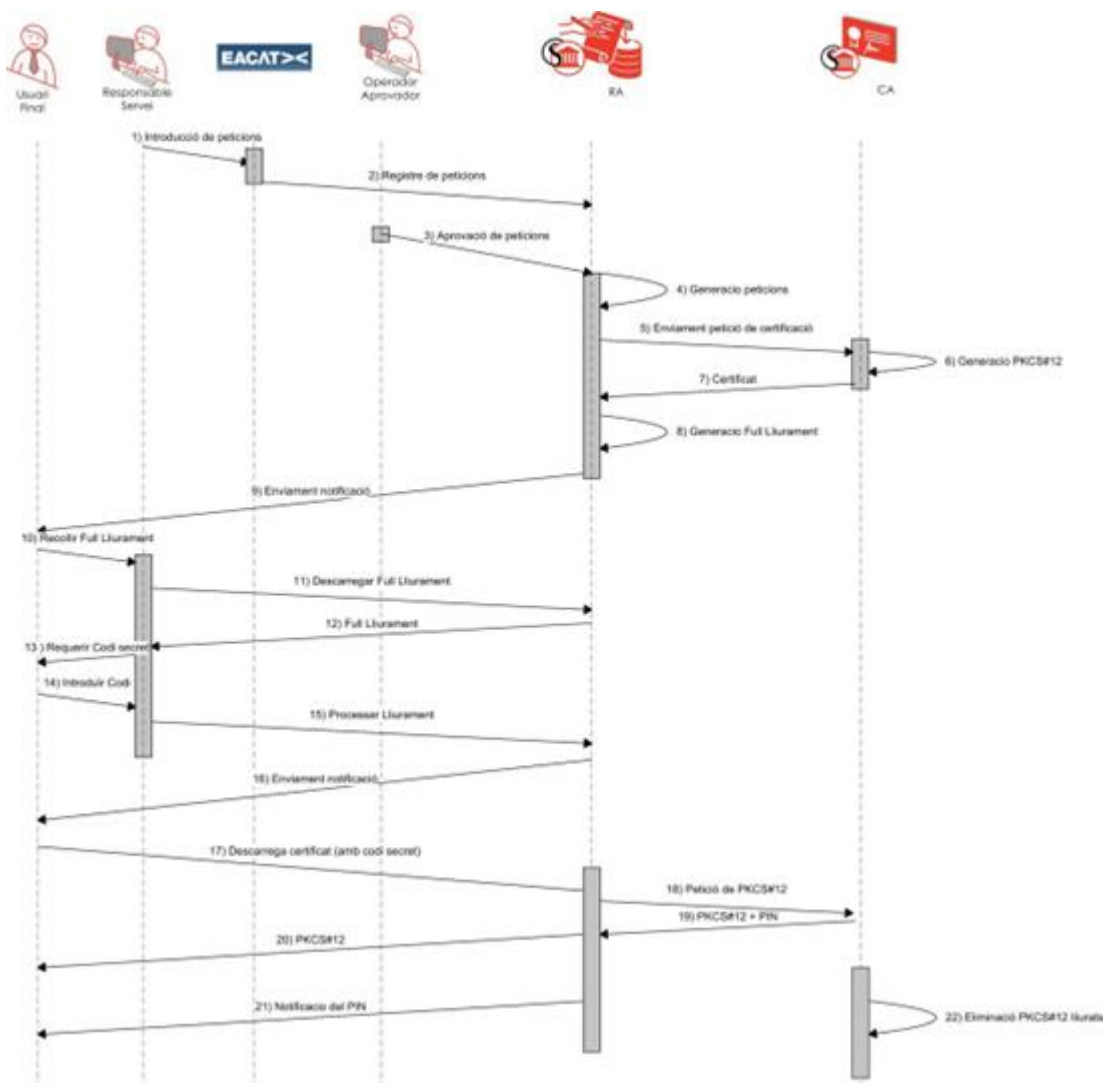
11.3.4.1 Procediment T-CAT

El següent diagrama de flux representa el procediment de emissió estàndard d'una targeta T-CAT a través d'EACAT, sol·licitada per un ENS, emesa per la seva ER corresponent i amb el PIN/PUK enviats per correu-e:



11.3.4.2 T-CAT-P (Programari)

El següent diagrama de flux representa el procediment d'emissió estàndard d'un certificat T-CATP en programari amb la sol·licitud a través d'EACAT, amb personació física de l'usuari final davant del responsable de servei pel "lliurament" de la targeta, signatura del contracte i enviament del PIN i PUK per correu-e:



11.3.4.3 Mòdul de cessió de certificats

Aquest mòdul de la Carpeta del Subscriptor incorpora la possibilitat de delegar al Consorci AOC la descàrrega de les claus, en format pkcs#12, per als tipus de certificat de Segell electrònic de nivell mig.

Actualment les claus es generen a l'entitat de certificació, s'associen a un certificat del perfil de segell de nivell mig i s'importen al servei de signatura centralitzada pel seu ús per part dels clients tal i com es descriu a continuació al punt "11.4.5 Serveis per l'ús de certificats de segell electrònic centralitzats : el Servei Signador Centralitzat".

Els operadors del sistema amb rol "dipositari" són els responsables de descarregar aquests certificats i carregar-los al servei de signatura centralitzada en el magatzem corresponent de cada ens, identificat amb el codi INE10 (etiqueta DIPOSITARI de la missatgeria del servei). Els codis INE10 identifiquen internament al Consorci AOC i en l'àmbit de tots els serveis que ofereix, cada ens usuari dels serveis . En el moment de la càrrega s'informa l'etiqueta (etiqueta ROL de la missatgeria del servei) que s'utilitzarà per invocar el servei.

11.3.5 Gestió documental del Servei de Certificació T-CAT

El programari de l'ASCD d'EACAT, que gestiona el tràmit de sol·licitud de certificats T-CAT i les fitxes de subscriptors, s'integra amb el gestor documental del Consorci AOC per a la gestió de la documentació derivada del tràmit.

El gestor documental s'utilitza també per generar les comunicacions de finalització o rebuig de la tramitació sol·licitada, per tal d'informar als sol·licitants del tràmit del seu estat. Cal recordar que s'assigna un número de registre d'entrada des del mòdul ASCD d'EACAT i aquest és el número que s'utilitza per fer el seguiment de l'expedient.

La documentació de la fase de lliurament, és a dir, el contracte d'acceptació de les condicions d'acceptació de l'emissió dels certificats digitals, es fa a l'arxiu de cada ER vinculada. Cada Responsable del Servei de cada ER vinculada és responsable de descarregar el contracte i fer-lo signar al subscriptor del certificat, en el cas dels personals, o signar-lo ell mateix en el cas dels certificats de dispositiu. En tots dos casos, aquesta documentació en paper és custodiada per l'arxiver de l'ER vinculada durant el període legalment exigít.

11.3.6 Taula de relació entre rols i històries d'usuari del component ASCD

En la següent taula es mostren els rols amb les operacions que poden realitzar en el mòdul ASCD d'EACAT i que estan a l'abast d'aquest contracte:

Operació	Responsable Servei (RE)	Certificador de Dades (CD)	Sol·licitant certificats personals (SCP)	Sol·licitant certificats aplicació (SCA)	Editor de sol·licituds (ES)
Sol·licitud i renovació certificats personals			X		
Sol·licitud i renovació de certificats d'aplicació				X	
Sol·licitud de certificats de pseudònim o representant			X		
Sol·licitud de revocacions			X	X	
Sol·licitud i renovació de certificats d'operador			X		
Revocació de certificats d'operador			X		
Validació de sol·licitud de certificats		X			
Autenticació i Autorització	X	X	X	X	X

Consulta de sol·licituds	X	X			
Signatura Digital	X	X	X	X	

11.3.7 Històries d'usuari de les operacions de sol·licitud i gestió del cicle de vida dels certificats dins d'EACAT

11.3.7.1 Sol·licitud i renovació de certificats personals

Objectiu

És possible realitzar la sol·licitud per a la generació o renovació d'un certificat digital de tipus personal.

Precondicions

Els usuaris requerits hauran de tenir els rols corresponents a EACAT.

Procediment

El **sol·licitant** accedeix a la pàgina corresponent per iniciar el procés, on li apareix un assistent web amb diversos passos a seguir.

En el primer pas dins del procés se li demana a l'usuari establir la següent informació:

- Entitat de Registre destinatària
- Tipus de certificat a realitzar (Llista)
- Prioritat de la petició (Ordinària o Urgent)
- Comentari

En el següent pas, s'introdueix la informació corresponent al certificat, és possible afegir diversos certificats en la mateixa sol·licitud (formant una tramesa):

- Nom*
- Primer Cognom*
- Segon Cognom
- NIF/NIE*

- Correu electrònic*
- Unitat Orgànica
- Usuari Ms Windows
- Número d' expedient
- Expedient de facturació

En avançar, apareix un formulari on apareixen les dades del RE, permetent modificar la informació corresponent a:

- Nom
- Direcció
- Codi Postal
- Localitat

Selecciónem l'opció d'Enviar a Signar, que mostra un missatge de confirmació indicant que la petició quedarà pendent de signatura, mostrant-se també un formulari de resum amb les dades que s'han registrat per a la sol·licitud. En aquest punt seleccionem l'opció de Signar, que realitza una signatura digital associada a la sol·licitud.

L' operació finalitza i es mostra un missatge indicant que el procés ha finalitzat correctament, enviant un correu electrònic a l'usuari certificador amb el resum de l' operació.

11.3.7.2 Sol·licitud i renovació de certificats d'aplicació

Procés similar al de sol·licitud i renovació de certificats personals

11.3.7.3 Sol·licitud de certificats de pseudònim o representant

Procés realitzat 100% a través de formulari PDF

11.3.7.4 Sol·licitud de revocacions

Procés similar al de sol·licitud i renovació de certificats

11.3.7.5 Sol·licitud i renovació de certificats d'operador

Procés realitzat 100% a través de formulari PDF

11.3.7.6 Revocació de certificats d' operador

Procés realitzat 100% a través de formulari PDF

11.3.7.7 Validació de sol·licitud de certificats

Objectiu

Com **a certificador** és possible realitzar la validació d'una sol·licitud de certificats realitzada per un **sol·licitant**.

Precondicions

Hi ha una sol·licitud de certificats personals registrada correctament i pendent de validació.
L'usuari que realitza l'operació ha d'estar assignat com a **certificador** dins de l'Ens.

Procediment

El **certificador** fa login a l'aplicació i selecciona l'opció de veure les sol·licituds de certificats, i es va mostra una taula amb la llista de sol·licituds. A la taula es mostra el Tipus de la Sol·licitud, la Data, el Tipus del certificat i el nombre de certificats associats a la sol·licitud (tramesa). Per a les sol·licituds pendents, té l'opció de signatura.

El **certificador** selecciona de la llista una sol·licitud per signar, i es mostra un formulari amb el resum dels certificats sol·licitats associats, on té l'opció de realitzar la signatura, realitzant una signatura digital de les dades i confirmant la validació de la sol·licitud.

L'operació finalitza i es mostra un missatge indicant que el procés ha finalitzat correctament, enviant un correu electrònic al **sol·licitant** que va realitzar la sol·licitud amb el resum de l'operació.

11.3.8 Altres operacions

11.3.8.1 Autenticació i Autorització

L'Autenticació i Autorització es fa en base a les dades d'usuaris i rols, respectivament, que han estat informades en les fitxes d'ENS mencionades anteriorment i que s'han configurat a la base de dades d'usuaris i rols dins del propi EACAT.

11.3.8.2 Consulta de sol·licituds

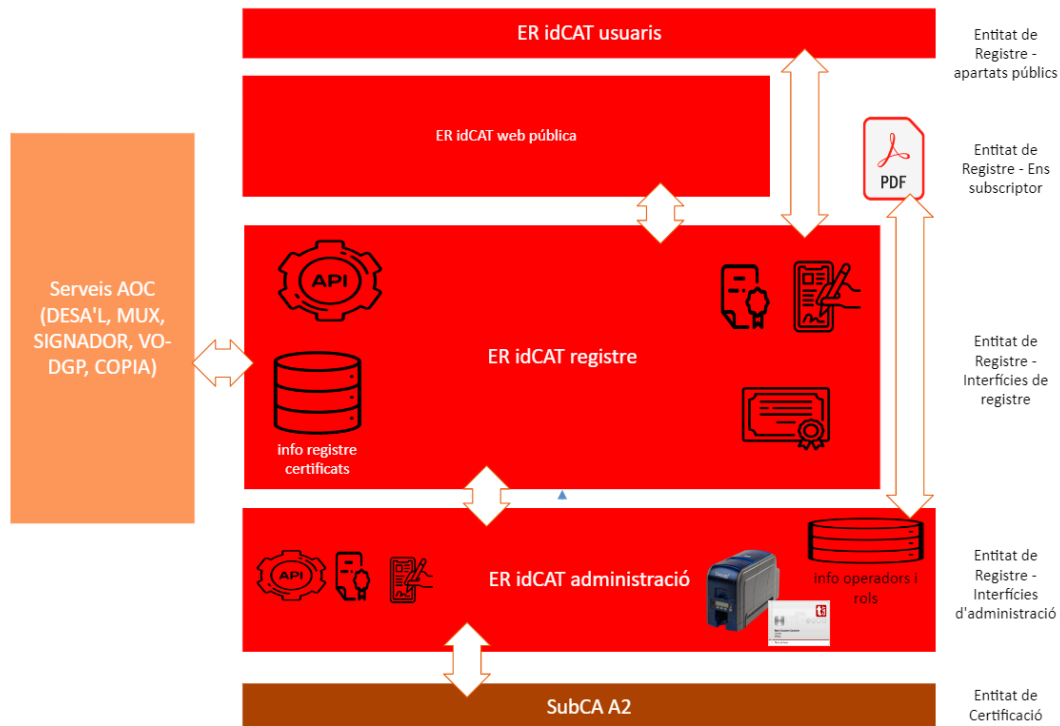
La consulta de sol·licituds es fa a través de la consulta de les traces d'enviament de les trameses de sol·licituds de certificats des del component ASCD d'EACAT cap a la ER a través del seu connector web.

11.3.8.3 Signatura Digital

La signatura digital de les evidències es realitza mitjançant el component Signador d'AOC. Les sol·licituds de certificats personals inclouen dos signatures (dels rols sol·licitant i certificador) i les de certificats de segell una única signatura (del rol SCD).

11.4 El servei de Registre de certificats personals per Ciutadania (idCAT)

Per la seva part, els operadors de les ERs idCAT treballen emprant un únic aplicatiu que és el Web idCAT (www.idcat.cat). L'equip de l'operador de l'ER, a part de la de disposar d'un lector per a la seves targetes amb el certificat d'operador, ha de disposar de la instal·lació de l'aplicació de signatura per emissió i revocació. El web idCAT consta de tres grans mòduls funcionals:



11.4.1 La web del ciutadà

Des d'on es pot fer la sol·licitud, cerca d'entitats de registre per fer la validació presencial, la descàrrega, la revocació i la renovació del certificat digital de ciutadà. La descàrrega del certificat es realitza en format pkcs#12.

11.4.2 La Web dels Operadors de Registre

Des d'on es fa el flux d'emissió, amb la corresponent generació de documentació del contracte a signar pel ciutadà; es controlen els permisos dels operadors del servei idCAT; i es fa la gestió del cicle de vida del certificat per a la seva suspensió, habilitació o revocació. El flux d'emissió consta de les fases de registre de les dades del ciutadà que sol·licita el certificat per part d'un operador identificat, la validació d'aquestes dades amb la base de dades de la Policia (a través del servei de Via Oberta del Consorci AOC, modalitat DGP) perquè es pugui emetre el certificat i la generació de la documentació.

11.4.3 La Web dels Operadors de Certificació o d'administració

Des d'on es controlen els permisos dels operadors del servei idCAT i es generen els certificats en targeta per a operadors del sistema.

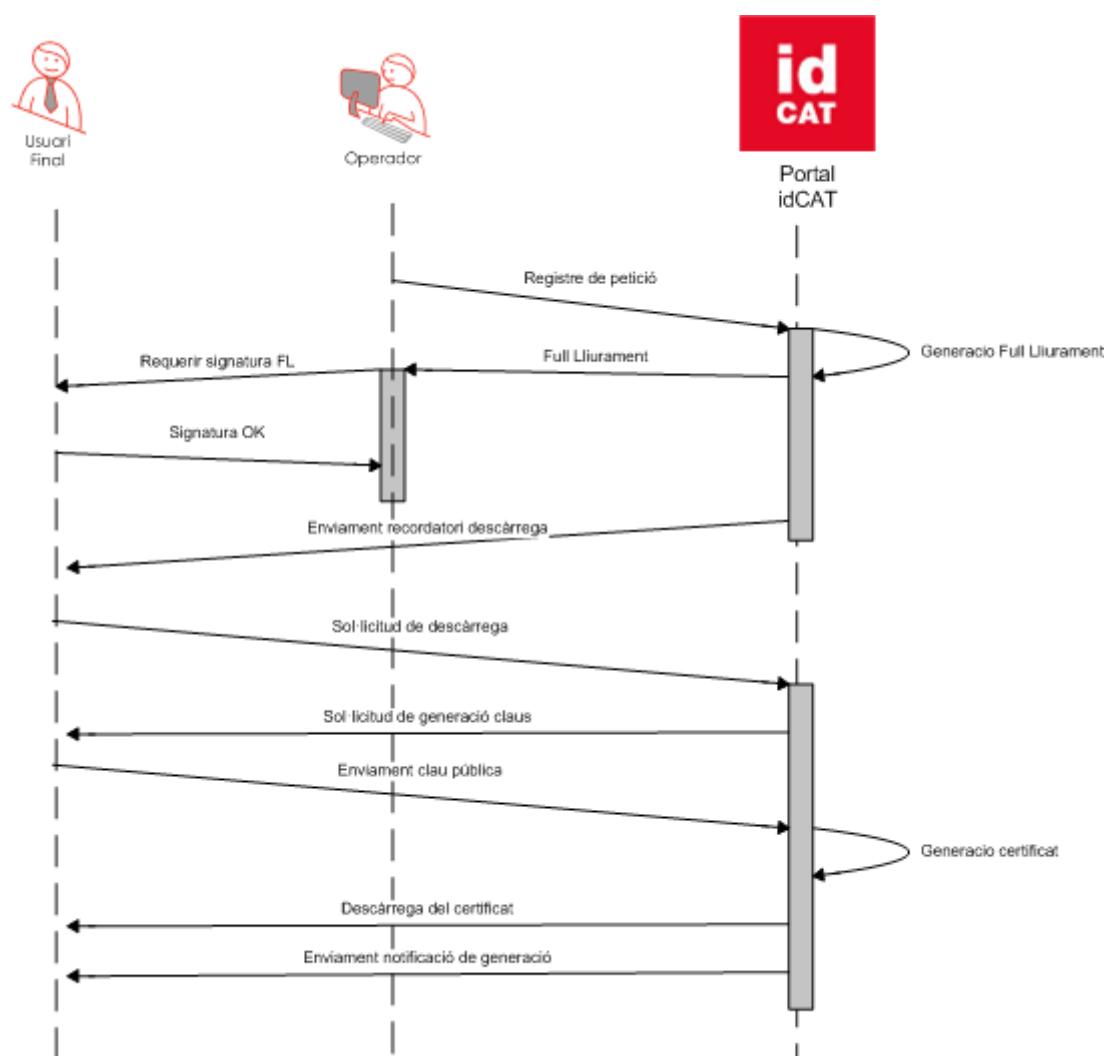
Dimensions ER idCAT:

- Número d'ERs: 372
- Número d'operadors de les ERs idCAT: 3.566

Finalment, la documentació contractual en paper generada i signada pels ciutadans subscriptors del servei és custodiada per l'arxiver de l'ER idCAT durant el període legalment aplicable.

11.4.4 Procediment de sol·licitud i emissió idCAT

La següent figura representa el flux de sol·licitud d'emissió i descàrrega en mode pre-validació. L'usuari no carrega les dades des de casa i ho fa l'operador a l'ER.



El flux pot introduir la variant del model de "sol·licitud" prèvia. És a dir amb càrrega de dades prèvia a l'aplicació per part del ciutadà i l'operador recupera la sol·licitud per validar-la.

11.4.4.1 Gestió documental del Servei de Certificació idCAT

La documentació de la fase de lliurament, és a dir, el contracte d'acceptació de les condicions d'acceptació de l'emissió dels certificats digitals, es fa a l'arxiu de cada ER vinculada. Cada Responsable del Servei de cada ER vinculada és responsable de descarregar el contracte i fer-lo signar al subscriptor del certificat. En tots dos casos, aquesta documentació en paper és custodiada per l'arxiver de l'ER vinculada durant el període legalment exigit.

11.4.5 Serveis per l'ús de certificats de segell electrònic centralitzats : el Servei Signador Centralitzat

Servei de custòdia centralitzada de certificats digitals de segell electrònic, integrat amb la PKI per a la provisió de certificats digitals, que en fa una custòdia centralitzada i segura, i que s'integra amb eines que permeten l'ús de les claus allí emmagatzemades per part dels usuaris titular o d'aplicacions que estiguin expressament autoritzades a fer-ne ús. En el servei es custodien segells electrònics de dos modalitats previstes en el procediment de sol·licitud actual (consultar [aquí](#)) i que són "Cedit en exclusivitat per ús dels serveis AOC" o bé "Cedit en exclusivitat per ús d'eines pròpies".

La integració amb el servei es realitza mitjançant webservice XML amb autenticació de client amb certificat digital, xifratge de transport HTTPS i TLS 1.2. L'autorització és mitjançant el certificat digital d'autenticació i les etiquetes Rol i Dipositari indicades al missatge. El servei permet fer signatures en format PDF amb enviament del document sencer, XML attached o detached. El format de hash per defecte és SHA2. La documentació d'integració del servei, amb més detall tècnic de l'exposat aquí, es pot consultar [aquí](#).

En relació amb les volumetries, el servei allotja actualment més de 1400 claus de tots els organismes de l'administració pública catalana, i es realitzen un volum de 5 milions de signatures mensuals amb pics de 600 transaccions per minut.

11.4.6 Actius de programari, codi i dades del servei actual a disposició de l'adjudicatari

A continuació s'enumeren els actius de programari, codi i dades del servei actual que es posaran a disposició de l'adjudicatari per assolir els objectius per la prestació dels serveis objecte del contracte. A l'apartat "6 DESCRIPCIÓ DELS SERVEIS OBJECTE DEL CONTRACTE" i els seus sub-apartats, es defineixen les condicions per al traspàs, posada en marxa, ús, manteniment, millora i retorn d'aquests actius per part de l'adjudicatari.

Les claus de les entitats subordinades a utilitzar per aquests serveis i que s'han esmentat al punt "5.1 El servei de certificació digital del Consorci AOC". Les claus es van generar en dispositius del fabricant ENTRUST, model XC Connect. El security world que les allotja és de nova creació a 2022 i està protegit per un conjunt de targetes ACS en configuració 3 de 8 i OCS de 2 de 5. Les targetes són del tipus que permeten operació remota.

El servei de signador centralitzat de segells s'ofereix a través de infraestructura pròpia del Consorci AOC i amb el producte TrustedX eSignature sota el llicenciament vigent del fabricant ENTRUST. El Consorci AOC disposa dels descriptors del servei web de la missatgeria de integració, les claus i configuració (relació ROL+DIPOSITARI) del servei així com els formularis d'alta al mateix.

En relació a l'Entitat de registre, el Consorci AOC disposa del codi de tots els components de interfícies d'usuari. També de la informació per a la integració amb els diferents serveis de backend oferts pels diferents components enumerats al punt "11.2 Situació actual de subsistemes i components del Servei". També les fitxes d'alta dels ENS i ER amb la seva informació verificada i els operadors i rols que les componen.

En relació als serveis de identificació i signatura de VALid i Signador, el Consorci AOC en duu a terme el cicle de vida de gestió del programari complet així com l'exploració i suport.

11.5 Serveis d'auditoria d'ER

El Consorci AOC duu a terme les auditories de les entitats de registre per garantir que el seu funcionament s'ajusta als procediments, funcions i responsabilitats que es transfereixen mitjançant les condicions específiques del servei.

L'objectiu de realitzar auditories als ens subscriptor i a les Entitats de Registre IDCAT i T-CAT és supervisar i controlar que tot el procediment d'emissió i gestió dels certificats digitals IDCAT i T-CAT es realitza de forma correcta i compleix amb els procediments operatius que el Consorci AOC proporciona a les ERs.

En el moment de licitació d'aquest contracte, aquest servei està adjudicat a un proveïdor extern a través del contracte "AOC-2020-53". El plec tècnic amb els detalls d'auditoria que el regeixen es poden consultar aquí : <https://contractaciopublica.cat/ca/detall-publicacio/a1fd1b13-5185-2ac8-80e5-efe217cfb5c5/60315938>

Les auditories poden ser presencials o virtuals i segueixen un procediment que el Consorci AOC estableix i que es pot consultar en el plec tècnic de l'esmentat contracte amb el nom "ER_idCAT_T- CAT_procediment_auditoria.pdf".

A principis de cada any el Consorci AOC acordarà amb l'adjudicatari la selecció de les ERs que s'hauran d'auditar durant aquell any, en base als criteris descrits al citat document; i amb l'objectiu que totes les ERs se sotmetin, com a mínim, a una auditoria cada 3 anys. També s'acordarà la planificació de les corresponents auditories.

11.6 Serveis evolutius i de personalització de programari actuals

Actualment, el programari desplegat demanda uns serveis d'evolució i personalització.

Aquests serveis es dediquen al manteniment evolutiu periòdic i a la resolució d'incidències derivades del dia a dia de les aplicacions associades a l'SCD. Inclouen tasques com ara:

- Diagnòstic de problemes i incidències derivades de dades incorrectes carregades al sistema i que generen problemes en el tractament de les mateixes.
- Tercer nivell de resolució d'incidències.
- Millores menors de gestió de l'SCD.
- Suport a la prestació i seguiment del servei.
- Suport a integracions de clients i entitats de registre.
- Altres peticions

11.7 ANS actual del servei de certificació

Actualment, el servei ordinari d'emissió i renovació de certificats T-CAT ofert pel Consorci AOC té el compromís de lliurar els certificats en el termini de 16 dies naturals, que es compten a partir de la recepció de la documentació correctament emplenada i signada.

Tanmateix, es posa a disposició dels usuaris un servei d'emissió i renovació urgent de certificats per a tots aquells que, per motius d'urgència no puguin esperar al termini ordinari de 16 dies laborables. Donada la naturalesa del servei, aquest es limita a cinc certificats per ens i setmana que es lliuraran en el termini de 4 dies laborables, comptats a partir de la recepció correcta de la sol·licitud.

Les ERs col·laboradores dels Consells Comarcals garanteixen un acord de nivell de servei que millora el del Consorci AOC:

- Certificats ordinaris: en un màxim de 5 dies laborables
- Certificats urgents: un màxim de 2 dies laborables

11.8 Formació i divulgació

El servei de certificació digital porta a terme accions de formació i divulgació dirigides a usuaris finals, ens subscriptors i els operadors i tècnics de les Entitats de Registre idCAT i T-CAT .

Durant l'any 2022 es van realitzar 45 activitats formatives, que suposen més de 1000 hores de cursos on line hores de formació impartida, durant les quals es van formar més de 400 assistents.

Pel que fa al servei de formació, es realitzen aquestes sessions amb aquests formats:

- Tallers de formació presencial T-CAT anuals a l'aula de formació del Consorci AOC (i amb el suport del servei de formació de l'AOC):
- 4 formacions virtuals a operadors d'ER T-CAT a l'any
- Curs virtual per a usuaris finals d'Usos del certificat digital T-CAT, obert i autodirigit
- 17 edicions del curs virtual per a operadors d'ER idCAT tutoritzat

El 5% d'aquestes accions formatives es van dur a terme de manera presencial i el 95% restant van ser formacions a distància.

En relació a la divulgació, aquesta es realitza principalment a través de la plataforma de formació del Consorci AOC.